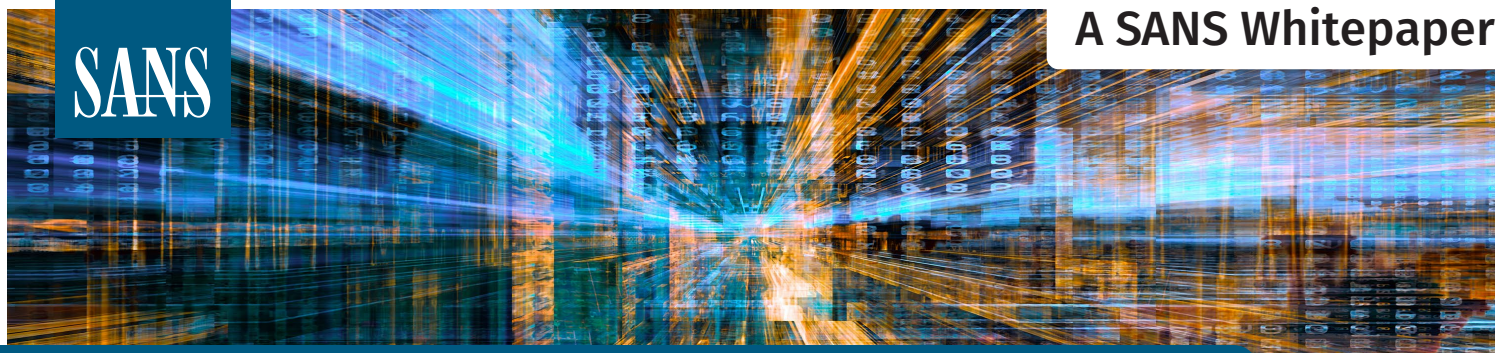
Responding to Incidents in Industrial Control Systems: Identifying Threats/Reactions and Developing the IR Process

Don C. Weber

SANS

A SANS Whitepaper



Responding to Incidents in Industrial Control Systems: Identifying Threats/Reactions and Developing the IR Process

Written by **Don C. Weber**

May 2020

Sponsored by:

Honeywell

Operational Technology Environments Under Attack

Cyber criminals are attacking businesses throughout the world and have been since the 1990s. They are attacking businesses that operate industrial control networks, but some organizations with OT environments have only recently come to accept this fact.

Some organizations thought these attacks were limited to critical infrastructure. *Critical infrastructure* refers to the companies that produce products that have, or can have, a significant impact on the community. Such impact may be in the form of affecting power to a large area with millions of people or the devastation of major waterways if spillage occurs. Some of these companies, because of their potential impact, are regulated and monitored by governing bodies to ensure that the availability and integrity of their digital infrastructure is more resilient to cyberattack.

Network isolation and segmentation do not constitute a complete cybersecurity program. Cyber criminals are learning that OT environments are viable targets.

Companies with OT environments not considered critical infrastructure are, typically, not governed by regulations. In the past, the lack of regulations meant that protecting the OT environments from cyberattacks was up to that individual organization. As with many businesses, some OT companies do cybersecurity better than others. Because OT environments are implemented with insecure protocols, brittle services, default/group passwords and embedded devices, the security considerations were often limited to basic network isolation and segmentation.

Network isolation and segmentation do not constitute a complete cybersecurity program. They provide a starting point but, in isolation, provide a small patch over a gaping hole. Cyber criminals are learning that OT environments are viable targets. The successes of Stuxnet malware in 2010[1] and the attacks on the Ukrainian power grid in 2015[2] have demonstrated that critical infrastructure can be infiltrated and manipulated to achieve desired operational physical effects to support the overall goals of the attacker. These successes also show that the equipment deployed within organizational processes are exploitable attack surfaces. Cyber criminals took notice of these weaknesses and started focusing on OT environments. Some companies were prepared. Most companies were not.

The role of cybersecurity in any organization is to deter, detect and defend. The act of defending often leads teams to discuss the likelihood and frequency of attacks. Understanding these concepts is important, but in OT processes the organization must consider the consequences of a successful attack.

To help organizations understand what this means, FERC Order 706[3] states the following about the frequency and likelihood of attacks on OT environments: "Because there is insufficient data available to determine frequency, it should be assumed that an event will occur." It also states, "Risk-based assessment methodology should focus on the consequences of an outage, not the likelihood of an outage."

Ultimately, these statements mean businesses should be prepared to respond to an attack. Cases of incident response in critical infrastructure are well-documented. Cases of incident response outside of critical infrastructure are a bit harder to identify. This situation is mainly due to organizations not being comfortable about documenting these incidents because they could be attributed to an immature security program. Fortunately, there are a few positive examples about security efforts and incident response from businesses with OT environments (see "Norsk Hydro's Response to a Malware Attack").

In addition to Norsk Hydro's noteworthy response to its malware attack, other organizations demonstrate solid preparation too. In 2019, Bayer published their annual sustainability report.[5] This report provides stakeholders and the public with details about how the company is doing and its efforts to improve. Bayer's plans for a cyberattack are specifically addressed within this report: "In 2019, for example, we simulated an extensive malware attack on our global IT to test our cyber defenses, internal reporting chains and reaction times. We also tested the restoration of IT systems and data for one of our global data centers at another site together with our IT service providers."

In order to defend, a cybersecurity team must understand what incident response is and the steps that lead to success. The rest of this paper will outline the incident response process in OT environments, discuss the areas that can be measured and improved, and provide examples of the pitfalls that increase the level of effort and cost when organizations are not prepared by seasoned incident responders.

Norsk Hydro's Response to a Malware Attack

In the first quarter of 2019, attackers gained access to assets within Norsk Hydro's corporate network.[4] On March 19 of that same year, the attackers initiated a ransomware attack against Norsk Hydro's assets. It took 14 days for the response team to regain control of their assets. Recovery of the network began on April 1, 2019, with a gradual ramp-up of their processes. Norsk Hydro's team was extremely forthcoming with information about their response efforts for their customers. Their actions demonstrate a mature team that prepared for eventual cyberattacks.

---

[1] https://en.wikipedia.org/wiki/Stuxnet

[2] https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack

[3] US Federal Energy Regulatory Commission Order No. 706, "Mandatory Reliability Standards for Critical Infrastructure Protection," Jan. 18, 2008, www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf, p. 69

[4] www.hydro.com/Document/Index?name=General%20cyber-attack%20presentation%20April%2012.pdf&id=28255

[5] "Bayer Sustainability Report 2019," www.bayer.com/en/bayer-ag-sustainability-report-2019.pdfx, p. 58.

IT and OT Incident Response Phases

The best way to manage stressful situations that require important decisions is to have a plan of action. Incident response plans require a structured approach to provide a path of success to an organization's team. Understanding the commonalities and differences related to incident response for IT and OT environments is essential.

PICERL Process

In business environments, information security teams and select members of IT teams are familiar with the common phases of incident response (IR). IR efforts require close management to ensure those efforts address specific goals and stay on task. These efforts can be extremely complex and, therefore, require organization similar to any emergency project. To organize IR efforts, SANS outlines and teaches a six-phase approach.[6] These phases are Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned, commonly referred to as PICERL.

Preparation	• People • Notes • Relationships • Policies	• Procedures • Comms Plan • Tools • Mgt Tng	• Training • Jump Bag
Identification	• Awareness • Need to Know • Unusual Processes • Unusual Security Evts • Alert Early	• Use OOB Comms • New Accts/Privs • Primary IR Handling • Passive Monitoring • Odd Sch Tasks	• Unusual Files • Analyze Logs • Chain of Custody
Containment	• Stop Bleeding • Categorize • Notify Mgt • Remove LAN Cbl • Memory Captures • Chg Pswds • Short-Term • Criticality	• Asgn Primary IRH • FW/IDS Filters • Adjacent Host Logs • Kill Backdoors • Back-Up • Sensitivity • Low Profile • ISP Coord	• Patch-Exploited Vuln(s) • Long-Term • Document Actions • Infected Vlan • Forensic Images
Eradication	• Del Artifacts • Apply All Patches • Black Hole IPs • Root Cause	• Addl FW/IDS Filters • Seek Other Host Footholds • Restore Back-Up	• Chg DNS Names • Wipe/Format/Rebuild • Remove Malware • Rescan Network
Recovery	• Return to Ops • Monitor (Signs/Shells/Artifacts/Events) • Move to Production (Approval) • Script Searches for Attacker Artifacts		
Lessons Learned	• Document Incident • All Affected Parties Review/ Comment on Draft • Finalize Report • Seek Required Changes • Immediately Upon Recovery Phase	• Provide Exec Summary • Seek Funding • Assign to On-Screen IRH • Reach Report Consensus • Address Process Not People • Update Procedures	

Figure 1. PICERL Phases[7]

For individuals new to IR, each of the PICERL phases can be a little confusing. More information is necessary to understand the overall goals of each phase to organize IR efforts with specific goals. Figure 1 provides a list of topics, courses of action and artifacts related to each phase. This representation should help team members understand the actions and efforts associated with each phase of the IR process.

[6] SANS Institute, "SEC504: Hacker Tools, Techniques, Exploits and Incident Handling," www.sans.org/course/hacker-techniques-exploits-incident-handling

[7] "SANS 504-B Incident Response Cycle: Cheat-Sheet," www.sans.org/media/score/504-incident-response-cycle.pdf

Effectively managed business projects maintain the project's life cycle as consistently as possible. At first glance, PICERL appears to have a natural flow from one phase to the next that mirrors a normal project life cycle. Many teams and organizations have discovered, however, that IR is complex and confusing. Teams may believe they have completed a phase only to discover they missed something or that there is new or additional information they need to address. The organization's leadership and the IR team may become confused and even extremely frustrated if they do not understand the dynamic ramifications of a cyberattack.

Fortunately, most security events will not become security incidents. For example, consider an application alert for 10,000 failed logins. Initially, inexperienced teams are going to assume the application is experiencing a brute force attack and decide they have identified an attack. The next steps, in their mind, should be to contain the attack by taking immediate action. While a large number of failed logins are investigable events, only structured and planned investigation can identify whether the failed logins are malicious. Large numbers of failed logins are often attributed to a broken administrative script, where the credentials were not updated after a password change. If this is the case, there is no need for containment. The team's process will most likely guide them to make notes about the events that will feed into the Lessons Learned phase of the process.

Where incident response becomes more challenging is during the later phases of the process. During Containment, Eradication or Recovery, it is not unusual for teams to identify new issues or new events that change the overall understanding of the situation. Discovering new issues will force the team, as shown in Figure 2, to return to previous phases and even force them to conduct actions across the organization multiple times. This situation will, over time, lead to fatigue and frustration, particularly when the individuals did not expect to repeat actions. Without training, team members and leadership consider repeating actions as setbacks rather than a natural part of the process.

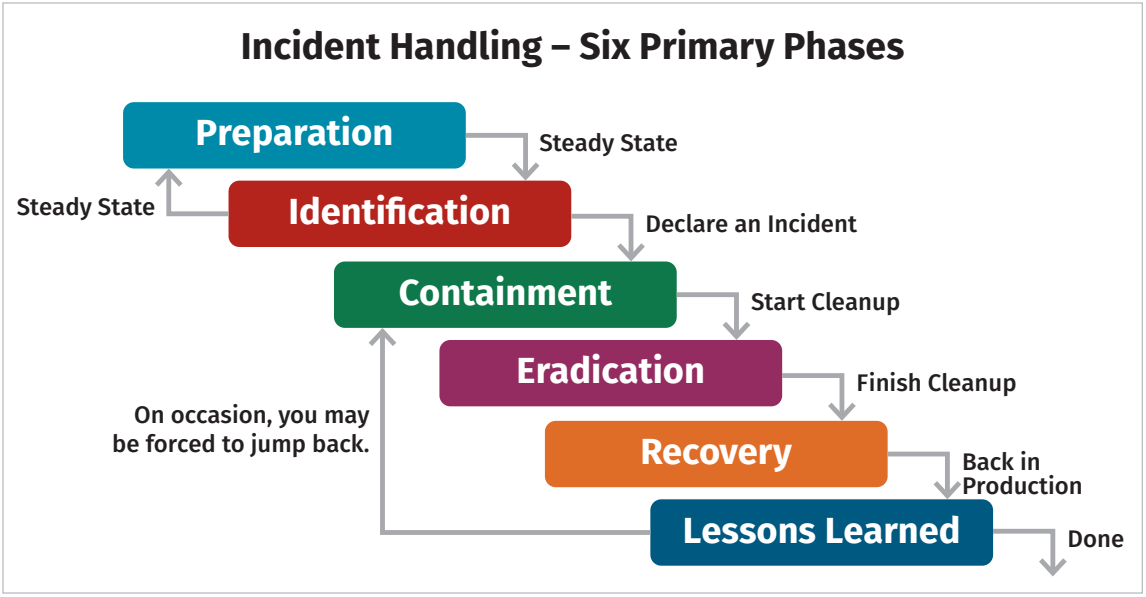


Figure 2. IR Phase Progression—Actual Incident[8]

[8] SANS Institute, "SEC504: Hacker Tools, Techniques, Exploits and Incident Handling," www.sans.org/course/hacker-techniques-exploits-incident-handling

OT Multi-Stage IR Process

Attacks on OT environments add to the complexity of the overall IR process. While the response aspect is the same, there are additional attacker activities to consider within the OT network of the organization. SANS expands upon this concept by expanding the Cyber Kill Chain model.[9]

The Cyber Kill Chain shown in Figure 3 is a description of how attackers approach achieving their goals within an organization. Stage 1 outlines the flow of an attack by outlining that attackers gather information, use this information to identify targets and develop tools, use these tools to implement the attack, and accomplish their mission. For most businesses, this is the extent of the cyberattack.

For organizations with OT environments, a cyberattack may not stop with Stage 1. Attackers with goals to disrupt, deny or destroy a business's process will progress from Stage 1 to Stage 2 of the ICS Cyber Kill Chain. This progression results in additional necessary attacker activity to understand the OT environment, develop additional attacks, test the attack to ensure viability and then implement the attack to achieve the desired goal.

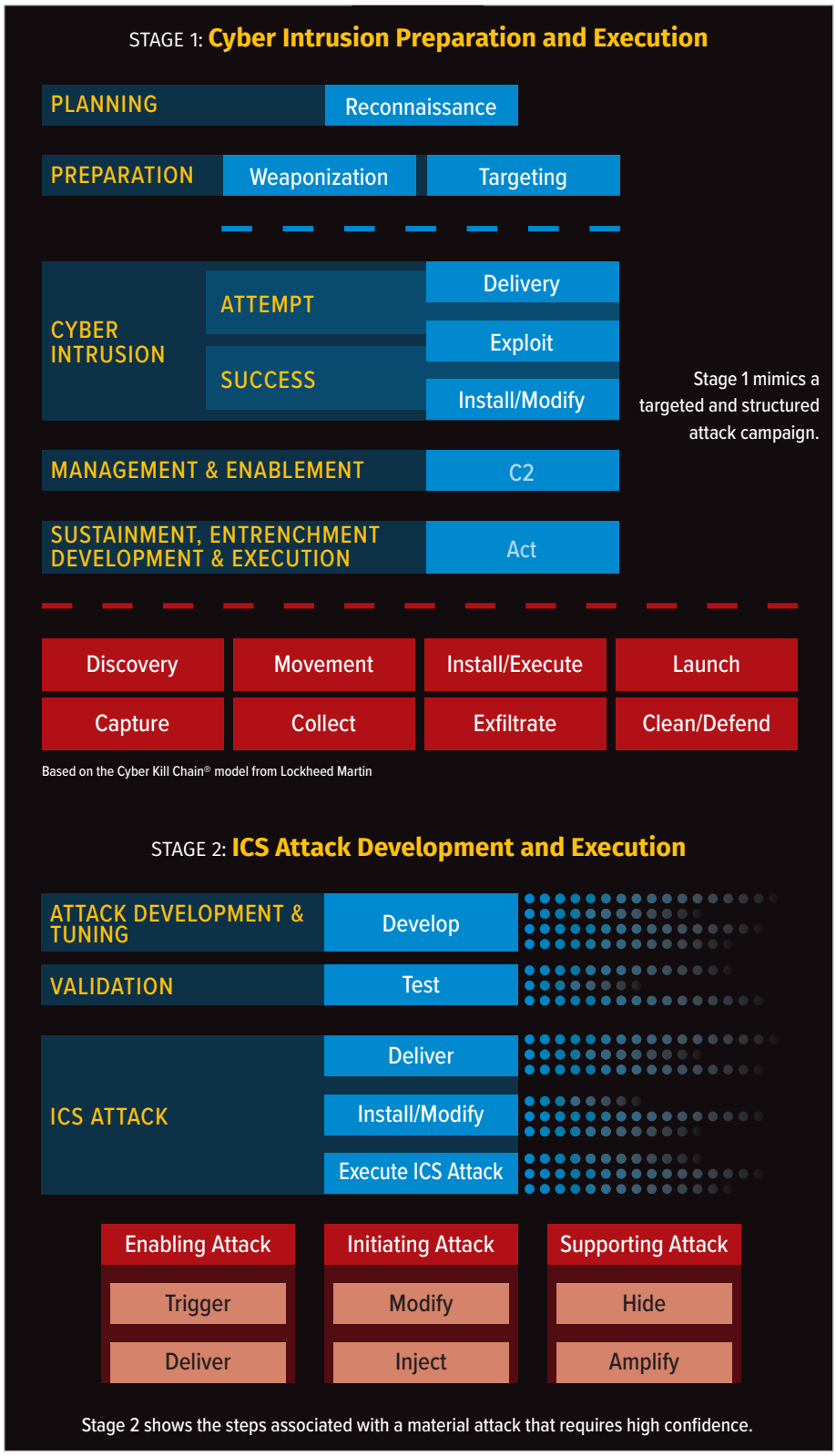


Figure 3. SANS ICS Cyber Kill Chain[10]

[9] www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[10] SANS Institute, Course materials for "ICS515: ICS Active Defense and Incident Response," www.sans.org/course/industrial-control-system-active-defense-and-incident-response

Cost of Gaps Between the Phases

Developing, implementing and executing an incident response process is the first step. Understanding the performance of the organization and the effectiveness of their actions during a cyberattack is the next step.

Gaps and Their Importance

Gaps are the subjective time periods between different events within the incident response effort. Shorter gaps typically indicate minimized impact on the business and reduce cost associated with the overall effort. Three common gaps used to measure how an organization managed a specific incident are outlined in "Three Most Common Gaps to Measure Incident Handling."

As described, compromises of OT environments occur in two stages. This makes calculating the CtD gap difficult for some teams. Do organizations base their calculations on when the compromise occurred within the corporate environment? Or is CtD for control networks calculated by when attackers gain access to OT assets? To clarify, a compromise is a compromise, no matter where the initial compromise vector was initiated. Thus, the CtD gap is measured by the first moment an attacker gained access to the organization—no matter whether it was corporate, OT or otherwise. However, understanding how and when an attacker gained access to assets on the control network is very important. The longer an attack has unfettered access to the OT environment, the more time they have to develop, test and deliver their attack. Reducing the CtD gap as much as possible is the best-case scenario for any attack.

OT teams are particularly challenged by the DtC gap. The SANS ICS team has noted that the real issue with understanding containment within OT environments is related to the limited detection, forensic tools and cybersecurity controls deployed within the control network. OT teams find it difficult to actually know whether they understand the incident completely enough to validate containment. Thus, when the team feels they have achieved containment, it is very likely that eradication and recovery efforts will uncover that the attackers are still present or that the control network has been re-infected.

The CtR gap is primarily a risk measurement, rather than a key performance indicator within OT environments. Taking down a facility to perform complete eradication and recovery activities may cause more of an operational impact than the attack itself. Decisions by leadership drive the actions taken by the incident response team. Leadership's decisions are driven by the facility's analysis and risk management programs to assess the risk of remaining operational during the incident. It is not unusual for a facility or process to remain operational while compromised until the next scheduled outage.

Three Most Common Gaps to Measure Incident Handling

- **Compromise to Detection (CtD) Gap—**The time period between initial compromise to initial detection, also known as *dwell time*. Requires an understanding of the initial infection vector or an educated guess built from system and network activity. *Detection time* is when the incident started, not the first logged system or network event—unless that event was acted upon and used to escalate the incident.
- **Detection to Containment (DtC) Gap—**The time period between initial detection (taken from the CtD Gap data) to containment of the event. *Containment time* is marked when the technical and business leadership agree that the incident response team understands the attacker's actions within the environment and can prevent additional attacker activities.
- **Containment to remediation (CtR) Gap—**The time period between containment of the incident (taken from the DtC Gap data), eradication of all attacker-related tools and control mechanisms, and thorough remediation (also known as *recovery*) of all affected assets.

Reducing the CtD gap is typically the most productive effort for an organization. The DtC and CtR gaps are subject to the actual incident and are improved by the information provided from tools and processes implemented to reduce the CtD gap. Reducing the CtD gap requires good vision into the events that occur within the environment. Good vision is a product of information, tools and personnel. Information comes from systems, applications, and networks—and their correlation. Tools help to produce additional information, alert to anomalous activity and provide a deeper understanding of the correlated data. Personnel leverage tools and experience to understand situations and extrapolate connections between events and the business environment or, in the case of OT, the processes. Good vision reduces false positive reactions, develops a concrete baseline of activity and reduces all three gaps. Figure 4 provides a visual breakdown of how each gap correlates with both stages of an attack on the OT environment and the security controls that play a part in reducing the incident response gaps.

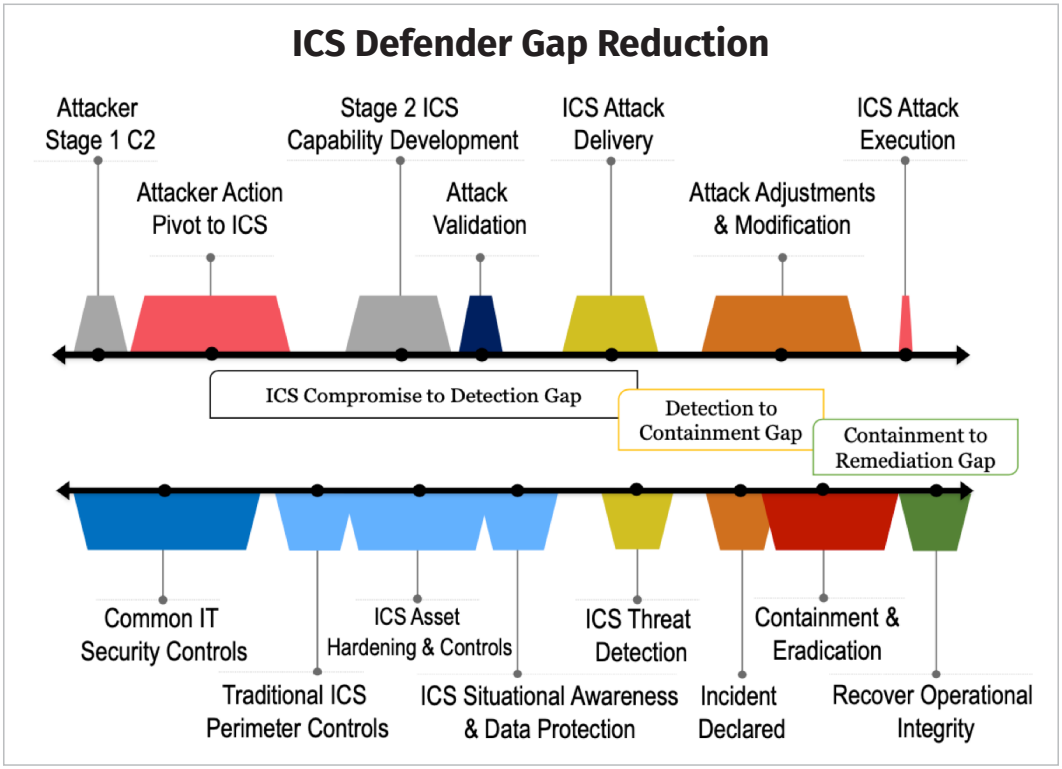


Figure 4. ICS Defender Gap Reduction[11]

Actual Gap Calculations

In 2019, SANS conducted two surveys related to incident response: "SANS 2019 Incident Response (IR) Survey: It's Time for a Change,"[12] and "SANS 2019 State of OT/ICS Cybersecurity Survey."[13] These surveys provide insight into the current state of incident response in companies with and without OT environments. The first survey provides detailed gap data from organizations with non-OT corporate environments. These environments may have included process environments but did not provide information that helped the author single out the OT sectors. The

The Hidden Control Network

Organizations may have OT environments but not recognize it. Businesses with online stores will often have warehouses with distribution lines. These distribution lines can contain OT assets, such as barcode scanners, PLCs to direct boxes along conveyor belts and wireless networks for forklifts. Other examples include the assets that make up building automation networks that control temperature, lighting and other business-critical infrastructure. If these assets have not been identified as OT assets or as a process, then they are very likely connected to the corporate environment or third-party networks.

[11] Image provided by Tim Conway for The SANS Institute

[12] "SANS 2019 Incident Response (IR) Survey: It's Time for a Change," July 2019, www.sans.org/reading-room/whitepapers/incident/paper/39070

[13] "SANS 2019 State of OT/ICS Cybersecurity Survey," June 2019, www.sans.org/reading-room/whitepapers/analyst/2019-state-ot-ics-cybersecurity-survey-38995

businesses responding to the survey provided the following information, shown in Figure 5, about the CtD, DtC, and CtR gaps they experienced in 2019.

The other survey did include companies with OT environments. These organizations outlined their 2019 incident response experiences and provided details about the gaps they experienced, as shown in Table 1.

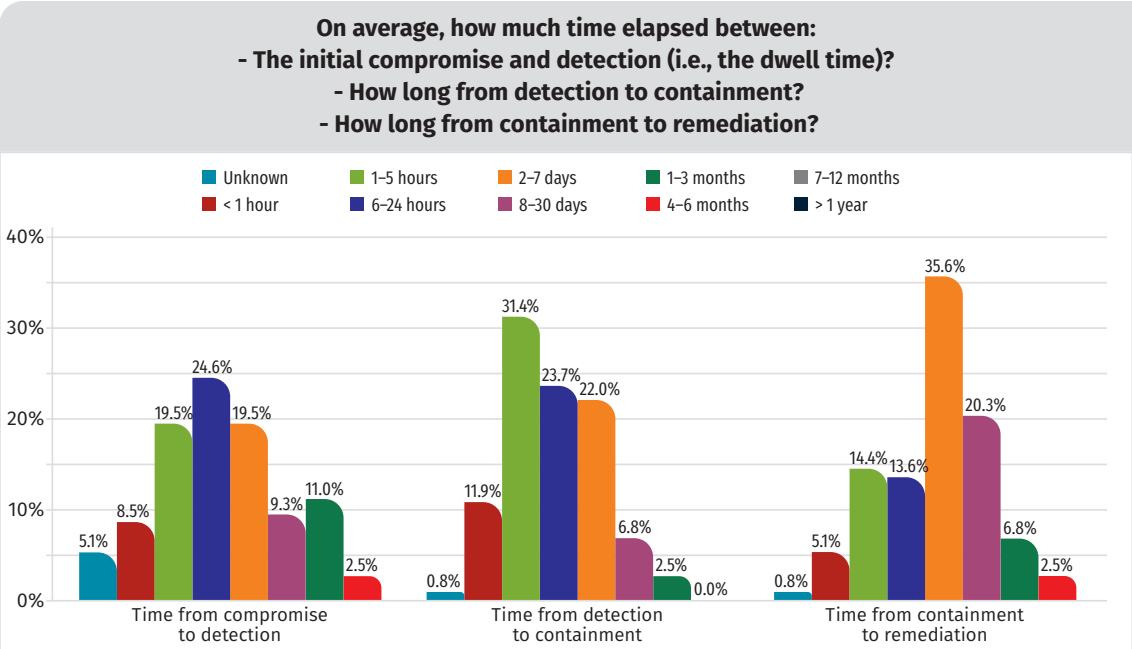


Figure 5. Compromise to Remediation Times[14]

The data from the corporate IR survey is a bit more granular than the information from the OT cybersecurity survey. Combining the data from the corporate information makes it easy to compare with the data from companies with OT environments (see Table 2).

Table 1. Timeline for Compromise to Remediation 2019[15]

Step	Timeline	Percentage
Compromise to Detection	2 to 7 days	44.8%
Detection to Containment	6 to 24 hours	53.6%
Containment to Remediation	2 to 7 days	53.9%

Table 2. Incident Response Gap Times by Corporation Type

Gap	Timeline	Corporate Companies	OT Companies
Compromise to Detection	2 to 7 days	72.1%	44.8%
Detection to Containment	6 to 24 hours	67.0%	53.6%
Containment to Remediation	2 to 7 days	68.7%	53.9%

The information in Table 1 shows a clear difference between the detection of an attack in corporate companies versus companies with a control network. While 72.1% of corporate organizations detected a compromise within seven days, only 44.8% of organizations with OT environments were able to do the same. The reality of the situation is most likely even worse, because this information is coming from organizations that have the experience and information necessary to generate these key performance indicators. Companies with OT environments that have this data often have it because of some type of regulation. Thus, information from businesses that do not have incident response teams within their OT environments are not represented in this data. If the missing data from non-regulated OT environments were included, it would, very likely, dramatically increase the time frames for each gap. Either way, this information clearly shows that the OT industry is falling significantly behind other organizations when it comes to identifying intrusions.

Two-thirds of businesses can detect a compromise within a week of the initial activity. Less than half of businesses with OT environments can detect breaches in their corporate networks within a week. Compromises of their OT infrastructure, most likely, take even longer to identify.

[14] "SANS 2019 Incident Response (IR) Survey: It's Time for a Change," July 2019, www.sans.org/reading-room/whitepapers/incident/paper/39070, p. 4, Figure 2.

[15] Adapted from "SANS 2019 State of OT/ICS Cybersecurity Survey," June 2019, www.sans.org/reading-room/whitepapers/analyst/2019-state-ot-ics-cybersecurity-survey-38995, p. 9, Table 3.

Data Used to Reduce Gaps

Both surveys also include valuable information about the data collected in preparation for and during an incident. The corporate survey provides a list of the information collected that was the most valuable to understanding the state of the environment and activities that occurred during an incident. Figure 6 shows the top three types of data that corporate incident response teams found most useful when investigating suspicious events. These three are a consolidation of network and system information that are stored and then fed into a correlation solution, such as a SIEM, to understand how the events relate to one another and build a picture of activity.

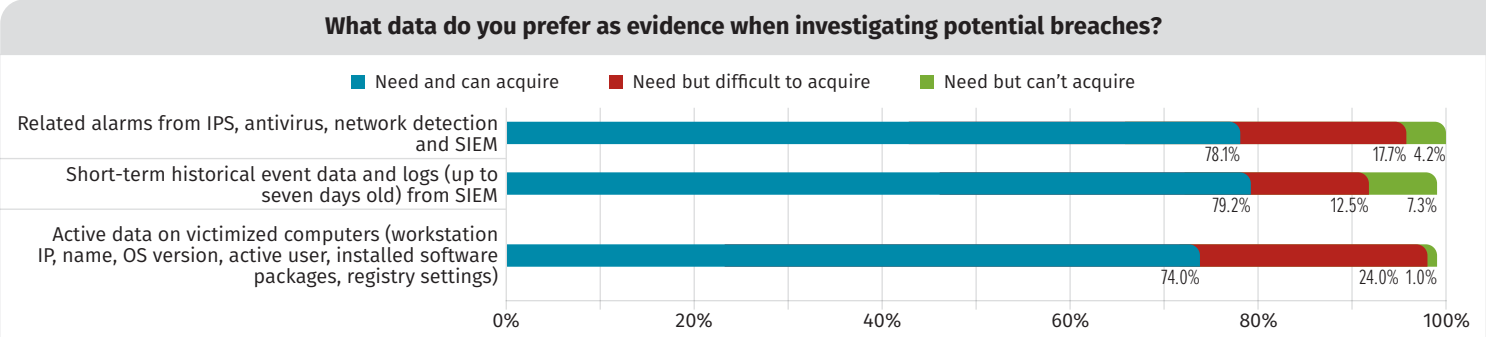


Figure 6. Sources of Evidence for Investigations[16]

The OT survey provides a percentage of organizations that collect data from different components within their OT environments. There is no indication that these organizations feed all of this data into a SIEM; therefore, we cannot make conclusions about how mature these organizations are when correlating and analyzing this information. The data does contain information about the impact the specific components have on the processes within the organization's environment. The red lines in Table 3 identify the top four components categorized by their impact. Information from the two highest impact components, embedded controllers and external field control network, were collected by fewer than half (indicated by the yellow line) of the

Table 3. OT/Control System Components Support of Visibility[17]

OT/Control System Components	Risk	Impact	Collection
Server assets running commercial OS (Windows, UNIX, Linux)	57.6%	32.7%	73.6%
Network devices (firewall, switches, routers, gateways)	30.2%	30.2%	65.3%
Connections to other internal systems (enterprise networks, system to system)★	42.0%	31.2%	54.4%
Engineering workstations	38.0%	29.3%	50.3%
Operator workstations	33.2%	28.8%	48.2%
Remote access appliances (VPN)★	25.4%	18.5%	43.5%
Connections to the field control networks (SCADA)★	36.1%	34.1%	38.9%
Physical access systems★	22.4%	16.6%	30.6%
Control system communication protocols	23.9%	20.5%	28.0%
Wireless communication devices and protocols★	27.8%	13.2%	27.5%
Process control application	16.1%	20.0%	21.2%
Plant historian	14.6%	13.2%	19.7%
Mobile devices (laptops, tablets, smartphones)★	36.1%	12.2%	19.2%
Embedded controllers or components (e.g., PLCs, IEDs)	22.9%	33.2%	18.7%
Field devices (digital sensors and actuators)	19.5%	19.0%	13.5%
Analog modems★	12.2%	6.3%	4.7%

[16] Adapted from "SANS 2019 Incident Response (IR) Survey: It's Time for a Change," July 2019, www.sans.org/reading-room/whitepapers/incident/paper/39070, p. 8, Figure 7.

[17] Adapted from "SANS 2019 State of OT/ICS Cybersecurity Survey," June 2019, www.sans.org/reading-room/whitepapers/analyst/2019-state-ot-ics-cybersecurity-survey-38995, p. 15, Table 6.

organizations in the survey. Red stars indicate components that provide external connectivity into the control network. Fewer than half of the organizations surveyed collected information about the activity used to access their OT environments, a significant and extremely concerning state of affairs.

Organizations should give external connectivity, digital and physical, extra consideration when calculating risk and impact. They represent the remote attack surfaces of the OT environment and should be associated with the enforcement boundaries identified by ISA/IEC 62443.

Cost of Not Preparing

Managed security service providers sit on the front lines for incident response. These organizations often provide remote security operation centers that monitor the system and network events generated by their clients. They often also provide security professionals to augment corporate teams when the company is affected by a cyberattack. They provide unique insight into useful strategies that prepare a company for incident response and explain how not preparing increases the gaps during the response efforts.

The difference between clients that are prepared and those that are not is striking and significant. John McGloughlin of GuardSight Inc. has experienced up to an 80% increase[18] in the level of effort during incident response for his customers:

> ***Those organizations that do not prepare or rationalize the lack of preparation as being connected to a view of their assets [as] not being high-value targets risk destruction or significant pain—statistically. There is a consistent decline in dwell time of more than 80% since 2018 in customers that endorse preparedness. That mark is consistent with industry data as a whole, which in some studies is as high as 90%.***

Another important consideration for preparation is asset management. The Center for Internet Security 20 Critical Controls lists hardware[19] and software[20] asset management as the first two critical controls. Tyler Hudak of TrustedSec enforced this categorization in a recent email to the author:

> ***Having good visibility into your hosts and network prior to an incident is key to ensuring the organization can move through the incident response phases quickly and effectively.***

He provided an example where the lack of visibility added days to the incident response efforts:

> ***... We recently worked multiple incidents where the organizations were compromised by ransomware. We found root cause (trickbot),[21] and needed to find if other systems in their environment had been compromised by the malware. Both organizations had Cisco Meraki firewalls. They had assumed the Meraki firewalls would have that data but, unfortunately, they do not; Cisco Meraki firewalls only keep general statistics on traffic and not on individual connections. So, in the end, it was not possible to get that data and delayed the overall investigation, and in turn, some of the remediation/recovery.***

---

[18] GuardSight, "Incident Response: Dwell Time," www.guardsight.com/blog/incident-response-dwell-time/ [Registration required.]

[19] CIS, "Inventory and Control of Hardware Assets," www.cisecurity.org/controls/inventory-and-control-of-hardware-assets/

[20] CIS, "Inventory and Control of Hardware Assets," www.cisecurity.org/controls/inventory-and-control-of-hardware-assets/

[21] https://isc.sans.edu/forums/diary/Trickbot+gtag+red5+distributed+as+a+DLL+file/25918/

In addition to knowing all of the assets in an environment, organizations must collect the activity on and from those devices. All cyberattacks produce system and network artifacts. Organizations are responsible for collecting this information, as noted by CIS Control 6: Maintenance, Monitoring, and Analysis of Audit Logs. Even the lack of an artifact is a significant event when considering the type of activity and sophistication of the attacker. The DtC gaps are significantly extended without these logs, as Hudak explains:

> ***The big difference in cost between having the log data to understand what happened and not having that data is that if the organization doesn't know how many systems have been affected by the intrusion, they have to apply remediation to many more systems out of an abundance of caution or risk having the intrusion continue on because they didn't thoroughly evict the attacker, leaving continued backdoor access.***

Not preparing for a cyberattack nearly always guarantees an extension of incident response efforts. Some organizations elect to shut down their processes to contain the attack. Other organizations elect to continue operations during these events. In either case, not preparing extends the effects of the intrusion by days and, at times, weeks.

Tabletop Scenarios from the Professionals

One of the more effective techniques for closing the gaps is to conduct periodic tabletop sessions. *Tabletop sessions* can be simple question and answer meetings or complex events that require team members to access data from systems, devices or controls within specific time frames. The ultimate goal is to get an understanding of how an organization's team will react to different situations. It also provides opportunities for team members to operate under stress during noncritical situations so that when actual incident occurs, the team is more prepared and can focus on the tasks at hand.

When helping an organization conduct its first incident response tabletop, Tyler Hudak of TrustedSec likes to start with discussing ransomware attacks. He explains that ransomware attacks are widely understood to be invasive and difficult to address. Most team members understand the amount of damage these infections can inflict on an organization. Additionally, response to ransomware attacks involves multiple business units: the affected business unit, help desk, consultant and administrators from many teams. The discussions about who will perform specific actions and which teams are responsible for containment and recovery efforts quickly identify misconceptions and weak communication channels. By walking through the actions required to address ransomware infections and discussing the response options, all team members learn what their colleagues think and how they will take action. This discussion provides the organization's leadership with actionable information to address shortcomings in the response, ultimately helping to reduce the incident response gaps.

Preparing for Remote Access Cyberattacks

Get OT and IT teams discussing cyberattacks involving remote access by starting with how the OT engineers access the OT environment from the IT network. Talk about how vendors and integrators access the OT network. For the latter, assume the vendor or integrator's credentials have been compromised and an attacker remotely accesses the OT network. Where can they go? What actions can they take on the environment? Would you know they were doing something wrong?

For more realistic tabletop scenarios, try conversing with key individuals from a specific department and get them to assist with a tabletop session. Sit down with individuals from their team and talk about real-world technologies, relationships between departments and corporate partners, and the situations that would be challenging or "bad." Build a list of situations and questions for the tabletop and enlist one or more teams to help provide realistic responses to inquiries and actions that would be taken by the team involved with the tabletop.

Conclusion

Even in the best of times, cybersecurity can be a challenge. The effort associated with conducting an organized and effective campaign to reduce the attack surface of any organization is staggering. Add the complexity and safety concerns of OT environments and the tasks are even more daunting. The only effective method for improving security is to prepare. Each security control and technique an organization implements should be used to generate information that feeds its administrators and leadership. This information is the fuel they need to make decisions based on fact, take the most appropriate actions and pivot fluidly with the shifting dynamics of a cyberattack.

Organizations with OT environments must remember that cyberattacks on control networks can be characterized by two distinct attack stages. The first stage is the corporate environment, where the most vulnerable assets—the enterprises' workforce—operate. Attackers must conduct reconnaissance and obtain a foothold within the corporate infrastructure before moving to objectives within the OT environments. The second stage involves very specific actions within the OT network. Attackers must gain access to and modify OT assets, computers or devices to implement their tools and achieve their objectives.

These two distinct phases provide excellent opportunities for organizations to identify and respond to attackers. The reconnaissance activities that attackers need to conduct are the footprints in the sand that identify their presence. Organizations need to listen in the proper locations and have personnel that understand the corporate and OT baseline of activity to identify anomalies generated by the attackers.

Understanding the common pitfalls of incident response efforts can also help an organization prepare its team for these events. These pitfalls include:

- Poor preparation due to lack of staff
- Slow identification because of a lack of detection capability
- Difficulty in containment due to loosely controlled data flow both over the network and via removable media
- Slowed eradication and recovery due to continuous production

Recognizing these issues and talking to your teams about them is crucial. What is to stop any team from gathering key individuals together and reading over those bullet points as a tabletop scenario? Honest conversations involving difficult questions with no apparent solutions is the starting point for overcoming adversity. Turn to your teams now, heed what they have to say and follow their recommendations because when a cyberattack happens, you are going to be turning to them anyway. Give your teams the things they need to succeed today, not when processes are shutting down.

About the Author

Don C. Weber, a SANS ICS instructor and founding member of the GIAC Ethics Council, has devoted himself to information security since 2002. He has extensive experience in security management, physical and information technology penetration testing, web assessments, wireless assessments, architecture review, incident response and digital forensics, product research, code review and security tool development. He is currently focusing on assisting organizations secure their business and ICS environments through program reviews, security assessments, penetration testing and training.

Sponsor

SANS would like to thank this paper's sponsor:

Honeywell

Last Updated: October 21st, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Sydney 2020	**Sydney, AU**	**Nov 02, 2020 - Nov 14, 2020**	**Live Event**
SANS Secure Thailand	**Bangkok, TH**	**Nov 09, 2020 - Nov 14, 2020**	**Live Event**
APAC ICS Summit & Training 2020	**Singapore, SG**	**Nov 13, 2020 - Nov 28, 2020**	**Live Event**
SANS Community CTF	**,**	**Nov 19, 2020 - Nov 20, 2020**	**Self Paced**
SANS Local: Oslo November 2020	**Oslo, NO**	**Nov 23, 2020 - Nov 28, 2020**	**Live Event**
SANS Wellington 2020	**Wellington, NZ**	**Nov 30, 2020 - Dec 12, 2020**	**Live Event**
SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**