



Conti cyber attack on the HSE

Independent Post Incident Review

Commissioned by the HSE Board in conjunction
with the CEO and Executive Management Team

03 December 2021

Important Notice

This document has been prepared only for the Health Services Executive (“HSE”) and solely for the purpose and on the terms agreed with the HSE in our engagement letter dated 21 June 2021, as amended on 6 August 2021. We accept no liability (including for negligence) to anyone else in connection with this document.

The scope of our work was limited to a review of documentary evidence made available to us and interviews with selected HSE personnel, CHOs, hospitals and third parties relevant to the review. We have taken reasonable steps to check the accuracy of information provided to us but we have not independently verified all of the information provided to us relating to the services.

A significant volume of documentation was provided to us throughout the course of the review. We have limited our review to those documents that we consider relevant to our Terms of Reference. We cannot guarantee that we have had sight of all relevant documentation or information that may be in existence and therefore cannot comment on the completeness of the documentation or information made available to us. Any documentation or information brought to our attention subsequent to the date of this report may require us to adjust our report accordingly.

Contents

	Executive summary	1
1	Learnings	11
2	Introduction and background	14
	2.1 Overview of the ransomware cyber attack	15
	2.2 Background to this post incident review	22
	2.3 Scope of our review	22
	2.4 Our review approach	22
	2.5 Structure of our report	26
3	Timeline of the Incident	27
4	Key recommendations and findings	34
	4.1 Strategic actions	35
	4.2 Immediate tactical actions	41
5	Focus areas - key findings and recommendation	44
	5.1 Focus area 1 - review of technical investigation and response	46
	5.2 Focus area 2 - review of organisation wide preparedness and strategic response	66
	5.3 Focus area 3 - preparedness of the HSE to manage cyber risks	93

Appendices	102
A. Scope of work	103
B. List of interviews	105
C. Key artefacts	106
D. List of key recommendations	110
E. Focus area 1 - detailed technical timeline	127
F. Focus Area 2 - detailed organisational timeline	138
G. Focus area and key recommendation mapping	142
H. HSE Risk assessment tool	144
I. Glossary and terms	147



The Board,
HSE,
Dr Steevens' Hospital,
Dublin 8, Ireland

03 December 2021

Subject : Post Incident Review into the Ransomware Cyber Attack

Dear Chair,

The Board of the Health Service Executive ("HSE") in conjunction with the Chief Executive Office ("CEO") and the Executive Management Team ("EMT") have requested an independent review into the recent ransomware cyber attack (the "Incident") and the circumstances surrounding this exfiltration of data from the HSE's Information Technology ("IT") systems. The purpose of the review is to:

- Urgently establish the facts in relation to the current preparedness of the HSE in terms of both its technical preparedness (Information and Communications Technology ("ICT") systems, cyber and information protections) and its operational preparedness (including Business Continuity Management planning) for a strategic risk of this nature.
- Identify the learnings from this Incident to identify improvements to the HSE's preparedness for and response to other major risks including immediate risks and incidents that cause major business disruption.
- Share those learnings within the HSE and externally with State and non-State organisations to inform their future preparedness.

Save as described in our contract or as expressly agreed by us in writing, we accept no liability (including for negligence) to anyone else or for any other purpose in connection with this report.

The subject matter and volume of information we reviewed as part of this process has been complex and significant in nature. Similarly, the timeline against which the review has been conducted has been challenging and has only been achieved with the cooperation of the many stakeholders involved, for which we are appreciative.

Yours faithfully,

PricewaterhouseCoopers

PricewaterhouseCoopers, One Spencer Dock, North Wall Quay, Dublin 1 Ireland T: +353 (0) 1 792 6000, F: +353 (0) 1 792 6200, www.pwc.ie
Fergal O'Rourke (Managing Partner - PricewaterhouseCoopers Ireland)

Olwyn Alexander Andy Banks Amy Ball Paul Barrie Brian Bergin Alan Bigley Fidelma Boyce Donal Boyle Ciara Breslin Sean Brodie Paraic Burke Damian Byrne Robert Byrne Pat Candon John Casey Mary Cleary Marie Coady Siobhán Collier Joe Conboy Keith Connaughton Mairead Connolly Tom Corbett Thérèse Cregg Garrett Cronin John Daly Richard Day Elizabeth Davis Fiona de Búrca Jean Delaney Liam Diamond John Dillon Ronan Doyle John Dunne Kevin Egan Colin Farrell Ronan Finn Laura Flood Ronan Furlong Fiona Gaskin Denis Harrington Aoife Harrison Harry Harrison Feilim Harvey Alisa Hayden Olivia Hayden Mary Honohan Gareth Hynes Ken Johnson Patricia Johnston Paraic Joyce Andrea Kelly Ciarán Kelly Colm Kelly Joanne P. Kelly Shane Kennedy Susan Kilty Fiona Kirwan David Lee Brian Leonard Gillian Lowth Vincent MacMahon Ronan MacNioclais Pat Mahon Declan Maunsell Kim McClenaghan Dervla McCormack Michael McDaid Enda McDonagh Declan McDonald Shane McDonald John McDonnell Gerard McDonough Ilona McElroy Mark McEnroe David McGee Dáire McGrath Ivan McLoughlin James McNally Stephen Merriman Pat Moran Paul Moroney Yvonne Mowlds Ronan Mulligan Declan Murphy John Murphy Andy O'Callaghan Colm O'Callaghan Jonathan O'Connell Aoife O'Connor Paul O'Connor Paul M O'Connor Emma O'Dea Doone O'Doherty Kieran O'Dwyer Munro O'Dwyer Mary O'Hara Irene O'Keeffe John O'Leary John O'Loughlin Ger O'Mahoney Liam O'Mahony Darren O'Neill Tim O'Rahilly Fergal O'Rourke Padraig Osborne Sinead Ovenden Ken Owens Keith Power Nicola Quinn Aoife Reid Peter Reilly Susan Roche Mary Ruane Stephen Ruane Gavan Ryle Emma Scott Colin Smith Ronan Somers Billy Sweetman Yvonne Thompson Paul Tuite David Tynan Joe Tynan Ken Tyrrell Stephen Walsh

Located at Dublin, Cork, Galway, Kilkenny, Limerick, Waterford and Wexford.
PricewaterhouseCoopers is authorised by Chartered Accountants Ireland to carry on investment business.

Executive summary

Background

The Health Service Executive (“HSE”) is a large geographically spread organisation which provides all of Ireland’s public health services through hospitals and communities across the country. The HSE consists of approximately 4,000 locations, 54 acute hospitals and over 70,000 devices (PCs, laptops, etc). Services are provided through both community delivered care and care provided through the hospital system as well as the national ambulance service. Corporate services and other services that support healthcare delivery are provided through the national centre.

The HSE is the largest employer in the Irish state, with over 130,000 staff including direct employees and those employed by organisations funded by the HSE¹. It therefore comprises an extensive community who are increasingly dependent on connected and reliable Information Technology (“IT”) solutions and varying levels of IT support from the HSE national centre to deliver clinical services. This includes the HSE’s national IT infrastructure. The HSE is classified as a critical infrastructure operator under the EU Network and Information Security Directive (“NISD”)², also known as an Operator of Essential Services (“OES”).

Introduction to the Incident

In the early hours of Friday 14 May 2021, the HSE was subjected to a serious cyber attack, through the criminal infiltration of their IT systems (PCs, servers, etc.) using Conti ransomware. The HSE invoked its Critical Incident Process, which began a sequence of events leading to the decision to switch off all HSE IT systems and disconnect the National Healthcare Network (“NHN”) from the internet, in order to attempt to contain and assess the impact of the cyber attack³. These actions removed the threat actor’s (the “Attacker”) access to the HSE’s environment.

This immediately resulted in healthcare professionals losing access to all HSE provided IT systems - including patient information systems, clinical care systems and laboratory systems. Non-clinical systems such as financial systems, payroll and procurement systems were also lost. Significant

disruption immediately occurred and many healthcare professionals had to revert to pen and paper to continue patient care. Healthcare services across the country were severely disrupted with real and immediate consequences for the thousands of people who require health services every day.

Normal communication channels, both at HSE’s national centre and within operational services were also immediately lost. This included email and networked phone lines. Staff switched to communicating using mobile and analogue phones; fax; and face to face meetings.

The aim of the Attacker was to disrupt health services and IT systems, steal data, and demand a ransom for the non-publication of stolen data and provision of a tool to restore access to data they had encrypted.

The HSE initially requested the assistance of the Garda National Cyber Crime Bureau, the International Criminal Police Organisation (“Interpol”) and the National Cyber Security Centre (“NCSC”) to support the response. The ransomware created ransom notes with instructions on how to contact the Attacker. The Attacker also posted a message on an internet chat room on the dark web, with a link to several samples of data reportedly stolen from the HSE. The HSE and the Irish Government confirmed on the day of the attack that they would not pay a ransom⁴.

The Incident had a far greater and more protracted impact on the HSE than initially expected, with recovery efforts continuing for over four months.⁵

Growing threat of cyber attacks

Cybercrime is increasing in frequency, magnitude and sophistication, with cybercriminals easily operating across jurisdictions and country borders. These incidents can cause major damage to safety and the economy⁶. As outlined in Ireland’s National Cyber Security Strategy, 2019-2024, “*recent years have seen the development and regular use of very advanced tools for cyber enabled attacks and espionage, and, likely for the first time, the physical destruction of Critical National Infrastructure by cyber enabled means*”⁷. In April 2020, Interpol, warned that cybercriminals were targeting critical healthcare institutions with ransomware⁸.

1 Health Service Employment Report: August 2021

2 This occurred in July 2016. See NIS Compliance Guidelines for Operators of Essential Service

3 Conti Cyber Response NCMT Structures Governance and Admin V1.10 31052021

4 <https://www2.hse.ie/services/cyber-attack/how-it-may-affect-you.html>

5 Weekly Brief, 21 September 2021

6 https://ec.europa.eu/commission/presscorner/detail/en/IP_13_94

7 National_Cyber_Security_Strategy.pdf

8 <https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware>

Ransomware attacks have risen significantly over the last few years. Whilst precise figures on the number of ransomware victims are not available, there are statistics that indicate the rate of growth of these attacks. For example, the US agency FinCEN's⁹ analysis of ransomware-related Suspicious Activity Reports (SARs) filed during the first half of 2021 indicates that \$590 million¹⁰ was paid in ransomware-related transactions (likely representing payments originating from the US to ransomware groups), which exceeds the value reported for the entirety of 2020 (\$416 million).

Despite claims by ransomware groups that they would not seek to harm people, there are several recent examples of attacks against healthcare providers. Hospitals including St. Lawrence Health System (USA), Sonoma Valley Hospital (USA), and Sky Lakes Medical Center (USA), all reported that they were impacted by ransomware attacks in 2020. On 20 May 2021, the Federal Bureau of Investigation ("FBI") identified at least 16 Conti ransomware attacks targeting US healthcare¹¹. Healthcare organisations that have been the target of similar attacks this year include, Waikato District Health Board, New Zealand (May 2021), Eskenazi Health, USA (August 2021), Memorial Health System, USA (August 2021) and Macquarie Health Corporation, Australia (October 2021). More recently, much of the provincial healthcare system in Newfoundland was impacted by a cyber attack (November 2021). The ransomware attack against the HSE would appear to be the first occurrence of an entire national health service being impacted by such an attack.

Scope of our review

In June 2021, PwC was commissioned by the Board of the HSE, in conjunction with the Chief Executive Officer ("CEO") and the Executive Management Team ("EMT"), to conduct an independent post incident review ("PIR") to urgently establish the facts in relation to the HSE's technical and operational preparedness for an incident of this nature; and to identify the learnings from this Incident both for the HSE and for State and non-State organisations to inform their future preparedness. We initially undertook a scoping phase, to develop our understanding of the Incident and our approach to the review, followed by the PIR engagement which was conducted over a 14 week period.

We took a sample approach to review the involvement of the hospitals and Community Healthcare Organisations ("CHO") within the HSE's

community, focusing on how the HSE's strategy was implemented at tactical levels and the effectiveness of the HSE's coordination of efforts.

This is a complex PIR. In recognition of this complexity, we brought together an experienced multi-disciplinary team of international cybersecurity and crisis management specialists. Our team included forensic investigation and response, IT / cybersecurity, crisis management, culture and behaviour, and regulatory experts with extensive experience in cybersecurity PIRs.

Timeline of the Incident

On 18 March 2021, the source of the cyber-attack¹² originated from a malicious software ("Malware") infection on a HSE workstation (the "Patient Zero Workstation"). The Malware infection was the result of the user of the Patient Zero Workstation clicking and opening a malicious Microsoft Excel file that was attached to a phishing email sent to the user on 16 March 2021.

After gaining unauthorised access to the HSE's IT environment on 18 March 2021, the Attacker continued to operate in the environment over an eight week period until the detonation of the Conti ransomware on 14 May 2021. This included compromising and abusing a significant number of accounts with high levels of privileges (typically required for performing administrative tasks), compromising a significant number of servers, exfiltrating data and moving laterally to statutory and voluntary hospitals.

The Incident was not identified and contained until after the detonation of the Conti ransomware on 14 May 2021, which caused widespread IT disruption. There were several detections of the Attacker's activity prior to 14 May 2021, but these did not result in a cybersecurity incident and investigation initiated by the HSE and as a result opportunities to prevent the successful detonation of the ransomware were missed. The key events from 18 March 2021 to 14 May 2021 are set out in the diagram overleaf.

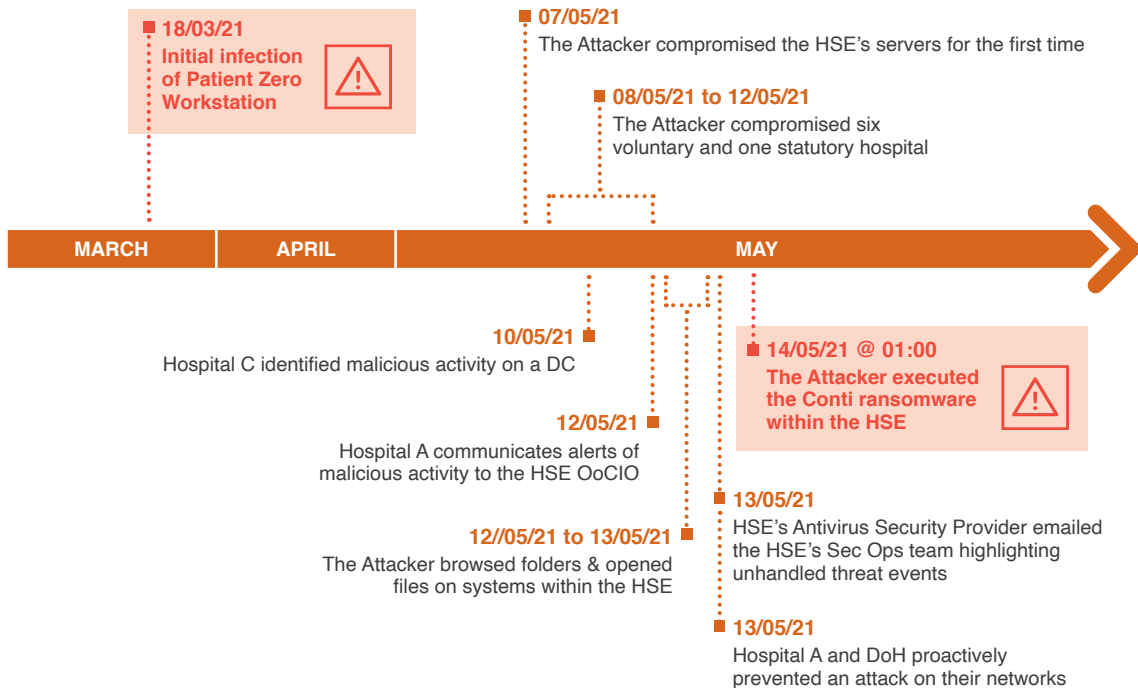
9 www.fincen.gov

10 https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

11 <https://www.ic3.gov/Media/News/2021/210521.pdf>

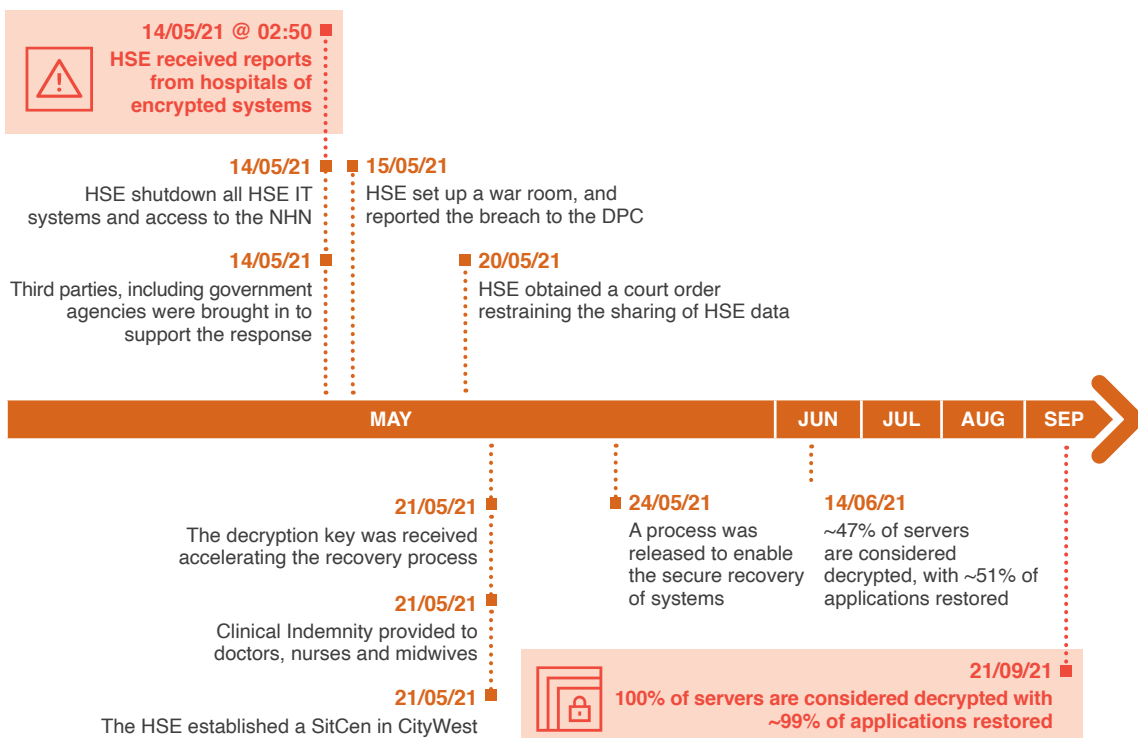
12 HSE's Incident Response provider Intrusion Investigation Report, September 2021

Figure 1: Summary Timeline 18 March - 14 May 2021



In the early hours of 14 May 2021, the HSE identified that they had been a victim of a cyberattack and they began to mobilise a response, drawing on their experiences from previous crises, including COVID-19. The key response and recovery events from 14 May 2021 are set out in the diagram below.

Figure 2: Summary Timeline 14 May - 21 September 2021



The HSE was assisted by the Defence Forces and the NCSC as well as third parties in the early weeks of the Incident, to provide structure to the response activities. The response teams could not initially focus on the highest priority response and recovery tasks due to the lack of preparedness for a widespread disruptive IT event e.g. through not having a pre-prepared list of prioritised clinical systems and applications to focus their efforts.

On 15 May 2021, the HSE senior management set up a war room at a third party's office building on Molesworth Street. On 20 May 2021, the Defence Forces attended Molesworth Street for further discussions around the level of support that was required by the HSE during the response and recovery phases of the Incident and on 21 May 2021, the HSE set up a physical situation centre ("SitCen") in CityWest to manage the response and recovery. The HSE engaged a third party Incident Response organisation ("HSE's Incident Response provider") to investigate the cyber attack.

On 20 May 2021, the HSE secured a High Court injunction¹³ restraining any sharing, processing, selling or publishing of data stolen from its computer systems. On the same day, the Attacker posted a link to a key that would decrypt files encrypted by the Conti ransomware. The HSE's Incident Response provider validated that the decryption key worked on 21 May 2021 and provided it to the HSE, allowing them to gain access to the data that had been encrypted by the Conti ransomware. Without the decryption key, it is unknown whether systems could have been recovered fully or how long it would have taken to recover systems from backups, but it is highly likely that the recovery timeframe would have been considerably longer.

From 22 May 2021 onward, the HSE Information and Communications Technology ("ICT") team moved from the response phase into the recovery phase, where they focused their efforts on decrypting systems, cleansing workstations, restoring systems and the recovery of applications. The HSE recovered their primary identity systems (██████████ Active Directory ("AD") domain) within days of the Incident, but decryption of servers and acute and community services applications took place largely over the following three months. By 21 September 2021, the HSE had recovered all servers and 1,075 applications, out of a total of 1,087 applications¹⁴.

At the time of issuing this report, the HSE had notified the Data Protection Commissioner ("DPC") in relation to the Incident, however, they have not made any

data subject notifications for personal data exposure or exfiltration. The HSE's Legal and Data workstream continues to work closely with the DPC in relation to this matter.

Mitigating factors impacting on the Incident

There were a number of mitigating factors which had a considerable effect in reducing the severity and impact of the Incident.

Relative simplicity of the attack and the release of the decryption key

Based on the forensic examination of the Attacker's activity, it would appear that the Attacker used relatively well-known techniques and software to execute their attack. A more sophisticated attack may have involved gathering intelligence in advance, before it could be successfully and subtly exploited. The impact of the Incident on the HSE and health services could have been significantly greater, with far more severe clinical impact. Some examples of this include, but are not limited to:

- if there had been intent by the Attacker to target specific devices within the HSE environment (e.g. medical devices);
- if the ransomware took actions to destroy data at scale;
- if the ransomware had auto-propagation and persistence capabilities, for example by using an exploit to propagate across domains and trust-boundaries to medical devices (e.g. the EternalBlue exploit used by the WannaCry and NotPetya¹⁵ attacks);
- if cloud systems had also been encrypted such as the COVID-19 vaccination system.

An additional mitigating factor was the release of the decryption key by the Attackers on 20 May 2021, which allowed for an accelerated recovery process. It is unclear how much data would have been unrecoverable if a decryption key had not become available as the HSE's backup infrastructure was only periodically backed up to offline tape. Therefore it is highly likely that segments of data for backup would have remained encrypted, resulting in significant data loss. It is also likely to have taken considerably longer to recover systems without the decryption key.

¹³ <https://www.hse.ie/eng/services/publications/order-perfected-20-may-2021.pdf>

¹⁴ Weekly Brief, 21 September 2021

¹⁵ <https://us-cert.cisa.gov/ncas/alerts/TA17-181A>

Significant 'in-the moment' efforts in response to the Incident

A recurring theme observed throughout the PIR was the dedication and effort observed at all levels during the response to the Incident. This included individuals from across the HSE, impacted hospitals, CHOs, and third parties all going "above and beyond" in their call of duty. This illustrates that, in times of significant challenge or emergencies, staff in the health services are resilient, respond quickly, and have an ability to implement actions and workarounds to maintain even a basic continuity of service to their patients.

National support

The impact of the Incident was at a national scale which encouraged support and presence from other state agencies and third parties, who provided structure, governance, technical expertise and resources to assist the response and recovery.

Lessons learned from COVID-19 and previous IT disruptions

Whilst the HSE had not previously encountered an incident of this scale, they have been exposed to other significant incidents both directly (e.g. COVID-19) and through observations of ransomware attacks on other healthcare organisations globally (e.g. WannaCry ransomware attack) over the past five years. Each of these incidents highlighted key learnings that have led to an improved level of crisis management maturity within the HSE.

Strategic recommendations and findings

The Incident demonstrated that the HSE and organisations connected to the NHN are vulnerable to common cyber attacks that can cause significant impact to the provision of health services. Transformational change is required across the technology foundation for provision of health services and its associated cybersecurity, that will need to be executed over the coming years.

In order to deliver a significant and sustainable change in the exposure to cybersecurity risk, four areas of strategic focus are required across the HSE and other parties connected to the NHN. There are dependencies across these four areas and they need to be progressed in parallel. They are summarised below, with further detail provided in Section 4.1. More detailed findings and recommendations are provided in Section 5.

1. Implement an enhanced governance structure over IT and cybersecurity that will provide appropriate focus, attention and oversight.

1.1 Establish clear responsibilities for IT and cybersecurity across all parties that connect to the NHN, share health data or access shared health services. Establish a 'code of connection' that sets minimum cybersecurity requirements for all parties and develop an assurance mechanism to ensure adherence.

One of the challenges faced by the HSE is that cybersecurity risk materialises as a 'common risk' to all organisations connected to the NHN given the interconnected nature of the IT systems. Under the governance constructs of the health service, organisations have varying levels of autonomy over IT and cybersecurity decision making, yet the risk is shared - with organisations dependent on each other for cybersecurity. There is no 'code of connection' for all parties that connect to the NHN, share health data or use shared services in order to set a minimum baseline of security standards.

1.2 Establish an executive level cybersecurity oversight committee to drive continuous assessment of cybersecurity risk and a cybersecurity transformation programme across the provision of health services.

Within the HSE, there is no dedicated executive oversight committee that provides direction and oversight to cybersecurity, both within the HSE and all organisations connected to the NHN. A known low level of cybersecurity maturity, including critical issues with cybersecurity capability, has persisted. It is important that the cybersecurity oversight committee includes participation from user groups, so that culturally cybersecurity moves from being perceived as an IT challenge, to being perceived as 'how we work'. The cybersecurity oversight committee should be accountable for ensuring compliance with the evolving requirements of the EU NISD for essential services across the health service.

1.3 Establish an executive level oversight committee for IT.

With a fragmented set of decision rights over IT development and support across the provision of health services, a necessary enabler for driving transformational change will be the establishment of an executive level committee, chaired by the Chief Technology and Transformation Officer (see Recommendation 2 below), that can agree the priorities for IT development and investment, and align all interested parties behind a clear vision, strategy and plan. Critical to its success will be the

participation of IT leaders from across the health service.

1.4 Establish a board committee (or repurpose an existing one) to oversee the transformation of IT and cybersecurity to deliver a future-fit, resilient technology base for provision of digitally-enabled health services, and ensure that IT and cybersecurity risks remain within a defined risk appetite. Consider the inclusion of further specialist non-executive members of the committee in order to provide additional expertise and insight to the committee.

Cybersecurity was recorded as a 'High' risk in the Corporate Risk Register in Q1 2019.¹⁶ At the time of the Incident, the risk rating for cybersecurity on the Corporate Risk Register was 16, based on a likelihood scoring of 4 (likely, with a 75% probability) and an impact scoring of 'Major'.¹⁷ The HSE's risk assessment tool is described in Appendix H.

Risks on the Register are subject to a quarterly review process and the quarterly reports are reviewed by the relevant Board Committee. The Performance and Delivery Committee of the Board reviewed the cyber risk with management in September 2020¹⁸ and this was followed by a revised mitigation plan. The Committee includes two experienced IT leaders in large organisations, although they are not cybersecurity specialists. This revised mitigation plan had a number of actions due to be completed post the date of the Incident. The actions completed prior to the Incident did not materially impact the risk faced in this area.

The HSE's IT-related risks had been presented at Board level on a number of occasions. However, the gravity of cybersecurity exposure was not fully articulated to the Board, given the HSE's level of vulnerability to a cyber attack, or assessed against a defined risk appetite. Known issues with cybersecurity capability have made limited progress over the course of several years.

Given the scale of change required across the provision of health services, it is recommended that a focused committee of the board is established, with relevant training provided. Consideration should be given to appointing additional individuals to that committee with specialist skills to act in a non-executive capacity and enhance the ability for the committee to support and oversee the IT and cybersecurity transformation. A key role for the committee will be to ensure that HSE requests for government funding (e.g. to the Department of

Public Expenditure and Reform ("DPER")) to invest in addressing IT and cybersecurity issues are clearly articulated, and the risks associated with lack of investment are communicated and understood.

2. Establish a transformational Chief Technology & Transformation Officer ("CTTO") and office to create a vision and architecture for a resilient and future-fit technology capability; to lead the delivery of the significant transformation programme that is required, and to build the increased function that will be necessary to execute such a scale of IT change.

The national health service is operating on a frail IT estate with an architecture that has evolved rather than be designed for resilience and security. The NHN is primarily an unsegmented (or undivided) network, and can be described as a "flat" network, to make it easy for staff to access the IT applications they require. However, this design exposes the HSE to the risk of cyber attacks from other organisations connected to the NHN, as well as exposing other organisations to cyber attacks originating from the HSE. This network architecture, coupled with a complex and unmapped set of permissions for systems administrators to access systems across the NHN, enabled the Attacker to access a multitude of systems across many organisations connected to the NHN and create the large-scale impact that they did.

The parts of the health service that were arguably best-equipped to maintain clinical services in the face of prolonged IT outages were those that rely on paper records for patient services. Whilst this was a positive feature in managing the Incident, it highlights the extent to which modernisation is required across the health service to enable the adoption of digital health services.

Reducing cybersecurity risk requires both a transformation in cybersecurity capability (see recommendation 3) and IT transformation, to address the issues of a legacy IT estate and build cybersecurity and resilience into the IT architecture.

2.1 Appoint a permanent CTTO with the mandate and authority to develop and execute a multi-year technology transformation, build an appropriate level of IT resource for an organisation the scale of the HSE and oversee the running of technology services.

The HSE has operated since the end of 2018 with an interim Chief Information Officer with limited

¹⁶ Q1, 2019 CRR COMBINED Document for April LT meeting.pdf

¹⁷ CRR Q4 2020 Full Report post EMT meeting February 2021 v0.1 09 02 21.pdf

¹⁸ Minutes-hse-performance-and-delivery-committee-18-september-2020.pdf

practical mandate, authority and resources to effect change across all organisations connected to the NHN. The level of resourcing in critical IT functions is significantly lower than we would expect for an organisation of this size.

The CTTO should assume responsibility for all capabilities that currently sit within the Office of the Chief Information Officer (“OoCIO”), as well as a broadened capability to drive rapid transformation. The CTTO should be a member of the EMT reporting to the CEO.

2.2 Under the office of the CTTO, develop an IT strategy to achieve a secure, resilient and future-fit IT architecture, required for the scale of the HSE organisation.

The HSE has had a plan for the development of IT that has been used to secure funding for individual projects. However it has not been tied to a vision, strategy and architecture that is deliverable over a period of years and that provides the necessary level of resilience through investment in enabling IT architecture and fallback solutions in the event of core technology failure. Many interviewees expressed frustration with an apparent approach of investing in ‘new projects’ or ‘new features’ rather than the holistic delivery and maintenance of a technology foundation for health service provision.

In order to deliver the transformation required, a clear strategy is required that can be used to secure commitment to execution across all organisations involved in the provision of health services, and the significant funding that will be required over many years.

3. Appoint a Chief Information Security Officer (“CISO”) and establish a suitably resourced and skilled cybersecurity function. Develop and drive the implementation of a cybersecurity transformation programme.

The HSE has a very low level of cybersecurity maturity (Section 5.3 of this report gives an evaluation of maturity against the industry standard “NIST CSF” framework). Examples of the lack of cybersecurity controls in place at the time of the Incident include:

- The IT environment did not have many of the cybersecurity controls that are most effective at detecting and preventing human-operated ransomware attacks;

- There was no security monitoring capability that was able to effectively detect, investigate and respond to security alerts across HSE’s IT environment or the wider NHN;
- There was a lack of effective patching (updates, bug fixes etc.) across the IT estate that is connected to the NHN; and
- Reliance was placed on a single antivirus product that was not monitored or effectively maintained with updates across the estate. For example, the workstation on which the Attacker gained their initial foothold did not have antivirus signatures updated for over a year.

The low level of cybersecurity maturity, combined with the frailty of the IT estate, enabled the Attacker in this Incident to achieve their objectives with relative ease. The Attacker was able to use well-known and simple attack techniques to move around the NHN, extract data and deploy ransomware software over large parts of the estate, without detection.

3.1 Appoint a CISO and establish a suitably resourced and skilled cybersecurity function

The HSE does not have a single responsible owner for cybersecurity at either senior executive or management level to provide leadership and direction. This is highly unusual for an organisation of the HSE’s size and complexity with reliance on technology for delivering critical operations and handling large amounts of sensitive data. As a consequence, there was no senior cybersecurity specialist able to ensure recognition of the risks that the organisation faced due to its cybersecurity posture and the growing threat environment.

The CISO should be at National Director level, a direct report to the CTTO, and have appropriate access to the EMT and their agenda, to ensure that cybersecurity risks are understood and considered in all decision-making. Whilst recruitment of a permanent CISO may take some time, appointment of an interim CISO should be considered in the short term.

The HSE also had only circa 15¹⁹ full-time equivalent (“FTE”) staff in cybersecurity roles, and they did not possess the expertise and experience to perform the tasks expected of them.

¹⁹ This comprises eight FTE within the Information Security Framework and Control team (two of which are students), the Security Operations team of five FTE and the Security, Standard and Policies team of two FTE. Figures are based on interviewee assertion and/or OoCIO Operating Model – 2020 Current State, December 2019.

A critical requirement for the HSE to begin to develop the ability to prevent and detect a similar incident in the future is the appointment of senior cybersecurity leadership and the development of a suitably skilled and resourced cybersecurity function. These skilled resources are currently scarce and the HSE may need to consider co-sourcing arrangements to support resource requirements in this area.

3.2 Develop and drive the execution of a multi-year cybersecurity transformation programme to deliver an acceptable level of cybersecurity capability for a national health service.

A multi-year programme to transform cybersecurity capability in a holistic way is required to be led by the CISO, to ensure that the provision of health services in Ireland, and the data that those health services handle, becomes less vulnerable to cyber attacks. This programme will include the formalisation of cybersecurity training and awareness.

Implement a clinical and services continuity transformation programme reporting to the National Director for Governance and Risk, and enhance crisis management capabilities to encompass events such as wide-impact cyber attacks or large-scale loss of IT.

4.1 Implement a clinical and services continuity transformation programme reporting to the National Director for Governance and Risk. Establish an Operational Resilience Policy and Resilience Steering Committee to drive integration between resilience-related disciplines, and an overarching approach to resilience.

The HSE has recognised that clinical and services continuity (business continuity) as a risk discipline has not developed at the pace needed with executive oversight and focus. A National Director for Governance and Risk (equivalent to a Chief Risk Officer) was appointed on 14 June 2021, and assigned responsibility for establishing a clinical and services continuity framework, through which risk management and continuity plans will be reviewed, maintained and validated. Responsibility for clinical and service continuity under the HSE's accountability structure will remain with operational and functional managers. A programme and resource is required to develop the consistency and breadth of planning across the health service, including establishing clear requirements for disaster recovery capability to be implemented by the IT transformation programme, and the mapping of clinical processes to IT systems and data.

The HSE should establish an Operational Resilience Policy and Steering Committee to drive integration between resilience-related disciplines across the organisation, such as incident management, crisis management, clinical and services continuity and enterprise risk management plus disciplines that can impact on resilience such as cybersecurity and physical security.

4.2 Enhance crisis management capabilities to encompass events such as wide-impact cyber attacks or large-scale loss of IT.

The HSE has extensive experience in managing crises, for example in the critical role it has fulfilled for the nation in navigating the COVID-19 crisis. This has resulted in some effective mechanisms for crisis management not just being designed, but regularly used.

However, the nature of the crisis resulting from the ransomware attack was different, and required elements of capability that have not previously been required. For example: communicating with all staff in the health service without internal emails or other IT collaboration tools; establishing a wide variety of communication channels and forums to gather information and feedback to prioritise recovery of systems, and issuing clear guidance to all parties impacted by the Incident that was relevant to their localised situation.

The nature of a ransomware attack, resulting in effectively total loss of IT, makes it particularly challenging to manage with a unique set of issues to be navigated. Investment is required in crisis management planning, resourcing and tools and processes in the HSE and associated organisations in order to be prepared to manage this kind of crisis in the future.

Tactical recommendations

Given the high risk of exposure at present, below are tactical recommendations which require immediate attention to achieve urgent impact and to contribute to the development and implementation of the strategic recommendations. These recommendations are described in more detail in Section 4.2 of this report. Further detail of key findings and recommendations are included in Section 5 of this report.

1. Response to the Incident

- 1.1.** Complete the ongoing work being performed by the Legal and Data workstream and continue to work closely with the Data Protection Commissioner (DPC).

- 1.2. Continue to reconcile medical data stored and managed through interim processes post the ransomware attack and place centralised governance over these activities.
- 1.3. Collate and manage artefacts created in response to the Incident, including initial production of an asset register.
- 1.4. Appoint an interim senior leader for cybersecurity (a CISO) to be responsible for driving forward tactical cybersecurity improvements, managing third-parties that provide cybersecurity services and leading the cybersecurity response to cyber incidents.
- 1.5. Formalise a programme and governance to respond to tactical recommendations arising from the Incident Response investigation and provide assurance over their implementation.

2. Security monitoring

- 2.1. Ensure that the HSE's Incident Response provider's managed defence service or an equivalent is maintained to detect and respond to incidents on endpoints (i.e. laptops, desktops, servers etc.) to provide protection to the entirety of the NHN.
- 2.2. Establish an initial cybersecurity incident monitoring and response capability to drive immediate improvement to the ability to detect and respond to cybersecurity events.

3. Ability to respond to a similar incident in the near future

- 3.1. Review the process for managing internal crisis communications including resources.
- 3.2. Develop a plan for response and management of an NHN-wide similar incident taking recent learnings into account.
- 3.3. Establish retainers with appropriate service level agreements ("SLAs") for third party incident and crisis management response support, together with processes and sufficient internal expertise to direct and manage the third-parties

4. IT environment

- 4.1. Implement an upgrade to National Integrated Medical Imaging System ("NIMIS") to allow Windows 10 upgrade,

thereby addressing known vulnerabilities and support issues associated with current wide deployment of Windows 7.

- 4.2. Formalise existing roles and responsibilities for IT across the entities accessing the NHN and establish SLAs for centrally-provided services, while also ensuring information security policies align with those responsibilities.

Next Steps

The seriousness of the deficiencies identified persist and necessitate transformational change in the HSE as well as immediate tactical actions. We recommend that the HSE improve their cybersecurity, IT and operational resilience governance, leadership and capability, to allow them to stand up a remediation programme to address our recommendations.

In 2021, the HSE had a combined revenue and capital budget of nearly €22 billion, which included an IT operating budget of €82 million and IT capital budget of €120 million (including €25 million for Covid-19 capital spend)²⁰. The HSE is currently estimating its IT operating budget will increase to €140m and its IT capital budget will increase to €130m in 2022. Whilst it is outside the scope of the PIR to quantify the incremental cost to the HSE of implementing the recommendations set out in this report, it is clear that it will require a very significant investment on an immediate and sustained basis.

The HSE will need to develop an investment case for this remediation programme, as the successful implementation of the strategic and tactical recommendations will be dependent on a well resourced plan, against which funding will need to be secured and progress tracked. This will be a complex programme, with interdependencies between our recommendations, and the programme will also need to be highly integrated with existing project delivery and business as usual operations. The investment case will be complex to develop due to for example: i) it can be challenging to segregate core IT spend and cybersecurity investment (e.g. upgrading to Windows 10 or Individual Health Identifier); ii) costs to release and backfill service staff i.e. clinical and operational subject matter experts who are critical to complex e-health projects, will be a relevant cost of the remediation programme and this will need to be incorporated into the investment commitment; and iii) a significant number of cybersecurity and clinical and service continuity resources need to be put in place, to deliver on the execution of the plan.

²⁰ HSE National Service Plan 2021

The cost of the remediation programme, in addition to underlying technology and operational resilience costs, is likely to be a multiple of the HSE's current capital and operating expenditure in these areas over several years. Our recommendations need to be developed into a prioritised plan, with tactical recommendations implemented on an accelerated basis. On the basis of this plan, cost estimates for year one can be established with a reasonable level of accuracy. Subsequently, within the first year, high level cost estimates for years 2-5 can be estimated (possibly over a longer duration, depending on interdependencies with other change programmes).

Learnings for other organisations

A number of the vulnerabilities that the ransomware attack highlighted are not unique to the HSE, and issues identified in this report will be found in other organisations. All organisations therefore need to consider the extent to which they are protected from a major cyber incident, and be prepared to respond and recover should they experience such an event. We have outlined these recommendations in Section 1 of this report.

Conclusion

While reviews of this nature tend to focus on what went wrong to identify learnings, it is also important to recognise that the Incident was caused by an Attacker and the HSE was the victim of a cybercrime. There was a considerable effort made by personnel, including IT and operations personnel in HSE centre, the hospitals and CHOs, and healthcare professionals in all areas, to respond to the Incident, to recover from the Incident and to continue to provide patient care throughout the Incident. If this significant effort had not been made by these people, the impact of the Incident on the Irish public healthcare system would certainly have been much worse.

The HSE is operating on a frail IT estate that has lacked the investment over many years required to maintain a secure, resilient, modern IT infrastructure. It does not possess the required cybersecurity capabilities to protect the operation of the health services and the data they process, from the cyber attacks that all organisations face today. It does not have sufficient subject matter expertise, resources or appropriate security tooling to detect, prevent or respond to a cyber attack of this scale. There were several missed opportunities to detect malicious activity, prior to the detonation phase of the ransomware.

The relative disadvantage in this Incident for organisations who have greater dependency on technology services, illustrates the critical need for

resiliency to be built into the IT architecture and systems, to foster the confidence required to enable future migration to more digital provision of health services.

Emergency and crisis planning at the HSE previously focused on scenarios such as adverse weather, pandemic, serious accidents and terrorist action, which generate a temporary surge in demand for acute services. The assumption was that all critical infrastructure and processes would remain available to support the response. Similar to many other organisations, the HSE did not conduct contingency planning for a cyber attack or any other scenario involving the complete loss of infrastructure, people, or facilities. Clinical and services continuity has not been a corporate priority in the HSE until recently. In order to maximise the learnings from the response to the Incident, the HSE must expand upon initiatives already started, and implement a coherent operational resilience capability, including clinical and services continuity and crisis management, across the organisation.

Reducing cybersecurity risk requires both a transformation in cybersecurity capability and IT transformation, to address the issues of a legacy and complex IT estate and build cybersecurity and resilience into the IT architecture. Whilst this will need to be executed over a period of several years, there is an imperative for the HSE to act with urgency to ensure that the necessary plans, vision, leadership, committed investment and resourcing are in place to drive this significant change to build a secure, resilient and future-fit technology foundation for provision of national healthcare services. The required investment commitment is likely to be a multiple of the HSE's current expenditure on technology and operational resilience, but is essential to protect the HSE against future attacks which are inevitable and have the potential to be even more damaging.

The HSE, the State and non-State organisations now have an opportunity to take the key lessons from this major Incident to build a more robust and resilient cyber frontier nationally.

The HSE remains vulnerable to cyber attacks similar to that experienced in the Incident, or cyber attacks that may have an even greater impact.

1

Learnings

Whilst the purpose of this report is to highlight recommendations and findings specific to the HSE to be taken from the Incident, there are a number of recommendations and key learnings that can be applied to all organisations.



As dependency on technology deepens across society, the impact of destructive cyber attacks such as ransomware will undoubtedly grow even further. Investing in cybersecurity needs to be a priority even for organisations that previously have not considered cyber attacks as a threat to their operations. A number of the vulnerabilities that the ransomware attack highlighted are not unique to the HSE, and issues identified in this report will also be found in many other organisations. All organisations therefore need to consider the extent to which they are protected from a major cyber incident, and be prepared to respond and recover should they experience such an event.

The points below are presented as recommendations that all organisations should consider in the light of the experience of the HSE, in order to learn lessons from this Incident more broadly. They are not intended to be exhaustive, but act as an instructive set of learnings to consider in response to this Incident.

Governance and cybersecurity leadership

1. Understanding of technology dependency and governance of technology risk

Boards and executive leadership of organisations should ensure that they understand the extent to which their critical operations are dependent on technology. Governance must ensure that risks associated with technology are properly understood and actively managed, including the resiliency of the organisation to widespread technology failure or compromise from an attack (which may occur indirectly through the supply chain). Governance over technology should ensure that sufficient investment is focused on: maintenance of robust foundational technology infrastructure; realising opportunities from new technology (such as infrastructure and applications in the cloud) to manage risks in a new way, and managing risks that arise from new application of technology.

2. Cybersecurity strategy and leadership

Organisations should ensure they have a cybersecurity strategy that defines the key cybersecurity risks to the organisation, how those risks are being mitigated and the resourcing and investment to execute the strategy. Organisations should have a single accountable senior leader responsible for delivering the strategy. An element of the strategy should be consideration of the cyber risk posed by legacy IT, how this risk can be mitigated in the short-term, and how technology modernisation

will address the root-cause issue.

Effective cybersecurity capability

3. Ransomware-specific assessment

Organisations should perform a cybersecurity assessment specific to the threat of ransomware, given the heightened threat posed by ransomware attacks. This will highlight the extent to which the organisation's cybersecurity controls are appropriate and effective to defend against this threat, and identify areas that may require urgent investment.

Key examples of cybersecurity controls that should be assessed include: sufficiency of security monitoring to detect and contain ransomware attacks in the early stages, ability to prevent and detect the compromise of 'privileged' (e.g. systems administrator) accounts, and the robustness of user authentication.

Several organisations that provide ransomware-response services can provide such assessments, and publicly available frameworks and guidance are available from organisations such as the Cybersecurity & Infrastructure Security Agency ("CISA") in the USA.

4. Effective cybersecurity monitoring and response

Organisations must possess an effective security monitoring capability that can detect and respond to the tools and techniques used by human-operated ransomware groups. This should include deploying a capable 'Endpoint Detection & Response' tool to detect and prevent malicious activity on workstations (fed by current cyber threat intelligence) and ensuring the development of skilled resources and processes so that security alerts are rapidly triaged, investigated and responded to.

5. Testing of cybersecurity capability through simulated attacks

Testing of cybersecurity capability through the use of ethical hackers simulating end-to-end attack techniques (i.e. 'red team' testing) is essential to provide a threat-based perspective of an organisation's vulnerability to ransomware and other types of attacks. This can be used to rapidly identify and prioritise key security improvement areas and ensure that the organisation can effectively detect common attacker tools, with the necessary people

and processes are in place to investigate and respond to alerts.

Preparedness to respond and recover

6. Cybersecurity-specific incident response and crisis management plans

Organisations should develop and exercise cybersecurity-specific incident response and crisis management plans that define how a response should be led, managed and coordinated. These should be challenged to ensure they are effective in a catastrophic ransomware scenario where all IT platforms, cybersecurity tools and usual communication channels are unavailable, and recovery efforts may have to be sustained for weeks or months.

7. Business continuity planning and IT disaster recovery planning for a ransomware scenario

Organisations should prioritise business continuity planning and disaster recovery planning that would ensure provision for continuity of critical operations and the ability to recover in the face of a ransomware attack that results in total loss of IT and associated data.

Business continuity planning should be based on rigorous 'Business Impact Analysis', and ensure that workarounds are defined for the scenario of total loss of IT for up to several weeks.

Organisations' IT disaster recovery plans should be based on a prioritised list of applications and systems to recover, should the technology base of the organisation have to be rebuilt or recovered, informed by an up-to-date asset register and mapping of critical operations to technology. Offline backups (or backups that are verified as inaccessible to attackers with full control of production IT) must be available for all critical systems, data and infrastructure, including core IT infrastructure such as Active Directory ("AD"), with a well-defined and tested restore procedure that includes verification of ability to recover all systems to a common point-in-time.

8. Retained incident and crisis support

Organisations should establish contractual retainers with key third parties that may be required to support a crisis response. Third party support that may likely be required during an incident include: forensic and technical incident response; crisis response; external legal counsel, and public relations.

Retainers should include: service level agreements; specification of third party roles and responsibilities; reviews of the technical preparedness of the organisation for incident response (by forensic and technical incident response providers), and pre-agreed legal requirements (such as non-disclosure agreements). These will ensure that partners can be engaged to support, and be integrated into, a response immediately and scale to the size of the response required.

2

Introduction and background



2.1 Overview of the ransomware cyber attack

In the early hours of Friday 14 May 2021, the HSE became aware of a major cyber attack (the “Incident”) against their IT systems. The Incident was carried out by the criminal infiltration of these systems using Conti ransomware.²¹ As a result of the Incident, the HSE shut down all IT systems and disconnected networks causing significant disruption to healthcare services across the country.

At the time of the Incident, the HSE was over a year into a complex crisis response to the unprecedented emergency of the global COVID-19 pandemic. The national healthcare service was subject to one of the most serious cyber attacks ever in Ireland, one which affected almost every part of the critical infrastructure of the country’s healthcare system. It was reported by HSE management that 80% of the HSE’s environment across corporate IT services, hospitals, CHOs and electronic health records (“EHR”) was encrypted²², causing a severe and long lasting disruption to healthcare services.

In the immediate aftermath of the Incident, many hospitals were forced to cancel outpatient appointments completely while others were operating with significant delays and reverted to using pen and paper to continue recording patient care. Over half of the hospitals in the country announced cancellations of at least some of their outpatient appointments.²³ The impact of the Incident on services varied depending on several factors including the type of care being offered, the reliance on software applications to record and manage patient data, existing IT infrastructures and local IT support.²⁴ The Incident had a significant impact on diagnostic services due to loss of NIMIS and also laboratory systems. There was a significant impact on radiotherapy services, with cessation of radiation treatment across the five HSE centres (a Model 3

Hospital (“Hospital B”), a Model 4 Hospital (“Hospital A”), a Model 4 Hospital (“Hospital N”), a Model 4 Hospital (“Hospital H”) and a Maternity Hospital (“Hospital E”)).²⁵

In the community, primary care staff were unable to access patient appointment lists or contact details, patient history, treatment plans, x-ray facilities or monitoring of instrument sterilisation tracking.²⁶ In many cases, in order to maintain a level of service, patients were issued with a contingency Medical Record Number (“MRN”). Work is ongoing to reconcile these records with existing patient records and to update systems for hardcopy data recorded during the period.

Background

The HSE is responsible for delivering health and social care services to the population of Ireland, estimated to be 5.01 million in August 2021.²⁷ Services are provided through a network of operational services covering both community delivered care and care provided through the hospital system as well as the National Ambulance Service. In 2021, the HSE had a combined operating and capital budget of nearly €22bn²⁸.

Community healthcare services are delivered across nine geographically organised CHOs while acute hospital services are delivered across a network of six Hospital Groups and Children’s Health Ireland (“CHI”). Within the Hospital Groups, there are 54 acute hospitals. These are made up of public hospitals directly under the authority of the HSE and voluntary hospitals who receive state funds through the HSE. The latter are independently owned and provide services on behalf of the HSE under Section 38 of the Health Act, 2004. They have their own IT teams and infrastructure but also utilise the national IT infrastructure as referred to below.

The HSE employs approximately 130,000 people, including those directly employed by the HSE²⁹ as well as those employed by organisations funded by the HSE. It is the largest employer in the State.

21 Ransomware Attack on Health Sector - https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf

22 Percentage confirmed in interview by the CTO within OoCIO Infrastructure and Technology

23 HSE cyber attack – which hospitals are affected? Here is everything you need to know. Source: Irish Independent. Date: May 16 2021 <https://www.independent.ie/irish-news/hse-cyber-attack-which-hospitals-are-affected-here-is-everything-you-need-to-know-40432288.html>

24 Healy, O. Dr. A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare IT failure, Dated 30th September 2021.

25 HSE press release 15 05 21

26 Healy, O. Dr. A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare IT failure, Dated 30th September 2021.

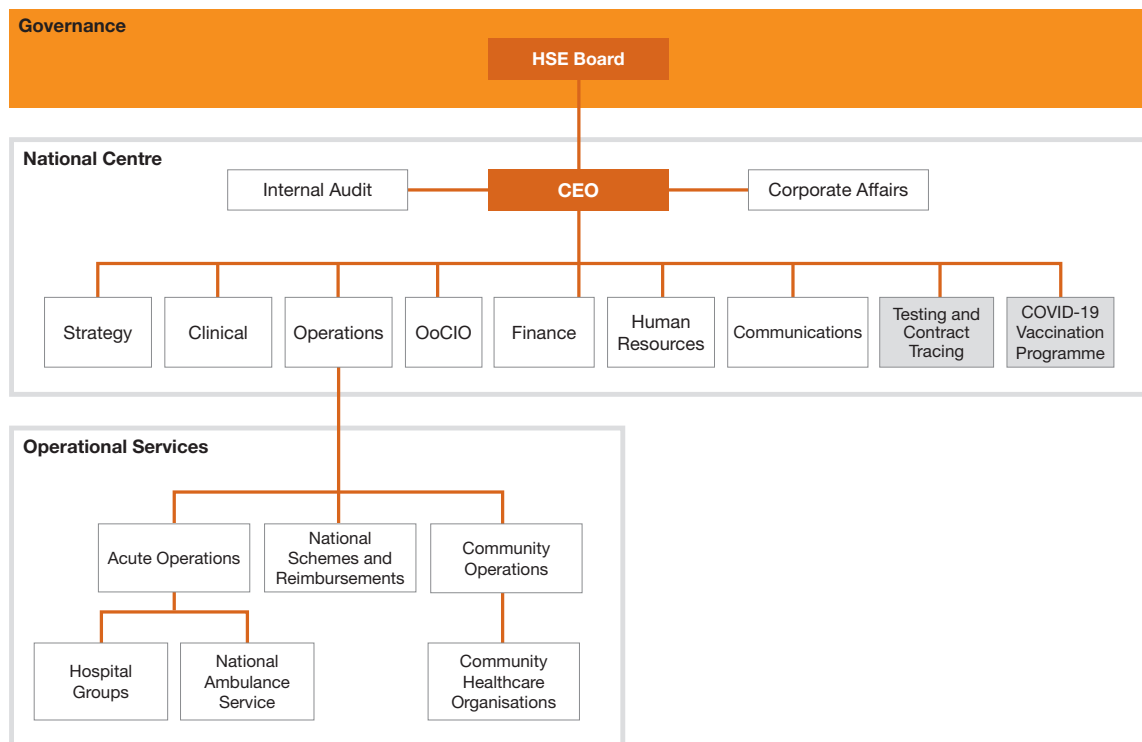
27 <https://www.cso.ie/en/releasesandpublications/ep/p-pme/populationandmigrationestimatesapril2021/>

28 HSE National Service Plan 2021

29 Health Service Employment Report: August 2021

HSE organisational structure at the time of the Incident

Figure 3: HSE organisational structure at the time of the incident



National Centre

Corporate services and other services that support healthcare delivery are provided through the National Centre. These services include Internal Audit, Corporate Affairs, Communications, Finance, Human Resources, Strategy and Operations as well as the OoCIO and the office of the Chief Clinical Officer. The Centre also manages the National Testing and Contract Tracing service as well as the COVID-19 vaccination programme.

The HSE undertook a Corporate Centre Review in 2020, in order to examine how the HSE's corporate services (delivered through the National Centre) are organised to best support operational services, building on insights gained from responding to the COVID-19 crisis. There were no recommendations for major changes to IT or cybersecurity in this review (outside the change outlined below). However, the change did create a more centralised governance and risk function with the appointment of a National Director for Governance and Risk (equivalent to a Chief Risk Officer) with responsibility for establishing Enterprise Resilience and Business Continuity Frameworks, through which risk management and business continuity plans will be reviewed, maintained and validated. Responsibility for clinical and service continuity under the HSE's accountability structure will remain with operational and functional managers.

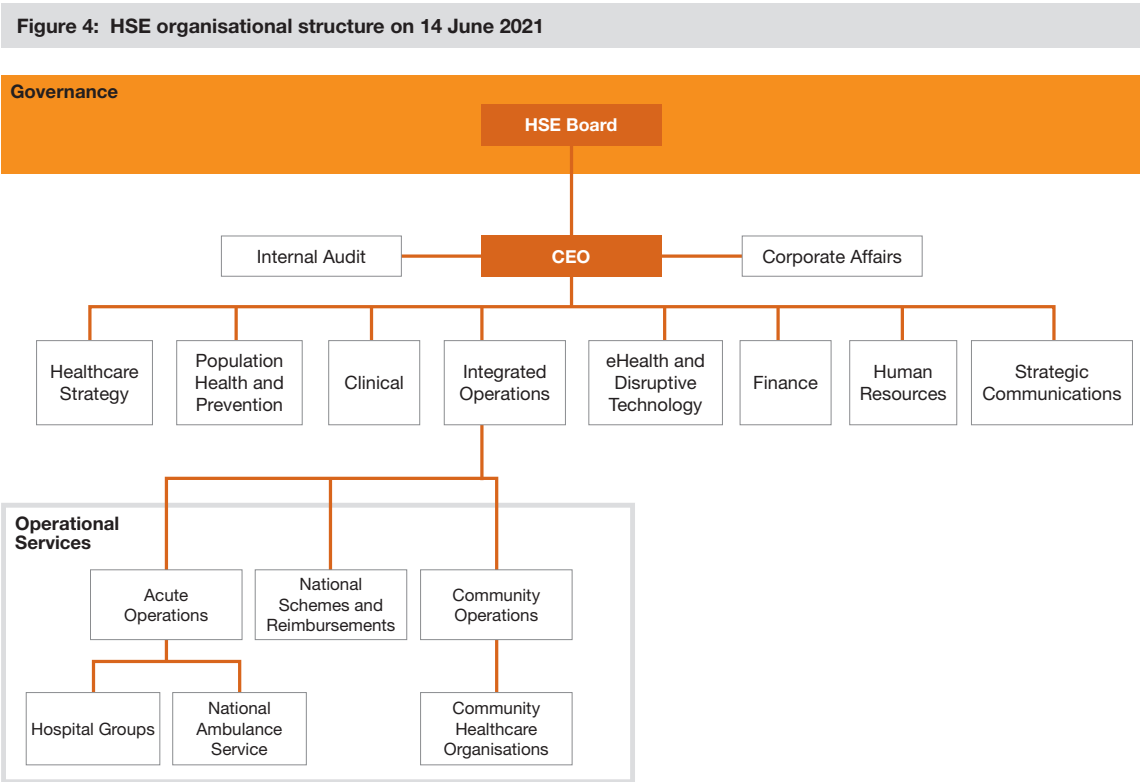
These and other initial organisational changes took effect approximately 1 month post the Incident, on 14 June 2021, including:

- Healthcare Strategy (to include Strategy and Research, Change and Innovation, Governance and Risk and Capital and Estates);
- Clinical (to include Quality & Patient Safety, Integrated Care Design and Innovation);
- Integrated Operations (to include Service Planning, Patient and Service User Experience, National Schemes and Reimbursement, Operational Performance and Integration);
- eHealth and Disruptive Technology (to include SAP Centre of Excellence);
- Finance (to include Financial Costing and Pricing, Finance Shared Services and Procurement);
- Human Resources (to include Capability and Culture, HR Shared Services and the National Integrated Staff Records & Pay Programme ("NiSRP")); and
- Audit (to include Health Care Audit).

It is planned that further changes will be made to the National Centre, including a Population Health and

Prevention function that will include the areas of Test and Trace, Public Health, Environmental Health and Health and Wellbeing, as well as a move towards a more integrated structure for Acute and Community Services.

HSE organisational structure on 14 June 2021



Acute hospital care

Acute hospital services are delivered across the network of six acute Hospital Groups and CHI and provide scheduled care, unscheduled care (unplanned or emergency care), diagnostic services, specialist services, cancer services, trauma services, maternity and children’s services and the National Ambulance Service. Hospital services are provided through a mix of HSE funded and directly managed hospitals and voluntary public hospitals funded predominantly through State funds.

Community healthcare services

Community healthcare services include primary care, social inclusion, older persons’ and palliative care services, disability and mental health services for both children and adults. Community healthcare services are currently delivered across nine geographically organised CHOs and are provided through a mix of HSE directly provided services and indirectly provided services through voluntary section 38 and 39 service providers, GPs and private providers.

In health services, there is an extensive community who are increasingly dependent on connected and reliable technological solutions and varying levels of IT support from the HSE National Centre to deliver clinical services. This includes the HSE's national IT infrastructure that enables patient care and patient safety as referred to further below.

c.350 IT Staff

Over 70k Devices

130k Staff

4000 Locations

54 Acute Hospitals

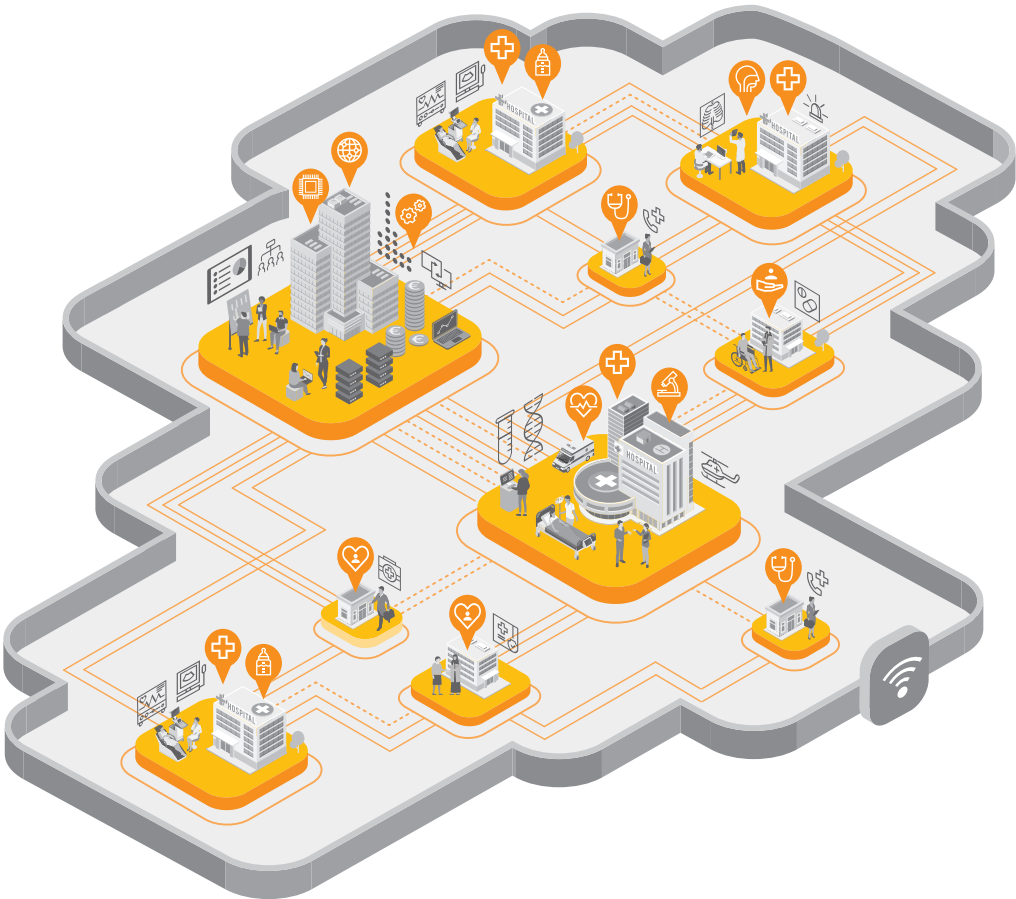
Over 1000 Applications

30 Cyber Security Board Awareness Draft V7.2.pptx
31 Weekly Brief, 21 September 2021
32 Cyber Security Board Awareness Draft V7.2.pptx

National Healthcare Network

The HSE utilises a NHN for the connectivity and delivery of critical national health services. The management of the NHN is the responsibility of the OoCIO within HSE National Centre, but it is accessed by the many organisations within the health services.

Figure 6: National Healthcare Network



The NHN is primarily a ‘flat’ network to make it easier for staff to access the IT applications they require. However, this design exposes the HSE to the risk of cyber attacks from other organisations connected to the NHN, as well as exposing other organisations to cyber attacks originating from the HSE - since once an attacker has a presence on the network they have ‘freedom to roam’.

The HSE has a complex IT environment including a significant number of legacy systems. At the time of the Incident just under two thirds of the server estate were described as modern³³, with the remaining estate deemed end of life and operating on extended

support or out of support.³⁴ HSE also had over 30,000 Windows 7 workstations that were deemed end of life by the vendor.³⁵ The HSE assessed its cybersecurity maturity rating as low.³⁶ For example they do not have a CISO or a Security Operation Centre established.

33 Software that is in mainstream support from the vendor

34 As confirmed by the General Manager Head of Technology Infrastructure & Deployment
35 Data provided from the antivirus management server (the [REDACTED] server) of systems that last communicated with [REDACTED] within the last three months, September 2021
36 VI Cybersecurity effectiveness assessment

The HSE is classified as a critical infrastructure operator under the EU NISD³⁷, also known as an OES. The purpose of this classification system is to ensure there is a common, high level security of network and information systems for Operators of Essential Services (“OES”) in each EU member state. The NCSC produces guidelines to assist OES in meeting these requirements.³⁸

Impact of the Incident on healthcare services

Healthcare services across the country were severely disrupted by the Incident, with real and immediate consequences for the thousands of patients who require healthcare services on a daily basis. In frontline healthcare delivery, patient care and patient safety is enabled by IT applications, such as diagnostic systems (primarily laboratory and radiology systems), electronic health records and pharmacy systems.³⁹ Some of the main impacts of the Incident were in the areas of patient identification, ordering and performing diagnostics, reporting results, prescribing medication and delays in providing treatment.⁴⁰ Whilst there is no evidence of the Attacker compromising medical devices directly, there was a loss of information flows in and out of those devices whilst IT systems were down.

The impact on clinical care processes was evident immediately and the HSE issued guidance that directed providers towards emergency, urgent and time scheduled care only⁴¹. Clinical contingency arrangements were put in place with providers curtailing services. On the morning of the Incident, 31 of the 54 acute hospitals announced cancellations of at least some of their services.^{42 43} Cancellations varied by hospital and included some outpatient clinics, diagnostic imaging, radiotherapy, certain pathology tests and certain elective surgeries.

Emergency care continued.

The disruption impact varied by service provider, depending on its reliance on IT in provision of its services and its reliance on the NHN and national systems in particular. Community based services tended to have less reliance on IT other than email as compared to the acute hospitals. The COVID-19 testing centres were able to repurpose Healthmail to generate appointments. The vaccination program continued with the online vaccination system taken offline for a few hours only, although the COVID-19 reporting system was lost for a period of time.⁴⁴ The National Ambulance Service was not impacted.

HSE business continuity plans did not envisage a severe but plausible total IT loss scenario for a period of weeks. Workarounds were quickly put in place in many instances, to ensure continuity of services for as long as possible. Certain hospitals had a manual approach pre-prepared for particular processes, whilst others did not and staff needed to be innovative in their approach.

Impact example: For laboratory tests, healthcare professionals reverted to handwritten forms, with staff taking them to the lab to be manually entered and analysed with a similar process for returning results. This resulted in an increased likelihood of delay and risk of error with these manual processes.

There was no access to patient information systems such as Integrated Patient Management System (“iPMS”). This resulted in challenges in identifying patients, retrieving patient paper files, accessing contact details, managing DNAs (Did Not Attends), transferring patients between services and managing patient waiting lists.

37 This occurred in July 2016. See NIS Compliance Guidelines for Operators of Essential Service

38 <https://www.ncsc.gov.ie/oes/>

39 Healy, O. Dr. A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare IT failure, Dated 30th September 2021.

40 Healy, O. Dr. A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare IT failure, Dated 30th September 2021.

41 CCO Clinical Memo 1 15.05.2021

42 HSE cyber attack – which hospitals are affected? Here is everything you need to know. Source: Irish Independent. Date: May 16 2021

<https://www.independent.ie/irish-news/hse-cyber-attack-which-hospitals-are-affected-here-is-everything-you-need-to-know-40432288.html>

43 HSE website - Acute Hospital in Ireland <https://www.hse.ie/eng/services/list/3/acutehospitals/hospitals/hospitalist.html>

44 Reporting on epidemiology of COVID-19 from the national Computerised Infectious Disease Reporting (CIDR) system to recommence on 02/09/2021. Source: HSE website. Date: September 2 2021 <https://www.hpsc.ie/a-z/respiratory/coronavirus/novelcoronavirus/surveillance/recommendationofreportingfromcidr/>

Impact example: A GP received a phone call from a consultant surgeon questioning the location of a patient due for surgery, when that patient had already been operated on.

Impact example: One example hospital had no way to access their appointment data. Unless people showed up with their appointment letter in their hand, they did not know how to process them.

Where electronic healthcare records were relied upon, access to these records was no longer available. For example the four maternity hospitals using the Maternal & Newborn Clinical Management System (“MN-CMS”) no longer had access. These hospitals switched to paper records and charts. Whilst business continuity plans envisaged an IT outage on MN-CMS for a short period, for example due to a system upgrade, a data centre outage or similar issue, the length of time without MN-CMS access increased risks to patient care, particularly due to the lack of access to patient history.

Diagnostic systems such as the shared service for handling medical imaging, NIMIS and compuscope system were unavailable.

Impact example: For some oncology patients in the middle of treatment, the Incident meant that hospitals didn’t have access to the patient’s radiotherapy plans and could not safely continue treatment without new medical imaging. Some hospitals used adjacent private facilities where available, to take new medical images to continue providing radiotherapy treatment to patients.

At the time of the PIR, there is a lack of empirical data to clearly identify the impact of the Incident on patient care during this period. This is partially due to incomplete data in many areas due to a backlog of manual records, but also the difficulty in separately identifying the impact of the Incident from other issues affecting public healthcare services during this time, such as COVID-19, shortage of consultants and other capacity issues.

The Incident disrupted public hospitals’ ability to provide complete waiting list data to the National Treatment Purchase Fund (“NTPF”), therefore no data was published for June 2021.⁴⁵

This extremely difficult operating environment, caused by the Incident, put additional stress on a system of healthcare professionals that were already exhausted by four waves of the COVID-19 pandemic. Frustrations were expressed at not being able to provide care in the normal way. Administration and

other staff experienced difficulties dealing with varying levels of frustration and aggression from patients and members of the public.⁴⁶

Impact example: “Staff is (sic) fatigued as they continue to deal with the pandemic, along with IT issues and workarounds”. “It has had an impact on staff – the two serious issues coming one after the other, we haven’t experienced anything like it before”.

Impact example: During the response, the CIO, Head of Occupational Health and the National Ambulance Service identified a risk of staff burnout. It was at this point Occupational Health were requested to attend the war room to check responders’ health, and staff rotas were implemented.

The HSE has commissioned a study⁴⁷ to review the mitigations and contingencies which were adopted to minimise the impact of the Incident on patient safety, with a focus also on what worked well to inform future planning for IT outages. It is a longitudinal study so will take into account the longer term impact from the Incident. We were provided with a draft report of this study, but the study is ongoing and therefore the report is incomplete at the date of this PIR report. This study when completed will provide further insight into the impact of the Incident on healthcare services.

There were also many non-clinical impacts from the Incident on the HSE and organisations that are funded by it. These are varied and wide ranging. Some examples include:

Impact example: Whilst payments of wages and salaries to HSE staff generally continued, travel and subsistence claims could not initially be paid. Pandemic Placement Grant (“PPG”) for student nurses and midwives, which was due to be paid by the 1st June 2021, was delayed in many areas and in some instances was only partially paid.

Impact example: Inability to use HSE email accounts led to a delay in the General Register Office process leading to delays in child benefit payments for new births or delays in issuing passports.

⁴⁵ <https://www.ntpf.ie/home/outpatient.htm>

⁴⁶ Healy, O. Dr. A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare IT failure, Dated 30th September 2021.

⁴⁷ A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare ICT failure.

2.2 Background to this post incident review

Under the HSE's Incident Management Framework, the Incident has been categorised as a Category 1: Major or Extreme Incident as per the HSE's Risk Impact Table⁴⁸ which requires a Comprehensive Review. Given the seriousness of the Incident, the impact it has had on people dependent on health services and the associated patient safety risks as well as the heightened vulnerability for the HSE as a result of the current disruption, it was agreed by the Board of the HSE ("the Board") in conjunction with the CEO and the EMT that this review would be carried out as an independent PIR.

In June 2021, PwC was commissioned by the Board in conjunction with the CEO and the EMT to undertake an immediate and independent PIR into the circumstances surrounding the infiltration of the HSE's IT systems. The PIR was carried out under the terms as set out in the HSE's Incident Management Framework. Following an initial four week scoping phase, the PIR was conducted over a period of 14 weeks.

The purpose of the PIR was to:

- Urgently establish the facts in relation to the current preparedness of the HSE in terms of both its technical preparedness (Information and Communications Technology ("ICT") systems, cyber and information protections) and its operational preparedness (including Business Continuity Management planning) for a strategic risk of this nature;
- Identify the learnings from this Incident to identify improvements to the HSE's preparedness for and response to other major risks including immediate risks and incidents that cause major business disruption; and
- Share those learnings within the HSE and externally with State and non-State organisations to inform their future preparedness.

2.3 Scope of our review

The scope of the PIR covers the HSE National Centre and their provision and interaction with the nine CHOs, the six Hospital Groups and CHI.

We took a sample approach to review the involvement of the CHOs and the hospitals within the Hospital Groups, specifically looking at how the HSE's strategy was implemented at tactical levels

and the effectiveness of the HSE's coordination of efforts. We selected a sample of two CHOs and nine hospitals, each of which were impacted by the Incident. This sample included a mix of voluntary and HSE managed hospitals, a geographical spread and differences in disruption levels caused by the Incident. We did not review the technical and operational preparedness and response of each individual hospital or CHO.

The review did not cover other agencies such as TUSLA or third party healthcare service providers. Our review did not cover the cyber attack at the Department of Health ("DoH"), though the timing of this attack is referenced in our review.

The scope of the review did not cover an evaluation of the appropriateness of the HSE's current or historic spend on cybersecurity/ defence or the appropriateness of its annual IT expenditure generally. We did not validate the work performed as part of any previous information security audits or related work on which the HSE historically made decisions.

A technical forensic investigation was carried out by the HSE's Incident Response provider after the Incident. Though we relied on outputs from the HSE's Incident Response provider to inform our assessment, we did not re-examine the HSE's Incident Response provider's evidence nor did we re-perform their forensic analysis as part of the review. Moreover, we limited analysis of technical security controls to those implemented to address the specific attack techniques identified to be used during the Incident.

More details of the scope of our review can be found in Appendix A.

2.4 Our review approach

Undertaking a review of this nature is complex and requires a deep understanding of the context in which the Incident occurred, the environment in which the HSE operates, the structure of public healthcare services in Ireland and the structure of the HSE itself. In order to rapidly understand and analyse the intricacies of the HSE's preparation and response for this Incident, we brought together an experienced team of IT and cybersecurity experts in both Ireland and the UK as well as specialists in crisis management, forensic investigation and response, data privacy, healthcare and regulatory experts with extensive experience in cybersecurity PIRs.

⁴⁸ HSE Incident Management Framework & Guidance - 2020

In recognition of the complexity and multifaceted nature of the Incident, we approached our review through the lens of three connected but distinct areas of focus.

Focus area 1

To review the technical investigation and response

Focus area 2

To review the organisation-wide preparedness and strategic response

Focus area 3

To review the preparedness of the HSE to manage cyber risks

Focus area 1

In this area, we reviewed the technical investigation and response to the Incident and the subsequent recovery and investigation activities undertaken by the HSE. We reviewed the effectiveness of the response and recovery, the sufficiency of the investigation to support the conclusions made and the ability of the HSE to detect and prevent similar incidents in the future.

We took a phase-based approach to this focus area, looking at preparedness to defend against and respond to a ransomware cyber attack, response to the Incident, recovery from the Incident and sustainable reduction of risk since the Incident. We used our proprietary “Ransomware Capability Framework”⁴⁹ to assess the cybersecurity controls in place at the time of the Incident. In addition, we reviewed the HSE’s network and AD structure, including the architecture of the NHN and conducted an analysis of the recovery of specific applications.

In each phase, we deep-dived into specific areas of interest that were identified during our review. This was done through:

- review of relevant documentation including a sample of daily incident Situation Reports (“SITREP”s), investigation reports, RAID logs and recovery plans;
- interviews with key stakeholders involved in the response, the investigation and the recovery and

- interviews with technical teams to understand the cybersecurity controls in place at the time of the Incident and assess these against our “Ransomware Capability Framework”.

Focus area 2

In this area, we reviewed the organisation-wide preparedness and the strategic response to the Incident and the corresponding response and recovery activities completed by the HSE, including the subsequent communication and coordination activities undertaken.

This review was carried out through a three-phased approach looking at

- crisis preparedness;
- crisis response ; and
- crisis recovery.

It was structured using the International Organisation for Standardisation (“ISO”) and technical specifications guiding the implementation and maintenance of both business continuity and crisis management capabilities. *ISO 22301:2019 “Security and resilience - Business continuity management systems (BCMS) - requirements* guides the construction, maintenance and validation of an effective Business Continuity Management System. In the context of the HSE, the term clinical and services continuity is used throughout the report, rather than business continuity. It refers to all acute and community services, as well as corporate services, including, but not limited to HR, procurement, finance, training, ICT etc. PD CEN /TS 17091:2018 is the internationally recognised specification which provides guidance to strategic decision makers to plan, implement, establish, operate, monitor, review, maintain and continually improve a crisis management capability. The review was done through;

- review of relevant documentation relating to the structure of the HSE, crisis management and business continuity procedures in place prior to the Incident,
- a sample review of SITREPs, morning briefings and other communication channel conversations used during the response;
- interviews with key stakeholders involved in the organisational response to the Incident;

⁴⁹ PwC’s proprietary ransomware readiness framework lists the most important cybersecurity controls we have identified to prevent, detect and respond to human-operated ransomware attacks.

- workshops to examine:
 - risk, business continuity, incident and crisis management structures and processes in place at the time of the Incident;
 - impacts on operational and clinical services;
 - crisis response effectiveness;
 - security control failures and organisational security cultural and behavioural causes.

Focus area 3

In this area, we performed an assessment of the HSE's cyber preparedness, resilience and ability to respond to future incidents. To carry out this assessment, we developed a "PIR Cybersecurity Framework" which was based on the NIST Cybersecurity Framework⁵⁰ and Control Association Control Objectives for Information and Related Technologies ("COBIT"). These are both internationally recognised standards used frequently by organisations to assess their information security capabilities and IT governance processes. Our "PIR Cybersecurity Framework" incorporates NIST's five key domains and 23 supporting sub-domains along with the governance aspects from COBIT. This was performed through:

- review of relevant documentation relating to the HSE's information security controls and processes to measure their effectiveness and maturity in terms of NIST CSF;
- review of relevant documentation to assess the resilience of the HSE's information security controls and processes with a focus on people and business continuity management using COBIT as a reference;
- interviews with key stakeholders involved in information security and IT governance.

Our approach in summary

In summary, our review involved:

- The analysis of more than of 2,500 artefacts including documents, records and data.
- A total of 81 interviews with over 190 people from the National Centre, hospitals, CHOs, GPs as well as third parties including:
 - 53 one to one interviews with National Centre personnel;
 - Four workshops with National Centre personnel;
 - Meetings with representatives of nine hospitals;
 - Meetings with representatives of two CHOs;
 - Workshop with GP representatives; and
 - 12 interviews with third parties involved in the immediate response to the Incident.
- Detailed analysis of a wide range of aspects of the review;
- Factual accuracy checking and verification exercises.

Important comment on our approach:

Activities relating to the HSE's response have been evidenced up to 31 July 2021 throughout this report. Where applicable, some evidence of activity after 31 July 2021 has been included to provide further context, but this has been highlighted and noted specifically in relevant sections.

During our historic review of the preparedness for the Incident and the HSE's structure, processes and infrastructure, the maximum period of look back is five years.

50 <https://www.nist.gov/cyberframework>

Summary approach to focus areas:

Figure 7: Summary approach to focus areas		
Focus area 1	Focus area 2	Focus area 3
The technical investigation and response to the Incident	The organisation-wide preparedness and strategic response	The preparedness of the HSE to manage cyber risks
Review of the technical response to the incident including effectiveness of measures taken to contain the incident;	Documenting of timeline of known facts relating to the incident and response activities to date;	Using key areas from the NIST CSF and the governance aspects of COBIT to assess key areas of information security;
Review of investigation activities and comment on their sufficiency to support conclusions made;	Assessment of timeliness and effectiveness of incident identification, reporting and escalation;	Review of cybersecurity governance and leadership, IT / cybersecurity operating model and executive preparedness in the event of a cyber attack;
Identification of any gaps in the investigation or in the scope of evidence analysed;	Review of how the incident was managed and coordinated by the organisation;	Examination of resilience and protection of data, as well as wider business continuity planning;
Identification of technical control gaps that contributed to the incident occurring using our "Ransomware Capability Framework";	Examination of the effectiveness of the business-wide strategic response;	Identification of key capability gaps to prevent a major incident reoccurring and reduce exposure to major cybersecurity risks;
Analysis of the technical impact of the incident, and review the recovery of key business critical applications;	Review of communications with stakeholders;	Consideration of any inflight or planned/budgeted improvements resulting from the Incident.
Review of technical improvements planned or implemented to prevent this, or similar, incidents reoccurring;	Assessment of clarity of accountability and processes for decision making;	
Review of detective and monitoring controls in place to provide confidence there is no further Attacker activity in the environment.	Review of response strategies and how they impacted response and recovery efforts;	
	Assessment of how playbooks and policies supported the response;	
	Understand how organisational culture contributed to root causes and response.	
Recommendations to improve preparedness and response to a major incident		
Recommended improvements to increase the HSE's ability to respond and recover from cybersecurity incidents from a technical and strategic perspective		
Recommended improvements to increase the HSE's preparedness for cybersecurity incidents from a technical and strategic perspective		
Recommended improvements to reduce the HSE's exposure to cybersecurity risks and remediate root-cause issues that allowed the incident to occur		
Recommended improvements to increase the HSE's resilience to major cybersecurity incidents		

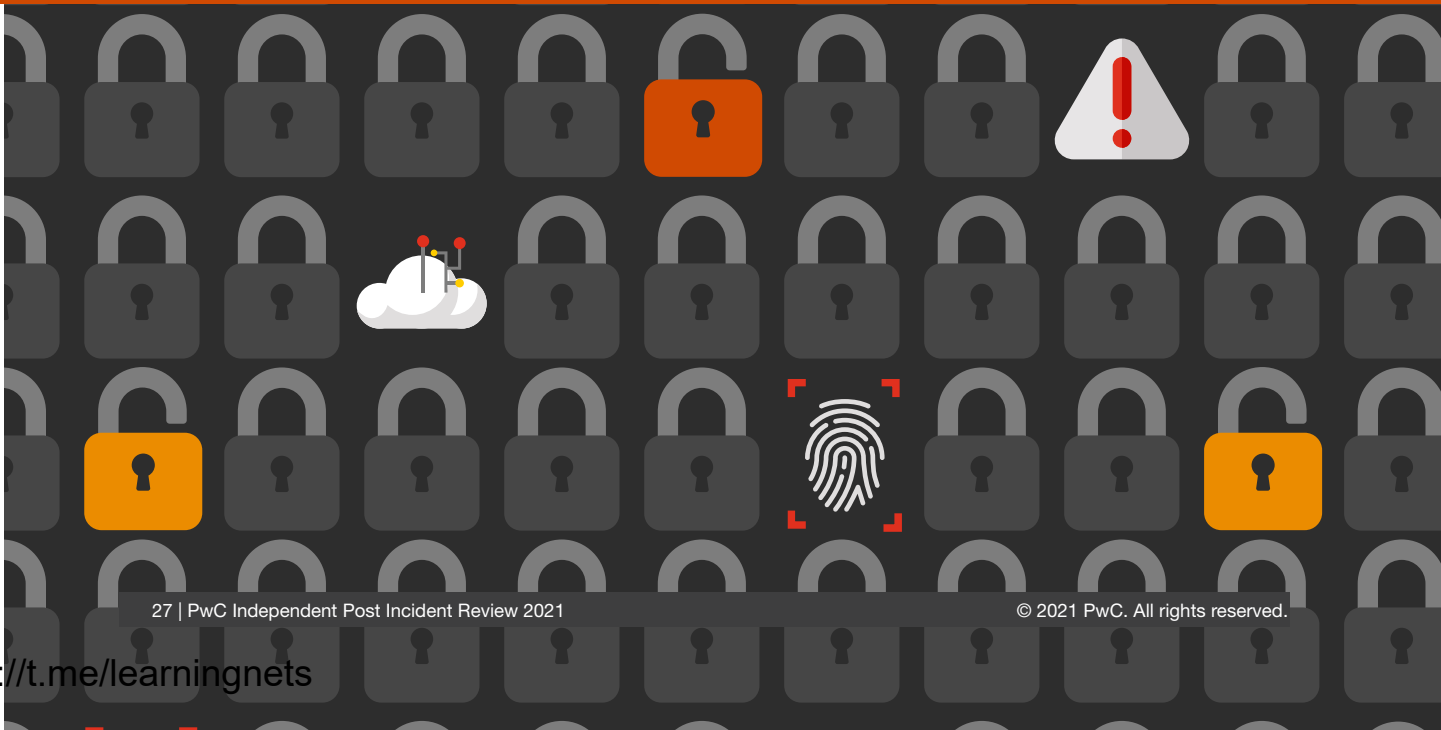
2.5 Structure of our report

In the following sections of our report we set out:

- **Timeline of the Incident:** A timeline of the Incident prior to and after the execution of ransomware, including actions taken by the HSE during the containment, investigation and recovery phases of the Incident, Section 3;
- **Key recommendations and findings:** Our assessment of the steps that should be taken to address the issues identified in our report and our strategic recommendations to remediate the issues, Section 4;
- **Detailed findings and recommendations by focus area:** Our further detailed findings and tactical recommendations by focus area, which includes the learnings that the HSE can take to protect themselves from a similar major cyber incident, Section 5

3

Timeline of the Incident

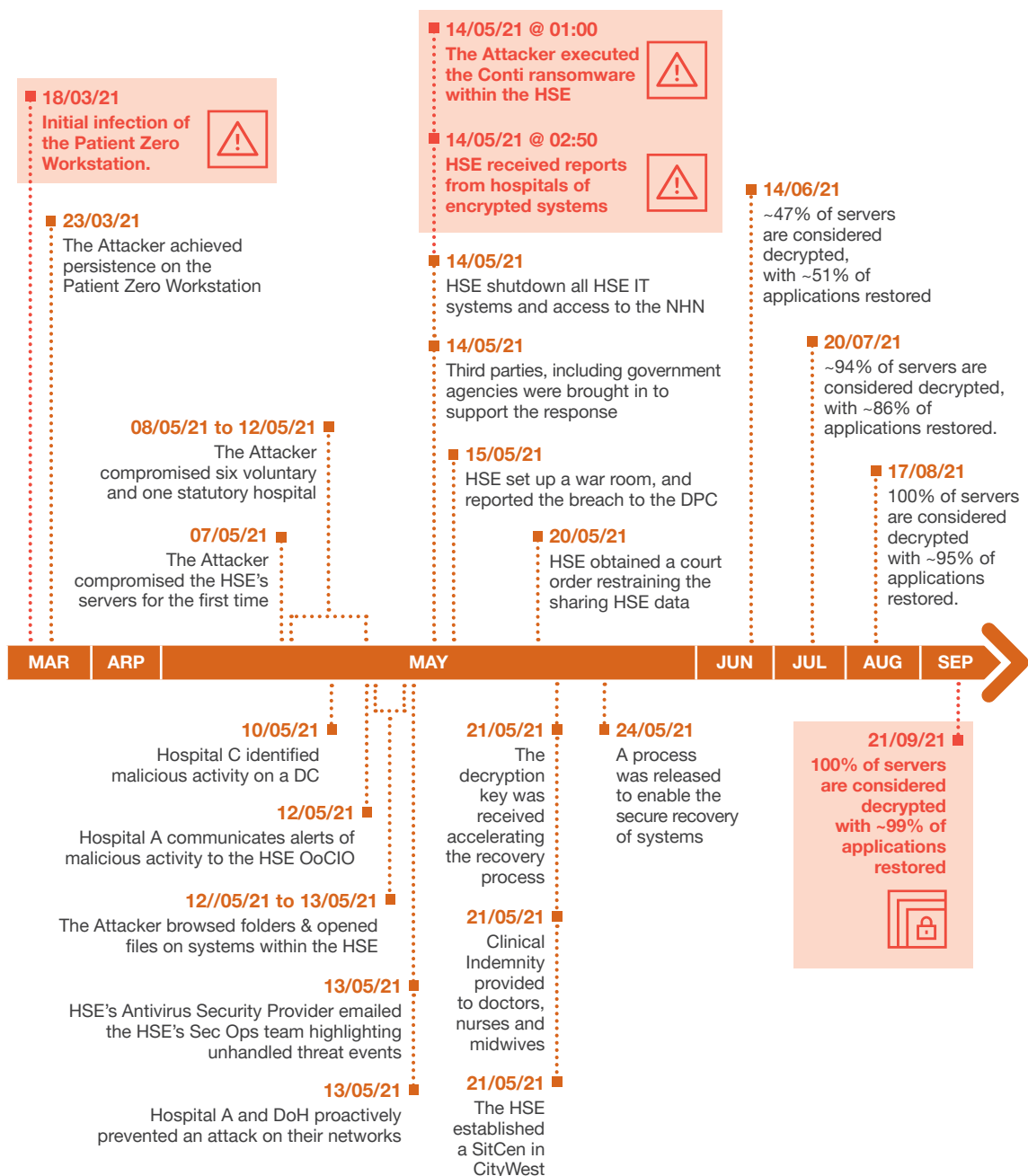


On 14 May 2021, the HSE was subjected to a significant cyber attack, through the criminal infiltration of its IT systems using Conti ransomware software. The Incident impacted all nine domains within the NHN, which included statutory and voluntary hospitals and CHOs across the country. A detailed timeline is included in Appendix E and F.

As part of the response, the HSE engaged the HSE's

Incident Response provider to undertake a forensic investigation to establish an understanding of what the Attacker did while present on HSE systems prior to the Incident. Evidence was identified as to how the Attacker was able to gain unauthorised access to the HSE's IT environment and what the Attacker did once they were able to gain this access. The key events identified during this investigation are set out in the diagram below:

Figure 8: Timeline of the Incident



The timeline of the Incident is broken down, in a chronological order of events from oldest to newest, under the following headings:

- Timeline prior to the Incident;
- Timeline prior to the Incident and the response at Hospital A, a Specialty Hospital (“Hospital C”) and the DoH;
- Timeline of the Incident and the response at the HSE on 14 May 2021;
- Timeline post the Incident and the response and recovery at the HSE.

Timeline prior to the Incident

This section provides a timeline of what the Attacker did while present on HSE systems prior to the execution of the Conti ransomware, including the actions taken by the HSE in response to antivirus detections.

On 18 March 2021, a HSE staff member interacted with a malicious Microsoft Office Excel file attached to a phishing email. This resulted in a Malware infection of the Patient Zero Workstation.

On 23 March 2021, the Attacker created a persistence mechanism on the Patient Zero Workstation to ensure the Attacker retained access to the HSE’s environment if the Patient Zero Workstation was rebooted or powered off.

On 31 March 2021, the HSE’s antivirus software detected the execution of two software tools commonly used by ransomware groups: Cobalt Strike and Mimikatz, on the Patient Zero Workstation. The antivirus software was set to monitor mode so it did not block the malicious commands.

The HSE’s Incident Response provider identified no significant Attacker activity between 1 April 2021 and 6 May 2021.

On 7 May 2021, the Attacker installed additional persistent Malware on the Patient Zero Workstation, conducted AD and domain reconnaissance, and compromised further systems within the HSE. The Attacker was identified as using highly privileged accounts for the first time.

On 8 May 2021, first identified evidence of the Attacker compromising systems within Hospital K and Hospital D.

On 9 May 2021, first identified evidence of the Attacker compromising a system within Hospital J.

On 10 May 2021, first identified evidence of the Attacker compromising systems within Hospital C and Hospital L. Hospital C’s antivirus software detected Cobalt Strike on two systems but failed to quarantine the malicious files.

On 11 May 2021, first identified evidence of the Attacker compromising a system within Hospital A. After numerous failed logon attempts, the Attacker likely exploited an unpatched known vulnerability, [REDACTED], to gain access to the domain. Hospital A’s antivirus software detected and deleted the malware on several systems.

On 12 May 2021, first identified evidence of the Attacker compromising a system within Hospital B. The Attacker was identified browsing folders, opening files, creating archives and accessing or attempting to access file sharing websites on systems within Hospital A, Hospital B and Hospital D. The HSE’s cybersecurity solutions provider emailed the HSE’s Security Operations team to escalate alerts on two servers and requested a full on demand scan be completed.⁵¹ The HSE responded on the same day to confirm the scans had been executed.⁵²

On 13 May 2021, first identified evidence of the Attacker browsing folders, opening files, creating archives and accessing a file sharing website on systems within the HSE. The HSE’s cybersecurity solutions provider emailed the HSE’s Security Operations team and outlined that there were unhandled threat events since 7 May 2021 on at least 16 systems; the HSE Security Operations team requested that the Server team restart servers.

On 14 May 2021, the Attacker executed ransomware on systems within the HSE, Hospital C, Hospital K, Hospital D, Hospital L, Hospital J and Hospital B.

Timeline prior to the Incident and the response at Hospital A, Hospital C and the DoH

Two voluntary hospitals, Hospital A and Hospital C, identified suspicious activity prior to the Incident. In addition, the DoH, a third party to the HSE’s environment, successfully acted on a detection of the Attacker which prevented the execution of the Conti ransomware across the vast majority of the DoH.⁵³

51 Email with subject RE: Threat not handled, 13 May 2021

52 Email with subject RE: Threat not handled, 13 May 2021

53 <https://www.gov.ie/en/news/d48b2-a-note-for-the-public-on-the-recent-cyber-attack-on-the-department-of-health/>

The following timeline describes the key activities at Hospital A, Hospital C and the DoH prior to the Incident.

On 10 May 2021, Hospital C asked Hospital C's cybersecurity solutions provider whether they should be concerned about Cobalt Strike alerts. They were advised by Hospital C's cybersecurity solutions provider that since the threat had been remediated by their antivirus software, their risk was low.⁵⁴ Hospital C did not initiate a cyber incident response investigation.

On 12 May 2021, Hospital A engaged Hospital A's Incident Response provider to investigate alerts of malicious activity. They reset passwords for 4,500 accounts⁵⁵ and made firewall configuration changes⁵⁶ to contain the activity, and made contact with the HSE to request information on two IP addresses.⁵⁷ To further contain the activity, Hospital A utilised their existing security tooling across their environment.

On 13 May 2021, the HSE identified the IP addresses reported by Hospital A related to two servers within the HSE's [REDACTED] domain. The HSE conducted an investigation into the activity identified by Hospital A and incorrectly concluded in an email between the HSE teams⁵⁸ that the suspicious activity originated from Hospital A, rather than the other way round.

On 13 May 2021, DoH's cybersecurity solutions provider⁵⁹ alerted the DoH to a potential attack on their network. DoH contacted the NCSC and engaged DoH's IR Provider⁶⁰ who installed endpoint detection and response ("EDR") security tooling on the majority of their systems. These actions blocked the execution of the Conti ransomware across the vast majority of the DoH's infrastructure, including critical and data servers.

Timeline of the Incident and the response at the HSE on 14 May

The following timeline describes the key activities at the HSE on the day of the Incident, 14 May 2021.

On 14 May 2021 at approximately 01:00, the Attacker executed ransomware on systems within the HSE, Hospital C, Hospital K, Hospital D, Hospital L, Hospital J and Hospital B.

- | | |
|----|---|
| 54 | Logging call with Hospital C's cybersecurity solutions provider on 10/05/2021 17:06 |
| 55 | Information gathered from an interview with Hospital A |
| 56 | Information gathered from an interview with Hospital A |
| 57 | Email with subject: Recognise these addresses??. May 2021 |
| 58 | Email with subject RE: Summary, May 2021 |
| 59 | Information gathered from an interview with the NCSC |
| 60 | Information gathered from an interview with the NCSC |

At 02:50, the HSE's national service desk received the first of multiple reports from hospitals of multiple systems being unavailable as a result of the Incident.⁶¹

At 04:36, the HSE identified malicious encryption on multiple servers in the HSE's data centre.⁶²

At 04:41, due to the widespread reports of encryption, and the presence of ransomware in the HSE's data centre, the HSE invoked their Critical Incident Process.

At 05:10, an initial critical incident call was held between network and infrastructure subject matter experts ("SMEs"). Decisions were taken to contain the threat including removing all internal and external connectivity for the NHN, and to begin engagement with voluntary hospitals.

At approximately 06:00, the CEO notified the Board of the Incident.

At 07:00, RTÉ News released a news bulletin on the Incident. Shortly afterwards, the CEO notified the EMT and National Crisis Management Team ("NCMT").

At 07:28, HSE Live, the HSE contact centre, issued a tweet notifying the public of an incident and the shutdown of services. Shortly afterwards, the HSE's Data Protection Officer ("DPO") rang the office of the DPC.

At 08:30, the first meeting of the NCMT was held.⁶³

At 09:22, The HSE informed Primary Care Reimbursement Service ("PCRS") of the cyber incident and PCRS decided to shut down their systems.

At 10:00, it was reported during a Major Incident ("MI") call that the HSE had initiated a preventative lockdown strategy to contain the impact of the attack by switching off all systems within the HSE. The Garda National Cyber Crime Bureau, Interpol and the NCSC were brought in to support the response.

At 10:30, with the support of the NCSC, the HSE engaged the HSE's Incident Response provider to provide incident response services for the HSE. The HSE also engaged others such as Third Party C, Third Party A, Third Party D, Third Party B and Third Party E to provide tactical incident response and

- | | |
|----|--|
| 61 | CIM 2 - Conti Ransomware Incident coordination Form Ver 2.1(2), 2021 |
| 62 | CIM 2 - Conti Ransomware Incident coordination Form Ver 2.1(2), 2021 |
| 63 | Conti Cyber Response NCMT Structures Governance and Admin V1.10 31052021 |

recovery support.

At 12:00, it was reported that a Malware sample was sent to a threat research organisation for analysis.

At 14:00, it was reported that the HSE sent a text message to all HSE work devices notifying staff members of a ransomware attack impacting the HSE, and voluntary and statutory hospitals.

At 16:30, it was reported that the HSE's Incident Response provider began deployment of their endpoint security monitoring software to gain visibility of the HSE's environment and enable a full forensic investigation of systems within the HSE. The MI meeting established a once daily operating rhythm.

Late on the evening of 14 May 2021, the HSE informed the DPC about the Incident.⁶⁴

Timeline post the Incident and the response and recovery at the HSE

The following timeline describes the key activities post the Incident from a response and recovery perspective at the HSE.

Response

On 15 May 2021, the HSE senior management set up a war room at a third party's office building on Molesworth Street.⁶⁵ Initial workstreams were set up to enable a coordinated response and recovery from the Incident. The HSE's DPO issued a formal notification to⁶⁶ the DPC about the Incident and the HSE's Incident Response provider was engaged by voluntary hospitals to provide incident response support and questionnaires were sent to the voluntary hospitals to get an understanding of which entities were compromised. The HSE's senior leadership team were provided with clean Microsoft [REDACTED] mailboxes to allow for communication during the initial stages of the response, and a mailbox⁶⁷ was set up to deal with issues relating to the ransomware attack.

From 17 May 2021, the HSE coordinated daily incident management meetings between all parties supporting the response to the Incident to ensure that there was a forum to collect and share information. The OoCIO's Communications team also established a twice daily meeting rhythm. These forums were used to share information about the response and to communicate new processes to the rest of the business, in an effort to move to a recovery phase,

and to keep members of the public up to date on the response to the Incident. Key response activities over the following days included, but were not limited to:

- An initial list of priority applications was identified, the [REDACTED] AD domain was recovered which allowed the HSE to build their foundational IT infrastructure;
- A 'go-to-green' process was proposed for recovering systems and was communicated to internal stakeholders for consideration;
- A social media monitoring system Talk Walker was set up to scan the web for leaked patient data;
- The first call between the HSE and the Defence Forces was held to discuss support requirements;
- The application NIMIS was recovered with a Model 4 Hospital⁶⁸ being the first hospital with NIMIS to go live.

It was also within this timeframe that the CIO, Head of Occupational Health and the National Ambulance Service identified a risk of staff burnout. It was at this point, Occupational Health were requested to attend the war room to check responders' health, and staff rotas were implemented.⁶⁹

From 19 May 2021, key response activities included, but were not limited to:

- The first clean laptops were distributed to a select number of HSE staff members and HSE staff members were given derogation to use personal emails and devices for crisis communications;
- The initial list of priority applications was reprioritised and informed by clinical priorities, as dictated by the clinical and integrated governance structure that was initially set up to guide the operational response and in an effort to enable a two way flow of information; and
- The HSE established a Legal and Data workstream to oversee the appointment and subsequent work of their legal advisers and to support the work of the DPO in coordinating the HSE's data protection investigation, engagement with An Garda Síochána and subsequent reporting to the DPC.⁷⁰

Five days into the response, the lack of integrated programme management was recognised as a risk by

64 DPC Report 15 July 2021

65 Programme RAID Log, 2021

66 Original DPC Notification_May 2021

67 Minutes of Cyber Attack MI Meeting 10 am - 15052021

68 NIMIS RE-ENABLEMENT TRACKER CYBER ATTACK RECOVERY, 2021

69 Programme RAID Log

70 Document subject to legal privilege

the HSE. This led to a request for assistance from the Defence Forces who established defined Information Management processes which were scalable and agile and could cope with the complexity of a cyber crisis.

On 20 May 2021, the Defence Forces attended Molesworth Street for further discussions around the level of support that was required by the HSE during the response and recovery phases of the Incident. It was reported that on the same day, the Attacker posted a link to a software application that would decrypt files encrypted by the Conti ransomware during the Incident. The HSE's Incident Response provider, on behalf of the HSE, validated that the decryption software worked, reverse engineered its capabilities, and produced a new, more stable decryption software that was also supported by them.⁷¹ The HSE also secured a High Court injunction⁷² restraining any sharing, processing, selling or publishing of data stolen from its computer systems.

On 21 May 2021, the SCA recognised the enormous impact the Incident had on doctors, nurses, midwives and allied healthcare professionals, on the provision of health and social care services and clinical care within the HSE.⁷³ As these professionals were obliged to practice without the usual back up of essential systems, clinical imaging and other diagnostic-related results to assist in their assessment and treatment of patients, the SCA confirmed these professionals were fully covered by the Clinical Indemnity Scheme in relation to their ongoing clinical decision-making, in the absence of such clinical support. Separately, the physical SitCen was also established in CityWest.⁷⁴

On the same day, the availability of the decryption key allowed the HSE to create efficiencies during the recovery process by deploying a decryptor across the environment to decrypt files on impacted systems. This enabled HSE to scale their recovery effort and make the overall process more efficient.

Recovery

From 22 May 2021 onward, the HSE moved from the response phase into the recovery phase, where they focused their efforts on decrypting systems,

cleansing workstations, restoring systems and the recovery of applications.

On 24 May 2021, the HSE's Incident Response provider and the HSE released their 'go-to-green' processes to internal stakeholders, to ensure the secure recovery of systems, reduce the risk of further ransomware attacks, and to provide guidance in recovering systems. The HSE's Incident Response provider and the HSE developed requirements that every system within the HSE, voluntary hospitals and CHOs had to meet before being able to rejoin the network, and for organisations to be reconnected back to the NHN.

Figure 9: Summary of progress over the following three months

Duration	Progress made
One month after the Incident	The HSE had decrypted 47% of servers and fully restored 48% of Acute applications, 40% of Community Services applications and 64% of business services applications ⁷⁵ .
Two months after the Incident	This increased to 94% of servers decrypted and fully restored, 85% of Acute applications, 94% of Community Services applications and 79% of business services applications ⁷⁶ .
Three months after the Incident	The HSE reported that 100% of servers were considered decrypted and they had fully restored 95% of Acute applications, 98% of Community Services applications and 91% of business services applications ⁷⁷ .

By 21 September 2021, the HSE had recovered 1,075 applications, out of a total of 1,087 applications.⁷⁸ Finally, at the time of issuing this report the HSE had notified the DPC in relation to the Incident, however, they have not made any data subject notification for personal data exposure or exfiltration, however, they continue to work closely with the DPC in relation to this matter.⁷⁹

- 71 HSE's Incident Response provider, Intrusion Investigation Report
- 72 <https://www.hse.ie/eng/services/publications/order-perfected-20-may-2021.pdf>
- 73 https://stateclaims.ie/uploads/publications/State-Indemnity-Guidance-IT-cyber-attack-on-the-health-and-social-care-sector-from-14-may-2021_21.5.21_2021-05-21-150239_tytw.pdf
- 74 Conti Cyber Response NCMT Structures Governance and Admin V1.10, 31 May 2021

- 75 SITCEN SITUATION REPORT, 18:30 14 June 2021
- 76 Weekly Brief, 20 July 2021
- 77 Weekly Brief, 21 September 2021
- 78 Weekly Brief, 21 September 2021
- 79 Document subject to legal privilege

4

Key recommendations and findings

The Incident demonstrated that the HSE and other organisations connected to the NHN are vulnerable to common cyber attacks that can cause significant impact to the provision of health services. Transformational change is required across the technology foundation for provision of health services, and its associated cybersecurity, that will need to be executed over the coming years. There is an imperative for the HSE to act with urgency in ensuring the necessary plans, vision, leadership, resource and budget are in place to drive this significant change to build a secure, resilient and future-fit technology foundation for provision of national healthcare services.

Section 4.1 summarises from the detailed findings four strategic areas where transformational change is required, likely over a period of several years. Further details that underpin these can be found in Section 5.

Given the high risk exposure at present, we highlight in Section 4.2 some tactical recommendations for which immediate attention is required to achieve urgent impact and to contribute to the development and implementation of the strategic recommendations.

Section 5 describes in detail a number of recommendations to address learnings that the HSE should take from the Incident, with a supporting key recommendation mapping in Appendix G.

4.1 Strategic recommendations

In order to deliver a significant and sustainable change in the exposure to cybersecurity risk, four areas of strategic focus are required across the HSE and other parties connected to the NHN:

- Governance of IT and cybersecurity;
- Leadership and transformation of the IT foundation on which provision of health services depends;
- Leadership and transformation of cybersecurity capability; and
- Development of clinical and services continuity and crisis management capability to encompass 'service-wide' events such as prolonged total outage of IT.

There are dependencies across these four areas and they need to be progressed in parallel. They are described in the strategic recommendations below, with further supporting recommendations provided in Section 5 of this report.

1. Implement an enhanced governance structure over IT and cybersecurity that will provide appropriate focus, attention and oversight.

1.1 Establish clear responsibilities for IT and cybersecurity across all parties that connect to the NHN, share health data or access shared health services. Establish a 'code of connection' that sets minimum cybersecurity requirements for all parties and develop an assurance mechanism to ensure adherence.

One of the challenges faced by the HSE is that cybersecurity risk materialises as a 'common risk' to all organisations connected to the NHN given the interconnected nature of the IT systems. This has resulted from the direction of digital healthcare demanding greater interconnectivity, ability to share information and access to common services. Under the governance constructs of the health service, organisations have varying levels of autonomy over IT and cybersecurity decision making, yet the risk is shared - with organisations dependent on each other for cybersecurity. There is no 'code of connection' for all parties that connect to the NHN, share health data or use shared services in order to set a minimum baseline of security standards. The HSE's IT Security Policy was written in 2013, with the last update in 2014, and does not reflect the controls and capabilities required to manage cyber risk in 2021.

In order to manage the 'common risks' effectively, clarity is required over responsibilities and decision rights of all parties. In addition, the HSE must be able to set minimum standards for IT and cybersecurity, and ensure compliance to those standards by all organisations connected to the NHN. These minimum standards are required in order to ensure there is confidence in all organisations connected to the NHN that they are not themselves exposed due to inadequate cybersecurity controls in an organisation that they are connected to.

1.2 Establish an executive level cybersecurity oversight committee to drive continuous assessment of cybersecurity risk and a cybersecurity transformation programme across the provision of health services.

The HSE has initiated a number of tactical improvements post the Incident to better secure systems as they have been recovered. However, this will not lead to the level of cyber risk reduction required to significantly and sustainably reduce the risk of further ransomware (or other) attacks.

Within the HSE, there is no dedicated executive oversight committee that provides direction and oversight to cybersecurity, both within the HSE and all organisations connected to the NHN. A known low level of cyber security maturity, including critical issues with cybersecurity capability, has persisted for years with little progress. An Information Security Project Board ceased operating in 2013.

A challenge faced in ensuring cybersecurity of health systems is balancing the need for ease-of-use, especially for clinical staff, with cybersecurity imperatives. For example, implementation of increased levels of cybersecurity controls such as 'Multi Factor Authentication' will have an impact on working procedures. It is therefore important that the cybersecurity oversight committee includes participation from user groups, so that culturally cybersecurity moves from being perceived as an IT challenge, to being perceived as 'how we work'.

Finally, the cybersecurity oversight committee should be accountable for ensuring compliance with the evolving requirements of the EU NISD for essential services across the health service.

1.3 Establish an executive level oversight committee for IT.

With a fragmented set of decision rights over IT development and support across the provision of health services, a necessary enabler for driving transformational change will be the establishment of an executive level committee that can agree the priorities for IT development and investment, and align all interested parties behind a clear vision, strategy and plan.

This committee should be chaired by the Chief Technology & Transformation Officer (see Recommendation 2 below) and drive reporting on all aspects of IT hygiene (such as status of legacy systems) as well as progress in implementation of strategy. Critical to its success will be the participation of IT leaders from across the health service, in particular hospital groups, where a degree

of autonomy over IT decisions remains. It will also be crucial in directing the evolution of an IT infrastructure and service provision that aligns with the objectives of Sláintecare, and establishment of appropriate levels of resourcing.

1.4 Establish a board committee (or repurpose an existing one) to oversee the transformation of IT and cybersecurity to deliver a future-fit, resilient technology base for provision of digitally-enabled health services, and ensure that IT and cybersecurity risks remain within a defined risk appetite. Consider the inclusion of further specialist non-executive members of the committee in order to provide additional expertise and insight to the committee.

Cybersecurity was recorded as a 'High' risk in the Corporate Risk Register in Q1 2019.⁸⁰ At the time of the Incident, the risk rating for cybersecurity on the Corporate Risk Register was 16, based on a likelihood scoring of 4 (likely, with a 75% probability) and an impact scoring of 'Major'.⁸¹ The HSE's risk assessment tool is described in Appendix H.

Risks on the Register are subject to a quarterly review process and the quarterly reports are reviewed by the relevant Board Committee. The Performance and Delivery Committee of the Board reviewed the cyber risk with management in September 2020⁸² and this was followed by a revised mitigation plan. The Committee includes two experienced IT leaders in large organisations, although they are not cybersecurity specialists. This revised mitigation plan had a number of actions due to be completed post the date of the Incident. The actions completed prior to the Incident did not materially impact the risk faced in this area.

The HSE's IT-related risks had been presented at Board level on a number of occasions. However, the gravity of cybersecurity exposure was not fully articulated to the Board, given the HSE's level of vulnerability to a cyber attack, or assessed against a defined risk appetite. Known issues with cybersecurity capability have made limited progress over the course of several years.

Other organisations with a critical cybersecurity exposure, and a need to drive significant technology transformation have found a dedicated committee of the board beneficial in order to raise the priority and focus to an appropriate level and ensure risks are appropriately communicated and understood.

80 Q1, 2019 CRR COMBINED Document for April LT meeting.pdf

81 CRR Q4 2020 Full Report post EMT meeting February 2021 v0.1 09 02 21.pdf

82 Minutes-hse-performance-and-delivery-committee-18-september-2020.pdf

Given the scale of change required across the provision of health services, it is recommended that a focused committee of the board is established, with relevant training provided. Consideration should be given to appointing additional individuals to that committee with specialist skills to act in a non-executive capacity and enhance the ability for the committee to support and oversee the IT and cybersecurity transformation. A key role for the committee will be to ensure that HSE requests for government funding (e.g. to DPER) to invest in addressing IT and cybersecurity issues are clearly articulated, and the risks associated with lack of investment are communicated and understood.

2. Establish a transformational Chief Technology & Transformation Officer (CTTO) and office to create a vision and architecture for a resilient and future-fit technology capability; to lead the delivery of the significant transformation programme that is required, and to build the increased function that will be necessary to execute such a scale of IT change.

The national health service is operating on a frail IT estate with an architecture that has evolved rather than be designed for resilience and security.

The NHN is primarily an unsegmented (or undivided) network, and can be described as a “flat” network, to make it easy for staff to access the IT applications they require. However, this design exposes the HSE to the risk of cyber attacks from other organisations connected to the NHN, as well as exposing other organisations to cyber attacks originating from the HSE - since once an attacker has a presence on the network they have ‘freedom to roam’. This network architecture, coupled with a complex and unmapped set of permissions for systems administrators to access systems across the NHN, enabled the Attacker to access a multitude of systems across many organisations connected to the NHN and create the large-scale impact that they did.

Part of the frailty of the IT estate is an over-reliance on legacy systems. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

The HSE also has over 30,000 outdated Windows 7 legacy systems running on workstations. One reason cited for the continued proliferation of Windows 7 systems is that a key shared service for handling medical imaging,

NIMIS, is not supported by the manufacturer to function on more modern Windows desktops without being upgraded. The upgrade has not been rolled out, despite Windows 7 being deemed ‘end-of-life’ by Microsoft in January 2020, with many organisations upgrading to Windows 10 several years prior to that. Some hospitals have implemented an unofficial workaround to enable NIMIS to operate on Windows 10 machines, with potential implications on the support and warranty arrangements for their use of the application, and work to minimise the dependency on Windows 7 is continuing.

The parts of the health service that were arguably best-equipped to maintain clinical services in the face of prolonged IT outages were those that rely on paper records for patient services. Whilst this was a positive feature in managing the Incident, it highlights the extent to which modernisation is required across the health service to enable the adoption of digital health services. The relative disadvantage in this Incident for organisations who are more dependent on technology services illustrates the critical need for resiliency to be built into the IT architecture and systems to foster the confidence required to enable future migration to more digital provision of health services.

Reducing cybersecurity risk requires both a transformation in cybersecurity capability (see recommendation 3) and IT transformation, to address the issues of a legacy IT estate and build cybersecurity and resilience into the IT architecture.

2.1 Appoint a permanent Chief Technology & Transformation Officer with the mandate and authority to develop and execute a multi-year technology transformation, build an appropriate level of IT resource for an organisation the scale of the HSE and oversee the running of technology services.

The HSE has operated since the end of 2018 with an interim Chief Information Officer with a limited practical mandate, authority and resource to effect change across all organisations connected to the NHN. The level of resourcing in critical IT functions is significantly lower than we would expect for an organisation with the size of IT estate that the HSE has; the IT organisation consists of approximately 350 FTE, serving a population of over 70,000 end-user devices. This observation has been consistently made in interviews, both within the HSE and from external parties who interfaced with them during the Incident, and was a known issue within HSE prior to the Attack with an additional 300 FTE approved for recruitment shortly before the Incident.

The lack of investment in IT resources over a sustained period of time has clearly limited the ability of the HSE to drive modernisation and maintain

the IT estate to be resilient and secure. In addition, the scarce resource in critical IT functions resulted in significant key-person dependencies during the Incident management and recovery, which was undoubtedly a contributing factor to the extended length of the recovery process.

In interviews with hospitals and other providers, it was observed that this incident has highlighted the need to build greater IT resource within many of those organisations, as well as at HSE centre, including representation on leadership committees. The CTTO should develop a resourcing plan for the whole health service that will be sufficient to deliver a transformational strategy, and maintain a resilient and secure IT estate.

The CTTO should assume responsibility for all capabilities that currently sit within the OoCIO, as well as a broadened capability to drive rapid transformation. The CTTO should be a member of the EMT reporting to the CEO.

The ransomware incident has served to highlight the extent to which the provision of health services is dependent on an effective and resilient IT capability. The opportunity needs to be seized to reflect this increased understanding of the criticality of IT with a repositioning of leadership, funding and level of resource.

2.2 Under the office of the CTTO, develop an IT strategy to achieve a secure, resilient and future-fit IT architecture, required for the scale of the HSE organisation.

In order to deliver the transformation required to the technology foundation of the health service in Ireland, a clear strategy is required that can be used to secure commitment to execution across all organisations involved in the provision of health services, and the significant funding that will be required over many years.

The HSE has had a plan for the development of IT that has been used to secure funding for individual projects. However it has not been tied to a vision, strategy and architecture that is deliverable over a period of years and that provides the necessary level of resilience through investment in enabling IT architecture and fallback solutions in the event of core technology failure. Many interviewees expressed frustration with an apparent approach of investing in 'new projects' or 'new features' rather than the holistic delivery and maintenance of a technology foundation for health service provision.

The development of the IT strategy and target architecture also needs to explicitly address the

architecture for deployment of medical devices.

Whilst not in scope for this review, it is apparent that reliance is placed on medical device manufacturers to specify how they should be deployed within the overall IT architecture, with no HSE-mandated approach to ensuring they could not be impacted by a cyber attack.

A key requirement for the IT transformation plan that will be critical to the ability to recover from a similar incident in the future will be clear alignment between critical clinical services and the IT applications and infrastructure they depend on. The recovery activities following the ransomware incident would have benefited greatly from such a view, and speed of decision-making and recovery increased.

3. Appoint a Chief Information Security Officer (CISO) and establish a suitably resourced and skilled cybersecurity function. Develop and drive the implementation of a cybersecurity transformation programme.

The HSE has a very low level of cybersecurity maturity (Section 5.3 of this report gives an evaluation of maturity against the industry standard 'NIST' cybersecurity framework). Examples of the lack of cybersecurity controls in place at the time of the Incident include:

- The IT environment did not have many of the cybersecurity controls that are most effective at detecting and preventing human-operated ransomware attacks;
- There was no security monitoring capability that was able to effectively detect, investigate and respond to security alerts across HSE's IT environment or the wider NHN;
- There was a lack of comprehensive effective patching (updates, bug fixes etc.) across the IT estate of all organisations connected to the NHN; and
- Reliance was placed on a single antivirus product that was not monitored or effectively maintained with updates across the estate. For example, the workstation on which the Attacker gained their initial foothold did not have antivirus signatures updated for over a year.

The low level of cybersecurity maturity, combined with the frailty of the IT estate, enabled the Attacker in this incident to achieve their objectives with relative ease. The Attacker was able to use well-known and simple attack techniques to move around the NHN,

extract data and deploy ransomware software over large parts of the estate, without detection.

3.1 Appoint a CISO and establish a suitably resourced and skilled cybersecurity function.

The HSE has not had a single responsible owner for cybersecurity at either senior executive or management level, responsible for cybersecurity leadership and direction. This is highly unusual for an organisation of the HSE's size and complexity with reliance on technology for delivering critical operations and handling large amounts of sensitive data. As a consequence, there was no senior cybersecurity specialist able to ensure recognition of the risks that the organisation faced due to its cybersecurity posture and the growing threat environment.

The HSE lacked a detailed and holistic cybersecurity strategy, operating model and transformation plan that outlined the strategic, tactical and operational activities required to mitigate known weaknesses and reduce cyber risk exposure.

The CISO should be at National Director level, a direct report to the CTTO, and have appropriate access to the EMT and their agenda, to ensure that cybersecurity risks are understood and considered in all decision-making. They should be responsible for cybersecurity operations as well as driving strategic and tactical actions to transform cybersecurity capability, and providing updates to the Board. Whilst recruitment of a permanent CISO may take some time, appointment of an interim CISO should be considered in the short term.

The HSE also only had circa 15 FTE in cybersecurity roles, and they did not possess the expertise and experience to perform the tasks expected of them. For example, alerts were generated by antivirus software on key systems in the days leading up to the attack, which were passed to the cybersecurity team. However, there was insufficient expertise, and a lack of expertly-designed triaging processes to appreciate the significance of the alerts and take appropriately urgent action to prevent the attack resulting in significant disruption to systems. As a result, opportunities to prevent the crisis were missed.

A critical requirement for the HSE to begin to develop the ability to prevent and detect a similar incident in the future is the appointment of senior cybersecurity leadership and the development of a suitably skilled and resourced cybersecurity function. These skilled resources are currently scarce and the HSE may need to consider co-sourcing arrangements to support requirements in this area.

3.2 Develop and drive the execution of a multi-year cybersecurity transformation programme to deliver an acceptable level of cybersecurity capability for a national health service.

It is apparent that significant capability and controls need to be built and implemented across HSE and other organisations involved in the provision of health services, in order to achieve even a basic level of protection against cyber attacks. This will need to dovetail with the transformation of IT, but also extend beyond IT into 'the way people work' (see recommendation 1.2 above).

There will therefore need to be a multi-year programme to transform cybersecurity capability in a holistic way to ensure that the provision of health services in Ireland, and the data that those health services handle, becomes less vulnerable to cyber attacks. Further detail as to a suggested structure of the programme is given in Section 5.

4. Implement a clinical and services continuity transformation programme reporting to the National Director for Governance and Risk and enhance crisis management capabilities to encompass events such as wide-impact cyber attacks or large-scale loss of IT.

4.1 Implement a clinical and services continuity transformation programme reporting to the National Director for Governance and Risk. Establish an Operational Resilience Policy and Resilience Steering Committee to drive integration between resilience-related disciplines, and an overarching approach to resilience.

The HSE and associated organisations such as hospitals, CHOs, and GPs have dealt with a number of crises over recent years that have required development of clinical and services continuity plans and the 'muscle memory' that comes from repeatedly managing incidents. Indeed one voluntary hospital described the short-term outage of certain local IT systems as a regular occurrence that their Business-As-Usual processes were designed to accommodate.

It is apparent that much of the planning for clinical and services continuity (a more appropriate name for the 'business continuity' discipline in the HSE) has occurred at local level, for specific organisations, and there has not been a programme to ensure consistency of clinical and services continuity planning across all health service organisations and the HSE centre itself, and cross-sharing of leading thinking.

In addition, as is the case with many other organisations, the scenario of sustained loss of IT across the entire health service has not been planned for, with specific considerations and playbooks. As a result, both within organisations and at the HSE centre, great efforts were required 'in the moment' to manage the impacts of the ransomware attack on clinical services, implement workarounds and manage patient risk. The success of these efforts was significantly due to the personal commitment, energy and ingenuity of individuals across all organisations, with no plans or playbooks for such an event that could be relied upon.

A particular challenge faced during the recovery process was the identification and prioritisation of critical systems for recovery. Processes were rapidly developed during the days and weeks following the Incident, to identify the most critical health services for recovery and to map them back to IT systems and infrastructure. However, the understanding and map of the dependencies between specific clinical services and IT systems had not been developed prior to the Incident. Development of this dependency map is a critical requirement for clinical and services continuity planning for future similar events.

During the recovery process in the days following the ransomware attack it became apparent that disaster recovery (DR) arrangements for IT systems were ad hoc and inconsistent. With the Attacker able to corrupt some primary data stores for disaster recovery, there was a requirement to identify secondary stores and attempt to recover from them. A workstream was initiated to attempt to locate them and test the viability of recovery. Were systems to have been recovered using this method, they would have been recovered to different points in time that backups were available for, and there was no confidence in the completeness (or in some cases tested viability) of recovery solutions. As a result, when the decryption key became available from the Attacker, the decision was made to abandon work to recover from backups, and instead recover systems from their production environment, using the decryption capability provided by the Attacker. It cannot be confidently asserted that all health services would have been able to recover in a timely manner (or even at all) without the provision of the decryption key by the Attacker.

The HSE has recognised that clinical and services continuity as a risk discipline has not developed at the pace needed with executive oversight and focus. A National Director for Governance and Risk (equivalent to a Chief Risk Officer) has been appointed, and assigned responsibility for establishing a clinical and services continuity framework, through which risk management and continuity plans will be reviewed, maintained and

validated. Responsibility for clinical and service continuity under the HSE's accountability structure will remain with operational and functional managers. A programme and resource is required to develop the consistency and breadth of planning across the health service, including establishing clear requirements for disaster recovery capability to be implemented by the IT transformation programme, and the mapping of clinical processes to IT systems and data.

In addition, the HSE should establish an Operational Resilience Policy and Steering Committee to drive integration between resilience-related disciplines across the organisation, such as incident management, crisis management, clinical and services continuity and enterprise risk management plus disciplines that can impact on resilience such as cybersecurity and physical security.

4.2 Enhance crisis management capabilities to encompass events such as wide-impact cyber attacks or large-scale loss of IT.

It is indisputable that the HSE has extensive experience in managing crises, for example in the critical role it has fulfilled for the nation in navigating the COVID-19 crisis. This has resulted in some effective mechanisms for crisis management not just being designed, but regularly used. In addition, significant effort has been expended in planning for large-scale external events that the health service will be required to manage such as a plane crash or security incident in a city. Mechanisms that have been developed from previous crises served well in managing this crisis - of particular note was the effectiveness of communications out to the general public and media.

However, the nature of the crisis resulting from the ransomware attack was different, and required elements of capability that have not previously been required. For example: communicating with all staff in the health service without internal emails or other IT collaboration tools; establishing a wide variety of communication channels and forums to gather information and feedback to prioritise recovery of systems, and issuing clear guidance to all parties impacted by the Incident that was relevant to their localised situation. Even establishing a coherent set of facts from which to build communications to the public proved to be challenging, as is typical in a ransomware recovery situation.

The establishment of a crisis management centre and working group, initially in a third party organisation's offices and subsequently in City West, were examples of crisis management structures that had to be developed 'in-the-moment' rather than

being pre-planned. Support from the Defence Forces and other parties enabled an effective structure and set of information flows to be developed rapidly, but this evolved over several days and critical time was lost in the recovery process as a result.

The nature of a ransomware attack, resulting in effectively total loss of IT, makes it particularly challenging to manage with a unique set of issues to be navigated. Investment is required in crisis management planning, resourcing tools and processes in the HSE and associated organisations in order to be prepared to manage this kind of crisis in the future.

4.2 Immediate tactical actions

As highlighted above, there is a requirement for a transformational body of work over several years to make strategic changes to the governance, leadership and capability across IT, cybersecurity, clinical and services continuity and crisis management. Given the high risk exposure at present, we highlight in this section some tactical recommendations for which immediate attention is required to achieve urgent impact and to contribute to the development and implementation of the strategic recommendations. Further information on these, and other recommendations, is given in Section 5.

1. Response to the Incident

1.1 Complete the ongoing work being performed by the Legal and Data workstream and continue to work closely with the Data Protection Commissioner (DPC).

The HSE established a Legal and Data workstream to support the work of their Data Protection Officer (DPO) in coordinating the HSE's data protection investigation, engagement with An Garda Síochána, and subsequent reporting to the DPC.

Through forensic analysis of systems, and review of data sets, this workstream will need, to the extent possible, undertake the following actions:

- Assess the likelihood that the attacker took a copy of data from systems on the NHN;
- Assess the content of data sets at risk for personal data;
- Assess whether any potential breaches meet the threshold to be reported to the DPC;

- Determine the course of action to be taken, such as, informing data subjects and referring identified potential data breaches to other organisations.

The DPO should continue to work closely and maintain regular dialogue with the DPC until the conclusion of the HSE's data protection investigation (see key recommendation FA2.KR20 in section 5.2).

1.2 Continue to reconcile medical data stored and managed through interim processes post the ransomware attack and place centralised governance over these activities.

As the HSE has moved out of the 'crisis phase' of responding to the ransomware attack, it should put in place sustainable governance to manage and resolve the risks and issues originating from the Incident to HSE's data (see FA2. KR22.2 in section 5.2).

During the Incident, workarounds were implemented across the HSE, Hospital Groups/hospitals and CHOs to allow clinical services to continue operating. This often resulted in teams reverting back to paper-based records. There are multiple ongoing efforts to reconcile these paper based records with the data in recovered clinical applications. Until this is complete there is a risk that clinical services are impacted by patients not having up-to-date medical records in the appropriate systems.

Members of staff used personal email accounts and devices for information sharing and communication. The HSE issued a communication in August 2021 to stand down the use of personal emails and ensure all data was deleted from local storage areas. However, some stakeholders from hospitals and CHOs reported they have not received clear guidance on the steps required to address this risk.

The HSE should establish centralised governance over these activities. This should initiate a review of the scope of work required to resolve these risks and issues, provide the necessary resources to prioritise this work and track it through to completion, across all HGs/hospitals and CHOs.

1.3 Collate and manage artefacts created in response to the Incident, including initial production of an asset register.

The HSE should collect, organise and document artefacts created as part of the response and recovery to the ransomware cyber attack.

The HSE was able to gather a significant amount of information during the response to the Incident,

for example key information about the technology underpinning the clinical applications that were being used across the HSE, hospitals and CHOs. In addition, response processes and plans were developed that would be invaluable in the event of a similar attack in future.

These documents will provide a foundation for developing an up-to-date asset and application register, as well as plans that will assist in the response to future incidents (see key recommendation FA1.KR11 in section 5.1 for further detail).

1.4 Appoint an interim senior leader for cybersecurity (a CISO) to be responsible for driving forward tactical cybersecurity improvements, managing third-parties that provide cybersecurity services and leading the cybersecurity response to cyber incidents.

The HSE should appoint an interim senior leader for cybersecurity (a CISO) who has experience in rapidly reducing the vulnerability of organisations to threats, and designing cyber security transformation programmes (see key recommendation FA1.KR1 in section 5.1).

This role should be responsible for placing governance around cybersecurity improvements (see immediate tactical action 1.5), identifying a sustainable medium-term managed detection and response solution (see immediate tactical action 2.1), and leading the cybersecurity response to cyber incidents. The role should also be responsible for developing processes to manage third-parties that provide security services, and providing the expertise to oversee the successful delivery of these.

1.5 Formalise a programme and governance to respond to tactical recommendations arising from the Incident Response investigation and provide assurance over their implementation.

The HSE should mobilise a tactical cybersecurity improvement programme, with governance that feeds into the interim CISO (see immediate tactical action 1.4) and can provide updates on the programme's progress into the Board committee. Dedicated resources should be used to deliver this programme.

The programme should be structured around tactical work packages that can be delivered at pace using focused governance and reporting to drive accountability. The programme should also include a process to triage all third party recommendations, and fixes to security control gaps identified internally, into tactical or strategic activities.

HSE should also bring the governance of ongoing tactical IT and cybersecurity improvement projects, that have been initiated following recommendations from the retained Incident Response provider under the tactical cybersecurity improvement programme (see key recommendation FA1.KR7 and KR8 in section 5.1).

2. Security monitoring

2.1 Ensure that the HSE's Incident Response provider's managed defence service or an equivalent is maintained to detect and respond to incidents on endpoints (i.e. laptops, desktops, servers etc.) to provide protection to the entirety of the NHN.

The HSE has engaged their Incident Response provider to continue providing a managed detection and response service. This capability is the most crucial defence HSE has against further ransomware attacks at present, providing a valuable 'safety net' given the inherent weaknesses in cyber security controls across the estate (see key recommendation FA1.KR6 in section 5.1).

The HSE should identify a sustainable plan to ensure the HSE's Incident Response provider service or an equivalent service is continued across all organisations connected to the NHN. Whether through formalising the continuation of the current service, or replacing in parts of the NHN with a new service, the objective should be to ensure that equivalent levels of service are maintained, including: using Endpoint Detection and Response tooling to detect malicious activity on endpoints; 24/7 monitoring; and triage and investigation of security alerts.

2.2 Establish an initial cybersecurity incident monitoring and response capability to drive immediate improvement to the ability to detect and respond to cybersecurity events.

The HSE should drive immediate improvement to the ability to detect and respond to cybersecurity events, by augmenting the existing security operations function with additional team members with experience and expertise in cybersecurity monitoring and response. This augmented team should document, establish and operate an initial process to triage, investigate, contain and respond to cybersecurity events (see key recommendation FA1.KR11 in section 5.1).

3. Ability to respond to a similar incident in the near future

3.1 Review the process for managing internal crisis communications including resources.

The HSE should formalise and document the process required to manage internal communications during a crisis response similar to that required in the Incident, including cascading call trees and audience segmentation via secure 'out of band' notification and communication platforms (see key recommendation FA2.KR19 in section 5.2).

The HSE should assess the requirements of their internal communications process and plan for a crisis response similar to that required in the Incident and allocate adequate resources to grow the Internal Communications team (see key recommendation FA2.KR6 in section 5.2).

3.2 Develop a plan for response and management of an NHN-wide similar incident taking recent learnings into account.

The HSE should develop, document and exercise a plan for managing and coordinating a cybersecurity incident involving multiple organisations connected to the NHN. This plan should be invoked by any organisations connected to the NHN if they detected a security incident that may have wider implications.

The HSE IT and security teams should identify documents required to respond to a ransomware attack (e.g. network diagrams, asset list) and secure these in a cloud repository (see key recommendation FA1.KR11 f in section 5.1).

3.3 Establish retainers with appropriate SLAs for third party incident and crisis management response support, together with processes and sufficient internal expertise to direct and manage the third-parties.

The HSE should ensure it has a fit-for-purpose set of capabilities under retained contract with external providers to enable a more effective response to an incident similar to the Incident in the near future. This should include support for operation of crisis management functions, legal support and cybersecurity incident response services (see FA2.KR13 in section 5.2).

The HSE should also ensure that they have developed the processes to effectively manage these retained third-parties in the event of an incident, and that they have sufficient expertise to provide challenge and understand the implications of what

the third-parties are reporting to them (see immediate tactical recommendation 1.4).

The HSE should work with the retained cybersecurity incident response provider to ensure they have sufficient understanding of the HSE's organisation and technology, and be available within defined service level agreements to assist the HSE respond to security alerts (see key recommendation FA1.KR11 f in section 5.1).

4. IT environment

4.1 Implement an upgrade to NIMIS to allow Windows 10 upgrade, thereby addressing known vulnerabilities and support issues associated with current wide deployment of Windows 7.

The HSE should prioritise the remediation of critical legacy systems. Immediate efforts should focus on prioritising the upgrade of the NIMIS system, as this is currently inhibiting the upgrade of a significant proportion of 30,000 Windows workstations from Windows 7 to Windows 10.

In considering the acceleration of the NIMIS upgrade, HSE should review if the configuration changes made in one hospital (Hospital A) to enable the application to run on Windows 10 can be more widely implemented, and supported by the vendor, to expedite the central Windows 10 rollout plans (see key recommendation FA1.KR11 g in section 5.1).

4.2 Formalise existing roles and responsibilities for IT across the entities accessing the NHN and establish SLAs for centrally-provided services, while also ensuring information security policies align with those responsibilities.

The HSE should establish clear responsibilities for IT and cybersecurity across all parties that connect to the NHN, or share health data, or access shared health services. This formalisation of responsibilities should include specification of Service Level Agreements (SLAs) for centrally-provided services, including availability requirements.

The HSE should define a code of connection that defines the minimum acceptable level of security controls necessary to connect into the NHN, to be agreed by all parties connected to the NHN, including requirements for central reporting of cybersecurity alerts and incidents. The HSE should establish a programme to monitor and enforce ongoing compliance with this code of conduct. Compliance with the code of connection should become part of the onboarding process of any connecting organisation (see key recommendation FA1.KR11 e in section 5.1).

5

Focus areas - key findings and recommendations



Focus areas - key findings and recommendations

As outlined in section 2.3, our review focused on three connected but distinct areas. The detailed findings and recommendations in this section are categorised by these focus areas, as follows:

Focus area 1	Focus area 2	Focus area 3
Review the technical investigation and response	Review the organisation-wide preparedness and strategic response	Review the preparedness of the HSE to manage cyber risks

5.1 Focus area 1 - review of technical investigation and response

Focus area 1	Focus area 2	Focus area 3
Review the technical investigation and response	Review the organisation-wide preparedness and strategic response	Review the preparedness of the HSE to manage cyber risks
Summary of the Incident		
Key findings and recommendations		
Conclusion		

Summary of the Incident

The HSE's Incident Response provider's investigation⁸³ determined the ransomware attack originated from a malware infection on a workstation ("patient zero") on 18 March 2021. Patient zero was infected with malware after the workstation's user interacted with a malicious Microsoft Office Excel document that was attached to a phishing email received on 16 March 2021.

The user of patient zero was targeted with phishing emails with the same email subject on four other occasions between 14 December 2020 and 9 February 2021, but the workstation was not successfully infected with malware. The HSE's Incident Response provider attributed the phishing emails sent to patient zero to an Attacker⁸⁴ they refer to as UNC2633.⁸⁵ The investigation also identified additional workstations that were infected with malware (as a result of phishing emails sent by the Attacker UNC2633), with the earliest identified infection occurring on 24 November 2020. However, there is no evidence to indicate these infections contributed to the ransomware incident.

After this Attacker gained unauthorised access to the HSE's IT environment on 18 March 2021, a second Attacker continued to operate in the environment until the execution of ransomware on 14 May 2021. The HSE's Incident Response provider identified that the Attacker compromised 180 systems and at least ■■■ highly privileged accounts (typically required for performing administrative tasks ('highly privileged accounts')) across eight organisations and 19 domains. The Incident Response provider also identified over 2,800 servers and 3,500 workstations across 15 domains, with evidence of encryption. This likely represents a lower bound on the number of systems encrypted, as some systems were restored from backups or rebuilt prior to endpoint agent deployment, reducing the Incident Response provider's ability to determine if encryption had occurred.

The HSE's Incident Response provider attributed the second Attacker to be one that they refer to as UNC2727.⁸⁶ When investigating human-operated⁸⁷ ransomware attacks it is common to identify evidence of two Attackers, one that specialises in gaining access to organisations, and another that specialises in deploying ransomware and extortion. For the purpose of clarity, unless otherwise stated when this report refers to 'the Attacker', these references will be to the activity attributed to the second Attacker

⁸³ HSE's Incident Response provider Intrusion Investigation Report, September 2021

⁸⁴ An individual or a group posing a threat.

⁸⁵ This is a threat actor that sends phishing emails containing malicious attachments or links to gain access to organisations' networks

⁸⁶ This is a financially motivated group that the HSE's Incident Response provider has tracked since April 2021. This group is known to deploy Conti ransomware and / or exfiltrates victim data in support of their extortion efforts.

⁸⁷ Human-operated ransomware attacks are different to traditional ransomware attacks in that they are 'hands-on-keyboard' attacks. This involves human attackers using knowledge of offensive techniques and weaknesses in enterprise IT systems, to methodically compromise organisations' networks, compromise systems, overcome defence and cause maximum impact. The ransomware attack that impacted HSE is an example of a human-operated ransomware attack. For further details see: <https://www.pwc.com/jg/en/publications/responding-to-growing-human-operated-ransomware-attacks-threat.pdf>

that the HSE's Incident Response provider refer to as UNC2727.

The cyber attack was identified when the execution of ransomware on 14 May 2021 caused widespread IT disruption. Prior to this, none of the unauthorised access, which began as early as 14 December 2020, was actively identified or contained within the HSE environment. There were several detections of malicious activity, but these did not result in a cyber security incident or investigation being initiated.

It was reported by the HSE's management that 80% of the IT environment across corporate IT services, hospitals, CHOs and EHRs was encrypted,⁸⁸ severely disrupting healthcare services. The HSE's Incident Response provider identified encrypted files on 15 AD domains across the HSE, Hospital C, Hospital K, Hospital D, Hospital L, Hospital J and Hospital B.⁸⁹ The HSE's Incident Response provider's investigation identified information exposure events relating to email, AD data and file data across the HSE, Hospital A, Hospital B, Hospital C and Hospital D.⁹⁰

Our review noted that the impact of the ransomware attack could have been more severe, for example:

- if there had been intent by the Attacker to target specific devices within the HSE environment (e.g. medical devices);
- if the ransomware took actions to destroy data at scale;
- if the ransomware had auto-propagation and persistence capabilities, for example by using an exploit to propagate across domains and trust-boundaries to medical devices (e.g. the EternalBlue exploit used by WannaCry and NotPetya⁹¹);
- if cloud systems had also been encrypted such as the COVID-19 vaccination system.⁹²

Our review also noted that the timeframe for recovery could have been significantly longer had the decryption key not been sourced, as the HSE would have had to rely on recovering applications and systems from backups at scale.

For more detail on the technical timeline, see Appendix E.

Figure 10: Focus area 1 summary of key findings and recommendations

Thematic area	No. of key findings	No. of immediate key recommendations	No. of medium-term key recommendations
Preparation for a ransomware cyber attack	13		
Response to the Incident	14		
Impact & recovery from the Incident	12	11	4
Sustainable reduction of risk since the Incident	10		
Total no. of key findings & recommendations	49	11	4

Note: Recommendations are categorised as immediate (starting immediately and completed within six months) and medium-term (with a phased plan for implementation to be developed and completed within 18 months).

⁸⁸ Percentage confirmed in interview by the CTO within OoCIO Infrastructure and Technology

⁸⁹ HSE's Incident Response provider Intrusion Investigation Report, September 2021

⁹⁰ HSE's Incident Response provider Intrusion Investigation Report, September 2021

⁹¹ <https://us-cert.cisa.gov/ncas/alerts/TA17-181A>

⁹² The COVID-19 vaccination system was designed to be cloud hosted and separate from the HSE IT environment to increase security.

Focus area 1 - key findings

Preparedness to defend against and respond to a ransomware cyber attack

There was a lack of preparedness within the HSE to defend against or respond to a ransomware cyber attack. Key findings that contributed to this position include:

- 1. FA1.KF1 The HSE did not have a single responsible owner for cybersecurity, at senior executive or management level at the time of the Incident.** Limited scenario planning was performed to prepare for a ransomware incident (see focus area 2, area 12: scenario planning below for further detail). Nor were there clear articulations of the HSE's risk to a large-scale ransomware cyber attack that considered known cybersecurity weaknesses. These, alongside the lack of a detailed cybersecurity strategy, operating model or transformation plan can likely be attributed to this cybersecurity leadership absence.
- 2. FA1.KF2 There was no dedicated committee that provided direction and oversight of cybersecurity and the activities required to reduce the HSE's cyber risk exposure.** A cybersecurity forum⁹³ had previously been established within the OoCIO but subsequently disbanded before August 2019⁹⁴ without replacement. There was a process where risks were raised to OoCIO management, but there was no centralised decision making committee to provide direction and decide on a suitable course of action to mitigate these risks, considering the cybersecurity capabilities and controls required.
- 3. FA1.KF3 There were known weaknesses and gaps in key cybersecurity controls.** The Board presentation on cybersecurity⁹⁵ presented on 27 November 2020 highlighted there were many areas of known cybersecurity weaknesses, including known issues with excessive privileges on accounts.
- 4. FA1.KF4 The lack of a cybersecurity forum in the HSE hindered the ability for granular cyber risks to be discussed and documented, and for mitigating controls to be identified and rapidly delivered.** When gaps or issues with cybersecurity controls and capabilities were identified, there was no cybersecurity forum for these to be raised at by OoCIO staff⁹⁶ (see FA1.KF2). As a result, once cyber risks were identified, action was not always taken with sufficient priority. One interviewee reported that petitioning for security tool or process changes was a "war of attrition".
- 5. FA1.KF5 The HSE did not have a centralised cybersecurity function that managed cybersecurity risk and controls.** There was no centralised team to set the vision and tone for security and perform critical security functions, most notably security monitoring and cybersecurity control assurance activities. Further, it should be noted that at the time of the Incident the senior cybersecurity SME, the Information Security Manager, was not performing their business as usual role that included the NIST-based cybersecurity review of OES systems, but was working on evaluating the security controls for the COVID-19 vaccination system. This illustrates the lack of resources available for important cybersecurity activities.
- 6. FA1.KF6 It was a known issue that the teams that included elements of cybersecurity in their remit were under-resourced.**⁹⁷ Further, within the three cybersecurity teams (which had a total FTE of 15⁹⁸), team members predominantly had IT backgrounds, not expertise and experience in cybersecurity. These cybersecurity team sizes do not correlate with the 4,000 locations (1,200 networked), 130,000 staff,⁹⁹ over 70,000 devices and 54 hospitals¹⁰⁰ that make up the health service. The HSE was therefore overly reliant on its already stretched IT resources to perform cybersecurity activities in good faith, as evidenced by interview comments such as "security is not in my job description but I do it part time".

93 HSE OoCIO Security Advisory Group (SAG) Terms of Reference, February 2018

94 CLOSED - HSE Internal Audit Tracking_ICTA015OCIO0916_Internet Access Controls - Follow Up Audit, 28 August 2019

95 Cyber Security Board Awareness Draft V7.2.pdf, November 2020

96 Email with subject RE: FW: CI security solutions discussion document, UNDATED Reported as June 2020

97 Minutes of HSE Board Meeting, 27 November 2020

98 This comprises eight FTE within the Information Security Framework and Control team (two of which are students), the Security Operations team of five FTE and the Security, Standard and Policies team of two FTE. Figures are based on interviewee assertion and/or OoCIO Operating Model – 2020 Current State, December 2019.

99 <https://www.hse.ie/eng/staff/resources/our-workforce/workforce-reporting/health-service-personnel-census-aug-2021-v2.pdf>

100 Cyber Security Board Awareness Draft V7.2.pdf, November 2020

7. **FA1.KF7 The HSE's technology has grown organically and is consequently overly complex, increasing the vulnerability of the HSE to cyber attacks.** The HSE has a complex technological environment that includes a significant number of legacy systems, multiple on-premise email systems and multiple AD domains.

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] This included between 30,000 and 40,000 Windows 7 workstations¹⁰¹ that were deemed end of life by the vendor and operating on extended support. Projects to modernise, standardise and reduce complexity of the IT estate were incomplete at the time of the Incident. This can likely be attributed to: delays reported in interviews as caused by the response to COVID-19; the under-resourcing of technology teams; the lack of a single governed programme that maintained oversight, and the complexities of the IT environment.

8. **FA1.KF8 The HSE had a large and unclear security boundary that encompassed many of the organisations connected to the NHN.** The 'flat' design of the NHN with a lack of network segmentation, paired with bi-direction trust relationships between many AD domains, resulted in many of the organisations connecting to the NHN effectively being within the HSE's security boundary. This exposed the HSE to the risk of cyber attacks from other organisations connected to the NHN, as well as these other organisations connected to the NHN to cyber attacks originating from the HSE.

9. **FA1.KF9 The HSE's effective security boundary did not align with its ability to mandate cybersecurity controls.** The HSE created a network infrastructure where they did not have the ability to mandate cyber controls to prevent and detect ransomware attacks within all organisations that fell within its security boundary (see key finding FA1.KF8).

10. **FA1.KF10 There was no effective security monitoring capability that was able to detect, investigate and respond to security alerts across the HSE's IT environment.** The HSE did not have the modern security tooling needed to detect and prevent ransomware, nor did it have trained security analysts internally or within a Security Operations Center ("SOC") that were able to monitor the available antivirus alerts to investigate, triangulate and respond to potential threats.

11. **FA1.KF11 The antivirus tool ([REDACTED] Endpoint Security) was over-relied upon to detect and prevent threats on endpoints.** Solely relying on antivirus is not sufficient to protect against the tools and attack techniques used by ransomware groups (and many other modern attackers). Further it should be noted that this antivirus tool:

- was not monitored 24/7;
- was not deployed across the full endpoint environment;
- was evidenced as not being correctly configured on all workstations;
- was not configured to block malicious activity within the server estate, only to monitor it.

101 Data provided from the antivirus management server (the [REDACTED] server) of systems that last communicated with [REDACTED] within the last 3 months, September 2021
National health network (NHN) describes the technology network for the delivery of Health services primarily to HSE staff and secondarily to the staff in the voluntary sector

12. FA1.KF12 The IT environment had high-risk gaps relating to 25 out of 28 of the cybersecurity controls¹⁰² that are most effective at detecting and preventing human-operated ransomware attacks.¹⁰³ A high-level assessment of the HSE's cybersecurity capabilities, using PwC's proprietary ransomware readiness framework,¹⁰⁴ at the time of the Incident is shown in Figure 11. Further, of the cybersecurity controls implemented, limited assurance activities were performed to test their operational efficiency. This assessment has been performed to provide an illustration of the level of cybersecurity controls in place at the time of the incident specifically in relation to ransomware attacks.

A Board presentation¹⁰⁵ on cybersecurity presented on 27 November 2020 highlighted how several of these controls were areas of known cybersecurity weakness, although the link to a risk of widespread impact from a ransomware attack was not made. Implementing many of these controls would have been highly likely to have prevented or detected techniques used by the Attacker and therefore significantly increased the Attacker's difficulty in compromising the HSE and achieving their objectives.

13. FA1.KF13 The HSE did not have a documented cyber incident response plan and had not performed typical preparatory activities such as exercising the technical response.

The HSE did not have an exercised plan for managing and coordinating a cybersecurity incident that impacted the HSE as well as multiple organisations across the NHN. There were no documented cyber incident response runbooks or IT recovery plans (apart from documented AD recovery plans) for recovering from a wide-scale ransomware event.

¹⁰² Based on PwC's proprietary ransomware capability framework (see section Preparation: cybersecurity controls before the ransomware attack for further detail), HSE is scored high or very high risk against 25 of the 28 capabilities

¹⁰³ Human-operated ransomware attacks are different to traditional ransomware attacks in that they are 'hands-on-keyboard' attacks. This involves human attackers using knowledge of offensive techniques and weaknesses in enterprise IT systems, to methodically compromise organisations' networks, compromise systems, overcome defence and cause maximum impact. The ransomware attack that impacted HSE is an example of a human-operated ransomware attack. For further details see: <https://www.pwc.com/jg/en/publications/responding-to-growing-human-operated-ransomware-attacks-threat.pdf>

¹⁰⁴ PwC's proprietary ransomware readiness framework lists the most important cybersecurity controls we have identified to prevent, detect and respond to human-operated ransomware attacks. Focus area 1 used this framework as it allowed the review to evaluate HSE's cyber security controls at the time of the Incident against the specific threat of human-operated ransomware attacks. Focus area 3 have performed a wider review of HSE's cybersecurity preparedness and maturity levels using the NIST cybersecurity and COBIT framework

¹⁰⁵ Cyber Security Board Awareness Draft V7.2.pdf, November 2020

Figure 11: High-level assessment of the HSE's cybersecurity capabilities against PwC's proprietary ransomware readiness framework, colour coded by their risk rating, as at the time of the Incident.



Response to the ransomware cyber attack

There were opportunities to detect malicious activity prior to the detonation phase of the ransomware. Following the execution of ransomware, the HSE mobilised a response to overcome the significant challenges posed by both the attack and its lack of preparedness.

Key findings relating to the response to Attacker activity in the days leading up to the Incident include:

- 1. FA1.KF14 The cyber attack was not actively identified or contained prior to the ransomware execution, despite the Attacker performing noisy and 'unstealthy' actions.** The investigation determined that the ransomware attack originated from a malware infection on patient zero on 18 March 2021, when the user opened a malicious Microsoft Office Excel document that was attached to a phishing email. Following this, the Attacker continued to operate in the environment, including compromising and abusing a significant number of highly privileged (e.g., system administrator) accounts and moving laterally to both statutory and voluntary hospitals. Many of the tools and techniques employed by the Attacker during this time period (which included the use of basic and non-obfuscated malicious PowerShell commands), were well-known to be used by ransomware groups. As such, they would have almost certainly been identified by modern security monitoring tooling and a security monitoring capability. It should be noted that the HSE's antivirus tool (██████████ Endpoint Security) did record detections of these tools¹⁰⁶ but these were not actively identified or thoroughly investigated by the HSE's teams (see next finding).

- 2. FA1.KF15 The HSE's antivirus identified a tool commonly used by ransomware groups (Cobalt Strike) on six servers on 7 May 2021 (and several more servers in the following days) but these alerts were not appropriately actioned.** The HSE did not identify these alerts until after their cybersecurity solutions provider flagged them on 12 May 2021¹⁰⁷ and 13 May 2021.¹⁰⁸ At that point, the retained third party 'critical incident response service', was not invoked,¹⁰⁹ despite the alerts being for a tool commonly used by ransomware groups (Cobalt Strike) and being across multiple servers. The response to these detections was not sufficient as the HSE did not; invoke a cybersecurity incident; escalate the cybersecurity incident; identify the severity of the threat; or thoroughly investigate and contain the threat. This was a result of insufficient cybersecurity expertise to understand the significance of these detections and an absence of cyber response governance and processes to guide the response to cybersecurity incidents.
- 3. FA1.KF16 Two voluntary hospitals identified suspicious activity prior to the execution of ransomware, but a HSE centralised response was not initiated.** On 10 May 2021, Hospital C identified activity on a domain controller ("DC") that they suspected as malicious and so sought advice from Hospital C's cybersecurity solutions provider on whether the alerts warranted concern.¹¹⁰ The third-party stated that since the threat has been handled by their antivirus tool that "the risk is low here". As a result of the third party's email response, Hospital C did not initiate a cyber incident response investigation, and therefore did not identify a cybersecurity incident. On the evening of 12 May 2021, Hospital A notified the OoCIO that its network had been compromised¹¹¹ and suspected malicious activity was originating from the HSE.^{112,113} The HSE performed an IT-centric investigation on 13 May 2021 that incorrectly concluded that the HSE was "under threat from Hospital A, not the other way around".¹¹⁴ Following this, the HSE did not seek the help of an external cyber incident response firm nor the NCSC to investigate and provide guidance on how to respond to the detections.

106 HSE's Incident Response provider Intrusion Investigation Report, September 2021

107 Email from the HSE's cybersecurity solutions provider to the SecOps team with subject "Threat Not Handled", 12 May 2021

108 Email from the HSE's cybersecurity solutions provider to the SecOps team with subject "Threat Not Handled", 13 May 2021

109 Appendix 7: Services Contract, Health Service Executive and the HSE's cybersecurity solutions provider Information Systems Limited Agreement Relating to the Provision of Services pursuant to Request for Tenders for the Establishment of a Multi Supplier Framework for the provision of Security Software and Associated Reseller Services, 24 December 2017

110 Logging call with Hospital C's cybersecurity solutions provider on 10/05/2021 17:06, 10 May 2021

111 Email with subject: Query, 12 May 2021 23:53

112 Email with subject: FW: Recognise these addresses??, 12 May 2021 23:36

113 Email with subject: FW: Query, 12 May 2021 23:53

114 Email with subject: RE: Summary 13 May 2021 12:47

The HSE did not link these events to the antivirus tool detections that their cybersecurity solutions provider had notified.

4. **FA1.KF17 Two organisations successfully acted on detections of the Attacker preventing the deployment of ransomware within their estates.** The DoH and Hospital A successfully acted on alerts and detections of suspicious activity, and engaged third-party incident response services. The DoH quickly deployed EDR security tooling¹¹⁵ that was then able to prevent the ransomware from executing on the majority of its infrastructure, including critical and data servers. Hospital A engaged the Hospital A's Incident Response provider, who worked with them to use their already deployed security tool. Had the HSE responded in a similar fashion (particularly following the escalations made by Hospital A and the HSE's cybersecurity solutions provider) then it is likely that the widespread encryption of the HSE environment would have been prevented.

Key findings relating to the response to the detonation phase of the ransomware attack include:

1. **FA1.KF18 The HSE with the help of third-parties mobilised a response to the ransomware attack and overcame many of the significant challenges the ransomware attack presented, drawing on their experience responding to crises, including COVID-19.** The HSE recognised the need for additional resources and specialist skills and engaged third parties for incident response^{116,117} legal and forensics support early on. The impact of the Incident on a national scale encouraged goodwill from third party support and vendors, including the provision of pro bono work. This allowed a good cadence to be established within 24-48 hours that included multiple daily standups, Major Incident (MI) meetings and other programme governance. The HSE developed effective response structures and processes that evolved over the course of the response. The decision to set up a physical hub for operations in Citywest (on 21 May 2021¹¹⁸) was widely reported as being invaluable to working collaboratively between different response and recovery teams, whilst also boosting morale.

2. **FA1.KF19 The HSE was reliant on third-parties in the early weeks of the Incident to provide structure to the response activities.** The first physical hub for senior management was set up 15 May 2021¹¹⁹ in a third party organisation, before moving to accommodation at Citywest on 21 May 2021.¹²⁰ The Defence Forces were brought in 18 May 2021 and were widely reported in interviews to have provided key response structures.

3. **FA1.KF20 Time was lost during the response due to a lack of pre-planning for high impact technology events.** The HSE was not prepared to respond to a cyber incident of this scale ("everything going offline") due to the lack of defined and exercised response processes and plans. Key examples of this include:

- No cybersecurity response plans and playbooks;
- No security tooling capable of investigating and remediating security alerts;
- No centralised list of contact details for all HSE staff or asset register;
- No offline copies of key IT and security documentation were kept, for example network diagrams;
- No pre-established prioritised list of applications and systems for recovery, based on clinical services, that was cognisant of cross-technology dependencies;
- No pre-agreed, setup and tested out-of-band communication system that would enable users to communicate in the event of a cybersecurity incident. Multiple collaboration and communication platforms were used after the Incident resulting in confusion and team members not being able to easily communicate; increasing the day-to-day difficulty of responders.

115 Endpoint Detection and Response (EDR)

116 HSE's Incident Response provider Intrusion Investigation Report, September 2021

117 Minutes of Cyber Attack MI Meeting 10 am - 14052021, 14 May 2021

118 Conti Cyber Response NCMT Structures Governance and Admin V1.10, 31 May 2021

119 Programme RAID Log, 2021

120 Programme RAID Log, 2021

4. **FA1.KF21 The HSE spent a significant amount of time during the response gathering information about applications, as this information was not recorded and up-to-date in a central or offline application register.** The lack of centralised information about applications caused inefficiencies in the response as the HSE did not have up-to-date information on applications. This meant that as part of their response, they had to develop a list of applications that were in use within the corporate, acute and community spaces. As well as identify and define missing details such as the application's owner, its priority for recovery, details of the systems they were hosted on and in some cases the application's purpose. For some applications, the HSE was reliant on vendors to pull this information together, and provide the information critical to the application's recovery.
5. **FA1.KF22 There was a heavy reliance on specific individuals during the response. This likely contributed to a recovery timeline that was longer than could have been achieved.** There was a heavy reliance on key members of staff in IT teams that effectively caused bottlenecks. This was due to the large scope of their BAU IT roles and responsibilities, the lack of IT resourcing and a lack of documented and standardised information and procedures. This concentration of knowledge prevented opportunities for further delegation (such as acquiring more burst capacity from third parties) and meant that the HSE had limited response resilience if these individuals had become unavailable during the critical weeks of the response.
6. **FA1.KF23 The response initially prioritised the recovery of foundational systems, and applications on the OES list¹²¹, before advancing to an approach that focused on clinical risks and the recovery of end-to-end clinical services.** Before the incident there was not a complete and documented list that prioritised all HSE applications and systems. As a result IT teams initially focused on restoring the seven priority clinical applications that were identified in the OES list.¹²² The recovery strategy advanced from the restoration of these seven applications, to be centered around recovery of end-to-end clinical service (including the dependencies of applications to restore end-to-end clinical services) following the co-location of all responders to Citywest on 21 May 2021.¹²³
7. **FA1.KF24 There was a lack of clearly defined and delineated decision making authority between the HSE, hospitals and CHOs in the case of a health service-wide crisis.** After the ransomware attack was identified, the OoCIO gave a central mandate to power down systems and wait for instructions (whilst they assessed the impact and established next steps) as there was not a delineated decision making structure to allow for local nuances. At least one hospital (Hospital B) used a third party to review their environment and confirm that it was unaffected by the ransomware. Invoking local decision making during this initial interim period allowed the hospital to regain IT systems and provide critical radiotherapy services within the first week of the Incident.
8. **FA1.KF25 The OoCIO was not able to provide or source (through third party burst capacity) the scale of the IT support required by hospitals and CHOs during the extended response to restore applications, systems and services at pace.** The centralised IT team structure of the HSE meant that little IT subject matter expertise was available locally within the HSE's hospitals and CHOs. It was widely reported by hospitals and CHOs¹²⁴ that they were heavily reliant on the central OoCIO IT resources for response activities and on personal relationships with OoCIO IT teams to progress and unblock tasks. The OoCIO IT resources were however, already stretched performing national ransomware attack response activities and therefore struggled to effectively prioritise this help.
9. **FA1.KF26 The HSE had limited to no ability to investigate the attack using its own tooling.** The HSE was not centrally collecting and retaining logging from systems, network and security tooling. The central collation point for their antivirus alerts (the antivirus management server) was encrypted and deemed unrecoverable as a result of the ransomware attack. The encryption of the antivirus server meant that the HSE was unable to determine the circumstances and audit trail surrounding what detections were reported back to the central console in the lead up to the ransomware execution. Therefore, without the deployment of their Incident Response provider's

121 The Network and Information Systems Directive (NIS-D) 2016/1148 was signed into Irish law on 18 September 2018. It involves the application of security obligations on operators of essential services (OES). HSE interviewees referred to an 'OES application and system list' they compiled in line with NIS-D obligations.

122 DOE Application Catalogue and Critical Services as defined under NIS Directive Final

123 Conti Cyber Response NCMT Structures Governance and Admin V1.10, 31 May 2021

124 Observations made are based on interviews with a sample of nine hospitals (5 statutory and 4 voluntary) and 2 CHOs

endpoint agent the HSE would have had no ability to perform forensic analysis over their systems and therefore fully investigate the attack.

- 10. FA1.KF27 The HSE's Incident Response provider identified evidence of how the Attacker was able to gain unauthorised access to the HSE's IT environment and the Attacker's subsequent activities.** The HSE worked closely with their Incident Response provider to ensure they had the available information required to enable an effective investigation and response. This resulted in an investigation that identified evidence of how the Attacker was able to gain unauthorised access to the HSE's IT environment and what the Attacker did once they were able to gain this access.

Key findings from the investigation¹²⁵ included that the Attacker:

- gained unauthorised access to the HSE network through a phishing email on 18 March 2021 (this activity was attributed to the Attacker the HSE's Incident Response provider refer to as UNC2633);
- used a number of tools commonly utilised by human-operated ransomware groups to perform reconnaissance and move laterally through the HSE's environment (compromising 180 systems);
- used the network connectivity provided by the NHN as well as the bidirectional trust between several AD domains to easily move laterally across to six voluntary hospitals and one statutory hospital;
- used an exploit that was widely publicised as a critical patch¹²⁶ to gain access to the networks of two hospitals;
- compromised at least [REDACTED] highly privileged accounts¹²⁷ across HSE, Hospital A, Hospital K, Hospital L, Hospital J and Hospital B;¹²⁸
- browsed local or remote folders on systems across HSE and four organisations;

- opened files and attempted to view them using RDP;¹²⁹
- made copies of files;
- created archives (.zip and .rar) of files;
- accessed the file sharing website Domain A; and,
- deployed ransomware throughout several organisations connected to the NHN.

Additionally, the [REDACTED] malware (which includes an Outlook module to harvest contact information and email content from infected hosts) was identified on several hosts within the HSE's environment. An output from the execution of this module was identified on one system within the HSE's [REDACTED] domain.

The investigation was unable to identify conclusive evidence that data exposed to the Attacker was then successfully exfiltrated by the Attacker out of the HSE's environment (for example to a file sharing website). However, it is known that the Attacker provided samples of the HSE's and Hospital D's (a Section 38 hospital and therefore independent data controller¹³⁰) data in a chat room (accessed via a link in the ransom note) and that some data was published on the dark web.¹³¹ It is also known that the Financial Times published redacted extracts of the published data (which was verified as originating from the attack on 14 May 2021)¹³² and then worked to provide a copy of this data to the HSE's Incident Response provider on 25 May 2021.¹³³

Hospital D conducted its own review of the data provided by the Financial Times and made a decision to notify identified data subjects as per Article 34 GDPR.¹³⁴ The HSE reviewed the data provided by the Financial Times and confirmed that the HSE data related to a Statutory Hospital ("Hospital M"), for which the HSE is the data controller. The HSE assessed the personal data risk to the rights and freedoms of individuals within this data set to be low¹³⁵ and therefore it was deemed not necessary to inform the relevant data subjects.

¹²⁵ HSE's Incident Response provider Intrusion Investigation Report, September 2021

¹²⁶ The threat actor used the [REDACTED] exploit to gain access to the networks of Hospital A and Hospital B. The [REDACTED] exploit was widely publicised and given a Common Vulnerability Scoring System (CVSS which is a framework for communicating the characteristics and severity of software vulnerabilities) score of 10/10.

¹²⁷ The compromised accounts consist of two 'enterprise admins', 26 'domain admins', two 'administrator', one 'admin' and two 'service desk admin'.

¹²⁸ HSE's Incident Response provider Intrusion Investigation Report, September 2021

¹²⁹ Remote Desktop Protocol (RDP) provides a user a graphical interface to connect to a remote computer over a network connection.

¹³⁰ Response to questions raised by the Data Protection Commission to HSE DPO on June 2021, July 2021

¹³¹ Privileged and Confidential Terms of Reference Legal and Data Steering Group V004, June 2021

¹³² Privileged and Confidential Terms of Reference Legal and Data Steering Group V004, June 2021

¹³³ Draft OoCIO Cyber Governance Report v0.2, UNDATED

¹³⁴ Response to questions raised by the Data Protection Commission to HSE DPO on June 2021, July 2021

¹³⁵ Response to questions raised by the Data Protection Commission to HSE DPO on June 2021, July 2021

The HSE retained a third party to conduct additional in-depth forensic analysis on the systems identified by their Incident Response provider (where data was exposed to the threat actor), to determine the probability of data exfiltration from these systems and to identify any other potential data exposure and exfiltration sources. The HSE has also retained two third party services to perform ongoing dark web and web monitoring activities.

At the time of this report, the work aligned to the HSE's Legal and Data workstream established on 19 May 2021¹³⁶ is ongoing. As of yet, therefore the HSE has not made any data subject notifications but continues to work closely with the DPC.

The impact of and recovery from the ransomware cyber attack

Due to the scale and impact of the ransomware, paired with the complex and legacy IT environment, the technical recovery of IT systems has been challenging. Key findings on the technical impact of the Incident include:

1. **FA1.KF28 The impact of the ransomware on the IT environment was reported by the HSE's management to lead to 80%¹³⁷ encryption.** The HSE's Incident Response provider's investigation identified encrypted files on systems within the HSE and the following voluntary and statutory hospitals: Hospital C; Hospital K; Hospital D; Hospital L; Hospital J and Hospital B.¹³⁸ The HSE was the most impacted by the ransomware attack, with all nine of its domains displaying evidence of encryption.¹³⁹ In total, the HSE's Incident Response provider identified over 2,800 servers and 3,500 workstations across 15 domains, with evidence of encryption.¹⁴⁰ This likely represents a lower bound on the number of systems encrypted, as some systems were restored from backups or rebuilt prior to endpoint agent deployment, reducing the HSE's Incident Response provider's ability to determine if encryption had occurred.
 2. **FA1.KF29 The impact of the ransomware attack on communications was severe, as the HSE almost exclusively used on-premise email systems (Exchange and ██████████) that were encrypted, and therefore unavailable, during the attack.** The HSE had begun to migrate users to Exchange Online ██████████ but this was limited to pilot projects at the time of the Incident and had been identified by the HSE as a complex project to deliver. Had the HSE invested in reducing email complexity and completed migrating staff to Exchange Online, the impact of the ransomware on email would have likely been minimal, reducing the impact to team collaboration. See key finding FA1.KF38 for the detail regarding email recovery.
- Key findings on the recovery include:
3. **FA1.KF30 The HSE took action to contain the ransomware attack by powering down systems and disconnecting the NHN from the internet.** These containment steps restricted the ability of the Attacker to further their activities and in the face of spreading ransomware within an architecturally open environment were the most pragmatic. The HSE did not have the realistic option of carrying out a more compartmentalised approach that accounted for the impact on organisations, due to the open design of the NHN, the immaturity of cybersecurity controls and governance, and as this had not been planned for or rehearsed.
 4. **FA1.KF31 It is unclear how much data would have been lost if a decryption key had not become available.** It was reported that online backups were encrypted in places and that secondary backups to tape were only made periodically. Therefore it is highly likely that segments of data would have been unrecoverable from backups, and a full recovery of data was only possible due to the provision of a decryption key by the Attacker.
 5. **FA1.KF32 Without the decryption key, it is unknown how long it would have taken to recover systems from backups but it would have likely taken considerably longer.** Prior to receiving the decryption key, the HSE was recovering systems from backups. This would have required a significant amount of IT resources and equipment to be undertaken at the scale required to recover all servers and applications.

136 Privileged and Confidential Terms of Reference Legal and Data Steering Group V004, June 2021

137 Percentage confirmed in interview by the CTO within OoCIO Infrastructure and Technology

138 HSE's Incident Response provider Intrusion Investigation Report, September 2021

139 HSE's Incident Response provider Intrusion Investigation Report, September 2021

140 HSE's Incident Response provider Intrusion Investigation Report, September 2021

6. **FA1.KF33 The HSE missed opportunities for efficiencies in the recovery of systems and applications due to a lack of preparedness.**
The lack of preparedness for a widespread disruptive IT event often created bottlenecks and prevented teams from being able to get to work on the highest priority tasks. In particular, the lack of a comprehensive, current asset register mapped to critical services delayed recovery efforts due to the wait between teams as this information was gathered and through unknown dependencies creating inefficiencies.
7. **FA1.KF34 The processes and response structures for recovering systems and applications were designed and developed in response to the Incident.** Many of the processes used to recover systems and applications were developed during the crisis. This resulted in a lack of immediate awareness, understanding and implementation of agreed processes from staff members potentially increasing the HSE's cyber risk at the time of the response. For example, there was at least one instance of a potentially compromised system being reconnected to the network (before it was confirmed as clean and pre-authorised by the HSE's Incident Response provider and the Tech Team¹⁴¹), inadvertently exposing the HSE to a heightened level of risk.
8. **FA1.KF35 The HSE's Incident Response provider and the HSE, developed go-to-green processes^{142,143,144} to ensure the secure recovery of systems and reduce the risk of further ransomware attacks.** The HSE's Incident Response provider and the HSE developed requirements that every system within the HSE, voluntaries and CHOs must meet before being able to rejoin the network, and for organisations to be reconnected back to the NHN and the internet.
 - After one month, the HSE was able to decrypt 47% of servers and fully restore 48% of Acute applications, 40% of Community Services applications and 64% of business services applications.¹⁴⁶
 - After two months, the HSE was able to decrypt 94% of servers and fully restore 85% of Acute applications, 94% of Community Services applications and 79% of business services applications.¹⁴⁷
 - After three months, the HSE reported that 100% of servers were decrypted and they were able to fully restore 95% of Acute applications, 98% of Community Services applications and 91% of business services applications.¹⁴⁸
9. **FA1.KF36 The complexities of recovering applications and systems were not well understood.** Due to the unknown dependencies between systems and a lack of recovery process pre-planning, recovery efforts were complicated. For example, recovery teams reported that it was difficult to facilitate vendor support. As a result, workarounds (such as using screen shares to provide vendors with temporary access) had to be employed. These workarounds were also in some cases further complicated through the inconsistency in access to collaboration tools (see response to the detonation phase of the ransomware attack key findings FA1.KF18 - FA1.KF27).
10. **FA1.KF37 Despite the challenges presented by the ransomware attack and the lack of preparedness, the HSE was able to recover 1,075 applications and over 87,000 systems.¹⁴⁵** Our review consistently noted the willingness of HSE staff members across the organisation to come together and contribute wherever needed to deliver services to patients. The HSE recovered their primary identity systems ([REDACTED] AD domain) within a matter of days after the ransomware attack. The HSE was able to prioritise and restore applications and systems during the response including:
 - After one month, the HSE was able to decrypt 47% of servers and fully restore 48% of Acute applications, 40% of Community Services applications and 64% of business services applications.¹⁴⁶
 - After two months, the HSE was able to decrypt 94% of servers and fully restore 85% of Acute applications, 94% of Community Services applications and 79% of business services applications.¹⁴⁷
 - After three months, the HSE reported that 100% of servers were decrypted and they were able to fully restore 95% of Acute applications, 98% of Community Services applications and 91% of business services applications.¹⁴⁸

141 Minutes of Cyber Attack MI Meeting 11 am - 19052021, 19 May 2021

142 Voluntaries and Go-to-Green, 26 May 2021

143 CTO Document Device Go Green Draft Approach, 23 May 2021

144 CTO Document Remote Access Go Green Draft Approach, 24 May 2021

145 Weekly Brief, 21 September 2021

146 SITCEN SITUATION REPORT, 18:30 14 June 2021

147 Weekly Brief, 20 July 2021

148 Weekly Brief, 21 September 2021

11. FA1.KF38 HSE had significant issues with restoring email back to normal operations for users, resulting in ongoing disruption to employees. Due to the complexity of the email infrastructure, even when the service was itself restored, user level disruptions such as empty mail boxes continued to affect staff's ability to perform recovery and BAU activities. Ongoing disruption with email services impacted the staff's ability to recover applications and systems. Since the ransomware attack, there has been over 38,000 tickets raised with the national service desk relating to ongoing issues with email.¹⁴⁹ Over 20,000 of those tickets were raised between 20 July 2021¹⁵⁰ and 21 September 2021.¹⁵¹

12. FA1.KF39 The strategy to prioritise national systems recovery over local systems meant that statutory hospitals and CHOs that were not yet using 'standard' infrastructure (some with limited local IT resources) experienced recovery delays. Organisations not yet using 'standard' infrastructure (for example, organisations not using national applications) were effectively deprioritised by the strategy to prioritise national systems. This was then further compounded for hospitals and CHOs with little to no IT resource and who were therefore wholly reliant on the OoCIO for their recovery.

Sustainable reduction of risk since the ransomware attack

The focus of the HSE's activities since the attack has been on implementing recommendations provided by third parties and to continue to recover systems. Limited evidence has been provided to show that activity has yet to take place to ensure that the HSE's cyber risk exposure is reduced sustainably.

Key findings on the improvements made by the HSE post cyber incident, and on HSE's current approach and current ability to sustainably reduce cyber risk, include:

1. FA1.KF40 The HSE engaged their Incident Response provider to continue providing a managed detection and response service to March 2022. This capability is the most crucial defence the HSE has against further ransomware attacks at present, and provides a valuable 'safety net' given the inherent weaknesses in cyber security controls across the estate. The HSE has not yet identified a long-term replacement for the managed detection and response service, with the current solution ending in March 2022.¹⁵²

2. FA1.KF41 The HSE increased the scope of services provided by the current third parties to provide 24x7 monitoring capability of its antivirus tool¹⁵³ and cloud environment.¹⁵⁴

The HSE's cybersecurity solutions provider and Third Party B provide a 24x7 security monitoring service limited to the antivirus tool ([REDACTED] Endpoint Security) and Microsoft Cloud platforms¹⁵⁵ (which includes the HSE [REDACTED] tenancy¹⁵⁶) respectively.

3. FA1.KF42 Improvements to the HSE's in-house Security Operations capability (for example defining processes and documenting response roles) have not yet been implemented. These improvements along with other immediate improvements identified are critically important to ensure that alerts of malicious activity will be investigated and escalated with due care. As of yet there is little evidence to show that any 'quick fixes' to the HSE's security monitoring capability have been implemented beyond the retaining of third party monitoring services.

149 21 September 2021 Weekly Brief, 2021

150 20 July 2021 Weekly Brief, 2021

151 21 September 2021 Weekly Brief, 2021

152 <https://ir1.eu-supply.com/ctm/Supplier/PublicTenders/ViewNotice/248668>

153 Service Contract Agreement – Addendum 1 Managed Security Monitoring & Incident Response Service 24-Hours / 365 Days, Prepared 21 June 2021 (Unsigned)

154 Response to questions raised by the Data Protection Commission to HSE DPO on June 2021, July 2021

155 Response to questions raised by the Data Protection Commission to HSE DPO on June 2021, July 2021

156 Confirmed by the General Manager Head of Technology, Infrastructure & Deployment within OoCIO Infrastructure and Technology by email, 8 October 2021

4. **FA1.KF43 The HSE was not empowered to mandate that voluntary hospitals continue with the improved levels of security monitoring (or other security controls); this could expose the health service to the risk of further cyber attacks.** The HSE does not have the authority to mandate voluntary hospitals continue to use the HSE's Incident Response provider's Managed Defence monitoring agent or replace this with a like-for-like replacement (which will require ongoing cybersecurity expenditure). If voluntary hospitals do not maintain the current capability or procure a similar, market leading solution, then this will expose the HSE and wider health service to risk of further cyber attacks. This illustrates how the HSE's security boundary continues to be misaligned with their ability to mandate cybersecurity controls.
5. **FA1.KF44 A finalised security improvement plan^{157,158,159,160} does not exist and the draft security improvement plan and programme^{161,162,163,164} is unlikely to significantly reduce the risk of future ransomware attacks.** The current draft plan and programme is a consolidation of IT projects and identified gaps. It also highlights the need to create a final security improvement plan with defined governance and accountability across the organisation. Therefore at present no improvement plan exists that is structured or architected using a cyber threat view that centres on improvements around key cybersecurity capability areas that are most effective at detecting and preventing human-operated ransomware attacks. It does identify some gaps in these capability areas as items to be addressed in long-term planning¹⁶⁵ but it should be noted that improvement in these gaps are crucial to reducing the risk of ransomware attacks in the short term.
6. **FA1.KF45 A holistic view of cybersecurity improvement activities does not yet exist which increases the risk that foundational improvement activities will be missed.** There is a risk that the HSE's current approach to focus action around the remediation activities outlined by their Incident Response provider, will likely lead to a piecemeal approach that does not take account of the fundamental root causes of such issues. For example, at present it is well known that there are issues with the coordination and tracking of the response to security alerts between technology teams, but the resolution of this is not yet included within any finalised plans.
7. **FA1.KF46 There is no centralised governance programme that maintains oversight of identified cybersecurity improvements, resulting in a lack of clarity about what has been delivered and what remains to be done.** Improvement actions are currently being discussed at technological operational meetings and a programme management governance structure to oversee these activities and produce centralised progress figures against agreed milestones is yet to be developed. This has resulted in a lack of clarity around what security improvements have been delivered, and what security improvements still need to be delivered in response to the Incident.
8. **FA1.KF47 A cybersecurity transformation programme, that will sustainably reduce cybersecurity risk in the long term, has not been planned, approved or resourced.** Some initial security improvement documents^{166,167,168,169}, as outlined in key finding FA1.KF44, exist but these do not articulate the scale of necessary change or detail the plan for such a transformation. Both a cyber transformation plan and a framework to help achieve that plan are required that will redesign how the HSE manages and maintains its cyber risk within its extensive technological estate (see medium-term recommendation FA1.KR13 for further detail).

157 HSE IT Security Planning, UNDATED Last Modification recorded 15 September 2021

158 Cyber Security Risk Management, UNDATED Last Modification recorded 15 September 2021

159 CTO Document Security Improvement Programme Draft, 31 August 2021

160 OoCIO-07 Investment Plan 2020 -Cyber Security Draft, 1 June 2019

161 HSE IT Security Planning, UNDATED Last Modification recorded 15 September 2021

162 Cyber Security Risk Management, UNDATED Last Modification recorded 15 September 2021

163 CTO Document Security Improvement Programme Draft, 31 August 2021

164 OoCIO-07 Investment Plan 2020 -Cyber Security Draft, 1 June 2019

165 CTO Document Security Monitoring V1 HSE, 04 June 2021

166 HSE IT Security Planning, UNDATED Last Modification recorded 15 September 2021

167 Cyber Security Risk Management, UNDATED Last Modification recorded 15 September 2021

168 CTO Document Security Improvement Programme Draft, 31 August 2021

169 OoCIO-07 Investment Plan 2020 -Cyber Security Draft, 1 June 2019

9. **FA1.KF48 The HSE still has a significant amount of legacy IT that needs to be modernised.** [REDACTED]

10. **FA1.KF49 Key artefacts created within the response are not yet being centrally and systematically collated.** The HSE was able to gather a significant amount of information in the middle of a crisis about the applications that were being used across the HSE, hospitals and CHOs. In addition, design response processes were created such as communication structures and recovery tracking dashboards (for example the decryption tracking trello board). These artefacts will be invaluable in the event of a similar attack in future. It is therefore critical that information is now collated and appropriately managed going forward.

Focus area 1 - Key recommendations

Key recommendations are outlined below. These have been split between those that are for immediate consideration and those that should follow in the medium-term (as they require further planning and preparation). The HSE should begin planning for the delivery of medium term recommendations immediately, in parallel to implementing the immediate recommendations, and start the implementation phase of these medium-term recommendations within six months:

Immediate recommendation 1

1. **FA1.KR1 Appoint an interim senior leader for cybersecurity (a CISO) who has experience rapidly reducing organisations' vulnerability to threats and designing cyber security transformation programmes (see tactical recommendation 1.4 in Section 4.2).** The HSE should appoint an interim senior leader for cybersecurity to be responsible for placing governance around cybersecurity improvements, identifying a sustainable medium-term managed detection and response solution (see immediate recommendation FA1.KR6), identifying future strategy for detection and response and leading the implementation of the immediate recommendations from this review. This role

should also be responsible for planning and mobilising teams to deliver a cybersecurity transformation required to sustainably reduce the HSE's risk to ransomware attacks. The CISO should be at National Director level, a direct report to the CTTO, and have appropriate access to the EMT and their agenda, to ensure that cybersecurity risks are understood and considered in all decision-making. This interim senior leader should be given the ability to source the necessary expertise from the market to build a team that can give effect to the immediate recommendations listed in this section, and to begin planning for the implementation of medium-term recommendations. The prioritisation for the approval of a CISO and a cyber security team has been recorded within the Q2 Divisional Risk Register as an 'action control' to Risk ID 130 with a due date of 30 June 2022.¹⁷⁰

2. **FA1.KR2 Establish an executive-level cybersecurity oversight committee, to drive continuous assessment of cybersecurity risk across the provision of health services (see strategic recommendation 1.2 in Section 4.1).** A dedicated executive oversight committee is needed to provide direction and oversight to cybersecurity, both within the HSE and across other parties connected to the NHN.
3. **FA1.KR3 Create a Board committee, to oversee the transformation of IT and cybersecurity to deliver a future-fit, resilient technology base for provision of digitally-enabled health services (see strategic recommendation 1.4 in Section 4.1).** The HSE should consider the inclusion of further specialist non-executive members of the committee in order to provide additional expertise and insight to the committee.
4. **FA1.KR4 Plan a multi-year cybersecurity transformation programme, and identify and mobilise the resources to deliver (see strategic recommendation 3.2 in Section 4.1).** In parallel to delivering the tactical cybersecurity improvement programme, the HSE's appointed interim CISO should plan a cybersecurity transformation that will build lasting cybersecurity capabilities and sustainably reduce cyber risk exposure. This cybersecurity transformation programme should be validated at the Board level. The HSE should also identify suitable resources and expertise to plan and deliver this transformation.

¹⁷⁰ DRR Q2 2021, 19 November 2020

5. **FA1.KR5 Appoint a programme lead and define the governance framework for the cybersecurity transformation programme (see strategic recommendation 3.1 in Section 4.1).** A programme lead with experience in cybersecurity transformation should be appointed by the HSE's interim CISO to drive the execution of this transformation. It is critical that this programme lead can work hand in glove with the HSE's technologies teams, to help orchestrate secure technological transformation.
6. **FA1.KR6 Continue to use a managed detection and response service provided by a third party and identify a sustainable medium-term solution (see tactical recommendation 2.1 in Section 4.2).** The current service provided by the HSE's Incident Response provider is the most crucial defence the HSE currently has against further ransomware attacks. If the HSE decides to onboard a new managed detection and response service, it should ensure there is an overlap between this and the HSE's Incident Response provider's current service, so that there are no periods when the IT environment is not monitored.
7. **FA1.KR7 Mobilise a tactical cybersecurity improvement programme¹⁷¹ (while the cybersecurity transformation programme is being planned), with governance that feeds into the interim CISO and can provide updates on the programme's progress into the Board committee (see tactical recommendation 1.5 in Section 4.2).** Dedicated cybersecurity and technology resources should be used to deliver a tactical cybersecurity improvement programme, consisting of tactical work packages that can be delivered at pace using focused governance and reporting to drive accountability. To create these work packages, the HSE should action the following activities:
 - **Triage** - All third party recommendations and fixes to the security control gaps identified internally should be triaged into tactical or strategic activities. Tactical activities should be those that will rapidly reduce the risk of ransomware attacks and are achievable in 60 days or less. Note that where improvements are identified as strategic, the HSE should consider what additional tactical improvements can be implemented in the short-term to reduce risk and act as mitigating controls.
 - **Test and Assess** - As well as the recommendations it has received from

third parties, the HSE should also include recommendations by performing:

- AD security assessments;
- Vulnerability scanning of all internet-facing IP addresses;
- Vulnerability scanning of all internal IP address ranges;
- A comprehensive assessment of current capabilities and planned improvements against a framework that identifies key capabilities to defend against human-operated ransomware attacks (such as the proprietary ransomware readiness framework used in this report or that recently published by CISA¹⁷²).
- **Architect** - Following the triaging activity, the HSE should use cybersecurity experts to architect and manage a series of tactical work packages to deliver the tactical improvements identified by the triage process. These should be designed to deliver directly and rapidly reduce the risk of ransomware attacks, and be achievable in 60 days or less. Examples of tactical work packages include:
 - Uplift detection and response capability;
 - Remediate priority infrastructure vulnerabilities;
 - Lock down remote access methods;
 - Protect privileged accounts;
 - Improve service account hygiene;
 - Remediate AD hygiene issues;
 - Secure local administrator accounts;
 - Enforce Multi Factor Authentication (MFA) for all remote access methods;
 - Restrict internet access to servers.

This governance should directly feed progress updates into the Board committee. These progress updates should clearly articulate:

- the HSE's vulnerability to ransomware attacks;
- the risk reduction achieved by improvement activities that have been delivered;

¹⁷¹ A programme that is made up of work packages that rapidly reduce the risk of ransomware attacks and are achievable in 60 days or less

¹⁷² <https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat>

- the extent of the improvements required to reduce the risk of ransomware attacks to an acceptable level.
- 8. FA1.KR8 Bring the governance of ongoing IT and cybersecurity improvement projects under the tactical cybersecurity improvement programme (see tactical recommendation 1.5 in Section 4.2).** Governance of current on-going IT projects, that directly or indirectly result in cyber risk reduction, should be brought under the tactical cybersecurity improvement programme's governance (and therefore the CISO see key recommendation FA1.KR7), so the cyber risk reduction they deliver can be tracked, and any risk and issues can be resolved. For example, modernisation projects such as the upgrading of Windows 7 OS and platform modernisation.
- 9. FA1.KR9 Use security testing 'find and fix' to identify additional security weaknesses and vulnerabilities by simulating cyber attack techniques, before identifying and triaging pragmatic fixes (see tactical recommendation 1.5 in Section 4.2).** Security testing should be used to focus tactical improvement activities. By simulating the threat of human-operated ransomware attacks, improvements that make it more difficult for an Attacker to successfully compromise the organisation can be identified. The HSE should bring together red team experts¹⁷³ and cybersecurity engineers to identify pragmatic fixes to the vulnerabilities and weaknesses identified. These fixes should then be triaged with IT and Security teams to assess their feasibility and identify how best to deliver them (see key recommendation FA1.KR7 Triage). Security testing should then be used to validate improvements have been correctly implemented.
- 10. FA1.KR10 Schedule a 'red team' ethical hacking exercise for early 2022 to demonstrate the effectiveness of tactical improvements made and identify areas for further improvement (see tactical recommendation 1.5 in Section 4.2).** The HSE's interim CISO should schedule a red team for Q1 2022 to simulate a human-operated ransomware attack from end-to-end, to identify whether improvements have been effective, and to identify additional priority and focus areas for cybersecurity improvements. This should be scheduled in addition to the recorded plans within the Q2 DRR, which recorded an 'action control' to enhance penetration testing and red team exercises with a due date of 31 December 2021.¹⁷⁴
- 11. FA1.KR11 Implement the following tactical recommendations identified through this review, within the mobilised tactical cybersecurity improvement programme (see key recommendation F1.KR7) (see tactical recommendation 1.5 in Section 4.2):**
- a. Improve security monitoring capability
 - i. Document a process for how to respond to cybersecurity alerts, that clearly outlines how alerts should be triaged, investigated, contained and responded to. This process should also include coordinating the response to security alerts and incidents raised by any organisations connected to the NHN.
 - ii. Augment the Security Operations team with cybersecurity expertise.
 - b. Secure privileged access
 - i. Develop and implement a robust privileged access strategy that aligns with Microsoft good practice and reduces the risk of privileged accounts being compromised.
 - c. Build a vulnerability management capability
 - i. Stand up a vulnerability management capability that continuously scans for vulnerabilities that can be exploited by attackers.
 - d. Harden the security boundary
 - i. Define and communicate a 'security boundary' for the HSE to provide a clear boundary of cybersecurity responsibilities.
 - ii. Perform hardening activities on the defined perimeter of the HSE.
 - iii. Identify secure methods for clinical staff in voluntary hospitals to access applications hosted by the HSE.
 - iv. Use security testing to validate that the HSE can not be compromised by malicious activity from outside its security boundary.

¹⁷³ Red team experts are ethical hackers who perform simulated cyber attacks through the use of the same tactics, techniques and procedures (TTPs) used by attackers

¹⁷⁴ DRR Q2 2021, 19 November 2020

e. Improve governance over the NHN

- i. Risk assess the 'flat' network design and implement segmentation controls that align to the defined level of risk appetite.
- ii. Establish clear responsibilities for IT and cybersecurity across all parties that connect to the NHN, or share health data, or access shared health services.
- iii. Increase the resourcing of first and second line network teams in line with defined security responsibilities.
- iv. Define a security code of connection for connecting to the NHN.
- v. Define a minimum security standard for the networking of medical devices.

f. Improve preparedness for a ransomware attack

- i. Collect, organise and document artefacts created as part of the response and recovery to the ransomware cyber attack.
- ii. Identify documents required to respond to a ransomware attack (e.g., network diagrams, asset list) and secure these in a cloud repository. This should be aligned with work to develop an IT continuity and recoverability process which was recorded in the Q2 DRR as an 'action control' with a due date of 30 September 2021.¹⁷⁵
- iii. Setup and test out-of-band communication medium that would enable IT and security teams, as well as employees, to communicate in the event of a cybersecurity incident.
- iv. Ensure that the HSE has a fit-for-purpose incident response service with complementing and embedded internal processes for its invocation.
- v. Review backups and plan for a wide-spread failure recovery mode.
- vi. Document a prioritised list of applications for recovery.

g. Accelerate foundational IT projects

- i. Accelerate the move to cloud based email [REDACTED] by prioritising the resources available for IT and cybersecurity improvements programmes.
- ii. Prioritise the remediation of critical legacy systems. Particular attention should be paid to the NIMIS application to understand whether the configuration changes made in one hospital (Hospital A) to enable the application to run on Windows 10 can be more widely implemented to expedite the central Windows 10 rollout plans. It should be noted that a legacy risk was recorded in the Q2 DRR, with an aligned 'action controls' to risk assess the existing estate and increase investment for replacing outdated structures both with due dates of 31 December 2021.¹⁷⁶
- iii. Define a minimum standard for legacy operating systems. For systems that must run on outdated operating systems, sufficient mitigation measures must be defined.
- iv. Define minimum standard requirements for OS of medical devices.
- v. Perform asset discovery activities to continually update asset lists.

Medium-term recommendations

1. **FA1.KR12 Appoint suitable long-term senior leadership for cybersecurity (a CISO) and establish a suitably resourced and skilled central cybersecurity function (see strategic recommendation 3.1 in Section 4.1).** The CISO should be at National Director level, a direct report to the CTTO, and have appropriate access to the EMT and their agenda, to ensure that cybersecurity risks are understood and considered in all decision-making. They should be empowered to execute on a defined security vision, strategy and transformation to achieve sustainable cybersecurity risk reduction across the HSE. In line with this appointment the cybersecurity governance and operating model should be defined and subsequently resourced (ideally with burst capacity resources used during any interim periods that occur while recruitment takes place). This model should align to the three line of defence model. Responsibilities,

¹⁷⁵ DRR Q2 2021, 19 November 2020

¹⁷⁶ DRR Q2 2021, 19 November 2020

accountabilities, reporting lines and resourcing across the extended organisation of the HSE must all be defined. This includes within the HSE's cybersecurity and IT teams and between these central teams and those within its extended organisation.

2. FA1.KR13 Deliver a multi-year cybersecurity transformation programme to build defence in depth over time and address root-cause issues (see strategic recommendation 3.2 in Section 4.1).

Investment is needed in a single programme of work delivered over the next two - four years to develop core cybersecurity capabilities in a sustainable manner over the short, mid and long term. We would propose this transformation is structured according to a two-track delivery model with dedicated resources and defined target states:

- a. Tactical track** - the HSE should bring together red team experts and cybersecurity engineers to identify pragmatic fixes to the vulnerabilities and weaknesses identified. These should then be triaged between this tactical track and the strategic track for any

longer term strategic activities. Within the tactical track each activity should be defined as being achievable within either 'two-week agile sprints' or '60-days work packages', to deliver rapid risk reduction by addressing exposure to specific attack techniques. Once the cybersecurity transformation programme is operational this track should absorb the tactical cybersecurity improvement programme.

- b. Strategic track** - To build the sustainable and enabling foundations that deliver long-term reduction and mitigation of cyber risk, the HSE should define strategic work packages for activities that will take longer than 60 days to implement. This will include the medium recommendations made in this report. For improvements that are identified to be delivered strategically, suitable mitigations should be put in place in the short-term to reduce risk.

It would be typical for tactical and strategic track work packages to be defined across topics/work streams such as those shown in Figure 12:

Figure 12: Overview of key pillars in a cybersecurity transformation. This identifies elements that should be considered when scoping a cybersecurity transformation programme

IT Foundations Improving the hygiene of an organisation's IT estate through tactical activities like enabling security features on the Active Directory and strategic initiatives like embedding good practice data retention, backup and recovery and patch management.	Security Foundations Understanding business drivers and defining the structure and blueprints for security through tactical activities like defining the technical boundary and strategic initiatives like designing the security strategy and frameworks for risk management and architecture.	Access Management Securing identity and access through tactical activities like cleaning up local admin accounts and strategic initiatives like onboarding critical accounts onto a PAM solution and setting up strong authentication & SSO.
Data Security Implementing protective and detective measures to secure critical data through tactical activities like restricting file share open access and strategic initiatives like data classification and data loss prevention capabilities.	Network Security Monitoring network activity and improving protective capabilities through tactical activities like reviewing and hardening key firewalls and strategic initiatives like implementing network segmentation and ONS Security.	Threat Detection & Response Identifying and setting up response capabilities for key threats through tactical activities like developing priority detection content and strategic initiatives like enhanced security monitoring, crisis readiness and IoT/OT threat management.
Attack Surface Reduction Setting up a robust vulnerability management framework and processes through tactical activities like remediating priority vulnerabilities and strategic initiatives like defining secure configuration baselines and DevSecOps processes.	End User Security Protecting the end user compute estate with in the environment through tactical activities like limiting the use of MS Office macros and strategic initiatives like enhancing technical endpoint protection capabilities, and improving email threat mitigation.	Security Culture Improving security awareness through tactical activities like training high risk users and strategic initiatives like designing and delivering security awareness and phishing campaigns.

For example, within the 'IT Foundations' work stream tactical work packages might include the remediation of stale data or extending the scope of the identity directory. Strategic work packages within this work stream could include decommissioning end of life systems or implementing an operational CMDB to maintain an updated list of all systems and applications in the environment.

- 3. FA1.KR14 Plan the HSE's future IT transformation that reduces cybersecurity risk (see strategic recommendation 2.2 in Section 4.1).** The HSE's IT transformation lead should begin documenting and planning the future IT transformation. Executing an IT transformation will allow the HSE to sustainably reduce cybersecurity risk in the long-term, as issues within the legacy IT estate can be addressed, and cybersecurity and resilience can be built into the IT architecture.
- 4. FA1.KR15 Design and implement a single and centralised security monitoring capability for the defined security boundary of the HSE that reports into the CISO (see strategic recommendation 3.2 in Section 4.1).** This should be for all monitoring aspects including network, server and workstation environments, as well as services such as email. Any reduction in the visibility of assets for monitoring should be risk-assessed to ensure that the HSE's ability to monitor its full environment is within risk appetite. This implementation should involve establishing the following across the three fundamental pillars of people, process and technology:
 - **People** - Employing security monitoring and detection SMEs (either internally or through third parties) that are trained to identify and respond to threats detected within and across the HSE security boundary.
 - **Process** - Ensuring that detection and response processes are documented. This includes incident playbooks that outline the step-by-step response actions to be taken, as well as documented responsibilities and accountabilities for reporting security events between organisations (such as voluntary hospitals and reporting bodies like the NCSC).
 - **Tooling** - Deployment of modern endpoint detection and response tooling/endpoint protection platform tooling across the HSE environment and security boundary. This should be in addition to the implementation of a Security Incident and Event Manager ("SIEM") and Security Operations Centre ("SOC") to centrally analyse logs from systems and security tools.

Focus area 1 conclusion

The HSE was not sufficiently prepared to defend against or respond to a ransomware cyber attack. The HSE did not have sufficient subject matter expertise, resources or appropriate security tooling to detect, prevent or respond to a cyber attack of this scale and complexity. As a result, the attacker was able to enter the HSE environment and move around with relative ease and there were several missed opportunities to detect malicious activity, prior to the detonation phase of the ransomware.

Following the execution of ransomware, the HSE mobilised a response to overcome the significant challenges posed by both the attack and its lack of preparedness. Due to the scale and impact of the ransomware, paired with the complex and legacy IT environment, the technical recovery of IT systems was challenging. The timeframe for recovery could have been significantly longer had the decryption key not been sourced, as the HSE would have had to rely on recovering applications and systems from backups. The HSE would likely have encountered significant difficulties with this approach as the backup infrastructure was primarily designed to recover single systems only and not to recover multiple systems at scale and pace.

The focus of the HSE's activities since the attack has been on implementing recommendations provided by third parties and to continue to recover systems. A finalised cybersecurity improvement plan does not exist and limited evidence has been provided to show planning that will significantly and sustainably reduce the HSE's exposure to future ransomware attacks.

5.2 Focus area 2 - review of organisation wide preparedness and strategic response

Focus area 1	Focus area 2	Focus area 3
Review the technical investigation and response	Review the organisation-wide preparedness and strategic response	Review the preparedness of the HSE to manage cyber risks
	Key findings and recommendations	
	Conclusion	

Key findings and recommendations

Figure 13: Focus area 2 summary of key findings and recommendations

Themes	Areas	No. of key findings	No. of key recommendations
Prepare	Governance over crisis and business continuity management - HSE and across HGs and CHOs	2	2
	Incident/crisis management and clinical and services continuity planning - HSE and sample site hospitals and CHOs	3	3
	Crisis communications preparedness at the HSE	2	2
	Awareness, training and exercising capability - HSE, HG/ hospitals and CHOs	1	1
	Implementation of lessons learned	1	1
	Human factors and cultural contributors	1	1
Response	Notification and activation of NCMT and wider response workstreams	1	1
	Response structures, resourcing and logistics	2	2
	Information and data management in a crisis	3	3
	Response leadership, strategy setting and decision making	2	2
	Stakeholder management, crisis communications and reputation management	2	2
	Scenario planning	1	1
	Effectiveness of workarounds	1	1
Recovery	Services and data led recovery strategy	2	2
Total no. of key findings & recommendations		24	24

In reviewing the organisation-wide preparedness and strategic response, we have incorporated guidelines and principles from ISO 22301:2019 'Security and resilience - Business continuity management systems (BCMS) - requirements', BS 11200:2014 'Crisis Management. Guidance and good practice' and PD CEN/TS 17091:2018 'Crisis management - Guidance for developing a strategic capability.

ISO 22301 defines business continuity as 'the capability of an organisation to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption'.¹⁷⁷ In the context of the HSE, the term clinical and services continuity is used throughout this section of the report. It refers to all acute and community services, as well as corporate services, including, but not limited to HR, procurement, finance, training, ICT etc.

¹⁷⁷ ISO 22301:2019 'Security and resilience - Business continuity management systems (BCMS) - requirements', p. 2.

The European Technical specification for Crisis Management, PD CEN/TS 17091:2018 specifies that organisations should be prepared for an ‘unprecedented or extraordinary event or situation that threatens an organization and requires a strategic, adaptive, and timely response in order to preserve its viability and integrity, with clear, universally understood structures, roles and responsibilities’.¹⁷⁸ It defines crisis management as ‘the developed capability of an organization to prepare for, anticipate, respond to and recover from crises’¹⁷⁹ and states that an organisation’s crisis management capability is not normally part of routine organisational management, and should be consciously and deliberately built and sustained through capital, resource and time investment.

The findings and recommendations in this section are mapped against the key thematic areas derived from these standards (see section 2.4 - *Our review approach*). The findings and recommendations follow a numbering convention of FA2.KFX (Focus Area 2: Key Finding X) and FA2.KRX (Focus Area 2: Key Recommendation X).

See Appendix F for a detailed organisational timeline.

Crisis Preparedness

Area 1: Governance over crisis and clinical and services continuity management in the HSE and across HGs and CHOs

Introduction and Context

The HSE has shown itself to be well versed and proficient in major emergency management, a capability that has been demonstrated through its response to several recent events, most notably the 2020 COVID-19 pandemic and the 2019 nurses’ strike. The integration of the Major Emergency Management Framework with the wider national emergency management capability enables a comprehensive approach to plan for, to respond and to coordinate recovery from major emergencies which threaten persons or infrastructure at a national as well as local level.

The organisation’s approach to incident and emergency management is detailed in the following preparation documents:

- A Framework for Major Emergency Management;
- Area Emergency Management Plans;
- Hospital Major Emergency Plans;
- Emergency Management Operational Delivery Plan; and
- Incident Management Framework.

FA2.KF1 Crisis management and clinical and services continuity were not integrated within an overarching Operational Resilience Programme, leading to siloed work streams and capabilities

There was little active integration between clinical and services continuity, crisis management and the other closely aligned disciplines to ensure they directly informed planning and that preparedness evolved to prevailing conditions. The HSE is a large and diverse organisation with complex operational structures. Initiatives to achieve greater integration of resilience disciplines were proposed in September 2019, when an Enterprise Risk Management (“ERM”) programme was discussed at the Board meeting.¹⁸⁰ Following this Review the HSE’s new CEO and Board and Audit and Risk Committee led a programme of work to further develop the corporate governance of risk. This included greater oversight at Board and ARC level for corporate risks, significant reviews of the Corporate Risk Register led by the EMT, work undertaken between the Board and the EMT to improve the risk management process, the establishment of a Corporate Risk Support Team and increased investment provided in the 2021 National Service Plan to strengthen the corporate level risk team.

A subsequent review of the HSE’s corporate services commenced in December 2019,¹⁸¹ ultimately led to the proposal that a new role at National Director level would be established with responsibility for Governance and Risk (“ND G&R”). Responsibilities include the development of risk and business continuity management frameworks through which risk management and clinical and service continuity plans will be reviewed, maintained and validated. Responsibility for clinical and service continuity under the HSE’s accountability structure will remain with operational and functional managers.¹⁸² Resilience

¹⁷⁸ PD CEN/TS 17091:2018 ‘Crisis management - Guidance for developing a strategic capability’, p. 8.

¹⁷⁹ PD CEN/TS 17091:2018 ‘Crisis management - Guidance for developing a strategic capability’, p. 8.

¹⁸⁰ Minutes-hse-board-meeting-27-09-2019

¹⁸¹ Centre Review Slides June 2021

¹⁸² HSE_CCR_Phase2_HealthcareStrategy_Gov&Risk(Extract)

was also highlighted as a priority at the Performance and Delivery Committee meeting in June of 2021.¹⁸³

Board oversight of the wider risk and resilience capability is currently delivered through a number of different committees, under the consolidated oversight of the Audit & Risk Committee, as follows:

- Clinical and services continuity (currently described as business continuity) - Audit & Risk Committee; and previously People & Culture Committee until June 2020;
- Incident management - Safety & Quality Committee;
- Enterprise risk management - oversight and management - Audit and Risk Committee; and
- Cyber security - Performance & Delivery Committee.

The workstreams related to these risks often operated in silos. Additionally, when risks were identified, improvements to the HSE's response capability were not always informed by those risks. For example, the Board received a detailed briefing in November 2020 on the emerging cyber threats faced by the HSE and the increase of the ransomware risk to business continuity.^{184,185} Nevertheless, the Cybersecurity and Business Continuity risk ratings in the CRR remained constant (at a 'High' rating of 16).^{186,187,188,189}

Following the review of corporate services, the ND G&R (equivalent to a Chief Risk Officer) reports through the Chief Strategy Officer to the CEO, Audit & Risk Committee and Board on risk management. In a mature Operational Resilience Programme, we would expect to see the separate, but related disciplines of risk management, incident management, clinical and services continuity and crisis management integrated into a comprehensive resilience framework under the coordination of a senior executive, usually a Chief Risk Officer who has appropriate access to the EMT, the CEO and the Board. The framework allows for assurance over the operational capability that is being delivered by relevant owners.

FA2.KR1.1 Establish governance and oversight of an Operational Resilience Programme (see strategic recommendation 4.1 in Section 4)

The HSE should:

- Nominate an executive with responsibility for operational resilience which will include the coordination of component parts of crisis management (including major emergency management), incident management, clinical and services continuity and enterprise risk management;
- Establish a HSE Resilience SteerCo to oversee the design and delivery of an Operational Resilience Programme, reporting into the Board. This SteerCo should include senior representatives from the EMT who own the respective resilience disciplines and related functions (e.g. cyber security), and any additional key clinical and services and operations representatives.

FA2.KR1.2 Establish an Operational Resilience Policy and Programme scope, strategy and structure (see strategic recommendation 4.1 in Section 4)

The HSE should:

- Define an overarching policy that incorporates the above resilience disciplines. Clarify ownership of the programme (for example, under the ND G&R) and integration with existing policies. At a minimum, the policy should include a statement of leadership commitment, objectives and scope, roles and responsibilities, reference to relevant industry standards and an oversight regime;
- Define the Operational Resilience Programme scope, strategy and structure across the HSE and funded entities. Define the types of incidents in scope (e.g. physical, technological, people and cyber incidents) and how to build and maintain a capability to respond across the organisation. Define the operating model or the capability in terms of dedicated staff, reporting lines, roles and responsibilities within 'prepare' and 'respond and recover.' Specify which areas of the HSE and funded entities are included and identify accountable teams/individuals for delivering specific components of the programme. Agree the intended end state, the timetable to achieve the objectives and the resources required;

¹⁸³ <https://www.hse.ie/eng/about/who/board-members/committees-of-the-board/performance-and-delivery-committee/mintues-hse-performance-and-delivery-committee-18th-june-2021.pdf>

¹⁸⁴ Briefing for HSE Board on Cyber Security

¹⁸⁵ Cyber Security Awareness Draft V7.2

¹⁸⁶ CRR Full Report Post EMT 2nd Nov OCTOBER 2020 v0.2 03 11 20 FINAL

¹⁸⁷ CRR FULL Report Summary and Assessments HSE Board 23rd June 2020 pdf v0.1 23 06 20

¹⁸⁸ CRR Q1 2021 Review Report Final post EMT meeting 27 04 21 v1.0 27 04 21

¹⁸⁹ CRR Q4 2020 Full Report post EMT meeting February 2021 v0.1 09 02 21

- Design consistent tools and templates to be used by the HSE and to be cascaded down as resources for funded entities. Assign responsible leads to complete these tools and templates, and develop documentation and capability at operational sites.

FA2.KR1.3 Establish assurance over the Operational Resilience Programme (see strategic recommendation 4.1 in Section 4)

The HSE should:

- Develop programme reporting, including KPIs, a method and timetable for review, and risk management considerations. Ensure that operational resilience is a standing agenda at Board (or Board committee) meetings.

FA2.KR1.4 Embed the Operational Resilience capability via training and exercising (see strategic recommendation 4.2 in Section 4)

The HSE should:

- Ensure a commitment to maintain and test the resultant capability by designing an HSE-wide training and exercising programme. This includes a structured programme for delivering knowledge and skills training, and scenario-based exercises to all relevant stakeholders across the HSE and funded entities who have a role to play in any serious or significant incident or crisis; as well as additional training resources, validation programmes and independent Internal Audit review to the Board;
- Ensure ND G&R and at least one Board member has direct competency/experience in the area of operational resilience.

FA2.KF2 There was no effective governance or consistent ownership of clinical and services continuity across the HSE

There was no central Clinical and Services Continuity Management System Framework in place in the HSE prior to the cyber attack. Roles and responsibilities in respect of the management and oversight of clinical and services continuity were not documented, nor were there any structured governance mechanisms to implement, monitor and report progress on the objectives contained in the 2016 Business Continuity Policy.¹⁹⁰ In the absence of this framework, clinical and services continuity capability was not adequately resourced or embedded. This was identified in the review of the HSE's corporate services, initiated in 2019; and while enterprise risk management and

clinical and services continuity are now consolidated under the National Director for Governance and Risk (see also finding FA2.KF1), a significant body of work will be required to address this gap.

Due to the historic lack of governance and oversight over clinical and services continuity across HGs and the HSE funded entities, a fragmented and unvalidated capability was also apparent across individual hospitals and CHOs. There was no evidence of Clinical and Services Continuity Policies at any of the sample sites or of formalised steering committees with documented roles and responsibilities for the ongoing and continuous maintenance of the local Clinical and Services Continuity Management System. Senior members of the HSE commented that there was insufficient support and resources provided to HGs and CHOs to ensure standardised and consistent approaches to clinical and services continuity management at local site level. While continuity of services is implied in service level agreements with hospitals, there is no specific requirement to demonstrate a clinical and services continuity capability.¹⁹¹ Internal Audit scrutiny of all organisations funded by the HSE is permitted in the Audit and Risk Committees ToRs. However, there was no evidence of any audit of the clinical and services continuity capability in the HSE or funded entities.¹⁹²

FA2.KR2.1 Establish and document a formal governance structure to oversee clinical and services continuity in the HSE (see strategic recommendation 4.1 in Section 4)

The HSE should:

- Update the existing Clinical and Services Continuity Policy and present it to the Board for review and approval. This should be nested under the overarching Operational Resilience Policy (see also recommendation FA2.KR1) and clearly articulate the purpose, scope, applicability, review frequency, authority, Clinical and Services Continuity Management Framework, governance and monitoring of the policy and programme;
- Establish a programme of governance for clinical and services continuity - incorporated under the Operational Resilience Programme (see recommendation FA2.KR1.1) - which provides a central point of accountability for monitoring and reporting on the implementation, maintenance and validation of activities in line with policy objectives. Formally document roles and responsibilities, a Clinical and Services Continuity Steering Committee and an organisational chart.

¹⁹⁰ Business Continuity Management Policy 2016

¹⁹¹ Site Workshop 6 and 11 (Hospital C and Hospital A)

¹⁹² Audit and Risk Committee TORs

The scope should reference the HSE and all funded entities;

- Formalise robust reviews and challenges by appropriate personnel, of all stages of the Clinical and Services Continuity Programme, embedding Internal Audit into the clinical and services continuity lifecycle to provide independent assurance to the Board of the HSE's contingency capabilities;
- Secure formal clinical and services continuity qualifications for appropriate members of the steering committee/implementation team;
- Be prepared to consider the emerging requirements contained in the EU Critical Entities Resilience Directive ("CER").

FA2.KR2.2 Support funded entities (hospital groups, hospitals and CHOs) to establish governance over clinical and services continuity (see strategic recommendation 4.1 in Section 4)

The HSE should support funded entities (hospital groups, hospitals and CHOs) to:

- Implement Clinical and Services Continuity Steering Sub-Committees at HG, hospital and CHO levels, beneath the HSE Steering Committee; and establish a framework of governance. These groups should have a similar structure, terms of reference and roles and responsibilities as the overarching HSE group;
- Draft specific Clinical and Services Continuity Policies which complement the HSE's policy, according to the policy guidance listed above;
- Appoint relevant clinical and services continuity sponsors;
- Integrate clinical and services continuity into project and change management processes where appropriate.

Area 2: Incident / crisis management and clinical and services continuity planning at the HSE and sample site hospitals and CHOs

FA2.KF3 Clinical and Services Impact Analysis did not consistently inform clinical and services continuity workarounds

The Clinical and Services Impact Analysis¹⁹³ (referred to in standards as a Business Impact Analysis) identifies critical processes, and the associated people, premise, systems and infrastructure, which must be maintained to ensure a minimum viable organisation during an incident or crisis. Failure to conduct a comprehensive Clinical and Services Impact Analysis process hinders the development of adequate workarounds to maintain critical operations.

Standardised or formalised Clinical and Services Impact Analysis processes were not evident at HSE centre, support services, or sample hospital and CHO sites. Even those sample sites where the clinical and services continuity posture was proactive and mature (e.g. Site Workshop 11), a Clinical and Services Impact Analysis had not been conducted. Some hospital and CHO response teams reactively defined their recovery priorities during the initial phase of the attack because there was no Clinical and Services Impact Analysis. This diverted effort from the response towards tasks which should have been completed in advance of the cyber attack, eg., defining a schedule of systems for recovery based on pre-agreed Recovery Time Objectives ("RTOs") and Recovery Point Objectives ("RPOs"). Several interviewees noted that in the absence of a Clinical and Services Impact Analysis the early prioritisation scheme was driven by the OES list, before advancing to an approach that focused on clinical risks,¹⁹⁴ delaying the recovery of patient critical services (see also finding FA2.KF17). The extent of the initial disruption and maintenance of essential services varied significantly across the sample sites. There was also significant variance in the effectiveness and availability of workarounds or recovery strategies to ensure consistency of critical patient services.

¹⁹³ ISO 22317 Societal security - Business continuity management systems - Guidelines for business impact analysis (BIA)

¹⁹⁴ Site Workshop 8 (Hospital B)

FA2.KR3.1 Establish and embed a clear and consistent approach to Clinical and Services Impact Analysis across the HSE to inform recovery prioritisation (see strategic recommendation 4.1 in Section 4)

To ensure a standardised organisation-wide approach to the Clinical and Services Impact Analysis process, the Executive Sponsor for clinical and services continuity at the HSE and each HG/hospital and CHO should:

- Establish and embed a formal Clinical and Services Impact Analysis process, with clear ownership at each level, including the criteria for the “RTOs”¹⁹⁵ and “RPOs”¹⁹⁶;
- Ensure the results of the Clinical and Services Impact Analysis are formally reviewed and approved on a periodic basis, by senior management, and following any significant systems/process, operational, regulatory or personnel change.

FA2.KR3.2 Design clinical and services continuity workarounds, based on the Clinical and Services Impact Analysis, to enable the HSE to continue providing critical services while responding to an incident or crisis (see strategic recommendation 4.2 in Section 4)

The HSE should:

- Design and agree clinical and services continuity workarounds, for critical processes, with the agility and governance to be maintained for a prolonged period, and based on the Clinical and Services Impact Analysis;
- Assess all workarounds to ensure they do not pose an unacceptable risk to patient care or to the HSE through the transfer of data or other assets between systems;
- Align workarounds for similar systems or processes across the HSE to improve their effectiveness and inform a consistent response;
- Reflect the workarounds in the relevant Clinical and Services Continuity Plan.

FA2.KF4 There was no standardised approach to clinical and services continuity planning across

the HSE

There is no framework or mechanism in place at the HSE to ensure that the clinical and services continuity planning is aligned to the policy objectives. No integrated and comprehensive clinical and services continuity planning exists at the HSE. Additionally, while some hospitals had a level of clinical and services continuity planning in place, there was no evidence that this process was consistently formalised or conducted across sampled HGs, hospitals or CHOs, to deliver a local clinical and services continuity capability.¹⁹⁷ Where workarounds were in place, there was inconsistency in emphasis, layout and terminology and no evidence that the determination, adoption and resourcing of those workarounds had input or steer from the HSE centrally.

The absence of pre-prepared Clinical and Services Continuity Plans severely impacted the initial stages of the response to the cyber attack, as resources had to be diverted away from the response effort to compile essential information, create structures and prioritise services for recovery which should have been formalised and articulated during a preparatory phase.^{198, 199} Recurring examples given in interviews of this were construction of call trees, compiling asset registers, critical service prioritisation and definition and use of alternative communications methods. Furthermore, recovery solutions were often inaccessible as hard copies were not available.

FA2.KR4 Develop and embed consistent Clinical and Services Continuity Plans at strategic, tactical and operational levels that align with the Clinical and Services Impact Analysis (see strategic recommendation 4.2 in Section 4).

To ensure that Clinical and Services Continuity Plans are compatible with the recovery objectives, the HSE should:

- Implement Clinical and Services Continuity Plans at strategic, tactical and operational levels of the HSE, HGs/hospitals and CHOs and that they formally document workarounds and the steps involved to resume normal operations;

¹⁹⁵ Recovery Time Objective (RTO) is the period of time following an incident within which a product and service or an activity is resumed or resources are recovered (ISO 22300:2021).

¹⁹⁶ Recovery Point Objective (RPO) is the point at which information used by an activity is restored to enable the activity to operate on resumption (ISO 22300:2021)

¹⁹⁷ A sample of example plans include: Hospital C Business Continuity Plan Dec 2019, Hospital F Pandemic Preparedness Plan, Hospital E Internal Emergency Response Plan, Midlands SAP Payroll Business Continuity Plan

¹⁹⁸ Site Workshop 11 (Hospital A)

¹⁹⁹ Information Management & Coordination Workshop

- Benchmark the Clinical and Services Continuity Plan construction against ISO 22331, and ensure they are compatible with future Sláintecare objectives;²⁰⁰
- Incorporate the testing of these steps into the clinical and services continuity management training and exercising schedule/programme (e.g. through desktop walkthrough of the resumption procedures to identify any gaps or unforeseen dependencies);
- Ensure soft and hard copies of Clinical and Services Continuity Plans are available in appropriate areas.

FA2.KF5 The HSE did not have an adequate internal Crisis Management Framework or plans to support the response to the Conti attack, nor had they planned for severe but plausible total loss scenarios

The Major Emergency Management and Incident Management Frameworks (as well as interim Emergency Management governance arrangements published in 2020) have been invoked on multiple occasions and delivered an agile and effective response to short term surge demands on health services.^{201,202}

There is an inconsistent and interchangeable use of the terms ‘major emergency management’ and ‘emergency management’ and ‘crisis management’. Crisis planning throughout the HSE was focused on the scenarios which would mobilise major emergency management teams, such as adverse weather, pandemic, epidemic, serious accidents and terrorist action. There was no Crisis Management Plan in place to guide the HSE’s response to an internal crisis impacting the HSE itself, rather than an external crisis such as COVID-19 or Storm Emma; nor has it developed and exercised *scenario-specific* plans for the response to severe disruption scenarios, (e.g. total loss of premises, systems or people). A fundamental assumption of these plans is that all mission critical systems and infrastructure would remain available to the response teams. The HSE has not conducted any scenario planning for the total loss of a facility, system, process or service (see also finding FA2.KF21). While risks were noted on the Corporate Risk Register (especially cyber security and clinical and services continuity), there was limited evidence to suggest the HSE undertakes subsequent scenario planning to:

- Identify potential triggers and escalators for the worst, best and most likely scenarios per risk;

- identify likely impacts;
- undertake mitigating actions despite the fact that cyber security and clinical and services continuity were identified as strategic risks.

Such scenario-specific plans would outline the likely impacts caused by highly plausible organisational crises, as well as the key considerations, and corresponding pre-agreed decisions to guide the strategic response to those events.

FA2.KR5.1 Design an end-to-end Crisis Management Framework (integrated with the existing MEM and IM Frameworks) and overseen by the HSE Resilience Steering Group (see finding FA2.KR1.1 and strategic recommendation 4.2 in Section 4)

The HSE should review the existing incident and emergency management structures, and the structures established during the attack and other recent events (e.g. COVID-19), to establish a new integrated end-to-end organisation-wide Crisis Management Framework that is fit-for-purpose across a wide variety of crisis types. This Framework should incorporate all resilience disciplines responsible for implementing organisational preparedness activities (e.g. emergency/incident/crisis response, and clinical and services continuity management), and identify accountable teams/individuals for specific components, as well as define all levels of response required during an actual event at strategic, tactical and operational levels. It should also integrate with the relevant elements of the organisation-wide Major Emergency Management and Incident Management Frameworks.

The Framework should include the following elements:

- Hierarchy of teams required for response. Typically this will include three layers - operational, tactical and strategic - with command and control escalating according to the nature and severity of the incident;
- Defined roles and responsibilities, and decision making authority, for all those involved in the identification, escalation, response to and management of incidents;
- Escalation thresholds and formalised communication channels;
- Guidance on how and when to invoke response structure in line with the Incident Classification and Severity Matrix (see also finding FA2.KF14);

200 ISO 22331 Security and resilience - Business continuity management systems - Guidelines

201 Incident Management Framework 2020

202 A Framework for Major Emergency Management

- Agreed touchpoints and interaction between the HSE, and HGs and CHOs;
- Tools and templates to be used by all responders (across the HSE, HG and CHO levels) during an incident (e.g., situation report, classification and severity matrix, impact assessment, decision and action logs).

FA2.KR5.2 Design a suite of crisis response plans and procedures to underpin the Crisis Management Framework (see strategic recommendation 4.2 in Section 4)

The HSE should design:

- A Crisis Management Plan providing detailed roles and responsibilities for key positions in the NCMT and supporting tactical teams (e.g. HG/hospital and CHO leadership), including checklists of activities and considerations, and details of third party support available;
- A Technical/Operational Coordination Guide providing the details of how the technical (e.g. IT Ops) and operational teams (e.g. clinical response teams) would coordinate and work together. This includes detailed roles and responsibilities, information flows, processes, checklists of key activities and considerations and details of third party support available;
- Scenario-specific plans providing detailed step-by-step operational guides for specific scenarios (e.g. analyst response to malware, fire response plan). The HSE should, using the risks identified in the Corporate Risk Register, conduct a threat profile review and readiness assessment to determine high likelihood, high impact scenarios and create scenario-specific plans for response. This should include severe but plausible total loss scenarios;
- Functional Response Plans providing detailed function-specific guidance for non-technical teams, for example a Legal/Regulatory Team and Communications Team (see recommendation FA2.KR7);
- Site-Specific Response Plans templates and guidance, providing resources for standardised clinical and services continuity and crisis management planning at sites across the organisation.

Area 3: Crisis communications preparedness at the HSE

FA2.KF6 The HSE's Internal Communications Team was under resourced

Having only been established in 2019, the HSE's Internal Communications Team was not large enough to coordinate communications to 130,000 staff²⁰³ members. Whilst investment in the External Communications Team has increased to circa 76 full time employees (FTE), the Internal Communications Team consisted of circa six FTE.²⁰⁴ Stakeholders noted that the Internal Communications Team had struggled to deliver on their growth strategy because immediate crises and operational requirements had consistently diverted the attention of the team.²⁰⁵

FA2.KR6 Ensure that the resources assigned to internal communications are sufficient (see strategic recommendation 4.2 and tactical recommendation 3.1 in Section 4).

An effective Internal Communications Team is critical to disseminate information and guidance to all 130,000 HSE staff²⁰⁶ all operating across different levels of the response; this requires additional resources and staff to what is currently available. As part of their future crisis management planning, the HSE should assess the requirements of their crisis response communications strategy and allocate the resources necessary to grow the internal communications team, to reflect the HSE's current operational architecture, and taking into consideration the impacted and involved stakeholder base.

FA2.KF7 There was no documented HSE Crisis Communications Plan in place; and the crisis communications capability across HG/hospital and CHOs was fragmented

The HSE's external communications strategy in response to the ransomware attack, whilst well-executed, was based on previous experience for the organisation rather than a formally documented Crisis Communications Plan. The combined experience of the communications team, across multiple sectors (including PR, journalism and crisis communications) allowed them to create a governance structure for their workstream by 08:00 on the day of the attack

203 <https://www.google.com/url?q=https://www.hse.ie/eng/staff/resources/our-workforce/workforce-reporting/health-service-personnel-census-aug-2021-v2.pdf&sa=D&source=docs&ust=1634489485576000&usg=AOvVaw1RQuuJUGldbFXKLpmktsyu>

204 Comms Division Organisational Chart July 2021

205 Communications & Stakeholder Management Workshop

206 <https://www.google.com/url?q=https://www.hse.ie/eng/staff/resources/our-workforce/workforce-reporting/health-service-personnel-census-aug-2021-v2.pdf&sa=D&source=docs&ust=1634489498604000&usg=AOvVaw10xqQINj8e5bZNoLDcNAVZ>

and begin the process of integrating their response with other response and local communications teams.²⁰⁷ Whilst the absence of standardised plans and processes did not impact their communications response to this incident, these are important documents to have when onboarding new joiners or working in collaboration with other teams, to ensure response activities are completed to a consistently high standard.

The HSE's national communications teams, and the HG and CHO communications teams operate under separate governance structures. Whilst the HSE's national communications teams have a well established communications network, developed through weekly meetings during the COVID-19 pandemic, the local communications teams have varying levels of experience and available resources. The absence of a consistent communications strategy across HGs and CHOs resulted in different messages being conveyed to patients; some were told to come in unless told otherwise whilst others were told to stay at home unless explicitly told to come into the hospital. This disparity in experience and subsequent strategy has been flagged in the Corporate Risk Register since February 2020 under the risk of damage to the HSE's 'Organisational reputation', with a corresponding action to '*enhance communications functions in new Regional Health Areas*'.²⁰⁸

FA2.KR7 Document the Communications Team's existing response structures, processes, tools and templates in a Crisis Communications Plan (see tactical recommendation 3.1 in section 4)

The HSE should document a formal Crisis Communications Plan to ensure consistent and efficient communications management across the organisation during an incident/crisis, and to guide the actions of new members of the HSE's Communications Team.

- The Communications Team should document the response processes, tools and templates, and structures they have found most effective during previous incidents, ensuring the resulting plan dovetails into any existing Major Emergency and Crisis Management Plans and processes, in line with the Crisis Management Framework (see also finding FA2.KF5);
- The Crisis Communications Plan should be reviewed in conjunction with the Crisis

Communications Plans in place at the HGs and CHOs to ensure the structures and processes involved integrate effectively;

- Once finalised, all processes and templates, especially those requiring collaboration with other HSE teams, should be socialised and ratified to ensure they are fit for purpose and based on up-to-date information;
- The Crisis Communications Plan should be reviewed regularly to confirm the content is still correct and relevant, and to incorporate any lessons learnt from new incidents.

Area 4: Awareness, training and exercising capability at the HSE, HG/hospitals and CHOs

FA2.KF8 Awareness, training and exercising of the crisis management and clinical and services continuity capabilities were not formally embedded across HSE

Various emergency management exercises have been held across the HSE, covering responses to several scenarios such as extreme weather and exposure to infectious diseases. There was also evidence of more advanced training and exercising capabilities in place at some HGs and CHOs.^{209, 210} However, there was no evidence of a HSE-wide training and exercising programme to ensure the right people, at the right levels, were trained in their functions, roles and responsibilities in a crisis.^{211, 212} For example, there was isolated but limited evidence that staff involved in the Conti response had received training on the HSE's clinical and services continuity capability, priorities and plans prior to the crisis.

We found no evidence of strategic level exercises (delivered to its National Crisis Management Team), rehearsing the response to a clinical and services continuity event or crisis *impacting the HSE only*, e.g. the loss or denial of critical HSE systems or infrastructure, or a significant reputational issue. Additionally, while the HSE has participated in national multi agency major emergency exercises, they have not conducted any multi-team crisis desktop or simulation exercises in conjunction with

207 Communications & Stakeholder Management Workshop

208 CRR Full Report Summary and Risk Assessments v0.1 28 02 20

209 Site Workshop 5 (Hospital F)

210 Site Workshop 10 (Hospital I)

211 Site Workshop 5 (Hospital F)

212 Site Workshop 1 (CHO B)

key sites to simulate loss/denial scenarios of critical infrastructure. There was also a lack of evidence to show how the risks identified in the Corporate Risk Register informed the design of plausible scenario-based exercises.^{213, 214, 215}

Whilst there were pockets of good practice across the organisation where local entities deliver frequent emergency management exercises, there was no evidence that the clinical and service continuity exercises delivered followed a standard approach or aligned to best practice design as outlined in industry standards. The absence of a comprehensive approach to integrated crisis management training and validation across the organisation has resulted in the following findings, evidenced in a sample of hospitals:

- Plans did not capture challenges which could have been identified during a rigorous validation process; for example, the unavailability of hard copies of Clinical and Services Continuity plans, an inability to install WiFi post attack, absence of call trees and no alternative communications plan;²¹⁶
- The absence of well-articulated roles, responsibilities and crisis management structure (e.g. local level responders were unsure of their roles and the structures in place);²¹⁷
- No clear decision making authority, including delegated decision making to HGs/hospitals and CHOs, that is clear to the National Crisis Management Team and executives, as well as supporting teams and structures²¹⁸;
- No Crisis Communications Plan or recognition for the need of a HSE-wide internal alert system or alternative communications channels²¹⁹ to allow cascading information between the HSE, CHOs and HGs;
- At the time of the cyber attack, there was no expertise in the HSE on how to stand up an integrated coordination centre. The HSE therefore initially relied on significant third party assistance and then the Defence Forces to establish a SITCEN and the templates and protocols necessary to achieve an integrated command centre (see also finding FA2.KF15).²²⁰

FA2.KR8.1 Establish a formal training and exercising programme in support of the Operational Resilience Programme (see also Finding FA2.KF1 and strategic recommendation 4.2 in section 4)

The HSE should:

- Ensure this programme incorporates clinical and services continuity and crisis management requirements and that all relevant individuals and teams involved at every level of the HSE become familiar with their roles and responsibilities in a crisis or significant clinical and services continuity incident;
- Ensure it is aligned to *ISO 22398 Security and resilience - Guidelines for exercising and testing*. Define and implement standard training and exercising templates which articulate scope, objectives, assumptions, results, issues log and lessons learned.

FA2.KR8.2 Deliver training to staff in key responsible and supporting roles, and new managers (see strategic recommendation 4.2 in section 4)

The HSE should:

- Provide clinical and services continuity and crisis management training for staff in key responsible and supporting roles. Such staff should have knowledge of best practice in relation to each core element of an effective integrated command centre and of an effective Clinical and Services Continuity Management Programme including: risk assessment, Clinical and Services Impact Analysis, clinical and services continuity management strategy selection, plan testing techniques and processes for assessing effectiveness of plans;
- Include clinical and services continuity awareness training for new managers.

FA2.KR8.3 Conduct annual exercises to rehearse the operational resilience capability (see strategic recommendation 4.2 in section 4)

The HSE should:

- Conduct annual crisis management and clinical and services continuity desktop or simulation

213 Site Workshop 2 (CHO A)

214 Site Workshop 3 (Hospital E)

215 Site Workshop 10 (Hospital I)

216 Site Workshop 3, 9 and 11 (Hospital E, Hospital H and Hospital A)

217 Site Workshop 4 (Hospital E)

218 Site Workshop 4, 7 and 9 (Hospital E, Hospital G and Hospital H and) and Information Management & Coordination Workshop

219 Site Workshop 9 (Hospital H)

220 Site Workshop 4, 9 and 10 (Hospital E, Hospital H and Hospital I)

exercises with the NCMT and ensure scenarios extend beyond current focus to include other loss scenarios including loss/denial of mission critical infrastructure, unavailability of key persons, systems, processes and facilities;

- Conduct annual multi-team crisis management and clinical and services exercises involving key HSE functions (e.g. support services) and funded entities; increasing in complexity over time to continually build organisation-wide maturity and capability;
- Support the nominated responsible owner with responsibility for clinical and services continuity and crisis management to acquire relevant external training to maintain the currency of their expertise.

Area 5: Implementation of lessons learned

FA2.KF9 While there was a formal overarching post-incident review process and evidence of localised 'lessons learned' programmes, the process and outcomes were not consistently applied

The HSE Incident Management Framework outlines a process for conducting a post-incident review, followed by improvement planning and monitoring.²²¹ Whilst the HSE have not previously encountered an incident of this scale, they have been exposed to other significant incidents (COVID-19, nurses strike and WannaCry) over the last five years, each of which would have highlighted key learnings for improved crisis management maturity at localised level.

One example of lessons learned being incorporated, and a recurring theme from interviews²²², is that the NCMT meeting process, which was developed during the COVID-19 pandemic, was quickly adapted to respond to the Conti ransomware attack. This was demonstrated by the speed with which the NCMT first convened at 08:30 on 14 May and the clear governance and administrative structures put around their response activities.^{223, 224} Another example is that, with communications platforms unavailable across the HSE, the Internal Communications Team were still able to publish information to the HSE website; this was due to a previous decision

to reduce the website's dependency on the HSE infrastructure, based on lessons learned from previous IT disruptions.²²⁵

At the hospital and CHO level, several sample sites had proactively conducted after action assessments²²⁶ of the response to clinical and services continuity events and applied these in a lessons learned programme. Notable examples of this were CUH with comprehensive post event analysis of Storm Emma and laboratory outages. Moreover, examples of populated lessons learned spreadsheets were shared, illustrating that a wider awareness about the importance of a lessons learned process is in place.²²⁷

However, there is insufficient overarching governance and process to ensure that lessons from incident and major emergency response are not just identified, but assigned ownership, addressed, and disseminated to inform structural improvements across the HSE and funded entities. Specifically, where individual reviews were conducted, there was a lack of evidence indicating lessons learned were shared more broadly with other areas of the HSE, and with HGs and CHOs. Actions for implementing lessons learned do not appear to have been assigned owners to ensure they are completed, indicating that while lessons may be identified, they do not systematically lead to improvement or change.

FA2.KR9 Review and refine the post-incident review process to ensure ongoing and continuous improvement of the response capability (see strategic recommendation 4.2 in section 4)

Formal and consistent post-incident reviews should be conducted following all incidents or near misses to capture both areas of positive performance and opportunities for improvement. The Operational Resilience Steering Group should ensure that all post incident reviews are reported centrally to enable learnings to be disseminated across the HSE and funded entities (see also finding FA2.KF1). Mitigating actions should be assigned a responsible owner and tracked centrally until their completion. The process should be reflected in the end-to-end Crisis Management Framework (see also recommendation FA2.KR5.1).

²²¹ Incident Management Framework 2020

²²² Information Management & Coordination Workshop

²²³ Conti Cyber Response NCMT Structures Governance and Admin V1.10 31052021

²²⁴ Programme org chart v1 21.05.21

²²⁵ Communications & Stakeholder Management Workshop

²²⁶ Site Workshop 8 (Hospital B)

²²⁷ Lessons Learned_ Programme Lessons v0.2

Area 6: Human factors and cultural contributors

FA2.KF10 Emergency response was ingrained in the HSE's core operations; HSE staff had a natural ability to respond to emergencies, despite a lack of organisational preparedness

At the time of the cyber attack the HSE was over a year into a multifaceted and prolonged crisis response to the COVID-19 pandemic. All workshop participants stated that staff from all levels across the HSE, impacted hospitals, CHOs and third parties went above and beyond to support the cyber attack response effort.^{228,229,230,231}

In times of significant challenge or emergencies staff across the health service are able to demonstrate resilience, and exhibit efficient and quick decision making grounded in organisational values (e.g. prioritisation of patient service and care). A prevalent theme in interviews is that the staff are 'perpetually responding to emergencies'^{232, 233, 234}, and are therefore naturally skilled at it.

However, the significant majority of individuals interviewed also clearly stated that the HSE was not prepared to manage an event of this magnitude and scale.²³⁵ Clinical and services continuity and crisis *preparedness*, as opposed to emergency *response*, was not evidenced as a corporate priority in the HSE. Interviewees commonly commented that a reactive posture to crisis had largely been normalised and accepted day-to-day practice.²³⁶ The apparent normalisation of crises had led to a predominantly reactive posture towards crisis response, a confidence in the HSE's crisis management capability, and a reduced perceived need for significant advance preparation for wider incidents, organisational crisis or 'black swan' events.

The leadership style and decision-making process required during a crisis is necessarily different than that required during business as usual, even within high tempo, safety critical operations such as health care. Crises are associated with heightened stress

that impacts on the decision-making process, which is made more complex by the constraints of time, the volume of decisions to be made and the scarcity of available information. For example, decisions had to be made in the response to the Conti attack where supporting data was not available and where IT and clinical priorities were not understood or aligned (e.g. the decision to disconnect appliances from the network, made in the absence of a clinical and services impact analysis outlining the critical systems, the impacts to be caused, and service level agreements for recovery).

The consequence of being in perpetual 'crisis response' mode can also create wellbeing impacts on staff members, as illustrated in this case by the level of stress and fatigue experienced by staff members dealing with both the COVID-19 and concurrent cyber attack crises.²³⁷ Chronic stress without recovery, depletes energy reserves, leads to burnout and ultimately compromises the crisis response capability. This can subsequently compound the inability to act and lead clearly, and therefore has the potential to further increase the risk of patient safety incidents and clinical errors as well as further risk of harm to staff. Staff who had been deployed during the COVID-19 pandemic reported returning to their roles feeling fatigued before the ransomware attack; the concurrent crises were unlike anything they had ever encountered and the response was heavily fuelled by staff members' 'can-do attitude'.²³⁸

FA2.KR10 Instil a culture of preparedness in the HSE to reduce the negative impacts of disruption on its people (see *strategic recommendation 4.2* in section 4)

The HSE should aim to create a culture that values and emphasises crisis preparedness as well as having confidence in natural ability to respond to major emergencies. In addition to scenario-specific plans to prepare for crisis scenarios (beyond the current scope of floods, adverse weather and aviation disasters) recommended below (see *also findings FA2.KF8 and FA2.KF21*), the HSE should implement a comprehensive training and exercising programme to familiarise all crisis responders at operational (e.g. hospital/CHO, business support services, IT Security,

228 Information Management & Coordination Workshop

229 Site Workshop 5 (Hospital F)

230 Site Workshop 6 (Hospital C)

231 Site Workshop 1 (CHO B)

232 Site Workshop 2 (CHO A)

233 Site Workshop 4 (Hospital E)

234 Site Workshop 6 (Hospital C)

235 Information Management & Coordination Workshop

236 Communications & Stakeholder Management Workshop

237 Programme RAID Log

238 Healy, O. Dr. A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare IT failure, Dated 30th September 2021.

etc.), tactical (e.g. HSE, regional/area CMTs), and strategic (e.g. HSE NCMT) levels with their roles and responsibilities for crisis preparedness and response, as well as the unique key considerations and decisions required in various crisis scenarios (see also finding FA2.KF8). Conducting scenario-based desktop and simulation exercises will expose individuals to the (simulated) pressures they will experience, thereby reducing the negative impact imposed by external stressors and uncertainty in real life events. Transferring the skills gained in psychologically realistic exercises will facilitate more effective teamwork and decision making in actual crisis situations when they occur.

Crisis Response

Area 7: Notification and activation of NCMT and wider response workstreams

FA2.KF11 Core senior responders were notified and the NCMT invoked quickly; however, the notification of staff and wider stakeholders was ad hoc and did not follow a pre-planned notification process or channel

Core senior responders were notified quickly using best endeavours via phone on the morning of the attack, and the first NCMT meeting was held at 08:30 on the day of the Incident.²³⁹ An initial 'blast' notification was also issued to HSE mobile devices at 14:00²⁴⁰ via Vodafone and Three network providers²⁴¹, in an effort to inform wider HSE staff of the Incident. However, there was no evidence to show this process was formally prescribed and embedded in the Incident Management Framework,²⁴² Major Emergency Framework²⁴³ or a Crisis Communications Plan, nor was it aligned to an incident severity matrix to ensure the correct level of response was activated and involved (see also finding FA2.KF14). It was noted during interviews with several stakeholders, and in the *Lessons Learned Log* that receipt of the initial notification text was ad hoc and did not reach all HSE staff members and contractors.^{244, 245, 246} This was in

part because the recipient list did not include staff members or contractors on non-HSE devices.

Interviewees noted that as a result of the ad hoc notification process, some staff members and contractors first heard of the attack on the local news, or by experiencing the effects of the ransomware attack first hand. Others received multiple notices from various parties (including impacted hospitals) and through multiple channels, while some never received an initial notification.²⁴⁷

FA2.KR11 Design and implement an integrated notification and escalation process and acquire a means of mass notification to all HSE staff and contractors (see tactical recommendation 3.1 in section 4)

The HSE should implement a uniform and integrated notification and escalation process within the updated end-to-end response framework, supported by an Incident Classification and Severity Matrix and an 'Activation Membership' list detailing the stakeholders to be informed, across all levels of response, depending on the severity rating of that incident. This will allow critical responders to be notified of an event and convene at pace to instigate a response at the appropriate level to any incident or crisis impacting its operations or services.

The HSE should review whether the use of mobile phone network providers as a method of sending 'blast notifications' meets the required functionality for mass notification and, if not, should consider investing in a mass emergency notification and communications tool to improve its wider incident notification capability. The solution should include features for notifying all HSE staff members and contractors or smaller groups of staff about any serious incident, crisis or clinical and services continuity event (e.g., a data leak where formal notification and information needs to be disclosed with impacted persons, physical or medical events requiring safety instructions to be issued, or a total system outage/ransomware attack). Clear authority should be designated to an individual or individuals with an appropriate level of authority to send communications from this platform, to ensure all messages are consistent and have been signed off by the appropriate parties (e.g. legal).

239 Conti Cyber Response NCMT Structures Governance and Admin V1.10 31052021

240 Minutes of Cyber Attack MI Meeting 12 pm - 14052021

241 Information Management & Coordination Workshop

242 Incident Management Framework 2020

243 A-Framework-For-Major-Emergency-Management

244 Lessons Learned_ Programme Lessons v0.2

245 Site Workshop 2 (CHO A)

246 Site Workshop 5 (Hospital F)

247 Site Workshop 4 (Hospital E)

Area 8: Response structures, resourcing and logistics

FA2.KF12 The HSE did not follow a pre-defined and consistent crisis management structure in the initial phase of the response

Although the HSE ultimately established an effective crisis management structure during their response to the ransomware attack, it was designed reactively to apply to this specific incident.

The first NCMT meeting was convened less than four hours after the IT Critical Incident Process was invoked,²⁴⁸ in part due to the familiarity of operating NCMT established during the COVID-19 response.²⁴⁹ While invocation was prompt, several stakeholders noted that the initial supporting structures feeding into the NCMT were inconsistent and at times conflicted.²⁵⁰ Both the Regional CMTs²⁵¹ and the Area CMTs²⁵² were initially stood up based on different documentation, and subsequently stood down when alternate response governance structures, linking directly to the HGs and CHOs, were agreed.

Technology-focused response and recovery workstreams were established in parallel to the CMTs but were not reflected in any of the initial Emergency Response or Incident Management documentation. Additionally, a clinical and integrated governance structure (which later became the integrated clinical and operational risk subgroup of the NCMT) was set up to capture risks, guide the operational response based on clinical priority, and in an effort to establish clear communications between clinical operations and IT. This was a critical group that ultimately influenced the prioritisation of the recovery of the IT systems to enable the resumption of clinical services. Stakeholders noted that the legal workstream had not been considered as a required workstream for an emergency or incident response prior to the attack. Finally, it was identified in the *Lessons Learned Programme Log* that central reporting was difficult due to the way individual workstreams were established in silos and without clear central guidance (see also finding FA2.KF18).²⁵³

The lack of integrated programme management was recognised as a risk by the HSE five days into the response.²⁵⁴ This led to a request for assistance from the Defence Forces who established defined information management processes which were 'scalable and agile'²⁵⁵ and could cope with the complexity of a cyber crisis. Stakeholders interviewed noted a recurring sentiment that the Defence Forces' intervention was critical in allowing the HSE to establish tighter governance, better communication flows and create mental space for responders to focus on remediation and recovery activities.^{256, 257}

FA2.KR12 Establish a Crisis Situation Centre to manage an organisation-wide response to a crisis (see recommendation FA2.KR5.1 and strategic recommendation 4.2 in Section 4)

As part of the Crisis Management Framework (see recommendation FA2.KR5.1), the HSE should establish a Crisis Situation Centre construct to be stood up during a crisis response. This should incorporate the learnings from the Situation Centre introduced by the Defence Forces during the Conti response and include the following elements: Guidance on how and when it should be invoked in line with the Incident Classification and Severity Matrix (see also recommendation FA2.KR14);

- Guidance on how and when it should be invoked in line with the Incident Classification and Severity Matrix (see also recommendation FA2.KR14);
- The hierarchy of teams required;
- Roles and responsibilities and delineated decision authority of each response level;
- Escalation thresholds and formalised communication channels;
- Agreed touchpoints and interaction between the Situation Centre and HGs and CHOs;
- Tools and templates to be used by all responders (across the HSE, HG and CHO levels) during an incident (e.g., situation report, classification and severity matrix, impact assessment, decision and action logs).

248 Conti Cyber Response NCMT Structures Governance and Admin V1.10 31052021

249 Information Management & Coordination Workshop

250 Lessons Learned_ Programme Lessons v0.2; Information Management and Coordination Workshop

251 Emergency Management Services Delivery Plan 2019 - Regional CMTs

252 HSE EM Interim Governance Arrangements Jan 2020 - ACMTs

253 Lessons Learned_ Programme Lessons v0.2

254 Programme RAID Log

255 Information Management & Coordination Workshop

256 Information Management & Coordination Workshop

257 Communications & Stakeholder Management Workshop

FA2.KF13 There was lack of oversight and structure to the coordination and integration of third party support

The HSE recognised the need for additional resources and specialist skills and engaged third parties for incident response,^{258, 259} legal and forensics support early on. The impact of the Incident on a national scale encouraged goodwill from third party support and vendors, including the provision of pro bono work. The HSE was aware of the reliance they were placing on third parties and set objectives for each, to ensure they did not undertake activities beyond the required time period. The HSE also took ownership of tasks when sufficient progress was made and the internal resources became available.

It was noted in interviews that a significant amount of time was spent onboarding and integrating third parties, particularly educating them on the intricacies of the health sector and for example, differences between voluntary and statutory hospitals.²⁶⁰ Stakeholders also noted that data gathering activities were duplicated because HSE staff did not have visibility of third party activity or miscommunication between third parties and internal teams. This diverted focus from other efforts during the critical early stages of the response. The visual representation of each team's priorities at CityWest several days into the response addressed some of these issues, as it allowed responders to deconflict their activities and re-engineer their approach where required.

FA2.KR13 Establish formal retainers with key third parties that may be required to support a crisis response (see tactical recommendation 3.3 in Section 4)

The HSE should consider the third party support that may be required during an incident, including: crisis response, external legal counsel and public relations. These retainers should include service level agreements, clear descriptions of third party roles and responsibilities, and pre-agreed legal requirements (such as non-disclosure agreements) to ensure partners can be engaged to support, and be integrated into, a response immediately and scale to the size of the response required.

Work should be conducted with third parties providing technical support to familiarise them with the HSE's IT network, architecture and systems, to facilitate quicker engagement during an incident. The role of retained third parties should be reflected in response plans or playbooks and they should be involved in regular cross-organisation conversations and training exercises with the HSE, the HGs and CHOs to rehearse efficient coordination and communication flows.

Area 9: Information and data management in a crisis

FA2.KF14 The initial impact assessment was hindered due to the absence of an HSE-wide incident severity matrix

There was no integrated HSE-wide Incident Classification and Severity Matrix to guide the initial impact assessment following the attack. The 'HSE Risk Impact Table' in the *HSE Incident Management Framework* lists five impact levels from Negligible to Extreme across eight different categories.²⁶¹ While those categories reflect a spectrum of operational, financial, compliance and reputational impacts, there was no evidence to indicate that the initial impact assessment conducted during the ransomware attack was based on this guidance and subsequently used to inform decisions made and actions taken. There was also no evidence provided of an Incident Severity Matrix for IT or cyber incidents, specifically.

The *Managing a Major Incident* document is designed to be used in a 'critical' incident that attracts 'more attention or has a greater impact than "normal" critical incidents';²⁶² however, there were no associated definitions for those thresholds. It was also unclear how the impact assessment from an IT incident would be aligned with that of the 'HSE Risk Impact Table'. In the absence of an *integrated* HSE-wide Incident Classification and Severity Matrix (see also finding FA2.KF12), response teams did not have clear thresholds and criteria to assess the (actual and potential) business, operational, financial and reputational impacts of the cyber incident. As a result, the initial response centred on understanding 'the what', rather than quantifying the impact to inform and set the strategic response strategy for effective decision making.

258 M_HSE_Intrusion Investigation Report - REDACTED (FINAL).pdf, 2021

259 Minutes of Cyber Attack MI Meeting 10 am - 14052021

260 Site Workshop 9 (Hospital H)

261 HSE-2020-incident-management-framework-guidance

262 Managing a Major Incident v1 1 and IT Security Incident Plan

FA2.KR14 Develop an integrated HSE-wide incident classification and severity matrix for assessing the organisational impact of an incident (see strategic recommendation 4.2 in section 4)

The HSE should ensure it includes clear criteria to determine the level of actual and/or potential likely impacts of the Incident, and align with or supersede the 'HSE Risk Impact Table'.²⁶³ It should consider specific impact categories - operational, clinical, reputational, financial, regulatory/legal - and a method for estimating impact based on impact and likelihood.

This should be embedded across all organisational response plans and align with any technical severity matrices, such as those in a technical cyber response plan, to support consistency in response. This will ensure responders are using a consistent approach to anticipating immediate, ongoing and future impacts to support a shared situational awareness.

FA2.KF15 The lack of pre-defined information sharing processes led to inefficiencies in the creation of a shared understanding of the Incident

As mentioned in *finding FA2.KF12*, the tools and processes introduced by the Defence Forces on 18 May, enabled a more efficient meeting tempo and information management. Information sharing channels with HGs and CHOs via nominated liaison officers and coordinators subsequently also took shape.²⁶⁴

Several stakeholders noted that the sheer number of coordination and information sharing meetings required placed a strain on several critical HSE stakeholders, who struggled to attend all meetings and/or action response and recovery tasks.²⁶⁵ Interviewees from several HGs and CHOs also reported that some initial meetings with the HSE were time consuming, oversubscribed and, at times, difficult to follow.²⁶⁶ A recurring theme was that technical jargon generated confusion and delayed decisions and actions. The lack of in-report standards and a clear definition of what constituted 'Red', 'Amber' and 'Green' also led to initial confusion.²⁶⁷

There were instances when HGs and CHOs sent requests for clarification and further support, but did not receive a response and were unclear about how to proceed.²⁶⁸ Similarly, some hospital stakeholders

cited an example where ICT staff had been deployed to their site to clean laptops, but the hospital leadership were unaware that they were present and were still trying to work with the HSE to organise their attendance.²⁶⁹ These differing understandings may also have been compounded by use of unapproved or informal channels for communicating with stakeholders; for example many interviewees noted they resorted to individualised phone calls, WhatsApp and text messages to relay or obtain information first hand where relationships existed.^{270, 271}

FA2.KR15 Designate and train incident information managers (or coordinators) at all levels across an incident or crisis response to maintain a consistent overview of the situation as it develops (see strategic recommendation 4.2 in section 4)

Further to *recommendation FA2.KR12*, the HSE should ensure that each workstream beneath the SITCEN, at every command level and workstream, has an information manager (or coordinator) appointed as part of the Incident response team. This role should be implemented in all local hospital response teams, Regional/Area CMTs, and within each HSE workstream up to the NCMT. As the information manager completes their expected role (digesting all information to gain a view of the end-to-end incident), they should escalate their status and update upwards (as with the SITREPs). This will allow the SITCEN information manager to articulate one consolidated account of events, decisions and actions which will achieve situational awareness across all teams and parties involved.

To embed this capability the HSE should train those who have been assigned the role of information manager/coordinator and complete multi-team exercises to rehearse information sharing between teams to maintain situational awareness. Templates created as a result of the ransomware attack should be further developed and embedded into scenario-specific response plans, in order to support the information managers in their role. This structure and format should be used in all teams and work streams to maintain consistency.

²⁶³ HSE-2020-incident-management-framework-guidance

²⁶⁴ Information Management & Coordination Workshop

²⁶⁵ Programme RAID log

²⁶⁶ Programme RAID log

²⁶⁷ Lessons Learned_ Programme Lessons v0.2

²⁶⁸ Site Workshop 11 (Hospital A)

²⁶⁹ Site Workshop 7 (Hospital G- identifier to be removed from final report)

²⁷⁰ Site Workshop 1 (CHO B)

²⁷¹ Site Workshop 10 (Hospital I)

FA2.KF16 There was no pre-agreed 'out-of-band' technology solution to support coordination, collaboration and information sharing during a crisis response

The HSE's communications and information sharing platforms were severely impacted by the attack. A patchwork of technology solutions were brought together to address this gap. The NCSC introduced [REDACTED] - a secure online chat and file sharing platform - to support the HSE in coordinating and collaborating during the initial incident response. The HSE set up 'clean' email accounts for a handful of key responders on a new HSEmail.ie domain²⁷² and leadership issued a special derogation and guidelines for HSE staff to use personal emails for information sharing.²⁷³

The Defence Force SITCEN Information Manager established a directory and information sharing structure on a Teams instance to facilitate centralised coordination, collaboration and information sharing; however, it was noted that not all workstreams were storing their documentation in the Teams instance.²⁷⁴

More widely, HSE staff defaulted to the use of WhatsApp, text message and phone calls to share information. Stakeholders from HGs and CHOs also noted in interviews that, in some instances, they procured their own domains and IT infrastructure in order to communicate and share information.²⁷⁵

This ad hoc approach ultimately provided a means by which to share information; however, these solutions had not been pre-agreed, risk assessed or authorised for use by the HSE during 'prepare' phases prior to the Incident, nor were incident responders and staff made aware before the Incident that they should be used. As a result, the HSE, HGs and CHOs lacked a centralised and secure information sharing, collaboration and coordination platform from the outset of the Incident. This impeded the initial response efforts, as well as leading to a long data remediation tail (see also finding FA2.KF23).

FA2.KR16 Identify and acquire a secure and resilient 'out-of-band' technology solution to ensure an alternative means of information sharing and communication (see tactical recommendation 3.1 in section 4)

The HSE should ensure that the platform can facilitate email, file sharing, call hosting and the dissemination of communications to all staff and segmented audiences, and enable all responders to see situations reports, actions and decisions logs and other information necessary to support a shared understanding of the Incident.

Area 10: Response leadership, strategy setting and decision making

FA2.KF17 The overarching response strategy was underpinned by the core HSE value of patient care; however, the initial response was driven by technology priorities

It was widely acknowledged by stakeholders that the HSE's prioritisation strategy in the first week of the Incident was driven by the OES list, informed by regular communication between the HSE's OoCIO and COO functions and input from the CCO.^{276,277,278} Stakeholders noted that the response strategy progressed to an approach that focused on clinical risks and the recovery of end-to-end clinical services, underpinned by the core HSE value of patient care, following the co-location of all responders to City West.²⁷⁹

The introduction of a 'higher organisational intent' directed at restoring systems that enable patient care was formalised on day 11 of the response and reflected in the daily SITCEN meeting rhythm, which were aligned to facilitate a service-led response strategy.^{280, 281} This service-led approach was then consistently adopted and ensured patient care was at the heart of all decisions made. The HSE would have benefited from taking this approach earlier in the response to allow for a more efficient recovery

272 RAID Log, HSEmail.ie was agreed on 17 May 2021

273 Letter to all Staff - 1 on 26 May 2021

274 Lessons Learned_Programme Lessons v0.2

275 Site Workshop 11 (Hospital A)

276 Information Management & Coordination Workshop

277 Clinical Risk Group Workshop

278 Site Workshop 4 (Hospital E)

279 Site Workshop 11 (Hospital A)

280 20210524-Morning Update Brief - FINAL

281 20210525-Morning Update Brief - FINAL

programme, ultimately reducing impact on patient care.

FA2.KR17 Ensure the ‘higher organisational intent’ is aligned to the organisational values and drives the response and recovery strategy; review the strategy regularly throughout the response as the situation develops (see strategic recommendation 4.2 in section 4)

In this incident, the strategic priority was the restoration and protection of systems underpinning patient care services. The HSE should ensure that all incident response strategies consider both the technical and business response priorities, and are informed by the impacts and requirements of the hospitals, HGs and CHO.

Patient care may not always be restricted to the maintenance of healthcare systems; the possible implications of patient data exposure should be considered in conjunction with discussions on patient care, and incorporated into the HSE’s strategic intent during a response. Consideration should be given to how this strategy is cascaded to all levels of the organisation, to direct the actions of the tactical and operational response teams (see finding FA2.KF19) and to inform the activities of third party support.

The response strategy should be reviewed regularly during a response based on new information and circumstances to ensure it is still valid and appropriate. The development and implementation of a response strategy should be a key focus during crisis exercising, as this will facilitate a single consistent approach to response and recovery activities.

FA2.KF18 There was a lack of clearly defined and delineated decision making authority between the HSE, HGs and CHOs in the case of an HSE-wide crisis

Several interviewees noted that there was no strategic Crisis Management Plan or cyber response guide with a clearly defined and documented decision making process for senior leadership to follow, in the event of a total IT outage or cyber crisis.²⁸²

Senior HSE leadership exhibited agile, yet reactive, decision making in the absence of guidance that was driven by organisational values, and grounded in judgement and experience acquired from managing previous crises (see also findings FA2.KF7 and FA2.KF19). There was limited evidence of formal and documented decision-making authorities between the HSE, CHOs, HGs/hospitals during an HSE-wide crisis (see also finding FA2.KF12). Existing service level agreements between these organisations did not include provision for these authorities,^{283, 284, 285} and while the Incident Management Framework identifies the need for decision-making authority, no specific details were provided.²⁸⁶ Interviewees reported that this led to some confusion at the beginning of the response.²⁸⁷ The autonomy under which Voluntary hospitals operate makes centralised decision making more complex if the restrictions, constraints and permissions around decision making authority are not formally agreed and documented in advance.

For example, some hospital stakeholders reported that the unilateral HSE decision to disconnect national systems did not take into consideration the level of system dependencies between the HSE, HGs/hospitals and CHOs, and potential risks associated with rapid disconnection.²⁸⁸ There was also no evidence to indicate that the authority for that decision was documented and agreed.^{289,290} Conversely, some hospital and CHO stakeholders noted that local decisions were taken contrary to HSE guidance when deemed in the hospital’s or CHO’s best interest.²⁹¹

FA2.KR18 Agree delineated decision making authority across all teams in the organisation likely to be involved in an organisation-wide incident (see strategic recommendation 4.2 in section 4)

The HSE should establish an organisational crisis management structure, incorporating hospitals, HGs, CHOs and contracted third parties, which clearly defines the decision making authority at each level. This structure should be socialised and embedded as part of a regular training and exercising programme for all responders (see finding FA2.KR8.3) to ensure it meets the different priorities of all parties and remains fit for purpose. Additional training should be provided

282 Lessons Learned_ Programme Lessons v0.2

283 Site Workshop 6 (Hospital C)

284 Information Management & Coordination Workshop

285 Site Workshop 11 (Hospital A)

286 Incident Management Framework 2020

287 Site Workshop 4 (Hospital E)

288 Programme RAID Log

289 Site Workshop 6 (Hospital C)

290 Site Workshop 11 (Hospital A)

291 Site Workshop 11 (Hospital A)

for the HSE, HG and CHO leadership to support them in:

- creating a shared situational awareness across multiple sites or locations;
- developing effective communication flows between senior leadership across multiple sites or locations;
- establishing clear decision making and delegated authority for senior leadership across multiple sites or locations.

Critical stakeholders or response team members at every level should therefore receive communication about, and be trained and exercised in, the predefined response structures to ensure the hooks and handovers within every level of the command model is understood and seamless during an incident.

Area 11: Stakeholder management, crisis communications and reputation management

FA2.KF19 The lack of internal communications tools and diffuse nature of the health service hindered the ability to send nuanced and targeted messages to staff

The HSE Communications team managed the external communications and media agenda effectively, ensuring the focus of reporting was consistently brought back to patient service and care implications. Through interviews and workshops it was evident that EMT members involved in media messages displayed a consistent and informed approach, receiving support and coaching from the experienced senior Communications team members before any public event.²⁹²

In contrast, the internal communications capability was stretched to meet the demands of the Incident (see also finding FA2.KF6). The absence of a comprehensive mass emergency notification and communications tool meant only staff with HSE devices received the initial 'blast' messages (see also findings FA2.KF6 and FA2.KF7). There was no pre-prepared method by which to communicate with

staff in a segmented manner, therefore there was no capability to target different messages to distinct groups of staff. This was exacerbated by the vast and diffuse structure of the HSE, including multiple disparate smaller community organisations. The Internal Communications team ultimately facilitated a workaround whereby updates were published on the publicly available HSE website, and staff were directed via phone calls and social media to check for updates.²⁹³

Stakeholders noted that improvements to the internal communications capability were made following WannaCry in 2017 - replacing the 'antiquated' intranet with a new website - and the internal Communications Team was formally established in 2019; however, the capability is not adequate for responding to crises of this magnitude.²⁹⁴

FA2.KR19 Familiarise the Internal Communications Team with the 'out of band' technology solution to enable focused and targeted communications during a crisis (see also recommendation FA2.KR16 and tactical recommendation 3.1 in section 4)

The HSE should set up user accounts for all staff members pre-incident on the selected 'out of band' communication platform to expedite transition to the new platform during a system outage. Staff members should be familiarised with the platform and its functionality ahead of an incident. Details for all alternative user accounts should be recorded centrally and stored offline to ensure contact information for all staff members is readily available during any disruption to the HSE's standard communications channels. Crisis response and communications workstream leads should establish cascading contact trees to notify staff of an incident, to initiate the use of the out of band platform, and to enact specific channels for the discussion of response and recovery activities between core responders. This will allow workstreams to maintain a central repository of useful information and act as an audit trail for post incident review and reporting.

FA2.KF20 Potential data exposure has heightened risk to patients and created long remediation requirements

The HSE took several steps to manage the impact of potential data exposure following the cyber attack, despite the absence of scenario-specific plans²⁹⁵ and related workstream structures reflected in the MEM or IM Frameworks (see also findings FA2.KF5

292 Communications & Stakeholder Management Workshop

293 Communications & Stakeholder Management Workshop

294 Communications & Stakeholder Management Workshop

295 The Data Protection Breach Management Policy provides high level guidance but does not include specific steps for a ransomware scenario.

and FA2.KF12). They established the Legal and Data Workstream on the 19th of May to:

- Oversee the response and investigation from a legal and data protection perspective arising from the cyber attack;
- Maintain a consistent approach to data protection and legal actions to ensure all regulatory requirements are met;
- Support the Data Protection Officer (DPO) in coordinating the data protection investigation and reporting to the Data Protection and Commission;²⁹⁶
- Assist and report on the ongoing investigation of An Garda Síochána²⁹⁷

Related decisions, such as informing the Data Protection Commission (DPC),²⁹⁸ obtaining a court order to prevent the publication and sharing of stolen data and setting up web monitoring services,²⁹⁹ were actioned quickly to mitigate the potential impact of data loss. A Legal and Data Steering Committee was subsequently set up to oversee risk-based decisions relating to the approach to, and threshold for, breach notification to data subjects whose data may have been compromised and the wider public.³⁰⁰ Third parties were also called on to support this risk assessment. This work is ongoing and may continue for an extended period of time as the HSE reviews and seeks to mitigate any risk to data subjects' rights and freedoms. While thresholds for notification have been identified, the HSE is in the early stages of scenario and resource planning of the actual notification process, including the liaison with the HSE Communications team on how these notifications should be rolled out. As such the HSE has not yet made any data subject notifications, and no standard resources or templates for notification exist, or have yet been tailored/created for this event. The HSE continues to work closely with funded entities to understand the extent of the potential data exposure and share their risk assessment methodology for notification threshold.

FA2.KR20 Review processes, plans and resourcing for response to future potential data breaches (see strategic recommendation 4.2 in section 4)

The HSE should ensure the appropriate resources, tools and templates are created with sufficient advance notice and time prior to notifying data subjects of a breach. Having initial notification letters, FAQ's, responses, and sufficiently trained resources

to manage an influx of requests for information will be critical to ensuring a successful roll out of notification if and when required. The HSE should also review and document the processes established during the response to support their future preparedness. They should:

- Complete the work of the Legal and Data Workstream in response to the Incident. This includes reconciling all medical data stored and managed through interim processes post the attack, including data stored on personal devices/ accounts and in paper form;
- Embed the Legal and Data Workstream in the Crisis Management Framework (see also recommendation FA2.KR5.1 and FA2.KR12);
- Update the existing Data Protection Breach Management Policy to support the Legal and Data Workstream in future responses, including the data breach notification risk assessment;
- Rehearse the workstream's response both individually and as part of wider HSE exercising programme (see also recommendation FA2.KR8.3);
- Agree retainers with third parties for future web monitoring services;
- Ensure materials used to support the notification of data subjects, such as letters, FAQs and talking points, are agreed with the Communications Team;
- Conduct resource planning for future notification programmes; for example, call centres to respond to the significant influx of incoming requests once data subjects are notified.

Area 12: Scenario planning

FA2.KF21 Scenario planning did not inform response and recovery strategies

Stakeholders stated that, despite having dealt with a vast array of major emergencies, they felt ill-prepared for dealing with an IT outage or cyber crisis of this scale, or a specific ransomware attack (see also finding FA2.KF8). Specifically, individuals initially struggled to comprehend the scale and size of the Incident, and felt unable to foresee the contingent

296 Terms of Reference - Cyber Attack Legal and Data Workstream Steering Group June 2021

297 Terms of Reference - Cyber Attack Legal and Data Workstream Steering Group June 2021

298 DPC Report 15 July 2021

299 Data Protection Monitoring Process

300 Terms of Reference - Cyber Attack Legal and Data Workstream Steering Group June 2021

impacts that may occur over time.³⁰¹ As with many organisations impacted by ransomware attacks, there was initially a belief that the Incident would cause impact for several days to weeks, before a realisation dawned that these types of events, and their longer term impacts, play out over several weeks and months.

This uncertainty stemmed, in part, from a lack of any formal scenario planning process within the existing Major Emergency Management and Incident Management Frameworks and pre-prepared scenario-specific playbooks. Scenario-specific playbooks define the likely decisions and actions required of a senior team, given the potential risks and impacts of the scenario (*see also finding FA2.KF5*). The existence of a cyber response plan or ransomware playbook would have supported the NCMT's ability to foresee the likely impacts and consequences of the Conti attack, combatting what one stakeholder described as 'a failure of imagination'.

The HSE also does not have a formal overarching process or system to guide the use of scenario planning *during* crisis response, in order to inform the response and recovery strategy during an incident, irrespective of the nature of that event. This would involve identifying potential triggers and escalators for the worst, best and most likely scenarios; identifying consequent likely impacts; and implementing mitigating measures. While some stakeholders noted they were able to conduct hasty scenario planning during the Incident, particularly when determining patient care workarounds, this was performed in an ad hoc fashion at the hospital or CHO level.

FA2.KR21 Scenario planning should be informed by the risk register, the process embedded in the Crisis Management Plan, and the activity conducted throughout incident and crisis response (*see strategic recommendation 4.2 in section 4*)

The HSE should ensure that the risk register is used to drive the creation of severe but plausible scenarios against which the HSE should validate its resilience capability is validated. The process should be extended to engage individuals from the HSE's senior leadership team, risk management, clinical and services continuity and crisis management disciplines in regular scenario planning against the organisation's

top risks.^{302,303} This is best conducted in a workshop format to identify potential political, economic, sociological, technical, legal and regulatory, environmental and organisational impacts related to each of the HSE's top risks, and to then explore the worst, best and most likely scenarios for each.

Mitigating actions resulting from these workshops should be assigned to an owner with the appropriate level of authority to facilitate organisational change where required, and tracked throughout their lifecycle to confirm they are completed to an acceptable level. These actions and all other outputs from these activities should be used to inform preparation activities across resilience disciplines, to ensure that plans, processes and structures are fit for purpose; and where applicable specific response plans to be developed for the most plausible risks (*see also findings FA2.KR5.2*).

Scenario planning should be included in the Crisis Management Plan to support HSE to prepare for likely outcomes and mitigate subsequent impacts during a response.

Area 13: Effectiveness of workarounds

FA2.KF22 Emergency workarounds implemented across the HSE, HGs/hospitals and CHOs were ad hoc and not always based on predefined solutions or processes, and have caused long remediation tails.

It was widely reported that responders across the HSE, HGs/hospitals and CHOs implemented timely and agile workarounds that allowed core critical processes to continue in the absence of IT.^{304, 305 306}

The lack of preparedness for a cyber incident of this scale, including a lack of Clinical and Services Impact Analysis and scenario-specific playbooks for cyber response, meant that whilst many workarounds were pre-agreed and rehearsed, others were defined in an ad hoc manner; as there was no systematic approach to maintaining continuity of patient-critical processes (*see also findings FA2.KF3, FA2.KF4 and FA2.KF23*).

In some cases, predefined workarounds were familiar to responders and well-rehearsed, for example, where clinicians were able to switch from digital to paper-

301 Information Management & Coordination Workshop

302 The CRR should inform the development of severe but plausible scenarios against which Crisis Management Teams are exercised. The timing, nature and extent of testing should reflect the criticality of the underlying recovery solution / activity

303 CRR Q1 2021 Review Report Final post EMT meeting 27 04 21 v1.0 27 04 21

304 Site Workshop 6 (Hospital C)

305 Communications & Stakeholder Management Workshop

306 Information Management & Coordination Workshop

based procedures.³⁰⁷ However, several stakeholders noted that the workarounds were primarily designed for individual systems or processes and proved to be time limited, thereby not suitable for continued use throughout the recovery from a total and lasting IT outage. Additionally, whilst staff in community service environments had experience relying on paper patient charts and were able to adapt quickly, the after action review (AAR) collated by the HSE identified that some staff (clinical and non-clinical) had never worked in a paper-based system and so risked missing relevant information from the different format used in paper documentation.³⁰⁸ This introduced a risk of information loss if it was not ultimately uploaded into the patient data management system.

Other workarounds, although creative, were devised during the Incident and, as a result, had not been reviewed from an overarching security or risk perspective. Many workarounds were documented as issues in the Programme RAID Log,³⁰⁹ such as the use of runners to convey lab samples and test results, and the use of whiteboards and shared excel sheets on standalone laptops to populate hospital bed bureaux, due to the increased risk of human error. The risks associated with the continuation of clinical treatment and the use of operational workarounds were assessed and communicated on a regular basis, including clinical guidance on how treatments should be prioritised and managed.^{310, 311} Many of these workarounds carried a risk of loss or contamination of patient data, misplacement of patients and incorrect disclosure of patient data, all with a secondary risk of patient care being negatively impacted. One example quoted during interviews that illustrates the lack of accurate patient data, was of a surgeon questioning the whereabouts of a patient due for surgery, when that patient had already been operated on.

Several of the emergency workarounds established to support information sharing and allow individuals and teams to respond at pace, such as the use of personal emails and devices, WhatsApp and paper records, have resulted in an ongoing data remediation risk. Many stakeholders noted that some of the workarounds implemented were not designed with consideration of the need to consolidate and retrofit data when systems were restored.^{312, 313} Whilst some interviewees noted they had hired extra resources to manually enter paper-based clinical information to restored systems, the absence of IT systems has

resulted in large volumes of paper records, some of which are likely to include duplicate, incomplete or incorrect data that will need to be investigated and remediated. The backload of COVID-19 data in conjunction with the clinical data from the ransomware attack will likely take considerable time, people and resources to rectify.

The HSE issued a communication on 12 August 2021 to stand down the use of personal emails and ensure all data was deleted from local storage areas.³¹⁴ However, some stakeholders from hospitals and CHOs reported they have not received clear guidance on the steps required to address this risk. The absence of an assigned owner for the remediation of clinical data will make it difficult for staff members to direct enquiries relating to correct data handling and remediation, resulting in delayed resolution of the issue.

FA2.KR22.1 Design clinical and services continuity workarounds, informed by the Clinical and Services Impact Analysis (see *strategic recommendation 4.1 in section 4*)

The HSE should design and agree clinical and services continuity workarounds, for critical processes, with the agility and governance to be maintained for a prolonged period, and based on the Clinical and Services Impact Analysis (see *also recommendations FA2.KR3.1, FA2.KR4 and FA2.KR23*).

FA2.KR22.2 Design workarounds to support rapid data remediation post-incident or crisis (see *tactical recommendation 1.2 in section 4*)

The HSE should:

- Establish a pre-agreed out of band communications and information sharing platform (see *also finding FA2.KR16*) to ensure data generated by workarounds outside normal operations is captured in a format that can easily be retrofitted with the information held on HSE systems. As part of the organisation's stand-down process, each site and workstream should assign an individual with responsibility for overseeing the consolidation of patient and service data; and
- Reconcile all medical data stored and managed through interim processes post the attack,

307 Site Workshop 11 (Hospital A)

308 Healy, O. Dr. A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare IT failure, Dated 30th September 2021.

309 Programme RAID Log

310 CCO Clinical Memo 1 15.05.2021

311 CCO Clinical Memo 2 21.05.21

312 Site Workshop 1 (CHO B)

313 Site Workshop 5 (Hospital F)

314 Temporary Use of Personal ICT Resources.msg

including data stored on personal devices/ accounts and in paper form.

FA2.KR22.3 Rehearse workarounds in multi-team exercises (see strategic recommendation 4.2 in section 4)

The HSE, HGs and CHOs should participate in multi-team exercises to explore how high impact or likely scenarios could impact their operations. This is extremely important as it helps identify likely and potential impacts to the organisation and responders. These may often need a team and significant investment to resolve, however even the discussion and establishment of hypothetical workarounds will likely reduce the number of ineffective emergency protocols and allow space for creative thinking to consider the ideal solution for all parties involved (see also recommendation FA2.KR8.3).

FA2.KR22.4 Consider a review to establish the longer term clinical impacts of the Conti attack (see strategic recommendation 4.2 in section 4)

Finally, the HSE should consider conducting a review to understand the longer term clinical impacts that resulted from the Conti attack. This review should build on the findings of the draft research report into the effectiveness of the patient safety risk mitigation strategies following the Incident,³¹⁵ and inform future steps to improve the HSE resilience against potential future attacks and minimise the risk to patient care.

Crisis Recovery

Area 14: Services and data led recovery strategy

FA2.KF23 The lack of a comprehensive, current and accessible Clinical and Services Impact Analysis, Configuration Management Database, and asset register delayed recovery efforts

Whilst the HSE were clear in their intent to prioritise patient care and maintain its OES list, without an up to date clinical and services Impact Analysis or configuration management database (CMDB) response teams were initially unable to assess resource requirements and prioritise the recovery of critical services.

As part of the incident response, the HSE established a data workstream to build an understanding of all applications and their dependencies for recovery, collating data from unaffected systems, existing documentation and undocumented knowledge from HSE staff and supporting vendors. The requirement to build this list and then prioritise applications for recovery *during* the Incident, rather than being able to rely on an (offline and accessible) *pre-prepared* Clinical and Services Impact Analysis, Configuration Management Database and asset register, delayed recovery efforts. The HSE also noted in their *Lessons Learned Log* that the complexity and disparate ownership of the HSE IT combined with the lack of an overarching impact assessment (see also finding FA2.KF14), made it difficult to plan the recovery efforts.³¹⁶

The recovery priorities set centrally by the HSE initially focused on the priority restoration of core national applications, e.g., NIMIS.³¹⁷ While this approach was widely agreed, the subsequent prioritisation of the smaller and more disparate applications, particularly at the hospital and CHO level, was less straightforward. Stakeholders noted that following the restoration of core national applications, some peripheral applications used by CHOs (such as [REDACTED]) to communicate with patients and carers, were not prioritised adequately given their place underpinning critical CHO services, due to a lack of perceived importance.

Services were prioritised into three classifications: category A (national core applications), category B (major clinical applications) and category C (priority applications).³¹⁸ Applications moved between these categories throughout the response based on recommendations made during the daily Major Incident meetings. Responders attempted to prioritise systems based on the effectiveness of workarounds, and how long they could be maintained. However, this approach did not consider the connections between systems requiring restoration. A recurring finding was that several applications reported to be 'green' were not yet functional at the time of reporting, due to a lack of data on the dependencies between impacted infrastructure, applications and data. One example of this is when access to IPMS was initially blocked by delays in the restoration of Active Directory and Citrix,³¹⁹ a delay that took over two weeks to fix, postponing the resumption of business as usual services. The recovery of systems requires the restoration of trusted network connections and information exchanges, all of which

315 Healy, O. Dr. A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare IT failure, Dated 30th September 2021.

316 Lessons Learned_ Programme Lessons v0.2

317 App Priority List - 20210601 1415 and Site Workshop 7 (Hospital G)

318 Minutes of Cyber Attack MI Meeting 11 am - 18052021

319 Programme RAID Log

rely on a clear understanding of which systems are interconnected, and what is required for them to work together.

There was also limited consideration of how the IT landscape differed at a central and local level; CHOs and HGs found that third parties brought in to support the prioritisation and restoration of applications did not have a strong understanding of the local environments and their requirements for recovery, impeding the ability to set clear and sequenced recovery priorities.

FA2.KR23 Ensure the Clinical and Services Impact Analysis is informed by an up-to-date asset register and Configuration Management Database (see also findings FA2.KF3 and FA2.KF22.1 and tactical recommendation 1.3 in Section 4)

As part of this process, the HSE should work with CHOs and HGs to develop a clear overview of the interdependencies between all departments and local sites using HSE infrastructure or services, with the aim to create a prioritised list for systems at both a central and local level. This should be informed by a service model for delivering patient care. The HSE should reconcile all medical data stored and managed through interim processes post the attack, including data stored on personal devices/accounts and in paper form (see also finding FA2.KR22.2).

Contingency plans should be developed by the business owners and IT teams to maintain priority and critical services (as defined in a Clinical and Services Impact Analysis) during the disruption of one or more key systems. These plans should be socialised and embedded across the organisation, and a version of them stored offline, to ensure they can be implemented effectively during an incident. In the event of an incident impacting multiple systems, as within the Conti attack, recovery prioritisation should be addressed on a regular basis from the beginning of the response, to direct resources to the appropriate systems and services from the offset.

FA2.KF24 Recovery efforts were hindered by the lack of a predefined recovery process and targeted supporting resources

Several stakeholders noted that recovery efforts were hindered by the lack of resources and inability to allocate them in the most efficient manner. As mentioned in finding FA2.KF3, without a Clinical and Services Impact Analysis to clearly articulate priorities and sequences of recovery, the HSE, HGs and CHOs were unable to create an informed recovery

strategy in the initial days. This, coupled with the absence of information available on the HSE's assets and services (see also finding FA2.KF23), meant that technical teams relied on queries and information submitted to a central mailbox set up for the response and on data gathered from vendors and suppliers. The speed with which applications could therefore be prioritised and communicated to the technical recovery teams was not therefore optimal.

Specifically, responders noted that the absence of a predefined priority list and overall process flow meant the Tech and Data Ops teams were at risk of under- and over-utilisation due to workflow issues.³²⁰ This extended to third party support who relied on central coordination from the HSE to direct their recovery efforts. There were missed opportunities to recover applications in parallel and technical responders risked being redeployed onto other recovery areas,³²¹ delaying or preventing their return to application restoration once a new set of priorities was established. Indeed where responders were left without targeted guidance on what to restore they relied on informal conversations to determine which teams were struggling, and directed their attention there.

FA2.KR24 Map and document the people and technology resources and processes required to recover all critical systems in a pre-defined sequence (see tactical recommendation 1.3 in Section 4)

The HSE should ensure that the Cyber Incident Response Playbook³²² documents a pathway to recovery that maps the people, processes and technology requirements of each system, to provide a pathway to recovery in the event of single or multiple system failure. During a major outage or disruption, recovery priorities should be agreed with central and local response and IT teams and communicated to all responders to streamline the recovery of integrated and independent systems. Once recovery priorities have been agreed, incident response mechanisms need to be invoked that provide the most effective communication and coordination between teams.

Central coordination meetings should be held with the asset and application register acting as a tool to guide recovery activities. A read-only, and regularly updated, list of prioritised applications should be made available to all technical recovery teams to direct their activities and keep them informed of the actions being undertaken across the response.

³²⁰ Lessons Learned_ Programme Lessons v0.2

³²¹ Programme RAID Log

³²² Recommendation FA1: 4.1.1, Focus area 1- Technical investigation and response report

To achieve this an operational rhythm needs to be established by:

- Setting up a meeting cadence *at* and *between* each response level e.g., operational or “Bronze” (HG and CHO) meeting followed by a tactical or “Silver” (HSE) meeting, then a strategic or “Gold” (EMT) meeting to share a cascade of updates increasing in importance, escalating priorities.³²³ This waterfall flow between the command levels should also be used in reverse to share decisions and actions simultaneously to all teams and impacted sites;
- Each meeting following a set agenda to ensure all required areas are covered off, particularly in terms of situational awareness of the Incident;
- Use of uniform templates for collecting incident updates, action tracking and required decisions.

It is recommended that at each level of response there is a dedicated role to ensure coordination within and between teams. This can be the role of a Crisis Coordinator or SITCEN Information Manager (see also *finding FA2.KF15*).

Focus area 2 conclusion

Despite a lack of pre-prepared structures and processes, the HSE exhibited an agile and reactive response to the Conti ransomware attack in May 2021. Prior learnings, behaviours and processes, many of which were exercised during the COVID-19 response, were leveraged to ensure critical systems and processes were recovered, and to deliver safety critical patient care across the country. The lengths to which staff and vendors went to keep patients safe and facilitate a recovery within the operating constraints is a direct reflection of the leadership that was employed during this crisis. The behaviours, structures and processes designed reactively during the response to the attack should be leveraged and embedded into new crisis structures, to ensure the HSE is better able to respond at pace to future risks when they materialise.

Individuals within the HSE have described it as an organisation constantly responding to crises. To date, the HSE’s approach to preparedness for disruptive events has been driven through the Major Emergency Management Framework. Events previously in scope of the Framework can be categorised as short term, national events caused by adverse weather or accidents, which created a temporary surge in demand on the HSE’s clinical and acute services. The normalisation of crisis events in the HSE has

generated a sense of over confidence throughout the organisation, whereby the forward planning has become restricted to contingencies for predictable or recognisable threats and risks. Specifically, the HSE’s crisis planning has been based on the assumption that all critical infrastructure and processes would be available to support a crisis response. There was therefore no contingency planning for a cyber attack, or any other scenario involving the denial or loss of infrastructure, people, or facilities.

Prior to the cyber attack, outside of the Major Emergency Management Framework, there was no integrated organisation-wide Crisis Management Framework in place to deal with a major *internal* crisis event. In the absence of documented plans, the HSE’s COVID-19 response imparted a degree of inherent preparedness, which manifested itself in a flexible and agile response from all of its people across all levels. However, the structures required to respond to the crisis caused by the ransomware attack were only achieved with assistance from the Defence Forces in the weeks following the attack. The lack of pre-planned contingencies contributed to increased levels of stress and fatigue in HSE staff during the initial stages of the response and recovery. The HSE requires a Crisis Management Framework, which sits alongside the MEM Framework, but with a separate focus on responding to crises which do not necessitate an interagency response.

Clinical and services continuity has not been a corporate priority in the HSE until recently, when enterprise risk management and clinical and services continuity were consolidated under the National Director for Governance and Risk. Consequently the level of clinical and services continuity and crisis preparedness across the organisation varies significantly. Due to a historic lack of governance and oversight, a fragmented and incoherent clinical and services continuity capability has evolved across the organisation. This delayed the implementation of an initial coherent response and recovery effort during the Incident.

There are many learnings to be taken from any response to an incident this significant. The HSE must expand upon initiatives already taken and implement a coherent operational resilience capability, including clinical and services continuity and crisis management, across the organisation. Key actions for the HSE to take to establish organisation-wide preparedness to significant incidents and crises disrupting its operations include:

- Define the governance arrangements and structures to ensure clear and ongoing oversight,

³²³ “Gold, Silver, Bronze” is industry standard phraseology to refer to strategic/tactical/operational level decision making bodies in emergency and crisis management

management, and reporting of the operational resilience disciplines, with a particular focus on implementation and integration of the crisis and clinical and services continuity disciplines;

- Establish the Crisis Management Framework, detailing levels of response and supporting teams and processes to manage any significant incident or disruption impacting HSE operations;
- Develop supporting crisis documentation, including strategic, tactical and operational plans, procedures, tools and templates; scenario specific playbooks for pre-defined threats and risks, supported by clearly defined clinical and services continuity strategies, a resourcing assessment and cost base analysis of chosen solutions;
- Cascade the Framework, tools and templates throughout the organisation, and to HGs and CHOs, to ensure a coherent and standardised response across all parties involved in a crisis response;
- Embed crisis management and clinical and services continuity across the organisation by establishing a formalised HSE-wide training and exercising programme and schedule to develop awareness, familiarity, and competence for all stakeholders involved in incident response.

5.3 Focus area 3 - preparedness of the HSE to manage cyber risks

Focus area 1	Focus area 2	Focus area 3
Review the technical investigation and response	Review the organisation-wide preparedness and strategic response	Review the preparedness of the HSE to manage cyber risks
		Approach to focus area 3
		Key findings and recommendations
		Conclusion

Approach to focus area 3

To facilitate this review, PwC developed a PIR Cybersecurity Framework for the HSE which was based on the NIST CSF and the Information Systems Audit and Control Association Control Objectives for Information and Related Technologies (COBIT). Both NIST CSF and COBIT are internationally recognised standards that organisations frequently use to assess their information security capabilities and IT governance processes. The PIR Cybersecurity Framework incorporates NIST's 5 key domains and 23 supporting sub-domains along with the governance aspects from COBIT.

The PIR Cybersecurity Framework

The following table illustrates the 5 key domains of the PIR Cybersecurity Framework and their associated definitions:

Figure 14: The PIR domains and domain definitions

The PIR Cybersecurity Framework		
Domain	Domain definition	Sub domains
Identify	The Identify function assists in developing an organisation with understanding and managing cybersecurity risk to systems, people, assets, data, and capabilities.	- Asset Management - Business Environment - Governance - Regulation Compliance - Risk Management - Supply Chain Risk Management
Protect	The Protect function outlines appropriate safeguards to ensure the secure delivery of critical infrastructure services.	- People Security - Access Control - Data Security - Protective Technology including: Information Protection Processes and Procedures - IT Baseline Maintenance
Detect	The Detect function defines the appropriate activities to identify the occurrence of a cybersecurity event.	- IT Events & Threat Monitoring including: Detection Technology - Continuous Monitoring - Detection Processes
Respond	The Respond function includes the appropriate activities regarding a detected cybersecurity incident.	- Response Planning - Communications - Analysis - Mitigation Improvements
Recover	The Recover function identifies appropriate activities for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.	- Recovery Planning - Improvements - Communications

Capability Maturity Model Integration

Each domain and subdomain were allocated a rating in accordance with the definitions below. Ratings are based on the Capability Maturity Model Integration

(CMMI) cybersecurity process maturity. ISACA's CMMI cyber maturity model helps CISO's, CIO's, and large organisations build cyber maturity, and manage enterprise cybersecurity resilience, readiness and provide assurance to the Board.

Figure 15: ISACA CMMI cybersecurity process maturity ratings and associated descriptions

Level	Maturity rating	Description
0	Absent	At this level there is no evidence to demonstrate an active process is in place.
1	Initial	At this level, there are no organised processes in place. Processes are ad hoc and informal. Security processes are reactive and not repeatable, measurable, or scalable.
2	Repeatable	At this stage of maturity, some processes become repeatable. A formal program has been initiated to some degree, although discipline is lacking. Some processes have been established, defined, and documented.
3	Defined	Here, processes have become formal, standardised, and defined. This helps create consistency across the organisation.
4	Managed	At this stage, the organisation begins to measure, refine, and adapt their security processes to make them more effective and efficient based on the information they receive from their program.
5	Optimised	An organisation operating at this rating has processes that are automated, documented, and constantly analysed for optimisation.

Key findings and recommendations

Figure 16: Focus area 3 summary of key findings and recommendations

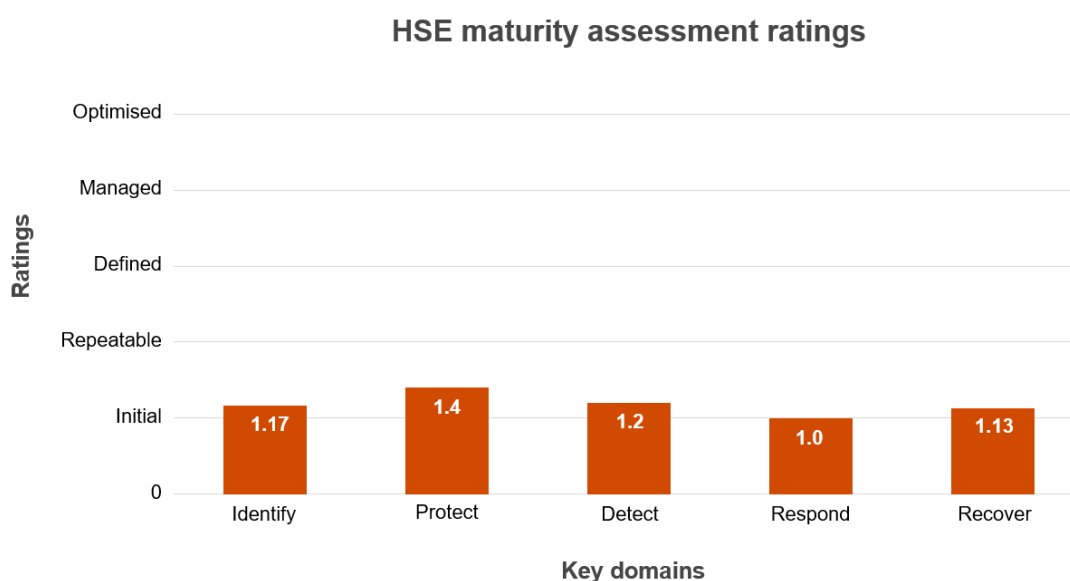
Area	No. of key findings	No. of key recommendations
Identify	6	6
Protect	5	5
Detect	3	3
Respond	5	5
Recovery	3	3
Total no. of key findings & recommendations	22	22

HSE maturity assessment ratings

Using the PIR Cybersecurity Framework, PwC conducted interviews with key stakeholders and reviewed key documents from the HSE and relevant third parties. This provided PwC with sufficient evidence to enable each of the 23 sub-domains to be assessed against the CMMI model. Assessments were then averaged per their domain and an overall maturity rating achieved.

A summary of the maturity ratings by key domain is illustrated below. Our assessment demonstrated that the HSE is at an “initial” CMMI maturity stage across the 5 key domains. Cybersecurity and governance processes are predominantly ad hoc, informal, and not well organised. This represents a very low level of maturity for cybersecurity and is significantly behind where an organisation of its size and risk profile should be. It is our experience that organisations with this level of maturity carry an unacceptable level of risk and frequently fall victim to cyber attack, and often regulatory action. An organisation like the HSE should be aiming for a rating of at least 3 and higher. The HSE OoCIO has an ambition³²⁴ to reach a maturity rating of between 2.6 and 3.5. Considerable resources and investment will be required to achieve this ambition across all 5 NIST domains. It should be noted that similar organisations that PwC has reviewed have ratings of between 2.6 to 2.95.

Figure 17: The assessment ratings of the key domains



³²⁴ Cybersecurity effectiveness assessment, IVI August 2018 (extract reported to the HSE Board November 2020)

Identify - The rating reflects the immaturity in the understanding of cybersecurity within the HSE. There was a lack of understanding of the business context, the resources that supported critical functions, and the related cybersecurity risks.

Protect - The rating is based on the lack of appropriate safeguards that should have ensured delivery of critical infrastructure services. A mature protect function would support the ability to limit or contain the impact of a cybersecurity event.

Detect - The rating reflects the absence of appropriate activities that were used to identify the occurrence of the cybersecurity event. The incident indicates that the HSE lacked the ability for timely discovery of the cybersecurity event.

Respond - The rating indicates that the appropriate activities to act regarding a detected cybersecurity incident were lacking in the HSE. The impact of a cybersecurity incident was widespread and was only contained by shutting down the network.

Recover - The rating reflects the immaturity in maintaining plans for resilience and the restoration of any capabilities or services that were impaired due to a cybersecurity incident in a timely manner, in a way to reduce the incident's impact.

Summary of NIST recommendations

Note: Recommendations are categorised as immediate (starting immediately and completed within six months) and medium-term (with a phased plan for implementation to be developed and completed within 18 months).

Figure 18: Focus area 3 key NIST recommendations

- | | |
|-----------------------|--|
| Immediate term | <ol style="list-style-type: none">1. Governance (see tactical recommendation 1.5 in Section 4.2) - The HSE should recruit a senior leader to act as an interim Chief Information Security Officer (CISO) to begin with the implementation of a cybersecurity incident management process to include detection and response strategies and to assign roles and responsibilities for cybersecurity incident response throughout the HSE. A tactical cybersecurity improvement programme with appropriate governance and dedicated resources that reports into the interim CISO and can provide updates on the programme's progress into the Board.2. Monitoring (see tactical recommendation 2.1 in Section 4.2) - The HSE should accelerate the deployment of a Security Incident Event Management ("SIEM") technology and build a Security Operations Centre ("SOC") to leverage the SIEM functionality. The SIEM, in conjunction with anti-virus tools and the threat intelligence inputs, will provide the HSE with greater threat management and the ability to detect and respond effectively to any future cybersecurity incident.3. Vulnerability management (see strategic recommendation 3.2 in Section 4.1)
- The HSE should begin a formal process of addressing all known vulnerabilities highlighted by Internal Audit and ICT across the HSE network. Acquire protective technology to monitor and block traffic that could remove sensitive data from the HSE or attempt to compromise systems supporting clinical services. Empower administrative staff via a phased deployment of Privileged Access Management and Network Administrator Software to enable the central and standard management of servers and network infrastructure. Continue with employee cybersecurity awareness training and run a phishing campaign to reinforce good cybersecurity hygiene in all employees. |
|-----------------------|--|

Medium term

- 1. Recruit a permanent CISO with a supporting team (see strategic recommendation 3.1 in Section 4.1)** - The CISO should be at National Director level, a direct report to the CTTO, and have appropriate access to the EMT and their agenda, to ensure that cybersecurity risks are understood and considered in all decision-making. The CISO should be responsible for cybersecurity operations as well as driving strategic and tactical actions to transform cybersecurity capability. The CISO should be provided with the resources to build a supporting cybersecurity team structure in the HSE. This structure would include all aspects of cybersecurity capability including operations, risk management, strategy, architecture, engineering, and investigations.
 - 2. Develop a specific cybersecurity strategy for the HSE (see strategic recommendation 4.1 in Section 4.1)** - to provide the HSE with a multi-year transformation programme to address highlighted issues from this PIR and build defence in depth over time. Such issues would include a complete IT asset register, a completed and managed CMDB that is aligned to a Service Catalogue to capture key Clinical and Corporate services, as well as a roadmap to address open Internal Audit findings each year.
 - 3. Governance (see strategic recommendation 1.1 in Section 4.1)** - Implement a dedicated cybersecurity Board oversight committee to report on risks on a regular basis. This committee should report on all relevant technology updates, patching, audit findings and threat intelligence. This committee should provide the Board with a contextualised perspective of cybersecurity risk across the HSE.
-

Summary of key findings and recommendations

From our assessment, PwC has identified cybersecurity capability gaps in the form of findings and designed tactical and strategic recommendations for each domain and subdomain. A summary of key findings and their corresponding recommendations are included below.

Figure 19: PIR Cybersecurity Framework

The PIR Cybersecurity Framework				
NIST domain	Rating	NIST CSF category/ sub-domain	Key findings	Key recommendations
Identify	Initial	Asset Management	FA3. KF1 The HSE did not have a complete and accurate IT asset register, a Configuration Management Database (CMDB) or a defined asset management methodology.	FA3. KR1 (see tactical recommendation 1.3 in Section 4.2) The HSE should continue to develop an asset register that is aligned to clinical and corporate services, as well as underpinning a process to ensure the register is maintained up to date. Doing so will allow the HSE to determine the potential impact of any future incident and effectively respond in a controlled and structured manner.
		Business Environment	FA3. KF2 The HSE did not have a defined and agreed cybersecurity strategy nor a formalised risk appetite statement that it could be aligned to.	FA3. KR2 (see tactical recommendation 1.4 in Section 4.2) The HSE should create a cybersecurity strategy, covering at a minimum incident detection, incident response and business recovery. It will also need to be aligned to the HSE strategy objectives and signed off by the HSE Board.
		Governance	FA3. KF3.1 An information cybersecurity governance framework (policy, process, standards) to manage cyber risk did not exist within the HSE.	FA3. KR3 (see strategic recommendation 3.2 in Section 4.1) The HSE should establish an appropriate cybersecurity risk and governance framework to ensure there is a consistent and clear allocation of responsibility, authority, and accountability. Including the need to establish reporting processes to ensure potential cybersecurity incidents are appropriately reported in all cases. This should provide a forum for key stakeholders e.g., Clinical Operations, Corporate Services, Third Party service managers, Sections 38s and 39s have a forum to discuss and align on cybersecurity priorities. Providing required assurance to the Board and facilitating effective management at Board level. The HSE should appoint a senior leader for cybersecurity (a CISO) who has experience rapidly reducing organisations vulnerability to threat, designing cyber security transformation programmes, and providing assurance to Boards of management. This should provide the required assurance to the Board in facilitating effective cybersecurity management.
			FA3. KF3.2 The HSE did not have a structured and robust process to ensure suspicious activity that was detected and/ or reported on applications or infrastructure (servers or on the NHN) was properly investigated and appropriately reported to the OoCIO SMT and the HSE EMT.	
			FA3. KF3.3 The HSE did not have adequate assurance processes in place to ensure the HSE EMT and Board had oversight of OoCIO operational processes. In the absence of assurance processes the HSE Board did not have sufficient visibility over the operation of these processes or comfort they were operating in line with HSE Policy and standards.	
		FA3. KF3.4 The HSE did not have a CISO or dedicated senior executive with responsibility for cybersecurity governance.		
		FA3. KF3.5 There was no dedicated committee that provided direction and oversight of cybersecurity and the activities required to reduce the HSE's cyber risk exposure.		

Identify	Initial	Regulation	FA3. KF4 The HSE had not completed its Operator of Essential Services (OES) return to comply with the Network and Information Systems Directive (NISD) since 2019. In addition, while continual progress was made to resolve HSE Internal Audit issues, a number remained unresolved.	FA3. KR4 (see tactical recommendation 2 in Section 4.2) The HSE should complete its required OES returns on an annual basis to ensure compliance with NISD regulations and to understand potential cybersecurity weaknesses with critical services.
		Risk Management	FA3. KF5 A cybersecurity risk framework for the HSE did not exist.	FA3. KR5 (see tactical recommendation 3 in Section 4.2) The HSE should develop a formal cybersecurity risk framework aligned to the business' operational risks and strategic plans.
		Supply Chain Risk Management	FA3. KF6 Third Party Risk (TPR) was not effectively managed as no formal process existed that would assess suppliers and manage this risk appropriately. Processes did not ensure Business System Managers were appointed in all cases to be responsible and accountable for the delivery of services within the assigned service area in line with nationally defined frameworks, standards and policies.	FA3. KR6 (see strategic recommendation 4.2 in Section 4.1) The HSE should implement a Third Party Risk Management framework that defines how third parties to the HSE are assessed for cybersecurity risks and what risk treatment plans are appropriate to address residual cyber risk.

The PIR Cybersecurity Framework				
NIST domain	Rating	NIST CSF category/sub-domain	Key findings	Key recommendations
Protect	Initial	People Security	FA3. KF7 There was no comprehensive formal cybersecurity awareness or training program in the HSE that ensured people were sufficiently trained to perform their duties in a manner consistent with policy.	FA3. KR7 (see strategic recommendation 3.2 in Section 4.1) The HSE should introduce a comprehensive, formalised cybersecurity training and awareness programme that is delivered to all staff at all grades across the organisation. This should be conducted on a regular basis.
		Access Control	FA3. KF8 The HSE Access Control Policy was last reviewed in 2014 and was not fit for purpose. In addition, there was no central access control process for all HSE applications.	FA3. KR8 (see tactical recommendation 3.1 in Section 4.2) The HSE should introduce centralised processes and procedures to manage and review the appropriate access and identities that require access to services and data. This should be in the form of an Identity Access Management (IAM) solution that would consistently manage access across users, System Admins and third parties.
		Data Security	FA3. KF9 ICT HSE should formalise a backup strategy to enable the efficient restoration of services.	FA3. KR9 (see strategic recommendation 4.1 in Section 4.1) ICT HSE should implement a structured process for performing data backups and storing this data off site. Regular testing of this data should take place to ensure success recovery.
		Protective Technology	FA3. KF10 Protective technology e.g., AV software was implemented in an ad-hoc manner, not consistently or against a clear set of threat-based requirements.	FA3. KR10 (see strategic recommendation 3.1 in Section 4.1) The HSE should develop a strategy for adopting the appropriate protective technologies and ensure consistent deployment across the HSE network.
		IT Baseline Maintenance	FA3. KF11 The HSE did not maintain security baselines for all operational hardware and software, and the patching processes did not ensure preventative maintenance and vulnerability management was performed in a timely manner.	FA3. KR11 (see strategic recommendation 3.1 in Section 4.1) The HSE should develop a process to maintain security baselines for all operational hardware and software, including but not limited to establishing preventative processes such as patch and vulnerability management processes.

The PIR Cybersecurity Framework				
NIST domain	Rating	NIST CSF category/sub-domain	Key findings	Key recommendations
Detect	Initial	IT Events and Threat Management (including: Detection Technology)	FA3. KF12 The HSE did not have the capability to detect security events relating to this incident, across its network due to a lack of technology deployed, ad hoc processes and very limited resources to monitor events.	FA3. KR12 (see tactical recommendation 4 in Section 4.2) The HSE should develop a cybersecurity threat profile that is informed by relevant sources to enable an effective monitoring capability. This should include threat intelligence feeds to provide an informed view of the latest cyber threats relevant to the HSE. These feeds should be used in conjunction with a SIEM to inform and provide IOCs for monitoring and detecting across the HSE ICT estate. Aligned to this the HSE should implement anti-virus consistently across the estate, ensure it as well as logging and EDR outputs are aggregated and obtain a 24x7 security operations centre (SOC) to monitor the entire business and detect anomalous behaviour and events.
		Continuous Monitoring	FA3. KF13 The HSE did not have an effective continuous monitoring capability that would identify and manage security events.	FA3. KR13 (see tactical recommendation 2 in Section 4.2) The HSE should implement alert monitoring on all network servers, endpoint devices, and firewalls for the external and internal networks. Specific use cases for each alert should be developed for the chosen SIEM.
		Detection Processes	FA3. KF14 The HSE did not have a structured and robust process to detect and respond to activity on the network, nor an effective escalation path to senior management for reporting and validation of events	FA3. KR14 (see strategic recommendation 2 in Section 4.1) The HSE should implement a holistic network detection and response functionality with a dedicated team to continually monitor for and respond to alerts.

The PIR Cybersecurity Framework				
NIST domain	Rating	NIST CSF category/sub-domain	Key findings	Main recommendations
Respond	Initial	Response Planning	FA3. KF15 The HSE had not identified the viable clinical and services continuity options across people, process and technology, nor had the HSE defined requirements for achieving clinical and services continuity in accordance with its risk appetite. In particular the HSE did not have an appropriate response policy, plan, or run books for cybersecurity incidents.	FA3. KR15 (see tactical recommendation 3 in Section 4.2) The HSE should develop an appropriate cybersecurity response policy, supported by plans and/or run books for cybersecurity incidents that are regularly reviewed and exercised so that it can mount an effective and efficient response in the event of a future incident.
		Communications	FA3. KF16 The HSE did not have an internal communication plan or a crisis communication system for sharing messages in the event of a cybersecurity incident.	FA3. KR16 (see strategic recommendation 4.2 in Section 4.1) The HSE should develop a formal internal communications plan where key internal parties such as senior leadership, voluntary hospitals, CHOs are receiving timely and consistent messages. Specifically, the HSE should develop specific runbooks and template responses for specific scenarios to aid a speedy response and ensure there is consistent communication.
		Analysis	FA3. KF17 The HSE lacked skilled resources to respond immediately to the Incident. The HSE was reliant on third party assistance.	FA3. KR17 (see strategic recommendation 2.1 in Section 4.1) The HSE should ensure that an appropriate response policy, plan, and process are in place to manage multiple security incidents, perform response investigations, and collect evidence to assess the best potential mitigation plan.
		Mitigation	FA3. KF18 The HSE did not have formal mitigation strategies and tactics to isolate, remove, and monitor threats.	FA3. KR18 (see tactical recommendation 3 in Section 4.2) The HSE should develop formal mitigation strategies and tactics to isolate, remove, and monitor threats. Key Performance Indicators (KPIs) should be put in place so that performance can be optimised.
		Improvements	FA3. KF19 The HSE Incident Management process did not have formal processes to ensure lessons were learnt and codified from all incidents.	FA3. KR19 (see strategic recommendation 4.2 in Section 4.1) The HSE should establish a formal process, as well as resources to ensure lessons were learnt and codified from all incidents and are maintained to reflect operational and organisational change.

The PIR Cybersecurity Framework				
NIST domain	Rating	NIST CSF category/sub-domain	Key findings	Main recommendations
Recover	Initial	Recovery Planning	FA3. KF20 The HSE did not have appropriate recovery plans for cybersecurity incidents. Clinical and services continuity requirements are not aligned to a formally defined risk appetite statement. Both contributed to the initial recovery response being focused on foundational technology and not clinical services.	FA3. KR20 (see strategic recommendation 4.1 in Section 4.1) The HSE should implement a cybersecurity recovery plan that links to an asset register detailing clinical, corporate, and other priorities and test this plan on a regular basis.
		Improvements	FA3. KF21 The HSE should formally document lessons learnt from all cybersecurity incidents to develop a continuous improvement methodology to manage any future cybersecurity incident.	FA3. KR21 (see strategic recommendation 1.1 in Section 4.1) The HSE should develop a formal process for capturing improvements/lessons learnt following an incident.
		Communications	FA3. KF22 The HSE's internal communications relating to the cybersecurity incident were ad-hoc and lacked an appropriately resourced team dedicated to manage the message to the organisation.	FA3. KR22 (see strategic recommendation 4.2 in Section 4.1) The HSE should consider developing a communications strategy for cybersecurity incidents.

Focus area 3 conclusion

PwC's NIST and COBIT based assessment of cybersecurity capability within the HSE clearly indicates that the organisation is operating at a level of maturity that is reactive, ad-hoc and significantly below the level needed to afford a basic level of protection against the rapidly increasing level of cyber threats that the organisation faces. Despite efforts and endeavours at the time of the Incident, the HSE was not well prepared to identify, understand, and respond to cybersecurity attacks. Significant gaps exist across all 5 NIST domains. The cyber attack was not detected prior to the ransomware execution, protective controls and technologies were not robust enough to prevent the spread of the ransomware. Furthermore, the response and recovery was based on ad hoc structures, including processes to identify and prioritise applications and systems to be recovered. Considerable resources and sustained investment will be required to remediate the gaps across all 5 NIST domains. However, the recommendations herein, which are both tactical and strategic, will support the HSE to safeguard and protect against future cyber attacks and will also significantly improve its cybersecurity maturity ratings across all 5 domains of NIST.

Appendices

- A. Scope of work
- B. List of interviews
- C. Key artefacts
- D. List of key recommendations
- E. Focus area 1 - detailed technical timeline
- F. Focus area 2 - detailed organisational timeline
- G. Focus area and key recommendation mapping
- H. HSE Risk assessment tool
- I. Glossary and terms

A. Scope of work

Our work comprised three focus areas as follows:

- Focus area 1: Review of the technical investigation and response to the Conti Incident
- Focus area 2: Review the organisation-wide preparedness and strategic response
- Focus area 3: Review the preparedness of the HSE to manage cyber risks

Focus area 1

In this area, we reviewed the technical response to the Incident and the subsequent recovery and investigation activities undertaken by the HSE. Key considerations included the effectiveness of the response and recovery, the sufficiency of the investigation to support the conclusions made, and the ability of the HSE to detect and prevent similar incidents in the future. To achieve this we separated our review into nine phases - in each phase we did a deep dive into specific areas of interest:

- Review of relevant documentation including daily incident SITREPs, investigation reports, RAID logs and recovery plans;
- Interviews with key stakeholders that were involved in the response, investigation and recovery to understand key information, including preparedness, the timeline of events, roles and responsibilities, and decision making;
- Interviews with contacts at the HSE's Incident Response provider to review their technical reporting;
- Interviews with technical teams to understand the Cyber Security controls that were in place at the time of Incident and assess these against our ransomware vulnerability framework;
- Review of documentation and interviews to understand HSE's network and AD structure, including the architecture of the NHN;
- A deep-dive into the recovery of specific applications and organisations, including statutory hospitals, voluntary hospitals and CHOs, including the adequacy of disaster recovery capabilities to contribute to operational readiness for a cyber attack;
- Review of Cyber Security improvements planned or implemented during the Incident to assess whether they would likely prevent a similar Incident reoccurring.

Focus Area 2

In this area, we reviewed the organisation-wide preparedness and strategic response to the Incident. The work comprised three phases as follows: Crisis Preparedness, Crisis Response, and Crisis Recovery.

The first phase focused on Crisis Preparedness with the following objectives:

- Assess the governance in place at HSE for risk, clinical and services continuity, incident and crisis management;
- Assess whether robust emergency, incident and crisis plans were in place prior to the Incident at strategic, tactical and operational level with clear roles and responsibilities per team/stakeholder;
- Assess whether robust BCM plans were in place prior to the Incident at strategic, tactical and operational level;
- Assess whether crisis communications plans were in place at HSE and CHO/hospital (group) level;
- Understand the level of security and crisis awareness, training and exercising pre-Incident;
- Assess whether lessons learned from previous large scale incidents or emergencies (e.g nurses' strike, COVID-19 response) were applied to the Conti response.

The second phase focused on Crisis Response with the following objectives:

- Assess whether effective and organised response structures were defined and implemented, when and by whom;
- Identify whether an effective operating rhythm, matching the pace of the crisis, was set and followed to ensure command, control and coordination was continuously achieved throughout the response;
- Identify whether information and data was shared effectively across workstreams and up to the HSE NCMT to inform understanding of clinical and operational impacts;
- Assess whether leadership established an agreed overarching response and recovery strategy, guided by clear values and response principles;
- Assess whether decisions were made effectively based on a situational assessment;
- Understand the impact of the prevailing HSE emergency response culture on the crisis response.

The third phase focused on Crisis Recovery with the following objectives:

- Assess whether leadership established a recovery strategy/plan;
- Assess whether recovery plan was aligned with existing clinical and services continuity, disaster recovery and risk management processes;
- Assess whether business/corporate/clinical priorities drove recovery plan;
- Determine the extent to which workarounds implemented at local hospital, HGO and CHO level were appropriate; and how this ability was impacted based on organisational preparedness and culture;
- Understand the long term impacts of the event on clinical activities, operations and staff wellbeing;
- Understand the planned changes in processes and culture driven by this event and how they align with HSE's organisational strategy.

Focus area 3

In this area, we conducted a review of the HSE's current cyber security capabilities from a strategic and operational perspective. Our objective was to determine the level of preparedness in the HSE's technical capability and operational resilience (including clinical and services continuity management planning) in terms of managing cybersecurity risk. To do this, we:

- Examined the appropriateness of any technical controls implemented and the likelihood they would prevent this or a similar Incident reoccurring. Specifically, in the area of Identity and Access Management, Data Protection and Content Control;
- Assessed IT response in terms of how it empowered the organisation-wide response and, the structuring and management of the recovery of applications supporting key patient care services in the HSE, hospitals, and CHOs;
- Assessed if lessons learnt have been implemented from this and other incidents, and have these been shared with State and non-State organisations to inform future preparedness;

- Determined if there were organisational, cultural or behavioural root causes in the IT areas that could be identified so that we could provide an informed view on the improvements the HSE should consider to improve its Cyber Security posture and prevent similar Incidents occurring again.

Scope exclusions

- We did not perform validation of the documentation provided to us.
- We did not conduct any testing of the operating effectiveness of controls.
- During our historic review of the Incident and HSE's structure, processes and infrastructure, the maximum period we looked back is five years.
- As the remediation work was ongoing during our review, we analysed the activity that had taken place up to 31 July 2021.
- We have performed a cyber preparedness assessment based on PwC's NIST CSF and COBIT Frameworks. We conducted this review based on the ten key areas we identified, using the above Frameworks. We note that an organisation-wide NIST assessment has not been fully completed to date by the HSE.
- We have not validated the work performed as part of any previous information security audits or related work on which the HSE historically made decisions.
- We have only reviewed how the HSE's strategy was informed by advice provided by third parties and how the HSE's response strategy allowed for effective coordination of third parties. We reviewed the effectiveness of third parties' response and recovery efforts.
- While we have identified learnings from this Incident which may apply to other major risks and incidents that could cause major business disruption to the HSE, we have not performed a full evaluation of other risks that HSE may face.
- While we have reviewed the HSE's clinical and services continuity plans, structures and processes; the scope of our review did not include preparing a new clinical and services continuity plan.

B. List of interviews



C. Key Artefacts

#	Key artefacts
1	Health Service Employment Report: August 2021
2	Conti Cyber Response NCMT Structures Governance and Admin V1.10 31052021
3	https://www2.hse.ie/services/cyber-attack/how-it-may-affect-you.html
4	Weekly Brief, 21 September 2021
5	https://ec.europa.eu/commission/presscorner/detail/en/IP_13_94
6	National_Cyber_Security_Strategy.pdf
7	https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware
8	https://www.ic3.gov/Media/News/2021/210521.pdf
9	HSE's Incident Response provider Intrusion Investigation Report, September 2021
10	https://www.hse.ie/eng/services/publications/order-perfected-20-may-2021.pdf
11	https://us-cert.cisa.gov/ncas/alerts/TA17-181A
12	Ransomware Attack on Health Sector - https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf
13	HSE cyber attack - which hospitals are affected? Here is everything you need to know. Source: Irish Independent. Date: May 16 2021
14	https://www.independent.ie/irish-news/hse-cyber-attack-which-hospitals-are-affected-here-is-everything-you-need-to-know-40432288.htm
15	Healy, O. Dr. A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare IT failure, Dated 30th September 2021.
16	HSE press release 15 05 21
17	https://www.cso.ie/en/releasesandpublications/ep/p-pme/populationandmigrationestimatesapril2021/
18	HSE National Service Plan 2021
19	Cyber Security Board Awareness Draft V7.2.pptx
20	VI Cybersecurity effectiveness assessment
21	https://www.ncsc.gov.ie/oes/
22	https://www.independent.ie/irish-news/hse-cyber-attack-which-hospitals-are-affected-here-is-everything-you-need-to-know-40432288.html
23	HSE website - Acute Hospital in Ireland
24	https://www.hse.ie/eng/services/list/3/acutehospitals/hospitals/hospitallist.html
25	Reporting on epidemiology of COVID-19 from the national Computerised Infectious Disease Reporting (CIDR) system to recommence on 02/09/2021. Source: HSE website. Date: September 2 2021
26	https://www.hpsc.ie/a-z/respiratory/coronavirus/novelcoronavirus/surveillance/recommencementofreportingfromcidr/
27	HSE Incident Management Framework & Guidance - 2020
28	PwC's proprietary ransomware readiness framework lists the most important cybersecurity controls we have identified to prevent, detect and respond to human-operated ransomware attacks.
29	https://www.nist.gov/cyberframework
30	Email with subject RE: Threat not handled, 13 May 2021
31	https://www.gov.ie/en/news/d48b2-a-note-for-the-public-on-the-recent-cyber-attack-on-the-department-of-health/
32	Logging call with the HSE's cybersecurity solutions provider on 10/05/2021 17:06
33	Email with subject: Recognise these addresses??, May 2021
34	Email with subject RE: Summary, May 2021
35	Information gathered from an interview with the NCSC
36	CIM 2 - Conti Ransomware Incident coordination Form Ver 2.1(2), 2021
37	DPC Report 15 July 2021
38	Programme RAID Log, 2021
39	Original DPC Notification_May 2021
40	Minutes of Cyber Attack MI Meeting 10 am - 15052021
42	NIMIS RE-ENABLEMENT TRACKER CYBER ATTACK RECOVERY, 2021
43	Programme RAID Log
44	Document subject to legal privilege

#	Key artefacts
45	The HSE's Incident Response provider, Intrusion Investigation Report
46	https://stateclaims.ie/uploads/publications/State-Indemnity-Guidance_IT-cyber-attack-on-the-health-and-social-care-sector-from-14-may-2021_21.5.21_2021-05-21-150239_tytw.pdf
47	Conti Cyber Response NCMT Structures Governance and Admin V1.10, 31 May 2021
48	SITCEN SITUATION REPORT, 18:30 14 June 2021
49	HSE OoCIO Security Advisory Group (SAG) Terms of Reference, February 2018
50	CLOSED - HSE Internal Audit Tracking ICTA015OCIO0916_Internet Access Controls - Follow Up Audit, 28 August 2019
51	Cyber Security Board Awareness Draft V7.2.pdf, November 2020
52	Email with subject RE: FW: CI security solutions discussion document, UNDATED Reported as June 2020
53	Minutes of HSE Board Meeting, 27 November 2020
54	https://www.hse.ie/eng/staff/resources/our-workforce/workforce-reporting/health-service-personnel-census-aug-2021-v2.pdf
55	Email from the HSE's cybersecurity solutions provider to the SecOps team with subject "Threat Not Handled", 12 May 2021
56	Email from the HSE's cybersecurity solutions provider to the SecOps team with subject "Threat Not Handled", 13 May 2021
57	Appendix 7: Services Contract, Health Service Executive and the HSE's cybersecurity solutions provider Information Systems Limited Agreement Relating to the Provision of Services pursuant to Request for Tenders for the Establishment of a Multi Supplier Framework for the provision of Security Software and Associated Reseller Services, 24 December 2017
58	Logging call with the HSE's cybersecurity solutions provider on 10/05/2021 17:06, 10 May 2021
59	Email with subject: Query, 12 May 2021 23:53
60	Email with subject: FW: Recognise these addresses??, 12 May 2021 23:36
61	Email with subject: RE: Summary 13 May 2021 12:47
62	Minutes of Cyber Attack MI Meeting 10 am - 14052021, 14 May 2021
63	DOE Application Catalogue and Critical Services as defined under NIS Directive Final
64	Response to questions raised by the Data Protection Commission to HSE DPO on June 2021, July 2021
65	Privileged and Confidential Terms of Reference Legal and Data Steering Group V004, June 2021
66	Draft OoCIO Cyber Governance Report v0.2, UNDATED
67	Minutes of Cyber Attack MI Meeting 11 am - 19052021, 19 May 2021
68	Voluntaries and Go-to-Green, 26 May 2021
69	CTO Document Device Go Green Draft Approach, 23 May 2021
70	CTO Document Remote Access Go Green Draft Approach, 24 May 2021
71	Weekly Brief, 20 July 2021
72	21 September 2021 Weekly Brief, 2021
73	20 July 2021 Weekly Brief, 2021
74	https://irl.eu-supply.com/ctm/Supplier/PublicTenders/ViewNotice/248668
75	Service Contract Agreement - Addendum 1 Managed Security Monitoring & Incident Response Service 24-Hours / 365 Days, Prepared 21 June 2021 (Unsigned)
76	Confirmed by the General Manager Head of Technology, Infrastructure & Deployment within OoCIO Infrastructure and Technology by email, 8 October 2021
77	HSE IT Security Planning, UNDATED Last Modification recorded 15 September 2021
78	Cyber Security Risk Management, UNDATED Last Modification recorded 15 September 2021
79	CTO Document Security Improvement Programme Draft, 31 August 2021
80	OoCIO-07 Investment Plan 2020 -Cyber Security Draft, 1 June 2019)
81	CTO Document Security Monitoring V1 HSE, 04 June 2021
82	DRR Q2 2021, 19 November 2020
83	https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat
84	AIISO 22301:2019 'Security and resilience - Business continuity management systems (BCMS) - requirements', p. 2.
85	PD CEN/TS 17091:2018 'Crisis management - Guidance for developing a strategic capability', p. 8.
86	Minutes-hse-board-meeting-27-09-2019

#	Key artefacts
87	Centre Review Slides June 2021
88	HSE_CCR_Phase2_HealthcareStrategy_Gov&Risk(Extract)
89	https://www.hse.ie/eng/about/who/board-members/committees-of-the-board/performance-and-delivery-committee/mintues-hse-performance-and-delivery-committee-18th-june-2021.pdf
90	Briefing for HSE Board on Cyber Security
91	CRR Full Report Post EMT 2nd Nov OCTOBER 2020 v0.2 03 11 20 FINAL
92	CRR FULL Report Summary and Assessments HSE Board 23rd June 2020 pdf v0.1 23 06 20
93	CRR Q1 2021 Review Report Final post EMT meeting 27 04 21 v1.0 27 04 21
94	CRR Q4 2020 Full Report post EMT meeting February 2021 v0.1 09 02 21
95	Business Continuity Management Policy 2016
96	Audit and Risk Committee TORs
97	ISO 22317 Societal security - Business continuity management systems - Guidelines for business impact analysis (BIA)
98	ISO 22331 Security and resilience - Business continuity management systems - Guidelines
99	Incident Management Framework 2020
100	Comms Division Organisational Chart July 2021
101	CRR Full Report Summary and Risk Assessments v0.1 28 02 20
102	Conti Cyber Response NCMT Structures Governance and Admin V1.10 31052021
103	Programme org chart v1 21.05.21
104	Lessons Learned_ Programme Lessons v0.2
105	Minutes of Cyber Attack MI Meeting 12 pm - 14052021
106	A-Framework-For-Major-Emergency-Management
107	Emergency Management Services Delivery Plan 2019 - Regional CMTs
108	HSE EM Interim Governance Arrangements Jan 2020 - ACMTs
109	M_HSE_Intrusion Investigation Report - REDACTED (FINAL).pdf, 2021
110	Minutes of Cyber Attack MI Meeting 10 am - 14052021
111	HSE-2020-incident-management-framework-guidance
112	Managing a Major Incident v1 1 and IT Security Incident Plan
113	RAID Log, HSEmail.ie was agreed on 17 May 2021
114	Letter to all Staff - 1 on 26 May 2021
115	20210524-Morning Update Brief - FINAL
116	20210525-Morning Update Brief - FINAL
117	Terms of Reference - Cyber Attack Legal and Data Workstream Steering Group June 2021
118	Data Protection Monitoring Process
119	CCO Clinical Memo 1 15.05.2021
120	CCO Clinical Memo 2 21.05.21
121	Temporary Use of Personal ICT Resources.msg
122	App Priority List - 20210601 1415 and Site Workshop 7 (Hospital G)
123	Minutes of Cyber Attack MI Meeting 11 am - 18052021
124	Cybersecurity effectiveness assessment, IVI August 2018 (extract reported to the HSE Board November 2020)
125	Cobalt_Conti Threat Events from [REDACTED], 2021
126	Email with subject FW: Server restart request, 13 May 2021
127	Email with subject FW: Server restart request, May 2021
128	Email with subject 'DDOS attack today', May 2021
129	Logging call with the HSE's cybersecurity solutions provider on 10/05/2021 17:06
130	Email with subject FW: Query, May 2021
131	SITCEN SITUATION REPORT, 10:30 7 June 2021
132	SITCEN SITUATION REPORT, 10:30 28 June 2021
133	SITCEN SITUATION REPORT, 10:30 7 July 2021
134	Weekly Brief, 27 July 2021
135	Weekly Brief, 3 August 2021

#	Key artefacts
136	Weekly Brief, 10 August 2021
137	Weekly Brief, 17 August 2021
138	Weekly Brief, 24 August 2021
139	Weekly Brief, 31 August 2021
140	Minutes of Cyber Attack MI Meeting 10 am - 1405202
141	Daily SITRPEPs scheduled for 0915 & 1830
142	Minutes of Cyber Attack MI Meeting 11 am - 17052021
143	Irish patients' data stolen by hackers appears online', Financial Times [https://www.ft.com/content/13d33a08-ce83-4f8a-8d93-a60a5e097ed8]
144	OoCIO Cyber Governance Report v0.2
145	Minutes of Cyber Attack MI Meeting 11 am - 21 May 2021
146	Minutes of Cyber Attack MI Meeting 11 am - 24052021
147	20210524-SITREP_HSE SITCEN-1015hrs
148	20210524-SITREP_HSE SITCEN-1930hrs
149	Minutes of Cyber Attack MI Meeting 11am - 25052021
150	20210526-SITREP_HSE SITCEN-1015hrs
151	Minutes of Cyber Attack MI Meeting 11 am - 26052021
152	Letter to all Staff-1 - 26 May 2021
153	Minutes of Cyber Attack MI Meeting 11 am - 28052021
154	Minutes of Cyber Attack MI Meeting 11 am - 01062021
155	Minutes of Cyber Attack MI Meeting 11 am - 01062021 People on site and assisting regional offices.
156	Minutes of Cyber Attack MI Meeting 11 am - 11062021
157	Governance RAID Log
158	Weekly Brief 20210824- Final V1
159	Weekly Brief 20210831- Final V1
160	Q1, 2019 CRR COMBINED Document for April LT meeting.pdf
161	Minutes-hse-performance-and-delivery-committee-18-september-2020.pdf

D. List of key recommendations

Figure 20: List of key recommendations

Ref #	Recommendation description
FA1.KR1	Appoint an interim senior leader for cybersecurity (a CISO) who has experience rapidly reducing organisations vulnerability to threats and designing cyber security transformation programmes. The HSE should appoint an interim senior leader for cybersecurity to be responsible for placing governance around cybersecurity improvements, identifying a sustainable medium-term managed detection and response solution (see immediate recommendation FA1.KR6), identifying future strategy for detection and response and leading the implementation of the tactical recommendations from this review. This role should also be responsible for planning and mobilising teams to deliver a cybersecurity transformation required to sustainably reduce the HSE's risk to ransomware attacks. The CISO should be at National Director level, a direct report to the CTTO, and have appropriate access to the Executive Management Team and their agenda, to ensure that cybersecurity risks are understood and considered in all decision-making. This interim senior leader should be given the ability to source the necessary expertise from the market to build a team that can give effect to the immediate recommendations listed in this section, and to begin planning for the implementation of medium-term recommendations. The prioritisation for the approval of a CISO and a cyber security team has been recorded within the Q2 DRR as an 'action control' to Risk ID 130 with a due date of 30 June 2022.
FA1.KR2	Establish an executive-level cybersecurity oversight committee, to drive continuous assessment of cybersecurity risk across the provision of health services. A dedicated executive oversight committee is needed to provide direction and oversight to cybersecurity, both within the HSE and across other parties connected to the NHN.
FA1.KR3	Create a Board committee, to oversee the transformation of IT and cybersecurity to deliver a future-fit, resilient technology base for provision of digitally-enabled health services. The HSE should consider inclusion of further specialist non-executive members of the committee in order to provide additional expertise and insight to the committee.
FA1.KR4	Plan a multi-year cybersecurity transformation programme, and identify and mobilise the resources to deliver. In parallel to delivering tactical cybersecurity improvements, the HSE's appointed interim CISO should plan a cybersecurity transformation that will build lasting cybersecurity capabilities and sustainably reduce cyber risk exposure. This cybersecurity transformation programme should be validated at the Board level. For more details on how this should be structured see recommendation FA1: 4.2.7 in section 4.0 Recommendations. The HSE should also identify suitable resources and expertise to plan and deliver this transformation.
FA1.KR5	Appoint a programme lead and define governance framework for the cybersecurity transformation programme. A programme lead with experience in cybersecurity transformation should be appointed by the HSE's interim CISO to drive the execution of this transformation. It is critical that this programme lead can work hand in glove with the HSE's technologies teams, to help orchestrate secure technological transformation. The programme lead should have a direct reporting line into the CISO and have a dotted line into the CIO and be able to provide updates on the programme's progress to the Board committee that oversees cybersecurity.
FA1.KR6	Continue to use a managed detection and response service provided by a third party and identify a sustainable medium-term solution. The current service provided by HSE's Incident Response provider is the most crucial defence the HSE has against further ransomware attacks. If the HSE decides to onboard a new managed detection and response service, it should ensure there is an overlap between this and the HSE's Incident Response provider's current service, so that there are no periods when the IT environment is not monitored.

Ref #	Recommendation description
FA1.KR7	Mobilise a tactical cybersecurity improvement programme (while the cybersecurity transformation programme is being planned), with governance that feeds into the interim CISO and can provide updates on the programme's progress into the Board committee. Dedicated cybersecurity and technology resources should be used to deliver a tactical cybersecurity improvement programme, consisting of tactical work packages that can be delivered at pace using focused governance and reporting to drive accountability. To create these work packages, the HSE should action the following activities: • Triage - All third party recommendations and fixes to the security control gaps identified internally should be triaged into tactical or strategic activities. Tactical activities should be those that will rapidly reduce the risk of ransomware attacks and are achievable in 60 days or less. Note that where improvements are identified as strategic, the HSE should consider what additional tactical improvements can be implemented in the short-term to reduce risk and act as mitigating controls. • Test and Assess - As well as the recommendations it has received from third parties, the HSE should also include recommendations by performing: ◦ AD security assessments; ◦ Vulnerability scanning of all internet-facing IP addresses; ◦ Vulnerability scanning of all internal IP address ranges; and, ◦ A comprehensive assessment of current capabilities and planned improvements against a framework that identifies key capabilities to defend against human-operated ransomware attacks (such as the proprietary ransomware readiness framework used in this report or that recently published by CISA³²⁵). • Architect - Following the triaging activity, the HSE should use cybersecurity experts to architect and manage a series of tactical work packages to deliver the tactical improvements identified by the triage process. These should be designed to deliver directly and rapidly reduce the risk of ransomware attacks, and be achievable in 60 days or less. Examples of tactical work packages include: ◦ Uplift detection and response capability; ◦ Remediate priority infrastructure vulnerabilities; ◦ Lock down remote access methods; ◦ Protect privileged accounts; ◦ Improve service account hygiene; ◦ Remediate AD hygiene issues; ◦ Secure local administrator accounts; ◦ Enforce Multi Factor Authentication (MFA) for all remote access methods; and, ◦ Restrict internet access to servers. This governance should directly feed progress updates into the Board committee. These progress updates should clearly articulate: • the HSE's vulnerability to ransomware attacks; • the risk reduction achieved by improvement activities that have been delivered; and, • the extent of the improvements required to reduce the risk of ransomware attacks to an acceptable level.

Ref #	Recommendation description
FA1.KR8	Bring the governance of ongoing IT and cybersecurity improvement projects under the tactical cybersecurity improvement programme. Governance of current on-going IT projects, that directly or indirectly result in cyber risk reduction, should be brought under the tactical cybersecurity improvement programme's governance (and therefore the CISO see key recommendation FA1.KR7), so the cyber risk reduction they deliver can be tracked, and any risk and issues can be resolved. For example, modernisation projects such as the upgrading of Windows 7 OS and platform modernisation.
FA1.KR9	Use security testing 'find and fix' to identify additional security weaknesses and vulnerabilities by simulating cyber attack techniques, before identifying and triaging pragmatic fixes. Security testing should be used to focus tactical improvement activities. By simulating the threat of human-operated ransomware attacks, improvements that make it more difficult for a threat actor to successfully compromise the organisation can be identified. The HSE should bring together red team experts and cybersecurity engineers to identify pragmatic fixes to the vulnerabilities and weaknesses identified. These fixes should then be triaged with IT and Security teams to assess feasibility and identify how best to deliver them (see key recommendation FA1.KR7 Triage). Security testing should then be used to validate improvements have been correctly implemented.
FA1.KR10	Schedule a 'red team' ethical hacking exercise for early 2022 to demonstrate the effectiveness of tactical improvements made and identify areas for further improvement. The HSE's interim CISO should schedule a red team for Q1 2022 to simulate a human-operated ransomware attack from end-to-end, to identify whether improvements have been effective, and to identify additional priority and focus areas for cybersecurity improvements. This should be scheduled in addition to the recorded plans within the Q2 DRR, which recorded an 'action control' to enhance penetration testing and red team exercises with a due date of 31 December 2021.

Ref #	Recommendation description
FA1.KR11	Implement the following tactical recommendations identified through this review, within the mobilised tactical cybersecurity improvement programme (see key recommendation FA1.KR7). a. Improve security monitoring capability i. Document a process for how to respond to cybersecurity alerts, that clearly outlines how alerts should be triaged, investigated, contained and responded to. This process should also include coordinating the response to security alerts and incidents raised by any organisations connected to the NHN. ii. Augment the Security Operations team with cybersecurity expertise. b. Secure privileged access i. Develop and implement a robust privileged access strategy that aligns with Microsoft good practice and reduces the risk of privileged accounts being compromised. c. Build a vulnerability management capability i. Stand up a vulnerability management capability that continuously scans for vulnerabilities that can be exploited by attackers. d. Harden the security boundary i. Define and communicate a 'security boundary' for the HSE to provide a clear boundary of cybersecurity responsibilities. ii. Perform hardening activities on the defined perimeter of the HSE. iii. Identify secure methods for clinical staff in voluntary hospitals to access applications hosted by the HSE. iv. Use security testing to validate that the HSE can not be compromised by malicious activity from outside its security boundary. e. Improve governance over the NHN i. Risk assess the 'flat' network design and implement segmentation controls that align to the defined level of risk appetite. ii. Establish clear responsibilities for IT and cybersecurity across all parties that connect to the NHN, or share health data, or access shared health services. iii. Increase the resourcing of first and second line network teams in line with defined security responsibilities. iv. Define a security code of connection for connecting to the NHN. v. Define a minimum security standard for the networking of medical devices. f. Improve preparedness for a ransomware attack i. Collect, organise and document artefacts created as part of the response and recovery to the ransomware cyber attack. ii. Identify documents required to respond to a ransomware attack (e.g., network diagrams, asset list) and secure these in a cloud repository. This should be aligned with work to develop an IT continuity and recoverability process which was recorded in the Q2 DRR as an 'action control' with a due date of 30 September 2021³²⁶. iii. Setup and test out-of-band communication medium that would enable IT and security teams, as well as employees, to communicate in the event of a cybersecurity incident. iv. Ensure that the HSE has a fit-for-purpose incident response service with complementing and embedded internal processes for its invocation. v. Review backups and plan for a wide-spread failure recovery mode. vi. Document a prioritised list of applications for recovery.

- g. Accelerate foundational IT projects
 - i. Accelerate the move to cloud based email [REDACTED] by prioritising the resources available for IT and cybersecurity improvements programmes.
 - ii. Prioritise the remediation of critical legacy systems. Particular attention should be paid to the NIMIS application to understand whether the configuration changes made in one hospital (Hospital A) to enable the application to run on Windows 10 can be more widely implemented to expedite the central Windows 10 rollout plans. It should be noted that a legacy risk was recorded in the Q2 DRR, with an aligned 'action controls' to risk assess the existing estate and increase investment for replacing outdated structures both with due dates of 31 December 2021³²⁷.
 - iii. Define a minimum standard for legacy operating systems. For systems who must run on outdated operating systems, sufficient mitigation measures must be defined.
 - iv. Define minimum standard requirements for OS of medical devices.
 - v. Perform asset discovery activities to continually update asset lists.

FA1.KR12**Appoint suitable long-term senior leadership for cybersecurity (a CISO) and establish a suitably resourced and skilled central cybersecurity function.**

The CISO should be at National Director level, a direct report to the CTTO, and have appropriate access to the EMT and their agenda, to ensure that cybersecurity risks are understood and considered in all decision-making. They should be empowered to execute on a defined security vision, strategy and transformation to achieve sustainable cybersecurity risk reduction across the HSE. In line with this appointment the cybersecurity governance and operating model should be defined and subsequently resourced (ideally with burst capacity resources used during any interim periods that occur while recruitment takes place). This model should align to the three line of defence model. Responsibilities, accountabilities, reporting lines and resourcing across the extended organisation of the HSE must all be defined. This includes within the HSE's cybersecurity and IT teams and between these central teams and those within its extended organisation

Ref #	Recommendation description
-------	----------------------------

FA1.KR13

Deliver a multi-year cybersecurity transformation programme to build defence in depth over time and address root-cause issues.

Investment is needed in a single programme of work delivered over the next two - four years to develop core cybersecurity capabilities in a sustainable manner over the short, mid and long term. We would propose this transformation is structured according to a two-track delivery model with dedicated resources and defined target states:

- a. **Tactical track** - the HSE should bring together red team experts and cybersecurity engineers to identify pragmatic fixes to the vulnerabilities and weaknesses identified. These should then be triaged between this tactical track and the strategic track for any longer term strategic activities. Within the tactical track each activity should be defined as being deliverable within either 'two-week agile sprints' or '60-days work packages', to deliver rapid risk reduction by addressing exposure to specific attack techniques. Once the cybersecurity transformation programme is operational this track should absorb the tactical cybersecurity improvement programme.
- b. **Strategic track** - To build the sustainable and enabling foundations that deliver long-term reduction and mitigation of cyber risk, the HSE should define strategic work packages for activities that will take longer than 60 days to implement. This will include the medium to long-term recommendations made in this report. For improvements that are identified to be delivered strategically, suitable mitigations should be put in place in the short-term to reduce risk.

Figure 21: Overview of key pillars in a cybersecurity transformation. This identifies elements that should be considered when scoping a cybersecurity transformation programme.

IT Foundations Improving the hygiene of an organisation's IT estate through tactical activities like enabling security features on the Active Directory and strategic initiatives like embedding good practice data retention, backup and recovery and patch management.	Security Foundations Understanding business drivers and defining the structure and blueprints for security through tactical activities like defining the technical boundary and strategic initiatives like designing the security strategy and frameworks for risk management and architecture.	Access Management Securing identity and access through tactical activities like cleaning up local admin accounts and strategic initiatives like onboarding critical accounts onto a PAM solution and setting up strong authentication & SSO.
Data Security Implementing protective and detective measures to secure critical data through tactical activities like restricting file share open access and strategic initiatives like data classification and data loss prevention capabilities.	Network Security Monitoring network activity and improving protective capabilities through tactical activities like reviewing and hardening key firewalls and strategic initiatives like implementing network segmentation and ONS Security.	Threat Detection & Response Identifying and setting up response capabilities for key threats through tactical activities like developing priority detection content and strategic initiatives like enhanced security monitoring, crisis readiness and IoT/OT threat management.
Attack Surface Reduction Setting up a robust vulnerability management framework and processes through tactical activities like remediating priority vulnerabilities and strategic initiatives like defining secure configuration baselines and DevSecOps processes.	End User Security Protecting the end user compute estate with in the environment through tactical activities like limiting the use of MS Office macros and strategic initiatives like enhancing technical endpoint protection capabilities, and improving email threat mitigation.	Security Culture Improving security awareness through tactical activities like training high risk users and strategic initiatives like designing and delivering security awareness and phishing campaigns.

For example, within the 'IT Foundations' work stream tactical work packages might include the remediation of stale data or extending the scope of the identity directory. Strategic work packages within this work stream could include decommissioning end of life systems or implementing an operational CMDB to maintain an updated list of all systems and applications in the environment.

FA1.KR14

Plan the HSE's future IT transformation that reduces cybersecurity risk.

The HSE's IT transformation lead should begin documenting and planning the HSE's future IT transformation. Executing an IT transformation will allow the HSE to sustainably reduce cybersecurity risk in the long-term, as it can address issues within the HSE's legacy IT estate and therefore can build cybersecurity and resilience into the IT architecture.

Ref #	Recommendation description
FA1.KR15	Design and implement a single and centralised security monitoring capability for the defined security boundary of the HSE that reports into the CISO. This should be for all monitoring aspects including network, server and workstation environments, as well as services such as email. Any reduction in the visibility of assets for monitoring should be risk-assessed to ensure that the HSE's ability to monitor its full environment is within risk appetite. This implementation should involve establishing the following across the three fundamental pillars of people, process and technology: • People - Employing security monitoring and detection SMEs (either internally or through third parties) that are trained to identify and respond to threats detected within and across the HSE security boundary. • Process - Ensuring that detection and response processes are documented. This includes incident playbooks that outline the step-by-step response actions to be taken, as well as documented responsibilities and accountabilities for reporting security events between organisations (such as voluntary hospitals and reporting bodies like the NCSC). • Tooling - Deployment of modern endpoint detection and response tooling/endpoint protection platform tooling across the HSE environment and security boundary. This should be in addition to the implementation of a Security Incident and Event Manager (SIEM) and Security Operations Centre (SOC) to centrally analyse logs from systems and security tools.
FA2.KR1.1	Establish governance and oversight of Operational Resilience Programme. The HSE should: • Nominate an executive with responsibility for operational resilience which will include the coordination of component parts of crisis management (including major emergency management), incident management, clinical and services continuity and enterprise risk management; and • Establish a HSE Resilience SteerCo to oversee the design and delivery of an Operational Resilience Programme, reporting into the Board. This SteerCo should include senior representatives from the EMT who own the respective resilience disciplines and related functions (e.g. cyber security) and any additional key clinical and services and operations representatives.
FA2.KR1.2	Establish an Operational Resilience Policy and Programme scope, strategy and structure. The HSE should: • Define an overarching policy that incorporates the above resilience disciplines. Clarify ownership of the programme (for example under the ND G&R) and integration with existing policies. At a minimum, the policy should include a statement of leadership commitment, objectives and scope, roles and responsibilities, reference to relevant industry standards and an oversight regime; • Define the Operational Resilience Programme scope, strategy and structure across the HSE and funded entities. Define the types of incidents in scope (e.g. physical, technological, people and cyber incidents) and how to build and maintain a capability to respond across the organisation. Define the operating model or the capability in terms of dedicated staff, reporting lines, roles and responsibilities within 'prepare' and 'respond and recover.' Specify which areas of the HSE and funded entities are included and identify accountable teams/individuals for delivering specific components of the programme. Agree the intended end state, the timetable to achieve the objectives and the resources required; and • Design consistent tools and templates to be used by the HSE and to be cascaded down as resources for funded entities. Assign responsible leads to complete these tools and templates, and develop documentation and capability at operational sites.
FA2.KR1.3	Establish assurance over the Operational Resilience Programme. The HSE should: • Develop programme reporting, including KPIs, a method and timetable for review, and risk management considerations. Ensure that operational resilience is a standing agenda at Board (or Board committee) meetings

Ref #	Recommendation description
FA2.KR1.4	Embed the Operational Resilience capability via training and exercising. The HSE should: • Ensure a commitment to maintain and test the resultant capability by designing an HSE-wide training and exercising programme. This includes a structured programme for delivering knowledge and skills training, and scenario-based exercises to all relevant stakeholders across the HSE and funded entities who have a role to play in any serious or significant incident or crisis; as well as additional training resources, validation programmes and independent Internal Audit review to the Board; and • Ensure ND G&R and at least one Board member has direct competency/experience in the area of operational resilience.
FA2.KR2.1	Establish and document a formal governance structure to oversee clinical and services continuity in the HSE. The HSE should: • Update the existing Clinical and Services Continuity Policy and present it to the Board for review and approval. This should be nested under the overarching Operational Resilience Policy (see recommendation FA2.KR1) and clearly articulate the purpose, scope, applicability, review frequency, authority, Clinical and Services Continuity Management Framework, governance and monitoring of the policy and programme; • Establish a programme of governance for clinical and services continuity - incorporated under the Operational Resilience Programme (see recommendation FA2.KR1.1) - which provides a central point of accountability for the implementation, maintenance, monitoring and validation of activities in line with policy objectives. Formally document roles and responsibilities, a Clinical and Services Continuity Steering Committee and an organisational chart. The scope should reference the HSE and all funded entities; • Formalise robust review and challenge by appropriate personnel, of all stages of the Clinical and Services Continuity Programme, embedding Internal Audit into the clinical and services continuity lifecycle to provide independent assurance to the Board of the HSE's contingency capabilities; • Secure formal clinical and services continuity qualifications for appropriate members of the steering committee/implementation team; • Be prepared to consider the emerging requirements contained in the EU Critical Entities Resilience Directive (CER).
FA2.KR2.2	Support funded entities (hospital groups, hospitals and CHOs) to establish governance over clinical and services continuity. The HSE should: • Implement a Clinical and Services Continuity Steering Sub-Committee at HG, hospital and CHO levels, beneath the HSE Steering Committee; and establish a framework of governance. These groups should have a similar structure, terms of reference and roles and responsibilities as the overarching HSE group; • Draft a specific Clinical and Services Continuity Policy which complements the HSE's policy, according to the policy guidance listed above; • Appoint a relevant clinical and services continuity sponsor; • Integrate clinical and services continuity into project and change management processes where appropriate.
FA2.KR3.1	Establish and embed a clear and consistent approach to clinical and services impact analysis across the HSE to inform recovery prioritisation. The HSE should: • Establish and embed a formal clinical and services impact analysis process, with clear ownership at each level, including the criteria for the RTO and RPO; and, • Ensure the results of the clinical and services impact analysis are formally reviewed and approved on a periodic basis, by senior management, and following any significant systems/process, operational, regulatory or personnel change.

Ref #	Recommendation description
FA2.KR3.2	Design clinical and services continuity workarounds, based on the clinical and services impact analysis, to enable the HSE to continue providing critical services while responding to an incident or crisis. The HSE should: • Design and agree clinical and services continuity workarounds, for critical processes, with the agility and governance to be maintained for a prolonged period, and based on the Clinical and Services Impact Analysis; • Assess all workarounds to ensure they do not pose an unacceptable risk to patient care or to the HSE through the transfer of data or other assets between systems; • Align workarounds for similar systems or processes across the HSE to improve their effectiveness and inform a consistent response; • Reflect the workarounds in the relevant Clinical and Services Continuity Plan.
FA2.KR4	Develop and embed consistent Clinical and Services Continuity Plans at strategic, tactical and operational levels that align with the clinical and services business impact analysis. To ensure that clinical and services continuity plans are compatible with the HSE recovery objectives, the HSE should: • Implement Clinical and Services Continuity Plans at strategic, tactical and operational levels of the HSE, HGs/hospitals and CHOs and that they formally document workarounds and the steps involved to resume normal operations; • Benchmark the Clinical and Services Continuity Plan construction against ISO 22331, and ensure they are compatible with future Sláintecare objectives; • Incorporate the testing of these steps into the clinical and services continuity management training and exercising schedule/programme (e.g. through desktop walkthrough of the resumption procedures to identify any gaps or unforeseen dependencies); and • Ensure soft and hard copies of Clinical and Services Continuity Plans are available in appropriate areas.
FA2.KR5.1	Design an end-to-end Crisis Management Framework (integrated with the existing MEM and IM Frameworks) and overseen by the HSE Resilience Steering Group (see also finding FA2.KR1.1). The HSE should review the existing incident and emergency management structures, and the structures established during the attack and other recent events (e.g. COVID-19), to establish a new integrated end-to-end organisation-wide Crisis Management Framework that is fit-for-purpose across a wide variety of crisis types. This Framework should incorporate all resilience disciplines responsible for implementing organisational preparedness activities (e.g. emergency/incident/crisis response, and clinical and services continuity management), and identify accountable teams/individuals for specific components, as well as define all levels of response required during an actual event at strategic, tactical and operational levels. It should also integrate with the relevant elements of the organisation-wide Major Emergency Management and Incident Management Frameworks. The Framework should include the following elements: • Hierarchy of teams required for response. Typically this will include three layers - operational, tactical and strategic - with command and control escalating according to the nature and severity of the Incident; • Defined roles and responsibilities, and decision making authority, for all those involved in the identification, escalation, response to and management of incidents; • Escalation thresholds and formalised communication channels; • Guidance on how and when to invoke response structure in line with the Incident Classification and Severity Matrix (see also finding FA2.KF14); • Agreed touchpoints and interaction between the HSE, and HGs and CHOs; • Tools and templates to be used by all responders (across the HSE, HG and CHO levels) during an incident (e.g., situation report, classification and severity matrix, impact assessment, decision and action logs).

Ref #	Recommendation description
FA2.KR5.2	Design a suite of crisis response plans and procedures to underpin the Crisis Management Framework. The HSE should design: • A Crisis Management Plan providing detailed roles and responsibilities for key positions in the NCMT and supporting tactical teams (e.g. HG/hospital and CHO leadership), including checklists of activities and considerations, and details of third party support available; • A Technical/Operational Coordination Guide providing the details of how the technical (e.g. IT Ops) and operational teams (e.g. clinical response teams) would coordinate and work together. This includes detailed roles and responsibilities, information flows, processes, checklists of key activities and considerations and details of third party support available; • Scenario-specific plans providing detailed step-by-step operational guides for specific scenarios (e.g. analyst response to malware, fire response plan). The HSE should, using the risks identified in the Corporate Risk Register, conduct a threat profile review and readiness assessment to determine high likelihood, high impact scenarios and create scenario-specific plans for response. This should include severe but plausible total loss scenarios; • Functional Response Plans providing detailed function-specific guidance for non-technical teams, for example a Legal/Regulatory Team and Communications Team (see recommendation FA2.KR7); and • Site-Specific Response Plans templates and guidance, providing resources for standardised clinical and services continuity and crisis management planning at sites across the organisation.
FA2.KR6	Ensure that the resources assigned to internal communications are sufficient. An effective internal communications team is critical to disseminate information and guidance to all 130,000 HSE staff all operating across different levels of the response; this requires additional resources and staff to what is currently available. As part of their future crisis management planning, the HSE should assess the requirements of their crisis response communications strategy and allocate the resources necessary to grow the internal communications team, to reflect the HSE's current operational architecture, and taking into consideration the impacted and involved stakeholder base.
FA2.KR7	Document the Communications Team's existing response structures, processes, tools and templates in a Crisis Communications Plan. The HSE should document a formal Crisis Communications Plan to ensure consistent and efficient communications management across the organisation during an incident/crisis, and to guide the actions of new members of the HSE's communications team. • The communications team should document the response processes, tools and templates, and structures they have found most effective during previous incidents, ensuring the resulting plan dovetails into any existing Major Emergency and Crisis Management Plans and processes, in line with the Crisis Management Framework (see also finding FA2.KF5); • The Crisis Communications Plan should be reviewed in conjunction with the Crisis Communications Plans in place at the HGs and CHOs to ensure the structures and processes involved integrate effectively; • Once finalised, all processes and templates, especially those requiring collaboration with other HSE teams, should be socialised and ratified to ensure they are fit for purpose and based on up-to-date information; and • The Crisis Communications Plan should be reviewed regularly to confirm the content is still correct and relevant, and to incorporate any lessons learnt from new incidents.
FA2.KR8.1	Establish a formal training and exercising programme in support of the Operational Resilience Programme (see also Finding FA2.KF1). The HSE should: • Ensure this programme incorporates clinical and services continuity and crisis management requirements and that all relevant individuals and teams involved at every level of the HSE become familiar with their roles and responsibilities in a crisis or significant clinical and services continuity incident; and • Ensure it is aligned to ISO 22398 Security and resilience - Guidelines for exercising and testing. Define and implement standard training and exercising templates which articulate scope, objectives, assumptions, results, issues log and lessons learned.

Ref #	Recommendation description
FA2.KR8.2	Deliver training to staff in key responsible and supporting roles, and new managers. The HSE should: • Provide Clinical and services continuity and crisis management training for staff in key responsible and supporting roles. Such staff should have knowledge of best practice in relation to each core element of an effective integrated command centre and of an effective Clinical and Services Continuity Management Programme including: risk assessment, Clinical and Services Impact Analysis, clinical and services continuity management strategy selection, plan testing techniques and processes for assessing effectiveness of plans; and • Include clinical and services continuity awareness training for new managers.
FA2.KR8.3	Conduct annual exercises to rehearse the operational resilience capability. The HSE should: • Conduct annual crisis management and clinical and services continuity desktop or simulation exercises with the NCMT and ensure scenarios extend beyond current focus to include other loss scenarios including loss/denial of mission critical infrastructure, unavailability of key persons, systems, processes and facilities; • Conduct annual multi-team crisis management and clinical and services exercises involving key HSE functions (e.g. support services) and funded entities; increasing in complexity over time to continually build organisation-wide maturity and capability; and • Support the nominated responsible owner with responsibility for clinical and services continuity and crisis management to acquire relevant external training to maintain the currency of their expertise.
FA2.KR9	Review and refine the post-incident review process to ensure ongoing and continuous improvement of the response capability. Formal and consistent post-incident reviews should be conducted following all incidents or near misses to capture both areas of positive performance and opportunities for improvement. The Operational Resilience Steering Group should ensure that all post incident reviews are reported centrally to enable learnings to be disseminated across the HSE and funded entities (see also finding FA2.KF1). Mitigating actions should be assigned a responsible owner and tracked centrally until their completion. The process should be reflected in the end-to-end Crisis Management Framework (see recommendation FA2.KR5.1).
FA2.KR10	Instil a culture of preparedness in the HSE to reduce the negative impacts of disruption on its people. The HSE should aim to create a culture that values and emphasises crisis preparedness as well as having confidence in natural ability to respond to major emergencies. In addition to scenario-specific plans to prepare for crisis scenarios (beyond the current scope of floods, adverse weather and aviation disasters) recommended below (see also findings FA2.KF8 and FA2.KF21), the HSE should implement a comprehensive training and exercising programme to familiarise all crisis responders at operational (e.g. hospital/CHO, business support services, IT Security, etc.), tactical (e.g. HSE, regional/area CMTs), and strategic (e.g. HSE NCMT) levels with their roles and responsibilities for crisis preparedness and response, as well as the unique key considerations and decisions required in various crisis scenarios (see also finding FA2.KF8). Conducting scenario-based desktop and simulation exercises will expose individuals to the (simulated) pressures they will experience, thereby reducing the negative impact imposed by external stressors and uncertainty in real life events. Transferring the skills gained in psychologically realistic exercises will facilitate more effective teamwork and decision making in actual crisis situations when they occur.

Ref #	Recommendation description
FA2.KR11	Design and implement an integrated notification and escalation process and acquire a means of mass notification to all HSE staff and contractors. - The HSE should implement a uniform and integrated notification and escalation process within the updated end-to-end response framework, supported by an Incident Classification and Severity Matrix and an 'Activation Membership' list detailing the stakeholders to be informed, across all levels of response, depending on the severity rating of that incident. This will allow critical responders to be notified of an event and convene at pace to instigate a response at the appropriate level to any incident or crisis impacting its operations or services; and - The HSE should review whether the use of mobile phone network providers as a method of sending 'blast notifications' meets the required functionality for mass notification and, if not, should consider investing in a mass emergency notification and communications tool to improve its wider incident notification capability. The solution should include features for notifying all HSE staff members and contractors or smaller groups of staff about any serious incident, crisis or clinical and services continuity event (e.g., a data leak where formal notification and information needs to be disclosed with impacted persons, physical or medical events requiring safety instructions to be issued, or a total system outage/ransomware attack). Clear authority should be designated to an individual or individuals with an appropriate level of authority to send communications from this platform, to ensure all messages are consistent and have been signed off by the appropriate parties (e.g. legal).
FA2.KR12	Establish a Crisis Situation Centre to manage an organisation-wide response to a crisis (see also recommendation FA2.KR5). As part of the Crisis Management Framework (see recommendation FA2.KR5.1), the HSE should establish a Crisis Situation Centre construct to be stood up during a crisis response. This should incorporate the learnings from the Situation Centre introduced by the Defence Forces during the Conti response and include the following elements: Guidance on how and when it should be invoked in line with the Incident Classification and Severity Matrix (see also recommendation FA2.KR14); - The hierarchy of teams required; - Roles and responsibilities and delineated decision authority of each response level; - Escalation thresholds and formalised communication channels; - Agreed touch points and interaction between the Situation Centre and HGs and CHOs; and - Tools and templates to be used by all responders (across the HSE, HG and CHO levels) during an incident (e.g., situation report, classification and severity matrix, impact assessment, decision and action logs).
FA2.KR13	Establish formal retainers with key third parties that may be required to support a crisis response. The HSE should consider the third party support that may be required during an incident include: crisis response, external legal counsel and public relations. These retainers should include service level agreements, clear descriptions of third party roles and responsibilities, and pre-agreed legal requirements (such as non-disclosure agreements) to ensure partners can be engaged to support, and be integrated into, a response immediately and scale to the size of the response required. Work should be conducted with third parties providing technical support to familiarise them with the HSE's IT network, architecture and systems, to facilitate quicker engagement during an incident. The role of retained third parties should be reflected in response plans or playbooks and they should be involved in regular cross-organisation conversations and training exercises with the HSE, the HGs and CHOs to rehearse efficient coordination and communication flows.
FA2.KR14	Develop an integrated HSE-wide incident classification and severity matrix for assessing the organisational impact of an incident. The HSE should consider the third party support that may be required during an incident include: crisis response, external legal counsel and public relations. These retainers should include service level agreements, clear descriptions of third party roles and responsibilities, and pre-agreed legal requirements (such as non-disclosure agreements) to ensure partners can be engaged to support, and be integrated into, a response immediately and scale to the size of the response required. Work should be conducted with third parties providing technical support to familiarise them with the HSE's IT network, architecture and systems, to facilitate quicker engagement during an incident. The role of retained third parties should be reflected in response plans or playbooks and they should be involved in regular cross-organisation conversations and training exercises with the HSE, the HGs and CHOs to rehearse efficient coordination and communication flows.

Ref #	Recommendation description
FA2.KR15	Designate and train incident information managers (or coordinators) at all levels across an incident or crisis response to maintain a consistent overview of the situation as it develops. Further to recommendation FA2.KR12, the HSE should ensure that each workstream beneath the SITCEN, at every command level and workstream, has an information manager (or coordinator) appointed as part of the Incident response team. This role should be implemented in all local hospital response teams, Regional/Area CMTs, and within each HSE workstream up to the NCMT. As the information manager completes their expected role (digesting all information to gain a view of the end-to-end incident), they should escalate their status and update upwards (as with the SITREPs). This will allow the SITCEN information manager to articulate one consolidated account of events, decisions and actions which will achieve situational awareness across all teams and parties involved. To embed this capability the HSE should train those who have been assigned the role of information manager and complete multi-team exercises to rehearse information sharing between teams to maintain situational awareness. Templates created as a result of the ransomware attack should be further developed and embedded into scenario-specific response plans, in order to support the information managers in their role. This structure and format should be used in all teams and work streams to maintain consistency.
FA2.KR16	Identify and acquire a secure and resilient 'out-of-band' technology solution to ensure an alternative means of information sharing and communication. The HSE should ensure that the platform can facilitate email, file sharing, call hosting and the dissemination of communications to all staff and segmented audiences, and enable all responders to see situations reports, actions and decisions logs and other information necessary to support a shared understanding of the Incident.
FA2.KR17	Ensure the 'higher organisational intent' is aligned to the organisational values and drives the response and recovery strategy; review the strategy regularly throughout the response as the situation develops. In this incident, the strategic priority was the restoration and protection of systems underpinning patient care services. The HSE should ensure that all incident response strategies consider both the technical and business response priorities, and be informed by the impacts and requirements of the hospitals, HGs and CHO, to ensure they are fit for purpose. Patient care may not always be restricted to the maintenance of healthcare systems; the possible implications of patient data exposure should be considered in conjunction with discussions on patient care, and incorporated into the HSE's strategic intent during a response. Consideration should be given to how this strategy is cascaded to all levels of the organisation, to direct the actions of the tactical and operational response teams (see finding FA2.KF19) and to inform the activities of third party support. The response strategy should be reviewed regularly during a response based on new information and circumstances to ensure it is still valid and appropriate. The development and implementation of a response strategy should be a key focus during crisis exercising, as this will facilitate a single consistent approach to response and recovery activities.
FA2.KR18	Agree delineated decision making authority across all teams in the organisation likely to be involved in an organisation-wide incident. The HSE should establish an organisational crisis management structure, incorporating hospitals, HGs, CHOs and contracted third parties, which clearly defines the decision making authority at each level. This structure should be socialised and embedded as part of a regular training and exercising programme for all responders (see finding FA2.KR8.3) to ensure it meets the different priorities of all parties and remains fit for purpose. Additional training should be provided for the HSE, HG and CHO leadership to support them in: • creating a shared situational awareness across multiple sites or locations; • developing effective communication flows between senior leadership across multiple sites or locations; and • establishing clear decision making and delegated authority for senior leadership across multiple sites or locations. Critical stakeholders or response team members at every level should therefore receive communication about, and be trained and exercised in, the predefined response structures to ensure the hooks and handovers within every level of the command model is understood and seamless during an incident.

Ref #	Recommendation description
FA2.KR19	Familiarise the Internal Communications Team with the ‘out of band’ technology solution to enable focused and targeted communications during a crisis (see also recommendation FA2.KR16). The HSE should set up user accounts for all staff members pre-incident on the selected ‘out of band’ communication platform to expedite transition to the new platform during a system outage. Staff members should be familiarised with the platform and its functionality ahead of an incident. Details for all alternative user accounts should be recorded centrally and stored offline to ensure contact information for all staff members is readily available during any disruption to the HSE’s standard communications channels. Crisis response and communications workstream leads should establish cascading contact trees to notify staff of an incident, to initiate the use of the out of band platform, and to enact specific channels for the discussion of response and recovery activities between core responders. This will allow workstreams to maintain a central repository of useful information and act as an audit trail for post incident review and reporting.
FA2.KR20	Review processes, plans and resourcing for response to future potential data breaches. The HSE should ensure the appropriate resources, tools and templates are created with sufficient advance notice and time prior to notifying data subjects of a breach. Having initial notification letters, FAQ’s, responses, and sufficiently trained resources to manage an influx of requests for information will be critical to ensuring a successful roll out of notification if and when required. The HSE should also review and document the processes established during the response to support their future preparedness. They should: • Complete the work of the Legal and Data Workstream in response to the Incident; • Embed the Legal and Data Workstream in the Crisis Management Framework (see also recommendation FA2.KR5.1 and FA2.KR12); • Update the existing Data Protection Breach Management Policy to support the Legal and Data Workstream in future responses, including the data breach notification risk assessment; • Rehearse the workstream’s response both individually and as part of wider HSE exercising programme (see also recommendation FA2.KR8.3); • Agree retainers with third parties for future web monitoring services; • Ensure materials used to support the notification of data subjects, such as letters, FAQs and talking points, are agreed with the Communications Team; and • Conduct resource planning for future notification programmes; for example, call centres to respond to the significant influx of incoming requests once data subjects are notified.
FA2.KR21	Scenario planning should be informed by the risk register, the process embedded in the Crisis Management Plan, and the activity conducted throughout incident and crisis response. The HSE should ensure that the risk register is used to drive the creation of severe but plausible scenarios against which the HSE should validate its resilience capability is validated. The process should be extended to engage individuals from the HSE’s senior leadership team, risk management, clinical and services continuity and crisis management disciplines in regular scenario planning against the organisation’s top risks. This is best conducted in a workshop format to identify potential political, economic, sociological, technical, legal and regulatory, environmental and organisational impacts related to each of the HSE’s top risks, and to then explore the worst, best and most likely scenarios for each. Mitigating actions resulting from these workshops should be assigned to an owner with the appropriate level of authority to facilitate organisational change where required, and tracked throughout their lifecycle to confirm they are completed to an acceptable level. These actions and all other outputs from these activities should be used to inform preparation activities across resilience disciplines, to ensure that plans, processes and structures are fit for purpose; and where applicable specific response plans to be developed for the most plausible risks (see also findings FA2.KR5.2). Scenario planning should be included in the Crisis Management Plan to support HSE to prepare for likely outcomes and mitigate subsequent impacts during a response.
FA2.KR22.1	Design clinical and services continuity workarounds, informed by the Clinical and Services Impact Analysis. The HSE should design and agree clinical and services continuity workarounds, for critical processes, with the agility and governance to be maintained for a prolonged period, and based on the Clinical and Services Impact Analysis (see also recommendations FA2.KR3.1, FA2.KR4 and FA2.KR23).

Ref #	Recommendation description
FA2.KR22.2	Design workarounds to support rapid data remediation post-incident or crisis. The HSE should: - Establish a pre-agreed out of band communications and information sharing platform (see also finding FA2.KR16) to ensure data generated by workarounds outside normal operations is captured in a format that can easily be retrofitted with the information held on HSE systems. As part of the organisation's stand-down process, each site and workstream should assign an individual with responsibility for overseeing the consolidation of patient and service data; and - Reconcile all medical data stored and managed through interim processes post the attack, including data stored on personal devices/accounts and in paper form.
FA2.KR22.3	Rehearse workarounds in multi-team exercises. The HSE, HGs and CHOs should participate in multi-team exercises to explore how high impact or likely scenarios could impact their operations. This is extremely important as it helps identify likely and potential impacts to the organisation and responders. These may often need a team and significant investment to resolve, however even the discussion and establishment of hypothetical workarounds will likely reduce the number of ineffective emergency protocols and allow space for creative thinking to consider the ideal solution for all parties involved (see also recommendation FA2.KR8.3).
FA2.KR22.4	Consider a review to establish the longer term clinical impacts of the Conti attack. Finally, the HSE should consider conducting a review to understand the longer term clinical impacts that resulted from the Conti attack. This review should build on the findings of the draft research report into the effectiveness of the patient safety risk mitigation strategies following the Incident, and inform future steps to improve the HSE resilience against potential future attacks and minimise the risk to patient care.
FA2.KR23	Ensure the Clinical and Services Impact Analysis is informed by an up-to-date asset register and configuration management database (see also findings FA2.KF3 and FA2.KF22.1). As part of this process, the HSE should work with CHOs and HGs to develop a clear overview of the interdependencies between all departments and local sites using HSE infrastructure or services, with the aim to create a prioritised list for systems at both a central and local level. This should be informed by a service model for delivering patient care. The HSE should reconcile all medical data stored and managed through interim processes post the attack, including data stored on personal devices/ accounts and in paper form (see also finding FA2.KF20). Contingency plans should be developed by the business owners and IT teams to maintain priority and critical services (as defined in a Clinical and Services Impact Analysis) during the disruption of one or more key systems. These plans should be socialised and embedded across the organisation, and a version of them stored offline, to ensure they can be implemented effectively during an incident. In the event of an incident impacting multiple systems, as within the Conti attack, recovery prioritisation should be addressed on a regular basis from the beginning of the response, to direct resources to the appropriate systems and services from the offset.

Ref #	Recommendation description
FA2.KR24	Map and document the people and technology resources and processes required to recover all critical systems in a pre-defined sequence. The HSE should ensure that the Cyber Incident Response Playbook documents a pathway to recovery that maps the people, processes and technology requirements of each system, to provide a pathway to recovery in the event of single or multiple system failure. During a major outage or disruption, recovery priorities should be agreed with central and local response and IT teams and communicated to all responders to streamline the recovery of integrated and independent systems. Once recovery priorities have been agreed, incident response mechanisms need to be invoked that provide the most effective communication and coordination between teams. Central coordination meetings should be held with the asset and application register acting as a tool to guide recovery activities. A read-only, and regularly updated, list of prioritised applications should be made available to all technical recovery teams to direct their activities and keep them informed of the actions being undertaken across the response. To achieve this an operational rhythm needs to be established by: • Setting up a meeting cadence at and between each response level e.g., operational or “Bronze” (HG and CHO) meeting followed by a tactical or “Silver” (HSE) meeting, then a strategic or “Gold” (EMT) meeting to share a cascade of updates increasing in importance, escalating priorities. This waterfall flow between the command levels should also be used in reverse to share decisions and actions simultaneously to all teams and impacted sites; • Each meeting following a set agenda to ensure all required areas are covered off, particularly in terms of situational awareness of the Incident; and • Use of uniform templates for collecting incident updates, action tracking and required decisions. It is recommended that at each level of response there is a dedicated role to ensure coordination within and between teams. This can be the role of a Crisis Coordinator or SITCEN Information Manager (see also finding FA2.KF15).
FA3. KR1	The HSE should continue to develop an asset register that is aligned to clinical and corporate services, as well as underpinning a process to ensure the register is maintained up to date. Doing so will allow the HSE to determine the potential impact of any future incident and effectively respond in a planned, controlled and structured manner.
FA3. KR2	The HSE should create a cybersecurity strategy, covering at a minimum incident detection, incident response and business recovery. It will also need to be aligned to the HSE strategy objectives and signed off by the HSE Board.
FA3. KR3	The HSE should establish an appropriate cybersecurity risk and governance framework to ensure there is a consistent and clear allocation of responsibility, authority, and accountability. Including the need to establish reporting processes to ensure potential cybersecurity incidents are appropriately reported in all cases. This should provide a forum for key stakeholders e.g. Clinical Operations, Corporate Services, Third Party service managers, Sections 38s and 39s to discuss and align on cybersecurity priorities. The HSE should appoint a senior leader for cybersecurity (a CISO) who has experience rapidly reducing organisations vulnerability to threat, designing cyber security transformation programmes and providing assurance to Boards of management. This should provide the required assurance to the Board in facilitating effective cybersecurity management.
FA3. KR4	The HSE should complete its required OES returns on an annual basis to ensure compliance with NISD regulations and to understand potential cybersecurity weaknesses with critical services.
FA3. KR5	The HSE should develop a formal cybersecurity risk framework aligned to the business’ operational risks and strategic plans.
FA3. KR6	The HSE should implement a Third Party Risk Management framework that defines how third parties to the HSE are assessed for cybersecurity risks and what risk treatment plans are appropriate to address residual cyber risk.
FA3. KR7	The HSE should introduce a comprehensive, formalised cybersecurity training and awareness programme that is delivered to all staff at all grades across the organisation. This should be conducted on a regular basis.
FA3. KR8	The HSE should introduce centralised processes and procedures to manage and review the appropriate access and identities that require access to services and data. This should be in the form of an Identity Access Management (IAM) solution that would consistently manage access across users, System Admins and third parties.

Ref #	Recommendation description
FA3. KR9	ICT HSE should implement a structured process for performing data backups and storing this data off site. Regular testing of this data should take place to ensure success recovery.
FA3. KR10	The HSE should develop a strategy for adopting the appropriate protective technologies and ensure consistent deployment across the HSE network.
FA3. KR11	The HSE should develop a process to maintain security baselines for all operational hardware and software, including but not limited to establishing preventative processes such as patch and vulnerability management processes.
FA3. KR12	The HSE should develop a cybersecurity threat profile that is informed by relevant sources to enable an effective monitoring capability. This should include threat intelligence feeds to provide an informed view of the latest cyber threats relevant to the HSE. These feeds should be used in conjunction with a SIEM to inform and provide IOCs for monitoring and detecting across the HSE ICT estate. Aligned to this the HSE should implement anti-virus consistently across the estate, ensure it as well as logging and EDR outputs are aggregated and obtain a 24x7 security operations centre (SOC) to monitor the entire business and detect anomalous behaviour and events.
FA3. KR13	The HSE should implement alert monitoring on all network servers, endpoint devices, and firewalls for the external and internal networks. Specific use cases for each alert should be developed for the chosen SIEM.
FA3. KR14	The HSE should implement a holistic network detection and response functionality with a dedicated team to continually monitor for and respond to alerts.
FA3. KR15	The HSE should develop an appropriate cybersecurity response policy, supported by plans and/or run books for cybersecurity incidents that are regularly reviewed and exercised so that it can mount an effective and efficient response in the event of a future incident.
FA3. KR16	The HSE should develop a formal internal communications plan where key internal parties such as senior leadership, voluntary hospitals, CHOs are receiving timely and consistent messages. Specifically the HSE should develop specific runbooks and template responses for specific scenarios to aid a speedy response and ensure there is consistent communication
FA3. KR17	The HSE should ensure that an appropriate response policy, plan, and process are in place to manage multiple security incidents, perform response investigations, and collect evidence to assess the best potential mitigation plan.
FA3. KR18	The HSE should develop formal mitigation strategies and tactics to isolate, remove, and monitor threats. Key Performance Indicators (KPIs) should be put in place so that performance can be optimised.
FA3. KR19	The HSE should establish a formal process, as well as resources to ensure lessons were learnt and codified from all incidents and are maintained to reflect operational and organisational change.
FA3. KR20	The HSE should implement a cybersecurity recovery plan that links to an asset register detailing Clinical, Corporate and other priorities and test this plan on a regular basis.
FA3. KR21	The HSE should develop a formal process for capturing improvements/lessons learnt following an incident.
FA3. KR22	The HSE should consider developing a communications strategy for cybersecurity incidents.

E. Focus area 1 - detailed technical timeline



[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[Redacted]

[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

F. Focus area 2 - detailed organisational timeline

A factual timeline detailing key events, identified from focus area 2, that occurred during the HSE's response to, and recovery from, the ransomware attack are detailed below:

The colour coding in this Figure is designed to easily identify key themes across the timeline. Some entries in the 'Date and Time' column are drawn from interviews and workshops, rather than documentary evidence, so are only attributable to a date or date range.

Figure 25: Factual timeline detailing key events

Date and Time	Theme	Event
14 May 2021 at 01:00	Ransomware deployment	First evidence of execution of ransomware and the encryption on the HSE systems ³²⁸ .
14 May 2021 at 02:50	Identification of ransomware attack	The National Service Desk received the first of multiple reports of encrypted systems from hospitals and CHOs as a result of the ransomware attack ³²⁹ .
14 May 2021 at 04:36	Identification of ransomware attack	Encryption identified on multiple servers in the data centre ³³⁰ .
14 May 2021 at 04:41	Invocation of response process	Due to the widespread reports of encryption, and the presence of ransomware in the data centre, the HSE invoked the Critical Incident Process ³³¹ .
14 May 2021 at 05:10	Invocation of response process	The first Critical Incident (CI) meeting was held ³³² .
14 May 2021 Pre-10:00	Invocation of response process	The COO and CIO decided to switch off the HSE's servers and discussed engagement with voluntaries.
14 May 2021 Pre-10:00	Invocation of response process	Decision made to disconnect the HSE links via the NHN and disable links to the e-Government services.
14 May 2021 Pre-10:00	Identification of ransomware attack	Email services were made unavailable as a result of the containment actions implemented (HSE removing network connectivity and powering off servers) ³³³ .
14 May 2021	Stakeholder communications	There was wider HSE awareness that the Incident was security related through text message communications, media reports, word of mouth and phone calls.
14 May 2021 at 07:00	Media coverage of the Incident	RTE News released a news bulletin on the Incident.
14 May 2021 at approximately 06:00	Stakeholder communications	The CEO notified the Board of the Incident.
14 May 2021 Early morning	Invocation of response process	The CEO notified the EMT / NCMT.
14 May 2021 at 7:00	Invocation of response process	First evidence that local Crisis Management Teams (CMTs) started to convene.
14 May 2021 at 07:28	Stakeholder communications	HSE Live issued a tweet notifying the public of an incident and the shutdown of services.
14 May 2021 Shortly after the Incident appeared on the news	Legal and regulatory	The Data Protection Officer rang the Data Protection Commission.
14 May 2021 Early morning	Invocation of response process	The Deputy COO, OoCIOI notified members of the Office of the CIO and directed them not to turn on machines.

328 M_HSE_Intrusion Investigation Report - REDACTED (FINAL).pdf, 2021

329 CIM 2 - Conti Ransomware Incident coordination Form Ver 2.1(2), 2021

330 CIM 2 - Conti Ransomware Incident coordination Form Ver 2.1(2), 2021

331 Conti Cyber Response NCMT Structures Governance and Admin V1.10 31052021

332 Conti Cyber Response NCMT Structures Governance and Admin V1.10 31052021

333 CIM 2 - Conti Ransomware Incident coordination Form Ver 2.1(2), 2021

Date and Time	Theme	Event
14 May 2021	Third party engagement	The OoCIO started gathering contact information for all contractors working with the HSE.
14 May 2021 at 08:30	Invocation of response process	The first meeting of the NCMT was held ³³⁴ .
14 May 2021 8:30- 09:00	Invocation of response process	Regional CMTs began to stand up.
14 May 2021 8:30- 09:20	Invocation of response process	The CIO notified PCRS of the Incident and PCRS shut their systems down
14 May 2021 Pre-10:00	Invocation of response process	The HSE initiated a preventative lockdown mode strategy to contain the impact of the attack ³³⁵ .
14 May 2021 Pre-10:00	Third party engagement	It was reported that the HSE engaged the Garda National Cybercrimes Unit, Interpol and the NCSC to support the response ³³⁶ . From this point the NCSC supported internal and external communications about the technical details of the Incident and helped coordinate the technical response through their [REDACTED] platform.
14 May 2021 at 10:00	Invocation of response process	The first Major Incident (MI) meeting was held ³³⁷ .
14 May 2021 at 10:30	Third party engagement	With the support of the NCSC, the HSE engaged the HSE's Incident Response provider to provide incident response services for the HSE. The HSE engaged Third Party C, Third Party D, and Third Party B to provide support.
14 May 2021 Pre-12:20	Stakeholder communications	The Internal Communications team set up and populated the public facing website.
14 May 2021 at 14:00	Stakeholder communications	The HSE sent a text message to the HSE staff work devices notifying staff members of a ransomware incident impacting the HSE, voluntary hospitals and CHOs ³³⁸ .
14 May 2021 at 16:30	Programme management	The MI Meeting established a once daily operating rhythm.
14 May 2021	Legal and regulatory	Informal communications between the Data Protection Officer and the Data Protection Commission.
15 May 2021	Programme management	The HSE's Senior Management Team set up a war room in an office on Molesworth Street ³³⁹ .
15 May between 00:00 - 23:59	Restoring systems	Senior management were provided with clean [REDACTED] mailboxes to allow for communication during the initial stages of the response.
15 May 2021 at 10:00	Stakeholder communications	Communicating with internal stakeholders, the HSE set up a cyber specific email address for the National Service Desk, for entities to report issues.
15 May 2021 at 13:16	Legal and regulatory	The Data Protection Officer formally reported the breach to the Data Protection Commission via the webform ³⁴⁰ .
16 May 2021	Programme management	The communications team established a twice daily ³⁴¹ meeting rhythm.
16 or 17 May 2021 Pre-11:00	Restoring systems	The HSE identified a list of their priority applications ³⁴² .
17 or 18 May 2021 Pre-11:00	Restoring systems	The HSE held an application prioritisation exercise ³⁴³ .

334 Conti Cyber Response NCMT Structures Governance and Admin V1.10 31052021

335 Minutes of Cyber Attack MI Meeting 10 am - 14052021

336 Minutes of Cyber Attack MI Meeting 10 am - 1405202

337 Minutes of Cyber Attack MI Meeting 10 am - 1405202

338 Minutes of Cyber Attack MI Meeting 10 am - 14052021

339 Programme RAID Log

340 Original DPC Notification_May 2021

341 Daily SITRPEPs scheduled for 0915 & 1830

342 Minutes of Cyber Attack MI Meeting 11 am - 17052021

343 Minutes of Cyber Attack MI Meeting 11 am - 17052021

Date and Time	Theme	Event
18 May 2021	Third party engagement	Initial meeting was held between the HSE Office of Emergency Management and the Defence Forces to discuss support requirements.
19 May 2021	Media coverage of the Incident	The Financial Times published an article on the attack ³⁴⁴ .
19 May 2021	Programme management	The CIO, Head of Occupational Health and the National Ambulance Service identified a risk of staff burnout. Occupational Health were requested to attend HQ to check responders' health and staff rotas were implemented ³⁴⁵ .
19 May 2021 at 11:00	Restoring systems	The go-to-green process for recovering systems was communicated to internal stakeholders on the Incident Management call.
19 - 21 May 2021	Media coverage of the Incident	Social media monitoring system Talk Walker was set up to scan the web for leaked patient data.
19 - 21 May 2021	Stakeholder communications	The HSE staff members were given derogation to use personal emails and devices for crisis communications.
20 May 2021	Legal and regulatory	The HSE received an injunction from the Irish High Court preventing the publication of leaked data ³⁴⁶ .
19 - 21 May 2021	Restoring systems	The first clean laptops were distributed to select HSE staff members.
21 May 2021 at 11:00	Restoring systems	It was reported that the decryption key was received by the HSE on the evening of 20 May 2021, and a new workstream was created to focus on decrypting impacted systems ³⁴⁷ .
21 May 2021	Programme management	The SITCEN Coordination Hub was established at CityWest. The Conference Suite and accommodation at CityWest were made available for the HSE responders ³⁴⁸ .
22 May 2021	Programme management	SITCEN daily briefings were established at 09:15 and 17:30. These were attended by the Garda National Cyber Crime Bureau (NCCB) ³⁴⁹ .
23 May 2021	Programme management	A specialist Information Manager was brought in to manage the response information architecture and directory.
24 May 2021 at 11:00	Stakeholder communications	It is reported that the HSE senior management requested a picture of service availability ³⁵⁰ .
24 May 2021 at 10:15	Programme management	The HSE was in the final stages of the 'assessment' phase, ³⁵¹ with the recovery phase gathering pace.
24 May 2021	Programme management	The HSE Workstream Leads were embedded with all Workstream Partner Leads ³⁵² .
24 May 2021 at 11:00	Restoring systems	The go-to-green document was released to internal stakeholders to provide guidance in recovering systems.
25 May 2021	Stakeholder communications	The Office of the CIO declared via WebEx a blanket ban on all internet access from the HSE systems ³⁵³ .
26 May 2021 at 10:00	Restoring systems	It was communicated through a SITCEN Situation Report that mobile and telephony networks were stabilised ³⁵⁴ .
26 May 2021 at 11:00	Restoring systems	It was reported that drop in centres were being established over a period of time to clean Community devices ³⁵⁵ .
26 May 2021	Stakeholder communications	Guidelines were issued on the use of personal ICT resources and email addresses in a letter to all staff ³⁵⁶ .
27 May 2021 at 11:00	Restoring systems	It was reported that personal devices were allowed to connect to the HSE network following a risk assessment.

- 344 'Irish patients' data stolen by hackers appears online', Financial Times [<https://www.ft.com/content/13d33a08-ce83-4f8a-8d93-a60a5e097ed8>]
- 345 Programme RAID Log
- 346 OoCIO Cyber Governance Report v0.2
- 347 Minutes of Cyber Attack MI Meeting 11 am - 21 May 2021
- 348 Conti Cyber Response NCMT Structures Governance and Admin V1.10 31052021
- 349 Conti Cyber Response NCMT Structures Governance and Admin V1.10 31052021
- 350 Minutes of Cyber Attack MI Meeting 11 am - 24052021
- 351 20210524-SITREP_HSE SITCEN-1015hrs
- 352 20210524-SITREP_HSE SITCEN-1930hrs
- 353 Minutes of Cyber Attack MI Meeting 11am - 25052021
- 354 20210526-SITREP_HSE SITCEN-1015hrs
- 355 Minutes of Cyber Attack MI Meeting 11 am - 26052021
- 356 Letter to all Staff-1 - 26 May 2021

Date and Time	Theme	Event
28 May 2021 at 14:00	Restoring systems	National [REDACTED] email was made accessible to 34,000 users ³⁵⁷ .
1 June 2021 at 11:00	Stakeholder communications	It was reported that the new National Cyber Support Service number went live ³⁵⁸ .
1 June 2021 at 11:00	Restoring systems	It was reported that the National Service Desk was functioning again ³⁵⁹ .
4 June 2021 at 11:00	Restoring systems	Application site-to-site VPN was set up for Attend Anywhere and Care Notes to allow vendors to access the HSE's environment.
8 June 2021	Standing down of response	The Defence Forces were transitioned out.
10 June 2021	Restoring systems	Access to the internet became critical for PCRS.
10 or 11 June 2021	Programme management	National Service Desk staff members were redeployed to support email restoration ³⁶⁰ .
18 June 2021	Standing down of response	The governance workstream was prepared to return to BAU ³⁶¹ .
18 June 2021	Third party engagement	The HSE had their first meeting with the Digital Government Oversight Unit.
28 June 2021	Programme management	MI meetings decreased in frequency to twice weekly.
4 July 2021	Restoring systems	Internet access was provided for EHIC and Medical Card Online.
26 July 2021	Standing down of response	The IM Communications Bridge was closed down.
The following events are outside the scope of the PIR (which details activity that took place up to 31 July 2021), but have been detailed as they provide context to recovery efforts.		
24 August at 13:00	Stakeholder communications	The mailbox that was set up to deal with issues relating to the ransomware attack was stood down ³⁶² .
31 August at 13:00	Stakeholder communications	In response to ongoing issues with the [REDACTED], the mailbox set up to deal with issues relating to the ransomware attack was reinstated ³⁶³ .

357 Minutes of Cyber Attack MI Meeting 11 am - 28052021

358 Minutes of Cyber Attack MI Meeting 11 am - 01062021

359 Minutes of Cyber Attack MI Meeting 11 am - 01062021 People on site and assisting regional offices.

360 Minutes of Cyber Attack MI Meeting 11 am - 11062021

361 Governance RAID Log

362 Weekly Brief 20210824- Final V1

363 Weekly Brief 20210831- Final V1

The Incident	The cyber attack on the HSE
The Patient Zero Workstation	A HSE workstation
The Attacker	The perpetrator of the cyber attack

G. Focus area and key recommendation mapping

Strategic Recommendation - Section 4	Focus Area - Key Recommendations
Strategic recommendation 1.1 - Establish clear responsibilities for IT and cybersecurity across all parties that connect to the NHN, share health data or access shared health services. Establish a 'code of connection' that sets minimum cybersecurity requirements for all parties and develop an assurance mechanism to ensure adherence.	FA3.KR21
Strategic recommendation 1.2 - Establish an executive level cybersecurity oversight committee to drive continuous assessment of cybersecurity risk and a cybersecurity transformation programme across the provision of health services.	FA1.KR2
Strategic recommendation 1.4 - Establish a board committee (or repurpose an existing one) to oversee the transformation of IT and cybersecurity to deliver a future-fit, resilient technology base for provision of digitally-enabled health services, and ensure that IT and cybersecurity risks remain within a defined risk appetite. Consider the inclusion of further specialist non-executive members of the committee in order to provide additional expertise and insight to the committee.	FA1.KR3, FA1.KR7, FA1.KR8, FA1.KR9, FA1.KR10 & FA1.KR11
Strategic recommendation 2 - Establish a transformational Chief Technology & Transformation Officer (CTTO) and office to create a vision and architecture for a resilient and future-fit technology capability; to lead the delivery of the significant transformation programme that is required, and to build the increased function that will be necessary to execute such a scale of IT change.	FA3.KR14
Strategic recommendation 2.1 - Appoint a permanent Chief Technology & Transformation Officer with the mandate and authority to develop and execute a multi-year technology transformation, build an appropriate level of IT resource for an organisation the scale of the HSE and oversee the running of technology services.	FA3.KR17
Strategic recommendation 2.2 - Under the office of the CTTO, develop an IT strategy to achieve a secure, resilient and future-fit IT architecture, required for the scale of the HSE organisation.	FA1.KR14
Strategic recommendation 3.1 - Appoint a CISO and establish a suitably resourced and skilled cybersecurity function	FA1.KR1, FA1.KR5, FA1.KR12, FA3.KR10 & FA3.KR11
Strategic recommendation 3.2 - Develop and drive the execution of a multi-year cybersecurity transformation programme to deliver an acceptable level of cybersecurity capability for a national health service.	FA1.KR4, FA1.KR13, FA1.KR15, FA3.KR3 & FA3.KR7

Strategic recommendation 4.1 - Implement a clinical and services continuity transformation programme reporting to the National Director for Governance and Risk. Establish an Operational Resilience Policy and Resilience Steering Committee to drive integration between resilience-related disciplines, and an overarching approach to resilience.	FA2.KR1.1, FA2.KR1.2, FA2.KR1.3, FA2.KR2.1, FA2.KR2.2, FA2.KR3.1, FA2.KR22.1, FA3.KR9 & FA3.KR20
Strategic Recommendation - Section 4	Focus Area - Key Recommendations
Strategic recommendation 4.2 - Enhance crisis management capabilities to encompass events such as wide-impact cyber attacks or large-scale loss of IT.	FA2.KR1.4, FA2.KR3.2, FA2.KR4, FA2.KR5.1, FA2.KR5.2, FA2.KR6, FA2.KR8.1 (see also Finding FA2.KF1), FA2.KR8.2, FA2.KR8.3, FA2.KR9, FA2.KR10, FA2.KR12, FA2.KR14, FA2.KR15, FA2.KR17, FA2.KR18, FA2.KR20, FA2.KR21, FA2.KR22.3, FA2.KR22.4, FA3.KR6, FA3.KR16, FA3.KR19 & FA3.KR22
Tactical Recommendation - Section 4	Focus Area - Key Recommendations
Tactical recommendation 1.2 - Continue to reconcile medical data stored and managed through interim processes post the ransomware attack and place centralised governance over these activities	FA2.KR22.2
Tactical recommendation 1.3 - Collate and manage artefacts created in response to the Incident, including initial production of an asset register	FA2.KR23 (see also Findings FA2.KF3 and FA2.KF22.1), FA2.KR24 & FA3.KR7
Tactical recommendation 1.4 - Appoint an interim senior leader for cybersecurity (a CISO) to be responsible for driving forward tactical cybersecurity improvements, managing third-parties that provide cybersecurity services and lead the cybersecurity response to cyber incidents.	FA1.KR1
Tactical recommendation 1.5 - Formalise a programme and governance to respond to tactical recommendations arising from the Incident Response investigation and provide assurance over their implementation	FA1.KR7, FA1.KR8, FA1.KR9, FA1.KR10, FA1.KR11 & FA3.KR2
Tactical recommendation 2 - Security monitoring	FA3.KR4 & FA3.KR13
Tactical recommendation 2.1 - Establish an initial cybersecurity incident monitoring and response capability to drive immediate improvement to the ability to detect and respond to cybersecurity events	FA1.KR6
Tactical recommendation 3 - Ability to respond to a similar Incident in the near future	FA3.KR5, FA3.KR15 & FA3.KR18
Tactical recommendation 3.1 - Review the process for managing internal crisis communications including resources	FA2.KR6, FA2.KF7, FA2.KR11, FA2.KR16, FA2.KR19, FA2.KR24 & FA3.KR8

H. HSE Risk assessment tool

Figure 26: Impact table

	Negligible	Minor	Moderate	Major	Extreme
Harm to a Person	Adverse event leading to minor injury not requiring first aid. No impaired Psychosocial functioning.	Minor injury or illness, first aid treatment required. < 3 days absence. < 3 days extended hospital stay. Impaired psychosocial functioning greater than 3 days less than one month.	Significant injury requiring medical treatment, e.g. Fracture and/or counselling. Agency reportable, e.g. HSA, Gardaí (violent and aggressive acts). > 3 Days absence. 3-8 Days extended hospital Stay. Impaired psychosocial functioning greater than one month less than six months.	Major injuries/ long term incapacity or disability (loss of limb) requiring medical treatment and/or counselling. Impaired psychosocial functioning greater than six months.	Incident leading to death or major permanent incapacity. Event which impacts on large number of service users or member of the public. Permanent psychosocial functioning incapacity.
Service User Experience	Reduced quality of service user experience related to inadequate provision of information.	Unsatisfactory service user experience related to less than optimal treatment and/or inadequate information, not being talked to & treated as an equal; or not being treated with honesty, dignity & respect – readily resolvable.	Unsatisfactory service user experience related to less than optimal treatment resulting in short term effects (less than 1 week).	Unsatisfactory service user experience related to poor treatment resulting in long term effects.	Totally unsatisfactory service user outcome resulting in long term effects, or extremely poor experience of care provision.
Compliance (Statutory, Clinical, Professional & Management)	Minor non compliance with internal PPPGs. Small number of minor issues requiring improvement.	Single failure to meet internal PPPGs. Minor recommendations which can be easily addressed by local management.	Repeated failure to meet internal PPPGs. Important recommendations that can be addressed with an appropriate management action plan.	Repeated failure to meet external standards. Failure to meet national norms and standards/ Regulations, (e.g. Mental Health, Child Care Act etc). Critical report or substantial number of significant findings and/or lack of adherence to regulations.	Gross failure to meet external standards. Repeated failure to meet national norms and standards/ regulations. Severely critical report with possible major reputational or financial implications.

	Negligible	Minor	Moderate	Major	Extreme
Objectives/ Projects	Barely noticeable reduction in scope, quality or schedule.	Minor reduction in scope, quality or schedule.	Reduction in scope or quality of project; project objectives or schedule.	Significant project over-run.	Inability to meet project objectives. Reputation of the organisation seriously damaged.
Business Continuity	Interruption in a service which does not impact on the delivery of service user care or the ability to continue to provide service.	Short term disruption to service with minor impact on service user care.	Some disruption in service with unacceptable impact on service user care. Temporary loss of ability to provide service.	Sustained loss of service which has serious impact on delivery of service user care or service resulting in major contingency plans being involved.	Permanent loss of core service or facility. Disruption to facility leading to significant 'knock on' effect.
Adverse Publicity/ Reputation	Rumours, no media coverage. No public concerns voiced. Little effect on staff morale. No review/ investigation necessary.	Local media coverage – short term. Some public concern. Minor effect on staff morale/public attitudes. Internal review necessary.	Local media – adverse publicity. Significant effect on staff morale & public perception of the organisation. Public calls (at local level) for specific remedial actions. Comprehensive review/ investigation necessary.	National media/ adverse publicity, less than 3 days. News stories & features in national papers. Local media – long term adverse publicity. Public confidence in the organisation undermined. HSE use of resources questioned. Minister may make comment. Possible questions in the Dáil. Public calls (at national level) for specific remedial actions to be taken possible HSE review/ investigation.	National/ International media/adverse publicity, > than 3 days. Editorial follows days of news stories & features in National papers. Public confidence in the organisation undermined. HSE use of resources questioned. CEO's performance questioned. Calls for individual HSE officials to be sanctioned. Taoiseach/ Minister forced to comment or intervene. Questions in the Dáil. Public calls (at national level) for specific remedial actions to be taken. Court action. Public (independent) Inquiry.

	Negligible	Minor	Moderate	Major	Extreme
Finance	0.33% budget deficit.	0.33-0.5% budget deficit.	0.5-1.0% budget deficit.	1.0-2.0% budget deficit.	>2.0% budget deficit .
Environment	Nuisance Release.	On site release contained by organisation.	On site release contained by organisation.	Release affecting minimal off-site area requiring external assistance (fire brigade, radiation, protection service, etc.).	Toxic release affecting off-site with detrimental effect requiring outside assistance.

Figure 27: Likelihood scoring

Rare/Remote (1)		Unlikely (2)		Possible (3)		Likely (4)		Almost Certain (5)	
Actual Frequency	Probability	Actual Frequency	Probability	Actual Frequency	Probability	Actual Frequency	Probability	Actual Frequency	Probability
Occurs every 5 years or more	1%	Occurs every 2-5 years	10%	Occurs every 1-2 years	50%	Bimonthly	75%	At least monthly	99%

Figure 28: Risk matrix

	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
Almost Certain (5)	5	10	15	20	25
Likely (4)	4	8	12	16	20
Possible (3)	3	6	9	12	15
Unlikely (2)	2	4	6	8	10
Rare/Remote (1)	1	2	3	4	5

I. Glossary and terms

Glossary

AD	Active Directory
BAU	Business as Usual
BCM	Business continuity management system
C2	Command and Control
CER	Critical Entities Resilience Directive
CISA	Cybersecurity & Infrastructure Security Agency
CTTO	Chief Technology & Transformation Officer
CEO	Chief Executive Office
CISO	Chief Information Security Officer
CHI	Children's Health Ireland
CHO	Community Healthcare Organisation
CSF	Cyber Security Framework
COBIT	Control Objectives for Information and Related Technology
DC	Domain Controller
DDoS	Distributed denial of service
DoH	Department of Health
DPO	Data Protection Officer
DPC	Data Protection Commission
DRR	Divisional Risk Register
DPER	Department of Public Expenditure and Reform
EDR	Endpoint detection and response
EMT	Executive Management Team
ERM	Enterprise Risk Management
EHR	Electronic health records
FTE	Full-Time Equivalent
FBI	Federal Bureau of Investigation
HG	Hospital Group
HSE	Health Service Executive
ICT	Information and Communications Technology

IT	Information Technology
iPMS	Integrated Patient Management System
MI	Major Incident
MiIPMS	Major Incident Integrated Patient Management System
MN-CMS	Maternal & Newborn Clinical Management System
MRN	Medical Record Number
ND G&R	National Director for Governance and Risk
NCMT	National Crisis Management Team
NCSC	National Cyber Security Centre
NHN	National Healthcare Network
NIMIS	National Integrated Medical Imaging System
NISD	Network and Information Systems Directive
NiSRP	National Integrated Staff Records & Pay Programme
NIST	National Institute of Standards and Technology
NTPF	National Treatment Purchase Fund
OES	Operators of Essential Services
OoCIO	Office of the Chief Information Officer
PPG	Pandemic Placement Grant
PCRS	Primary Care Reimbursement Service
PIR	Post Incident Review
RDP	Remote Desktop Protocol
RTO	Recovery Time Objectives
RPO	Recovery Point Objectives
SLA	Service Level Agreement
SCA	State Claims Agency
SOC	Security Operations Centre
SIEM	Security Incident and Event Manager
SitCen	Situation Centre
SITREP	Situation Report
SIEM	Security Incident Event Management
SME	Subject Matter Expert

Terms

Term	Definition
Acute hospital services	Acute hospital services are delivered across the network of seven acute Hospital Groups and provide scheduled care (planned care), unscheduled care (unplanned / emergency care), diagnostic services, specialist services (specific rare conditions or highly specialised areas such as critical care and organ transplant services), cancer services, trauma services, maternity and children's services and includes the National Ambulance Service. These services are provided in response to population needs and are consistent with wider health policies and objectives, including those of Sláintecare. Hospitals continually work to improve access to healthcare, whilst ensuring quality and patient safety initiatives are prioritised within allocated budgets, including the management of COVID-19 and other infections.
CMMI Model	The CMMI model is used across industries and is intended to guide process improvement across a project, division, or an entire organisation.
COBIT framework	COBIT helps organisations meet business challenges in the areas of regulatory compliance, risk management and aligning IT strategy with organisational goals.
Community healthcare services	Community healthcare services include primary care, social inclusion, older persons' and palliative care services, disability and mental health services, which are provided for children and adults, including those who are experiencing marginalisation and health inequalities. Community healthcare services are currently delivered across nine Community Healthcare Organisations (CHOs) and are provided through a mix of HSE direct provision as well as through voluntary section 38 and 39 service providers, GPs and private providers. The community healthcare budget accounts for almost 40% of the HSE spend.
Malware	Malicious software.
NIST cybersecurity framework	The framework integrates industry standards and best practices to help organisations manage their cybersecurity risks. It provides a common language that allows staff at all levels within an organisation to develop a shared understanding of their cybersecurity risks.
Penetration testing	Penetration testing (also called pen testing or ethical hacking) is a systematic process of probing for vulnerabilities in an organisations networks and applications.
Post Incident Review	A post incident review identifies which organisational and technical control mechanisms did not work properly, as well as which factors influenced the ability to detect and handle the incident.
Ransomware Capability Framework	PwC's framework to identify technical control gaps that contributed to the Incident occurring.

Term	Definition
Ransomware attack	A type of cyber attack where criminals hack into the victim's network and deploy ransomware to encrypt data, before attempting to extort organisations into paying ransoms.
Red Team	An exercise that simulates real-world hacker techniques to test an organisation's resilience and uncover vulnerabilities in their defences.
Sláintecare	Sláintecare is the ten-year programme to transform Ireland's health and social care services. The Sláintecare report was adopted by the Government and published in May 2017. The Sláintecare Implementation Strategy was approved by Government in July 2018.



<https://t.me/learningnets>

Redacted for security purposes.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with over 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.ie. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.
© 2021 PwC. All rights reserved. 06867