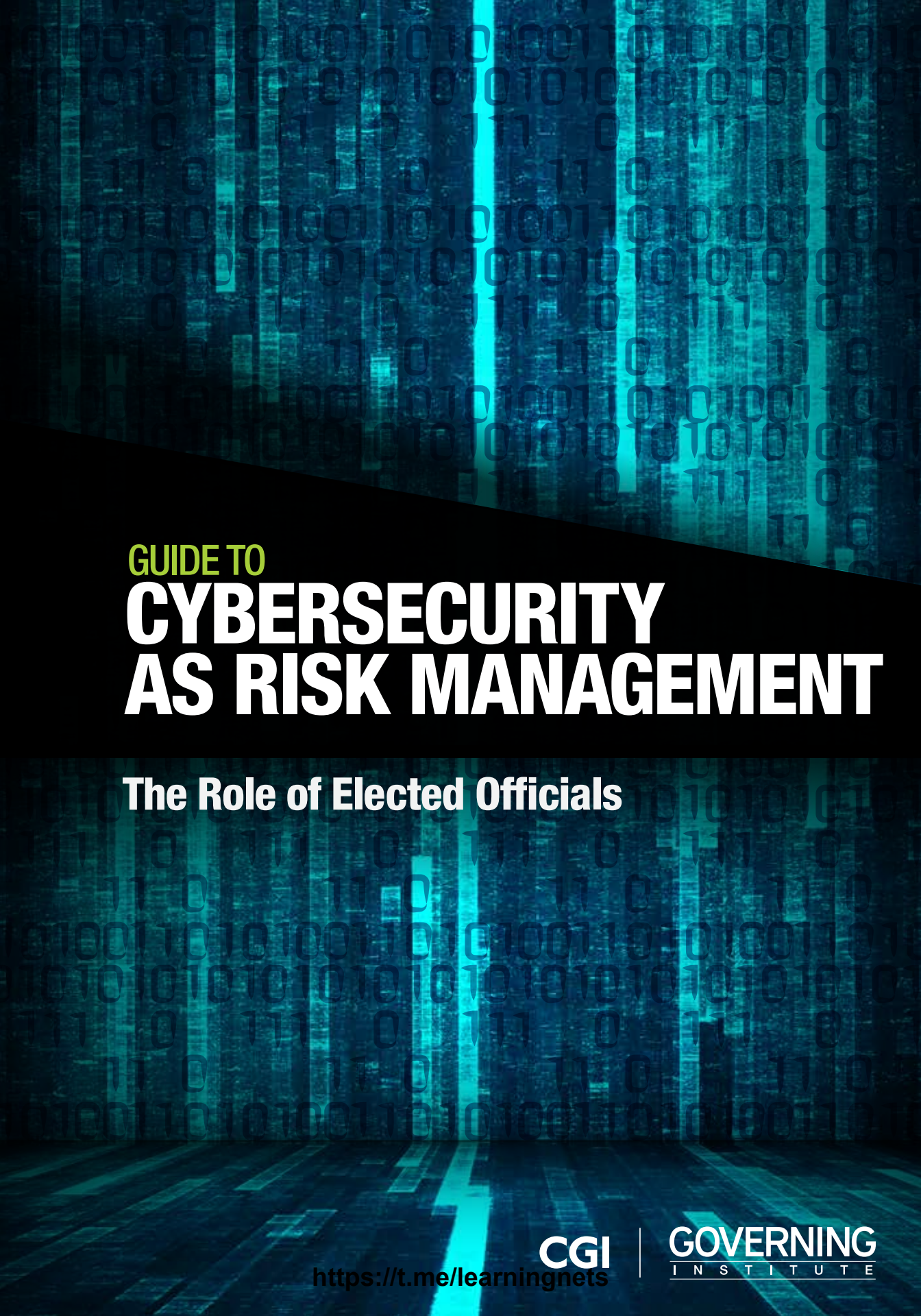


https://t.me/learningnets

GOVERNING
INSTITUTE

© 2015 E.REPUBLIC. ALL RIGHTS RESERVED
1100 CONNECTICUT AVE. N.W., SUITE 1300,
WASHINGTON, D.C. 20036
GOVERNING.COM

A DIVISION OF e.REPUBLIC

CGI

11325 RANDOM HILLS ROAD
FAIRFAX, VA 22030
CGI.COM

https://t.me/learningnets

SHUTTERSTOCK.COM

CONTENTS

https://t.me/learningnets

EXECUTIVE SUMMARY

Cybersecurity should be integrated into the overall risk management process of every government organization (e.g., jurisdiction, department or agency). Because the purpose of cybersecurity is to support and protect business functions, it must be aligned with business objectives and appropriately funded to match risks. Since a state, city or county comprises many agencies providing citizen services, it is important to note that overall risk is based on the risk postures of each of these supporting organizations. Basically, you are only as protected as your weakest link.

Within the familiar context of risk management and assessment, elected officials can balance business requirements with security risks to:

- Inform investment decisions
- Make financial recommendations
- Allocate resources
- Develop policies, strategies and plans

By defining the risk strategy and levels of acceptable risk, agency leaders and security teams are able to manage security risks to the most acceptable level, including budgeting commensurate with the relevant risk.

This guide, *Cybersecurity as Risk Management: The Role of Elected Officials*, a collaborative endeavor between the Governing Institute and CGI — a leading IT and business process services provider — helps elected leaders address cybersecurity risks by:

- Spelling out cybersecurity risks and providing information to help public officials fulfill their responsibilities and safeguard their communities
- Suggesting strategies for integrating cybersecurity into an organization's risk management framework, and developing and adapting cybersecurity and cyber disruption response policies and plans
- Discussing the private sector's role in government cybersecurity efforts; although governments are often leery of collaborating and sharing with third parties, when it comes to cybersecurity, the private sector's involvement is imperative
- Offering practical and actionable information to support the cybersecurity risk management efforts of elected officials

The private sector's role in government cybersecurity efforts is complex and multifaceted. Governments are often leery of collaborating and sharing with third parties, but when it comes to cybersecurity, the private sector's involvement is imperative.

https://t.me/learningnets

HOW TO USE THIS GUIDE

As an elected official, you have a unique role in government cybersecurity efforts and are held accountable for protecting critical government resources and data.

Too often, elected officials fail to prioritize cybersecurity until after a breach — when it's too late. Such failure to properly plan for and provide adequate cybersecurity resources can result in the exposure of large numbers of constituent records, which can damage the livelihoods of citizens and businesses, cost millions of dollars in unplanned expenses, spawn lawsuits and erode public trust. The loss of reputation and public trust is immeasurable, especially for government organizations.

Consider these facts:

- U.S. data breaches reached a record high in 2014, with a 27 percent increase over breaches in 2013. The public sector was third on the list of targeted industries.[1]
- Security breaches have significant fiscal impacts across the economy. In 2014, data breaches cost U.S. companies an average of $195 for each compromised record.[2]
- The cost to remediate data breaches has been rising 15 percent each year.[3]

The purpose of this guide is to make it easier for you to fulfill your responsibilities for ensuring the safety and privacy of your constituents' data, whether you're in the executive or legislative branch of government. Although elected and agency executives and legislators have different roles and responsibilities when it comes to cybersecurity, it's critical they work in harmony to accomplish the same goals.

The guide begins with checklists of the top cybersecurity action items for elected and agency executives and lawmakers. For more

https://t.me/learningnets

Cybersecurity might seem like an IT issue, but a security breach is a political flashpoint. Most security experts agree governments should adopt a "not-if-but-when" attitude towards cyber breaches.

detailed background, read further for an overview of public sector threats, assets and adversaries. You'll also find in-depth recommendations for integrating cybersecurity into an organization's risk management framework, and an introduction to the National Institute for Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework). This is followed by a brief discussion of staffing and external partnerships and a reference section on breach response.

Introduction: Not If. When.

State and local officials need to ensure cybersecurity is addressed in their jurisdictions. Imagine that your organization experiences every elected official's nightmare: a major cybersecurity breach. A server housing taxpayer data has been hacked, and hundreds of thousands of Social Security and bank account numbers have been stolen. What went wrong? Has the leak been secured or is the organization still losing data? Are other systems and data at risk? Who is the attacker? How should the breach be handled? Who will deal with the press, the public and law enforcement?

It turns out that a phishing attack against employees found at least a couple recipients willing to click on a link that infected their computers with credential-stealing malware. After several weeks of snooping undetected through systems using a remote access service, the hacker successfully used the employees' credentials to access a critical database and copy large amounts of unencrypted taxpayer data.

Ultimately, the cybercriminals made off with more than one million Social Security numbers and half a million bank account numbers. The bill for the breach is estimated to exceed $5 million, including the cost of remediation efforts, taxpayer notification, credit monitoring, and legal and public relations services. Meanwhile, angry citizens and the media are demanding answers.

As an elected official, you might be on the periphery of cybersecurity planning and implementation, but as this scenario illustrates, you can't ignore an attack. Cybersecurity might seem like an information technology (IT) issue, but a security breach is a political flashpoint. And, increasingly, breaches appear inevitable. Most security experts agree governments should adopt a "not-if-but-when" attitude towards cyber breaches. "We're in an era where we all must plan as if a breach will occur," says Molly O'Neill, CGI vice president. "This assumption requires a different approach to cybersecurity."

Information Security vs. Cybersecurity

Cybersecurity specifically refers to the protection of digital information transmitted over networks, computers or other systems. Cybersecurity is a subset of information security. Information security more broadly refers to the protection of all information, whether digital or physical. Although this guide focuses on cybersecurity, the practices and strategies discussed can apply to all information, regardless of form.

https://t.me/learningnets

CYBERSECURITY ACTIONS FOR ELECTED OFFICIALS

DAVID KIDD

In the absence of enterprise-wide cybersecurity standards and regulations, many security experts use a patchwork of government and industry mandates to direct their efforts. Compliance requirements can help organizations establish a cybersecurity baseline, but this approach lacks consistency across the public and private sectors as a whole. "There has been a degree of fracturing where different sectors and organizations rely on different standards, regulations and requirements," says Adam Sedgewick, senior information technology policy adviser for NIST.[4]

This compliance-based approach is not dynamic, and can be unresponsive to changes in the threat environment. "Government IT and security personnel are realizing cybersecurity isn't just a technology problem or a compliance issue," says CGI's O'Neill. "It's a business problem, so it has to be managed like one."

Instead of relying on mandates that drive cybersecurity strategies, cybersecurity efforts should be integrated within existing risk management and business continuity processes. The risk-based approach is driven by business requirements and will help leaders identify, assess and prioritize cybersecurity spend and strategies.

This guide's primary recommendation is to apply risk-based management to cybersecurity planning. It supports the adoption of the NIST Cybersecurity Framework, a risk-based, best practice-focused model that can be customized depending on business needs, risk tolerance, and available funding and resources.

Although elected and agency executives and legislators have different roles and responsibilities, they must collaborate closely with each other, third-party organizations and the private sector to accomplish critical cybersecurity objectives. The following checklists for elected and agency executives and lawmakers provide top action items for addressing the public sector's cybersecurity challenges.

https://t.me/learningnets

An Elected and Agency Executive MUST-READ: How to Be an Executive Cybersecurity Champion

By being a well-informed and vocal advocate for cybersecurity initiatives, the executive cybersecurity champion sets the tone for the entire agency. Furthermore, when elected and agency executives take on a leadership role in supporting their technical and security teams, they help build public and legislative awareness, a requirement for obtaining appropriate funding. "It really makes the job easy when you're working with a leader who understands the importance of cybersecurity," says David Behen, CIO for the State of Michigan. "When leadership gets it, they fight for it, and when they fight for it, there will be budget for it."[5]

Here's how leaders in the executive branch can fight for cybersecurity.

☑ **1. Ensure security is integrated into the agency's overall risk management strategy, and adopt the NIST Cybersecurity Framework.** Increase the importance of cybersecurity across the agency by requiring all departments to participate in ongoing planning and management activities and ensuring their compliance with appropriate mandates and participation in the risk management process.

☑ **2. Use the NIST Framework to measure the maturity of the agency's existing cybersecurity program.** Perform a risk assessment by inventorying the agency's most critical digital assets, information and systems. The inventory, which should include all data sets, will document data confidentiality and applicable security and privacy laws, enabling security pros to create a tailored plan for prioritizing data and protecting each data set, including the most appropriate breach response for each one.

☑ **3. Implement tools and technologies that provide constant measurement of capabilities** such as the Department of Homeland Security's (DHS) Continuous Diagnostic and Mitigation (CDM) program (see page 23) or software applications that communicate security posture via data analytics-based dashboards. Continuous analysis of its security posture helps an agency monitor the security of technology, networks and applications as they evolve.

☑ **4. Develop and maintain a strong cybersecurity team, starting with the CIO and CISO — a challenging task given the ongoing scarcity of qualified cybersecurity professionals.** Support IT and security leaders by empowering them with clear

Key Actions:

Apply risk-based management to cybersecurity planning. The primary recommendation of this guide is to apply risk-based management to cybersecurity planning. The risk-based approach is driven by business requirements and will help leaders identify, assess and prioritize cybersecurity spend and strategies.

Adopt the NIST Cybersecurity Framework. This risk-based, best practice-focused model can be customized according to business needs, risk tolerance, and available funding and resources.

Collaborate internally and externally. Agency executives and legislators should collaborate closely with each other, government chief information officers (CIOs) and chief information security officers (CISOs), third-party organizations and the private sector to address the public sector's cybersecurity challenges.

https://t.me/learningnets

authority and responsibility for cybersecurity planning and management. Work with them to develop a plan for recruiting, hiring and maintaining cybersecurity talent through cross-training programs and hiring initiatives such as targeted recruitment campaigns and college internships. Given the shortage of cybersecurity experts, it may be necessary to outsource some parts of cybersecurity to companies or experts.

5. Propose budgets that prioritize cybersecurity programs. Via the risk-based cybersecurity planning process, CIOs and CISOs can identify top cybersecurity priorities and programs. Collaborate with them and with your fiscal staff to develop appropriate budgets, and be a vocal advocate when presenting them to legislative bodies, committees and councils.

6. Vigorously promote a security culture by requiring all employees to undergo regular cyber-awareness training. Sharing relevant risks, threats and challenges with employees is effective because it gives them an active stake in protecting the agency. Cyber-awareness trainers can work with you to provide dynamic training that's customized according to employees' roles, business needs and current threats.

7. Ensure business continuity plans encompass cyber incidents. Cybersecurity breaches can bring down entire networks. This was the case with the Sony hack, which left the company with no network or computer access. Sony relied on phone trees, mobile devices, personal email accounts, and pen and paper to communicate.[6] Consider different continuity scenarios based on type of attack, and ensure the plan's effectiveness is tested in scheduled simulations. Many states are wrapping the cybersecurity scenario into their disaster recovery plans.

8. Create an incident response team and ensure a response plan is queued up in the event of an attack. An incident response plan goes into effect when an attack is confirmed. The response plan should define roles and responsibilities, outline how to recover systems to their pre-attack state, identify where data is backed up and determine a communication plan, among other essential activities. Like the business continuity plan, the incident response plan should be routinely tested to ensure its continued relevance and effectiveness.

9. Work hand-in-hand with legislative counterparts to increase the visibility of cybersecurity in your jurisdiction. This includes educating lawmakers, citizens and the private sector on the need for funding to implement security programs. Communicate the likelihood of a security breach to key stakeholders, including constituents, and assure them that appropriate containment and response plans are in place.

10. Collaborate with the private sector to create a secure, technology-friendly culture for conducting business. Support and promote risk-based cybersecurity management among private sector partners, and evaluate how the two sectors might work together to improve security across the jurisdiction.

11. Require dashboards that show progress on cyber program maturity and types of threats identified. Direct stakeholders to report from external collaborative working groups, incident response centers and internal resources to understand and prioritize actions to minimize exposure.

12. Review procurement processes. Procurement of any technology solution has recently become more complex with the emergence of cloud and "as-a-service" solution models that change where data is stored, how

https://t.me/learningnets

it is accessed and how it is protected. Make sure agencies are procuring adequate security services around data and infrastructure for these new as-a-service models.

A Legislator MUST-READ: How to Be a Legislative Cybersecurity Champion

A legislative cybersecurity champion will support and empower agency executives and technical and security teams by collaborating closely with them to understand business needs and risks, educate citizens and fellow lawmakers on the importance of cybersecurity, promote security and technology as key economic drivers, and secure appropriate funding and other resources. Here's how lawmakers can be a part of the cybersecurity effort.

☑ **1. Support and promote risk-based cybersecurity management** in both the public and private sectors, including the adoption of the NIST Cybersecurity Framework.

☑ **2. Collaborate closely with agency executives, CIOs and CISOs.** Invite them to appropriate legislative meetings to educate yourself and fellow lawmakers on the organization's cybersecurity philosophies, strategies and needs, and to help elevate their department and mission.

☑ **3. Be a vocal advocate for strong cybersecurity public education programs.** As a lawmaker, you can draw on increased public awareness of the importance of secure government technology infrastructure to pass legislation and secure funding.

☑ **4. Prioritize cybersecurity funding.** Work with the executive branch, agency heads and security experts to understand fiscal requirements. Do they have the appropriate levels of funding, staffing and other resources? If not, can they partner externally to supplement internal capabilities? Collaborate with agency experts and allies in the legislature and private sector to identify and support appropriate cybersecurity funding.

☑ **5. Promote cybersecurity as a key economic driver and a critical component of a thriving business and technology culture.** Develop business-friendly programs to understand community needs; provide education, training opportunities and job fairs to strengthen the cybersecurity workforce; and showcase security best practices and innovation.

☑ **6. Facilitate inter-governmental (i.e., executive, judicial, legislative, federal, state and local) communication and collaboration** about cybersecurity threats, issues and plans.

☑ **7. Propose and/or support legislation that enables easier sharing of information about cyber threats** among federal, state and local government agencies and with the private sector.

☑ **8. Work to toughen laws that protect citizen and government data.** For example, evaluate breach notification laws that determine when a breach has occurred, or the state's definition of personally identifiable information (PII). (See PII definition sidebar on page 11.)

☑ **9. Promote cybersecurity in schools.** A top hiring challenge nationally is finding qualified individuals with cybersecurity and data analytics talent. Promoting these programs in all levels of public and private education will not only help create a more educated society, but also will help solve a critical talent shortage and drive economic development in this emerging industry.

https://t.me/learningnets

GOVERNMENT THREATS, ASSETS & ENEMIES

SHUTTERSTOCK.COM

Elected officials must understand the economic impact of a cybersecurity breach. According to one study, the average cost to an organization for a data breach in the U.S. is $5.85 million, which includes costs associated with mitigation, fines, litigation, business disruption and lost productivity.[7]

A high-profile breach at the South Carolina Department of Revenue in 2012 exposed the tax records of 70 million people, and cost the state $41 million.[8] In Utah, the theft of 750,000 Medicaid records cost the state at least $9 million.[9] The total fiscal impact of such breaches across the U.S. economy is enormous.

The loss of public trust and reputation is an even greater risk for government, which

The average cost to the organization for a data breach in the U.S. is $5.85 MILLION, which includes costs associated with mitigation, fines, litigation, business disruption and lost productivity.

https://t.me/learningnets

Federal agencies reported slightly less than 30,000 information security incidents, both cyber and non-cyber, to the U.S. Computer Emergency Readiness Team (US-CERT) in 2009 and **over 61,000 incidents in 2013.**

is responsible for safeguarding critical assets, infrastructure and data, and notifying the public in the event their privacy or safety is compromised.

Governments ignore this responsibility at their own peril. "There's a great degree of anger and frustration over [the 2012 security breach]," says Tom Davis, a state senator from South Carolina. "This is information you've got to give the government; if you don't, they put you in jail. There's a real sense of betrayal."[10]

Know the Threat: The Age of the Targeted Attack

The chances that you'll have to deal with a cyber-attack are steadily increasing. The Government Accountability Office (GAO) found that federal agencies reported slightly less than 30,000 information security incidents, both cyber and non-cyber, to the U.S. Computer Emergency Readiness Team (US-CERT) in 2009 and over 61,000 incidents in 2013.[11] Recently, the Office of Personnel Management (OPM) announced that the personal data of 21.5 million federal employees, contractors, applicants and family members was stolen in a cyber-attack. This was after a previous breach earlier in the year exposed 4.2 million federal personnel records.[12]

What You Need to Know

Who poses a threat to cybersecurity?

- Scammers and thieves seeking information and planning advanced persistent threats (APTs), which are sophisticated, well-resourced attacks, usually backed by political or financial motivation
- Individual hackers or hacker collectives seeking fame, profit or publicity for activist agendas
- State-sponsored criminals who want to disrupt operations, create an atmosphere of fear and uncertainty, or steal sensitive information for profit or espionage
- Disgruntled employees, contractors and other insiders who aim to leak, steal or sell classified information
- Employees that inadvertently aid cyber thieves by falling for scams
- Organizations practicing poor security management, leading to non-malicious attacks or data leakage

What are the biggest targets/risks?

- Sensitive public safety information
- Intellectual property and security intelligence
- Constituent PII (see PII definition sidebar on page 11)
- Individually identifiable health information, often called protected health information (PHI)
- Critical infrastructure systems such as traffic management, utilities, government networks and even social media sites
- Confidential communications
- Vendors, suppliers and users of the above who are part of the supply chain

https://t.me/learningnets

State and local governments have experienced an increase in the number of breaches as well. In May 2014, officials in Los Angeles County discovered a break-in at a county health contractor's office that led to the theft of computers containing the personal information of more than 342,000 patients.[13] Each year, the State of Michigan's cybersecurity efforts result in blocking 2.5 million Web browser attacks, 179.5 million HTTP-based attacks and 5.2 million intrusions.[14] Many of these are crude attempts, but even with these prevention activities, threats continue to evolve and risks abound.

For many government executives, the threats to national and regional public safety and economic stability are uncomfortably vague. They evolve at an alarming pace, and are complicated by the increase in adoption of disruptive technologies such as cloud computing, social networking, mobile computing and multiple network interconnections. The scope and sophistication are dizzying, even for the most advanced security teams.

Cybercrime encompasses fraud, theft, extortion and more. It includes politically motivated crimes such as sabotage and espionage, large-scale network and system disruption by known terrorist organizations, and even the digital defacement of government websites and social media accounts. Cybercrimes occur via malware, hacking, viruses, denial of service (DoS) attacks, phishing and email scams, among many others.[15] (See sidebar "Glossary of Common Cybersecurity Threats" on page 13.)

Know Your Assets: What's Worth Protecting?

Governments maintain a wealth of assets that are at risk for being compromised by cybercriminals, including:

- Government information and systems
- PII, both for government employees and citizens (see sidebar to the right)
- Traditional public infrastructure

What is PII?

PII stands for "personally identifiable information." While state definitions may vary, the federal government defines PII broadly. According to federal practice: "Personally identifiable information refers to information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."[16]

PII can include:

- Names
- Addresses
- Personal identification numbers, including Social Security, passport, driver's license, taxpayer identification and patient identification numbers
- Date and place of birth
- Mother's maiden name
- Telephone numbers
- Photographs
- Biometric records
- Vehicle registration and title numbers
- Medical records
- Educational information
- Financial records, including bank account and credit card numbers
- Employment information

Other common subsets of PII can include:

- Health data
- Federal tax information
- Cardholder data protected by credit card industry standards

Additionally, most states now have data breach notification laws. Under these laws, an organization must notify individuals if their PII is breached. Typically, these state laws define PII more narrowly than the federal definition. Notification of individuals can be costly and embarrassing. In some states, the state breach notification law applies to subdivisions of the state and in others it does not.[17]

https://t.me/learningnets

Government information and systems. State and local organizations are responsible for maintaining and protecting sensitive and classified information and the information systems that keep the government and its services open for business. This includes:

- Preliminary research data
- Trade and other economic development information
- Internal budget or personnel information
- Network diagrams, Internet Protocol (IP) addresses, and server names and configurations
- External vendor and contract information
- Public safety information about transportation systems, utilities, water supply, etc.
- Protected intellectual property
- Security intelligence
- PII of government officials and their family members

Some bad actors care little about the information as their goal is to disrupt the government by shutting down systems and websites. Many state and local governments have been on the receiving end of cyber vandalism or defacement and DoS attacks. For example, protesters recently took the State of Hawaii's official website offline as part of an environmental protest.[18] And in 2014, hackers shut down the State of Colorado's voter registration system for several hours.[19]

Citizen PII. Government agencies are entrusted with protecting citizen information collected in the course of providing services and conducting electronic transactions.

PII is an attractive prize for crime rings looking to commit financial or identity theft and social services fraud. "The escalation of security breaches involving personally identifiable information has contributed to the loss of millions of records over the past few years," warns NIST, which is tasked with developing standards, guidelines, techniques, metrics and testing programs for securing federal enterprise data systems and data.[20]

Traditional public infrastructure. Transportation networks, the electrical grid, the water supply and other physical infrastructures are connected via complex networks and control systems, including network-connected traffic management systems, speed limit indicators and roadside information boards. In addition, utilities may be owned and operated by private and public sector entities that transmit usage information via network-connected smart meters.

> **"Today, our traffic lights, our routing system for trash pick-up, and so much more are electronic. Cybersecurity means protecting the basic services at the core of city government, and it means protecting our critical infrastructure like our port and airport, which we know are top targets."**
>
> Eric Garcetti, Mayor, Los Angeles

Cybercriminals may have the ability to remotely attack hardware, steal administrative credentials to take over systems and compromise physical assets with digital control systems. Hackers can also disrupt or undermine government operations via systems that help manage physical assets such as building, lighting and HVAC. "Today, our traffic lights, our routing system for trash pick-up, and so much more are electronic," says Los Angeles Mayor Eric Garcetti. "Cybersecurity means protecting the basic services at the core of city government, and it means protecting our critical infrastructure like our port and airport, which we know are top targets."[21]

https://t.me/learningnets

Glossary of Common Cybersecurity Threats

Backdoor: An unnoticed, hidden entry into a network or system that allows hackers to "sneak" in without an authorized login or password.

Cross-site scripting (XSS): An attack where the adversary/attacker is able to inject code (script) into a website in a manner not intended by the developer.

Denial of Service (DoS) and Distributed DoS (DDoS) attacks: A DoS attack is an automated attempt to "flood" or overwhelm an organization's server or website with requests, causing it to be unavailable to legitimate users. DDoS is a type of DoS in which a large, distributed number of devices share the attack load to overload a server and bring it down.

Keystroke logger: Hardware or software-based tools that surreptitiously log user keystrokes to steal sensitive information, including login IDs and passwords.

Malicious code: More commonly known as malware, malicious code includes:

- ☑ **Viruses:** malicious code attached to other computer files, activated by users when they open infected files
- ☑ **Worms:** malware that replicates and spreads among networked computers without user interaction
- ☑ **Trojans:** harmful software that tricks users into installing it because it looks legitimate
- ☑ **Spyware:** malicious code that searches infected devices for personal information and forwards it to criminals

---

Phishing: The attempt to trick email users into entering sensitive or private information through the use of an email that appears to come from a trusted source.

Social engineering: Digital mind games used to manipulate users into providing access to information and systems. It includes phishing, Trojans and other attacks that rely on tricking the user into divulging sensitive information.

Structured Query Language (SQL) injection: A computer code injection technique that allows malicious code to be injected or inserted into database entry fields, enabling attackers to gain control over the database contents.

Web app attack: A hacking attack that attempts to exploit vulnerabilities in Web applications and content management systems.

Zero-day attacks: A threat that takes advantage of a previously unknown system or network vulnerability that developers haven't yet had time to patch.

https://t.me/learningnets

A recent survey of 26 member countries of the OAS found **53 percent** have experienced an **increase in cyber-attacks** against critical infrastructure since 2014.

A recent survey of 500 security leaders of 26 member countries of the Organization of American States (OAS) reported that 53 percent have experienced an increase in cyber-attacks against critical infrastructure since 2014, and 54 percent reported attackers had tried to "manipulate equipment" through an industrial control system.[22]

The havoc that can be wreaked on traditional infrastructure by human error and equipment failure cannot be underestimated. For example, a human-caused computer glitch shut down trains in New York for two hours,[23] and controller equipment failure on a Washington, D.C., subway line caused a train crash resulting in nine fatalities.[24]

Know Your Enemy

Organizations of all sizes must defend against hacker collectives that have axes to grind, employees who mistakenly click on unsafe email links, disgruntled insiders and state-sponsored actors whose goal is to steal and exploit sensitive information for profit or espionage.

External threats. Cybercriminals can't be classified neatly. Gen. Michael Hayden, a former director of both the National Security Agency (NSA) and the Central Intelligence Agency (CIA), aptly describes their various motives. "Nation-state actors are coming at us, coming at you. For the most part, they just want to steal your stuff. They want your intellectual property. They want your trade secrets, your negotiating position. There are other actors out there now who are coming to your networks, not just to steal your stuff or maybe not even to steal your stuff. They want to hurt your network. And then there's something out there that troubles me, the third group … people who are mad at the world, and they have demands that maybe you and I can't understand."[25]

Internal threats. Government assets require protection not only from external attackers, but also from internal employees and contract employees whose aim is to leak, steal or sell classified information.

However, a bigger concern is unintentional internal human or machine error. A recent Associated Press (AP) report concluded employees were to blame for at least half of the 225,000-plus federal security incidents that it analyzed, noting they frequently "clicked links in bogus phishing emails, opened malware-laden websites and [were] tricked by scammers into sharing information."[26] Similarly, a White House review of federal breaches revealed:

- 21 percent were due to violation of policies by employees
- 16 percent were caused by lost or stolen devices
- 12 percent resulted from the improper handling of printed materials
- 8 percent were caused by employees either deliberately or accidentally installing malicious software
- 6 percent were due to phishing attacks[27]

For this reason, employee awareness training is a key part of cybersecurity planning. It is important to offer updated, relevant, engaging content. Awareness training that is offered as a "check the box" compliance-only exercise does not reduce risk. A security-conscious employee culture must evolve with changing cybersecurity needs and the introduction of new technologies and threats.

A best practice in some governments is to conduct tests to evaluate the effectiveness of cybersecurity awareness training. In these cases, the CIO or CISO sends a suspicious email to see how many employees click on the link.

https://t.me/learningnets

RISK MANAGEMENT: PRIORITIZING RESOURCES

SHUTTERSTOCK.COM

Historically, the public sector has developed cybersecurity programs based on a vast collection of federal, state and industry regulations, including:

- Federal Information Security Management Act (FISMA)
- NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
- IRS Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies
- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- State breach notification laws

But too often, the compliance-based approach to cybersecurity planning is unable to evolve with an organization's changing needs. A more effective alternative is a risk-based approach where organizations must understand their critical assets and the financial, reputational and regulatory risk should those assets be exposed. "You have to as an organization look at the amount of risk you're willing to take," says Michigan's Behen. "It's impossible to protect everything. You cannot fund it all."

For example, Behen explains, several years ago the state was treating open data and PII equally in terms of data protection. "Open data is already out there in public," he notes.

> **"You have to as an organization look at the amount of risk you're willing to take. It's impossible to protect everything. You cannot fund it all."**
>
> David Behen, CIO, State of Michigan

"I would much rather invest funds towards securing sensitive data."

Risk management-based cybersecurity is an ongoing process that must be constantly re-evaluated, with a feedback loop for adaptation and improvement:

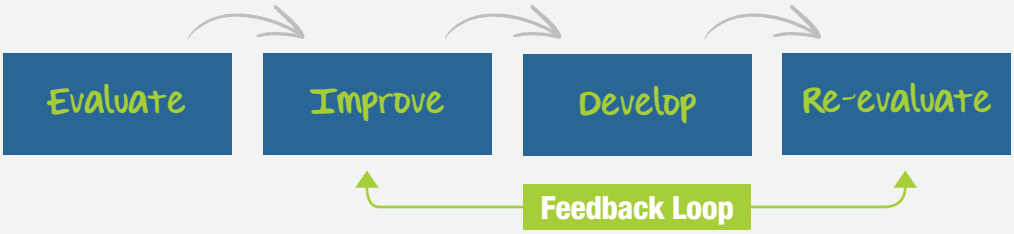
1. Evaluate existing protection, plans, protocols and policies.
2. Improve existing protection, plans, protocols and policies.
3. Develop an environment that responds and adapts to the constantly changing threat environment.
4. Re-evaluate constantly.

Risk Management: A Cure for the Budget-Strategy Disconnect

According to a survey of state government CISOs by the National Association of State CIOs (NASCIO), more funding was made available for cybersecurity programs in 2014 than in 2012. However, in what NASCIO describes as a "budget-strategy disconnect," adequate funding

https://t.me/learningnets

The Risk Management-Based Cybersecurity Process



continues to be a challenge.[28] Integrating cybersecurity into the risk management process can help agency executives prepare a business case for cybersecurity in the executive and legislative budget processes.

In the context of risk management, the cybersecurity effort is driven by business requirements. Consider the financial risks, including cost of notification, potential sanctions and fines, and the impact of the loss of key operational information. Also factor in the legal threats and the risks of reputation loss and loss of public trust. "Security can get buried in the weeds of IT spend," says Mike Watson, CISO for the Commonwealth of Virginia. "Risk management allows you to make wise cost-based decisions related to security."[29]

As part of the government's traditional decision-making and budgeting framework, security threats are identified, assessed and prioritized, and budget resources are assigned accordingly to minimize the likelihood and impact of a breach. "The risk-based approach helps you focus on what matters," agrees Behen. "You identify what you have; you determine what's most valuable; you prioritize what you want to protect the most; and then you figure out how to budget for it."

Elected officials in both the legislative and executive branches are critical to the cybersecurity funding process. When they understand the importance of cybersecurity and the nature of threats to an organization's assets, they can be powerful advocates for cybersecurity.

The risk-based management process will identify an organization's most valuable assets and enable technology professionals, agency leaders, elected officials and fiscal staff to work together to determine funding priorities and strategies. Executive officials must propose appropriate budgets and effectively communicate their needs to their legislative colleagues. Lawmakers should work with agency leaders to learn about the organization's assets and security threats, advocate for cybersecurity-forward budget proposals and educate the public on why funding is so critical.

Cybersecurity programs have grown exponentially due to the increasing complexity of threats to government operations. Funding continues to be a challenge, which is why prioritization and ongoing threat monitoring continue to be important parts of cybersecurity programs.

Over the past couple of years, states have been able to tap into federal funding. For example, DHS has allowed states to utilize grant funding for emergency management programs. In addition, state grant funding for implementing the Affordable Care Act (ACA) could be used to improve the security of important health records.

However, stable funding for cybersecurity will continue to be a challenge. Organizations such as NASCIO continue to advocate for changes that would allow states to spend federal dollars on enterprise-wide cybersecurity improvements, instead of tying federal support for state cybersecurity to specific programs. "Modernizing the federal cost allocation guidelines so when those dollars do flow to states, CIOs have flexibility and you're not really constrained in a particular funding path would be a huge step forward," says former NASCIO President Craig Orgeron, who is also the CIO of Mississippi.[30]

https://t.me/learningnets

RE-INVENTING CYBERSECURITY USING THE NIST FRAMEWORK

SHUTTERSTOCK.COM

For public sector organizations seeking to move to a risk-based approach to cybersecurity, **a logical place to start is the NIST Framework**, a risk-based model that relies on best practices from multiple standards bodies and industries.

For public sector organizations seeking to move to a risk-based approach to cybersecurity, a logical place to start is the NIST Framework, a risk-based model that relies on best practices from multiple standards bodies and industries to improve critical infrastructure cybersecurity.

Background of the NIST Framework

NIST released this framework in 2014 to improve critical infrastructure cybersecurity across both the public and private sector. Created as a result of Executive Order 13636 and based on NIST's Special Publication 800-53, it is the culmination of more than a dozen years of policy- and law-making.

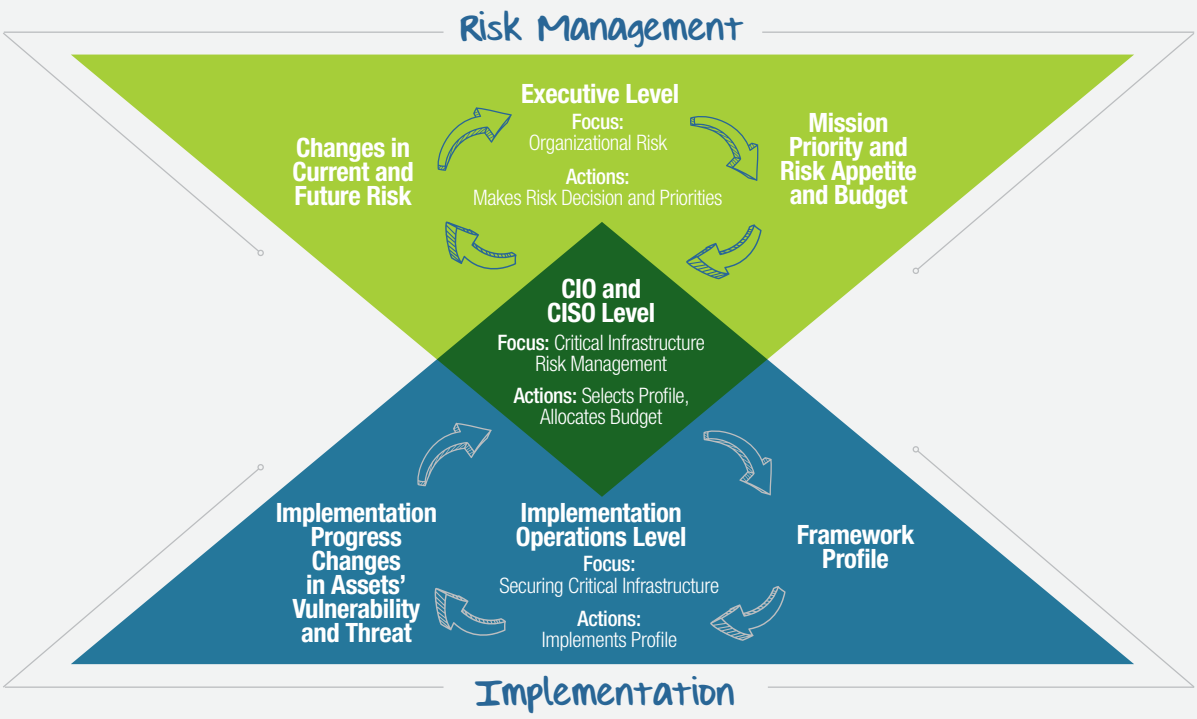
In fact, Virginia made a quick commitment to adhere to the NIST Framework because it had already aligned its existing cybersecurity program with Special Publication 800-53 several years before.[31] "A lot of the vendors in the D.C. area are familiar with NIST guidelines and requirements, and we saw the value of a risk management program, so we built our state requirements on top of [Special Publication 800-53]," says Virginia's Watson. "It was a natural fit for us to align with the framework later."

The NIST Framework is a federal risk-based approach reengineered for non-federal consumption. It synthesizes the recommendations of hundreds of public and private sector organizations and companies and suggests common best practices, terminology, strategies, principles and technologies that encourage public and private sector adoption. It also is adaptable. "It addresses all of the major issues and security controls, but you can customize it to meet specific needs," says Watson. "For example, Virginia has laws that require us to do things differently from the feds in terms of reporting incidents, and we have fewer classification categories for our systems."

The NIST Framework enables the comparison of security programs and encourages information sharing across organizations and sectors. It emphasizes cost-effective management of cyber risks based on business

https://t.me/learningnets

Implementation of the NIST Framework



Source: www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

needs — without imposing additional regulatory requirements. It's not mandatory, but it can serve as a valuable tool for organizing security programs because its primary components have been vetted against both industry and government standards. Notes Watson, "The backbone of IT and the Internet is a common set of standards. If there's general agreement that we have a common set of controls that work well then that's what we should follow."

Many private sector companies, including AIG, Apple, Bank of America, Intel, Kaiser Permanente, Pacific Gas & Electric, QVC, U.S. Bank and Walgreens are using or have committed to use the NIST Framework.[32] If it is broadly adopted, it may become the de facto standard for litigators and regulators. Therefore, adherence may help shield an organization against regulatory investigation or litigation.

How to Use the NIST Framework

Implementing the NIST Framework is an ongoing process that occurs in partnership among elected and appointed agency leaders, technology and security leaders, and their implementation teams (see above graphic). Agency executives, CIOs and CISOs work together initially to synchronize the organization's mission with its risk tolerance level and funding resources. Then CIOs and CISOs work with their technical and operational teams to assess current risks and communicate and use the results to inform the overall process.[33]

To begin the risk management process, the NIST Framework recommends assessing the

https://t.me/learningnets

current security posture — or Current Profile — and comparing it against standards and guidelines outlined in the framework. After determining the Current Profile, it should be compared to one of NIST's four Target Profiles, or tiers of cybersecurity maturity (see below chart for comparison).

State organizations, especially those managing PII, financial or other sensitive information, should strive to achieve the highest maturity level, Tier Four. It may be financially prudent for state-level organizations that don't manage sensitive or confidential data to target the next level down, depending on their mission and scope.

A comparison of Current and Target Profiles highlights gaps in policies and procedures and helps identify desired outcomes. Given budget limitations, states should prioritize agencies with the largest risks.

The NIST Framework describes five ongoing core activities of the risk management process.

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover[34]

When applied holistically, it helps organizations thoroughly evaluate their existing cybersecurity practices so they can see where to make changes and improvements to create a more practical, efficient program.

Following is an in-depth look at each step. Keep in mind there is no end to the process; it is an ongoing progression that will continue to evolve with the organization and current threat environment.

Step 1: Identify. This step determines the organization's most critical digital assets, information and systems by conducting and maintaining a thorough enterprise data inventory that includes all data sets. The inventory documents how confidential the data is, and what security and privacy laws are applied to it. This enables security professionals to create a tailored plan for protecting each data set, including the most appropriate breach response for each one.

The risk-based approach for protecting valuable resources includes managing them as assets throughout their life cycle, similar to managing physical assets such as real estate, vehicles, equipment and other tangible

NIST Cybersecurity Maturity Tiers[35]

Target Profile	Description
Tier 1: Partial	Ad hoc risk management process; limited insight into risks; no collaboration with others
Tier 2: Risk Informed	Some processes and programs established, but not at the enterprise level; no formal external collaboration
Tier 3: Repeatable	Formal process and programs established at the enterprise level; some external collaboration
Tier 4: Adaptive	Ongoing, proactive and collaborative risk management process; deeply embedded in organizational culture

https://t.me/learningnets

property. Applying risk-based management principles to data systems and assets enables organizations to understand the business context, critical resources and related cybersecurity risks associated with each item.

Step 2: Protect. In this step, appropriate technology, processes and practices — which can also be outsourced to the private sector — are deployed to protect assets. This includes tasks such as access control, employee awareness and training, technology deployment, data security, and development and maintenance of procedures.

Continuous infrastructure testing, monitoring and reviews help protect systems from cyber-attacks. This typically includes traditional security tools such as firewalls, filtering, data loss prevention and others that have long been the cornerstone of breach prevention strategies.

Data-driven security tools, such as log management and event correlation, intrusion prevention and detection, security incident and event management (SIEM), and data analytics, are increasingly becoming indispensable. These data-driven tools enable real-time monitoring and analysis of data generated by networks, endpoint devices and applications to reveal inconsistencies and deliver actionable intelligence for preventing security incidents. They deliver the information via easy-to-understand dashboards and visualizations that are designed to assist the end user in identifying unusual patterns and activities.

In both the public and private sectors, this is the domain of the security operations center (SOC), where the staff and tools for detecting, containing and remediating cybersecurity threats are managed. SOCs may operate at the state or agency level, depending on the size and complexity of the organization.

Step 3: Detect. This step involves implementing a procedure for timely identification of cybersecurity breaches. It includes understanding and identifying security anomalies and events, establishing continuous security monitoring and developing detection processes.

Early detection is crucial. Once a breach has been detected, the focus should be on isolating the threat, limiting infrastructure damage or data loss, and safely restoring systems and networks. Centralized control systems can be used to manage infrastructure that may be compromised by cyber disruptions. One of the benefits of having a 24/7 SOC is to have staff focused on detecting and isolating any security breaches. Experienced analysts can identify suspicious patterns that tools may not detect. This provides additional protection.

Step 4: Respond. This step develops the response process in the event of a breach. Activities include response planning and communications, breach analysis and mitigation, and system improvements.

Governments must have a plan for dealing with the eventual cyber disruption, including detection, response and recovery for incidents of all sizes and severity. A well-planned strategy serves as a model for preventing, responding to and mitigating breaches and other events.

Disruption of critical infrastructures, such as utilities, transportation and telecommunications, should be integrated into an organization's emergency management plans. For example, Michigan coordinates its response to cyber disruptions via the State Emergency Operations Center. In the context of emergency management, cyber disruptions can become part of the organization's business continuity/resiliency and disaster recovery plans.

Step 5: Recover. The final step is to create a recovery process in the event of a breach. To restore any capabilities or services impaired due to a cybersecurity event, an organization should undergo recovery planning and communications and system improvements.

https://t.me/learningnets

FINDING THE RIGHT SKILLS & EXPERTISE

SHUTTERSTOCK.COM

Across both the public and private sectors, CIOs and CISOs face a mounting staffing problem. One report suggests the demand for cybersecurity workers is more than double the overall IT job market; another says approximately 300,000 U.S. cybersecurity jobs are unfilled.[36] The private sector has the advantage of offering higher salaries; and 89 percent of state CISOs say salary is the biggest barrier to hiring security professionals. Other hiring issues include unclear career paths and lengthy hiring processes.[37]

As the public sector struggles to hire qualified cybersecurity experts, agency leaders and elected officials must support budgeting strategies and career paths that enable state and local governments to compete with the private sector. For example, the State of Delaware made drastic changes to its technology organization — such as consolidating IT operations into a single department and exempting IT hires from traditional pay scales — enabling it to attract more skilled cybersecurity workers. "While we are pretty well positioned now, it is a constant battle," says Ann Visalli, director of the Delaware Office of Management and Budget. "[The hiring process is] a little faster; it's a little more flexible; the pay is a little more competitive; and it allows for promotion and retention for employees who do achieve what they need to be achieving."[38]

The public sector can rely on a far-reaching and resilient web of external allies to effectively support, develop and execute comprehensive, cost-efficient

The demand for cybersecurity workers is more than double the overall IT job market, and approximately 300,000 U.S. cybersecurity jobs are unfilled.

https://t.me/learningnets

cybersecurity plans. "Many third parties can provide valuable services, advice and collaboration opportunities, especially the federal government, the private sector and a number of nonprofit organizations," says Dan Lohrmann, chief security officer and chief strategist at Security Mentor, Inc., and former chief security officer for the State of Michigan.

Don't Go It Alone: Trusted Third Parties

Information sharing among governments is crucial to success as it enables them to understand when particular events start to propagate against targets such as health insurance exchanges or utility infrastructure. Many trusted third parties provide valuable cybersecurity services, advice and collaboration opportunities.

Department of Homeland Security (DHS).

DHS provides a wealth of cybersecurity resources for state and local governments, including the National Cybersecurity and Communications Integration Center (NCCIC), a 24/7 cyber monitoring, incident response and management center. NCCIC shares information with the public and private sectors to improve situational awareness, mitigation and recovery.[39]

DHS' network of 78 fusion centers centralizes the receipt, analysis, gathering and sharing of threat-related information among the federal government and state, local and private sector partners. Located throughout the country, fusion centers help state and local public safety security personnel understand the local implications of national intelligence to improve situational awareness, conduct analysis and facilitate information sharing. Fusion centers are owned and operated by state and local entities with support from the federal government.

DHS has outreach efforts with NIST to hear from all stakeholders on how they are using the framework, where they have found success and what challenges they face, which could be prioritized in forthcoming updates. To achieve this, DHS sponsors the following State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC) Working Groups:

- Access Credentialing Working Group (ACWG) — aimed at enhancing collaboration on credentialing efforts to help organizations validate that the right people have access to the right data
- Automated Critical Asset Management System Working Group (ACAMSWG) — provides a forum to discuss and collaborate on infrastructure protection
- Cyber Security Working Group (CSWG) — provides guidance on improving cybersecurity while serving as a federal point of contact on new cybersecurity initiatives and proposals as they develop
- Homeland Security Advisor Working Group (HSAWG) — bridges communication gaps with the Governor's Homeland Security Advisory Council (GHSAC) and provides entry for the state critical infrastructure protection managers into the SLTTGCC
- Information Sharing Working Group (ISWG) — monitors and creates relationships and mechanisms to share information among federal, state, local and private sector critical infrastructure partners
- IP Gateway Working Group (IPGWG) — provides updates on DHS' efforts to undertake assessment tool integration and broader data sharing and analytics
- Policy and Planning Working Group (PPWG) — reviews feedback to DHS regarding federal, state and local critical infrastructure protection guidelines to help smooth the implementation of national critical infrastructure policies
- Regional Resiliency Assessment Program Working Group (RRAPWG) — provides a line of communication among states operating within or across critical infrastructure

https://t.me/learningnets

regions (defined by DHS based on supply chain) to devise solutions
- State Asset Criteria Working Group (SACWG) — collaborates to provide protection of critical assets within the supply chain

The Continuous Diagnostic and Mitigation Program (CDM) is being implemented at U.S. federal agencies. CDM includes a review of an agency's existing cybersecurity tools and processes to look for gaps or weaknesses on an ongoing basis. Tools are put into place to continuously monitor the security posture so that when a change occurs (e.g., a new application comes online), the agency's security posture changes automatically. This is important because of constant changes to agency technology, networks and applications. DHS has made its contract vehicle, along with the pre-negotiated highly discounted rates and approved vendors, available to states.

National Institute of Standards and Technology (NIST). NIST offers a variety of publications and training materials related to the NIST Framework. Particularly useful are case studies that demonstrate how organizations of different sizes, types and capabilities can use the NIST Framework.

Further, NIST hosts educational talks, presentations, forums and webinars throughout the year. Another important resource is the National Initiative for Cybersecurity Education (NICE), a NIST-driven initiative to improve cybersecurity education and training for the cybersecurity workforce.

Multi-State Information Sharing and Analysis Center (MS-ISAC). MS-ISAC is a key resource for state and local governments. MS-ISAC has been designated by DHS as a core provider of cybersecurity expertise and operations. Its membership is voluntary and provides organizations with tools to enhance situational awareness and cyber-threat analysis, enabling them to leverage economies of scale, share information and conserve resources.

MS-ISAC's 24/7 cybersecurity operations facility offers its members assistance and tools for real-time network monitoring, threat warnings and advisories, vulnerability identification, and mitigation and incident response.

National Governors Association (NGA). A bipartisan organization for state governors, NGA released a comprehensive cybersecurity primer, Act and Adjust: A Call to Action for Governors for Cybersecurity in 2013. This excellent resource contains recommendations for improving cybersecurity across state physical and digital assets and infrastructures using risk-based management and assessment.[40]

Via its Resource Center for State Cybersecurity, NGA provides governors with resources, tools and recommendations to help develop and implement cybersecurity policies and practices. The Resource Center is developing materials to help states improve their collaboration with DHS fusion centers, develop a more skilled security workforce, work with the federal government, and increase security around energy systems and infrastructure.

Trusted Third-Party Resources:

Many trusted third parties provide valuable cybersecurity services, advice and collaboration opportunities, including:

- ☑ Department of Homeland Security (DHS)
- ☑ National Institute of Standards and Technology (NIST)
- ☑ Multi-State Information Sharing and Analysis Center (MS-ISAC)
- ☑ National Association of State Chief Information Officers (NASCIO)
- ☑ National Governors Association (NGA)

https://t.me/learningnets

National Association of State Chief Information Officers (NASCIO). NASCIO is a nonprofit organization that brings together state IT executives and private sector members to examine key technology issues, craft research briefs and convene working groups focusing on organizational priorities. Local IT leaders may also join NASCIO.

Cybersecurity is a top NASCIO priority. The organization seeks to strengthen member awareness of important IT issues and promote the sharing of best practices, experiences and expertise. NASCIO helps its public sector members formulate security policies and technical controls; monitor security, privacy threats and vulnerabilities; and evaluate federal privacy and security legislation.[41]

A 2015 executive order from President Obama calls for more collaboration and open information sharing with the private sector. Proposed legislation also promotes greater information sharing between sectors, including liability protections for companies that share information about cyber threats.

Engaging the Private Sector

The private sector's role in government cybersecurity efforts is complex and multi-faceted. Governments are often leery of collaborating and sharing with third parties, but when it comes to cybersecurity, the private sector's involvement is required. Outsourcing some security functions to the private sector can help fill skills gaps.

"The government really has to figure out: How do you stop the bad guys here?" says Steve Chabinsky, former deputy assistant director of the FBI Cyber Division. "We've figured out in the private sector world how to professionalize security services that work with, not against, law enforcement. … How do you bring the private sector in a professionalized way to help with security?"[42]

Private sector engagement is critical to government cybersecurity because:

- Much of our nation's critical infrastructure — physical and digital — is owned, operated and managed by the public sector.
- The shortage of cybersecurity experts in the workplace requires many organizations to outsource significant security-related functions to the private sector.
- Private sector organizations are managing their own cybersecurity operations centers and have knowledge of cyber threats, some of which are global, that may cross over to the public sector.

A 2015 executive order from President Obama calls for more collaboration and open information sharing with the private sector. Proposed legislation also promotes greater information sharing between sectors, including liability protections for companies that share information about cyber threats.[43]

In addition, a new federal agency, the Cyber Threat Intelligence Integration Center (CTIIC), has been created to serve as a fusion center between existing agencies and the private sector for real-time use against cyber-attacks.[44]

To address the security challenges of collaborating and sharing with the private sector, Behen recommends requiring third-party vendors to comply with NIST guidelines, as Michigan is beginning to do. "Large- and medium-size vendors will want to follow these guidelines for their own cyber health, but it's harder for smaller vendors. But you have to question — if they can't achieve NIST, maybe they shouldn't be a public sector vendor."

https://t.me/learningnets

DAVID KIDD

BREACH RESPONSE BASICS FOR ELECTED OFFICIALS

How you and the affected organization respond to a cybersecurity breach will either strengthen or damage hard-earned public trust and reputation. There is no one-size-fits-all template for dealing with security breaches because each one is unique, complex and may rapidly evolve. The exact process that security teams will implement depends on many factors such as the type of breach and amount and type of data involved. This is not a step-by-step process, but rather a set of activities that needs to be completed to safely restore systems and protect critical data. We've divided the process into three distinct parts: pre-breach planning, breach mitigation and breach communications.

Most breach response activities fall to elected officials in the executive branch, but legislators with cybersecurity expertise or legislative responsibilities may be called upon to participate or serve as a media spokesperson.

https://t.me/learningnets

“I favor frequent public updates even if there’s not a lot to say. At the other extreme, I’ve seen organizations that don’t announce anything for months. That’s not customer-oriented.” Mike Watson, CISO, Commonwealth of Virginia

While security professionals work behind the scenes to mitigate the breach and contain the damage, elected officials will play a primary role in pre-breach planning and breach communications. Most breach response activities fall to elected officials in the executive branch, but legislators with cybersecurity expertise or legislative responsibilities may be called upon to participate or serve as a media spokesperson.

Pre-Breach Planning

Create an incident response team. Before any breach, work with the CIO and CISO to create an incident response team. Include key executives as well as risk management, finance, operations, communications/public affairs and legal staff. Assign a law enforcement liaison to support coordination and information sharing and assist with post-incident investigation. Minimize bureaucracy so the team can act quickly without waiting for approvals and responses from others. Establish relationships in advance with external partners such as security forensics experts, credit bureaus and other breach support services.

Develop a response plan. The response plan will define roles and responsibilities, outline how to recover systems to their pre-attack state, identify where data is backed up and how to access it, and determine a communications plan, among other essential activities. Routinely test the incident response plan to ensure its continued relevance and effectiveness. This will include a communications plan that identifies key staff, procedures and communication channels.

Mitigating a Breach

Assess the breach and evaluate its magnitude. Assemble the incident response team to act quickly and get the facts. Confirm a breach has indeed occurred via security tools and logs, and determine whether the breach is in progress or has ended.

Stop the source of the breach. If the breach is still in progress, quickly begin efforts to isolate it and shut it down. Document all mitigation efforts for compliance and future analysis. Cybersecurity events will occur. How quickly your teams identify, contain and stop data loss from occurring is key. Go beyond reporting vulnerabilities to partners and provide analytics on behavior, source, and predictive analysis of events and where/when those events may make their way into your organization.

Know your recovery plan. Sometimes the best way to stop a breach in its tracks is to recover your data and infrastructure. Direct teams to regularly test recovery processes, backups, endpoint protections (mobile and laptop) and backup sites.

Investigate internally. Find out which systems and data have been compromised, and determine whether citizen or employee PII has been exposed or is at risk of exposure. Determine the impact of the exposed data or disrupted systems and document this internally. Plan for external reporting to the public and media (see page 27), and provide law enforcement officials with information and assistance for their investigation.

https://t.me/learningnets

Evaluate legal obligations. Depending on the severity of the breach, compliance requirements and the type of systems and data involved, it may be necessary to communicate with individuals or government agencies. For example, if PII is exposed, affected parties may need to be notified.

Collaborate with third parties. Involve local, state and federal law enforcement to investigate the breach, and work with third-party vendors as needed to help mitigate the breach, provide forensics experts, monitor credit, notify citizens, provide citizen assistance, etc.

Communicating About a Breach

Work closely with communications staff to ensure outreach is made in a timely, coordinated manner to the appropriate press and social media outlets. Data forensics takes time, and you may be required by state breach laws to communicate before you have all the information. Accept the fact you may have to notify the public before you know everything. "I favor frequent public updates even if there's not a lot to say," says Virginia's Watson. "At the other extreme, I've seen organizations that don't announce anything for months. That's not customer-oriented."

Depending on roles and expertise levels, agency leaders should serve as the media spokespeople. Get comfortable with answering questions from the media and the public. If needed, security and technology professionals can assist in answering technical questions during public briefings. "Stand up and reassure the public. Let them know you're getting to the bottom of it, and tell them what you're doing to fix it," advises Michigan's Behen. "The chief executive needs to be visible and make sure people have confidence and trust in the organization."

Communicate timelines to the media and public. Let them know when to expect future briefings and updates. Be transparent and forthcoming, and don't withhold relevant or important information. Acknowledge the situation may change over time, and use phrases such as "At this time ..." and "We currently believe ..." Be accountable for the breach and apologize to those that have been impacted.

If citizen or employee PII has been compromised, your communications should reassure constituents. Let them know they will be provided with free identity protection and credit monitoring services, and if financial information has been exposed, that they won't be held responsible for any illegal purchases.

Above all, be composed and stay on message. "If you have a long briefing session but aren't on message, people will notice," Watson says. "You have to be able to answer questions succinctly and calmly."

Breach Response Checklist

Pre-Breach Planning

- ☑ Create an incident response team.
- ☑ Develop a response plan.

Mitigating a Breach

- ☑ Assess the breach and evaluate its magnitude.
- ☑ Stop the source of the breach.
- ☑ Know your recovery plan.
- ☑ Investigate internally.
- ☑ Evaluate legal obligations.
- ☑ Collaborate with third parties.

Communicating About a Breach

- ☑ Ensure outreach to the media is made in a timely, coordinated manner.
- ☑ Communicate timelines to the media and public.
- ☑ Be composed and stay on message.

https://t.me/learningnets

TYING IT ALL TOGETHER

SHUTTERSTOCK.COM

In some schools of thought, cybersecurity is considered a technical problem. But this limited viewpoint not only is outmoded, it's dangerous. Nowhere is this more relevant than in the public sector, which is entrusted with confidential PII, sensitive government data and public safety information.

Indeed, cybersecurity is an industry-wide problem that also extends to elected officials — the public face of state and local government. Throughout this guide, we have advocated for elected officials in both the executive and legislative branches to take an active role in protecting the government and its citizens from cyber-attacks.

Here are our key recommendations for elected officials:

1. Apply risk-based management to cybersecurity planning. Promote a risk-based model in which cybersecurity strategy is integrated into the organization's risk management framework and is aligned with business objectives to support and protect business functions. This will help leaders identify, assess and prioritize cybersecurity funding and strategies.

2. Adopt the NIST Cybersecurity Framework. This risk-based, best practice-focused model can be customized by government organizations according to their business needs, risk tolerance, and available funding and resources.

3. Collaborate internally and externally. Elected and agency executives and legislators should collaborate closely with each other and with government CIOs and CISOs to address cybersecurity challenges and achieve required funding. When required, look for technical assistance and cybersecurity expertise from trusted third-party organizations, such as federal agencies and industry associations, as well as the private sector.

4. Elected and Agency Executives: Be a cybersecurity leader and advocate. Take a leadership role in your organization by driving, prioritizing and funding cybersecurity strategy and initiatives throughout the organization, in the legislature and with constituents. Build a strong internal team of technical and security experts and stand behind your CIO and CISO.

5. Legislators: Educate and promote cybersecurity. Learn the government's business needs and risks, and educate citizens and fellow lawmakers on the importance of cybersecurity. Promote security and technology as key economic drivers and work to secure appropriate funding and other resources.

By following these recommendations, governments will be able to develop comprehensive strategies for protecting valuable public sector and citizen information and implementing the most effective plans for detection, response, mitigation and recovery from security incidents.

https://t.me/learningnets

Endnotes

1. http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html
2. https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=gts-LITS-bus-conn-NA&S_PKG=ov23509
3. Ibid.
4. http://www.govtech.com/security/Can-We-Talk-Creating-a-Common-Language-for-Cybersecurity.html
5. All information from David Behen taken from phone interview conducted March 24, 2015.
6. http://www.bankinfosecurity.com/sony-hack-business-continuity-lessons-a-7743
7. https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=gts-LITS-bus-conn-NA&S_PKG=ov23509
8. http://www.ncsl.org/blog/2014/12/18/states-must-have-cybersecurity-plan.aspx
9. http://www.sltrib.com/sltrib/news/56210404-78/security-breach-health-data.html.csp
10. http://investigations.nbcnews.com/_news/2012/11/20/15313720-one-email-exposes-millions-of-people-to-data-theft-in-south-carolina-cyberattack
11. http://gao.gov/assets/670/662227.pdf
12. http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/new-opm-data-breach-numbers-leave-federal-employees-anguished-outraged/
13. http://www.latimes.com/local/lanow/la-me-ln-county-data-encryption-20140527-story.html
14. http://www.michigan.gov/documents/cybersecurity/Mich_Cyber_Initiative_11.13_2PM_web_474127_7.pdf
15. http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy_2014.pdf
16. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf
17. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
18. http://www.hawaiinewsnow.com/story/28903787/alleged-cyber-attack-on-state-website-in-opposition-of-tmt-during-special-uh-regents-meeting
19. http://coloradopeakpolitics.com/2014/11/04/hacked-colorado-voting-system-attack-sos-warned-ahead-time/
20. http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
21. http://www.lamayor.org/mayor_garcetti_issues_executive_directive_on_cyber_security
22. http://www.emergencymgmt.com/safety/Hacking-Critical-Infrastructure-Is-Accelerating.html
23. http://newyork.cbslocal.com/2014/01/24/cause-of-computer-glitch-that-suspended-metro-north-lines-remains-unclear/
24. http://www.washingtonpost.com/wp-srv/special/metro/red-line-crash/crash.html
25. http://www.washingtonpost.com/postlive/gen-michael-hayden/2013/10/09/aa754bba-2aac-11e3-97a3-ff2758228523_story.html
26. http://www.itgovernanceusa.com/blog/half-of-federal-cybersecurity-breaches-caused-by-staff/
27. Ibid.
28. http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy_2014.pdf
29. All information from Mike Watson taken from phone interview conducted March 12, 2015.
30. http://www.govtech.com/state/NASCIO-Seeks-Stronger-State-Federal-Action-on-Cybersecurity.html
31. http://www.govtech.com/security/Can-We-Talk-Creating-a-Common-Language-for-Cybersecurity.html
32. https://www.whitehouse.gov/the-press-office/2015/02/13/fact-sheet-white-house-summit-cybersecurity-and-consumer-protection
33. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
34. Ibid.
35. Ibid.
36. http://www.govtech.com/security/Cybersecurity-Workforce-Gap.html
37. http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy_2014.pdf
38. http://www.govtech.com/security/Cybersecurity-Workforce-Gap.html
39. http://www.dhs.gov/about-national-cybersecurity-communications-integration-center
40. http://www.nga.org/files/live/sites/NGA/files/pdf/2013/1309_Act_and_Adjust_Paper.pdf
41. http://www.nascio.org/committees/security/
42. http://www.washingtonpost.com/postlive/steve-chabinsky/2013/10/09/4f8c08e6-2aad-11e3-97a3-ff2758228523_story.html
43. https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit
44. https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center

https://t.me/learningnets

GOVERNING
INSTITUTE

The Governing Institute advances better government by focusing on improved outcomes through research, decision support and executive education to help public-sector leaders govern more effectively. With an emphasis on state and local government performance, innovation, leadership and citizen engagement, the Institute oversees Governing's research efforts, the *Governing* Public Official of the Year Program, and a wide range of events to further advance the goals of good governance. **www.governing.com**

In collaboration with:

CGI

As a leading IT and business process services provider with 68,000 professionals worldwide, CGI delivers complex IT programs with a collaborative approach based on shared values with our clients. Since 1976, security has been a part of everything we do. We help clients understand cyber threats, assess potential risks, build strong security business cases, strengthen resilience and determine the return on their security investments. CGI also provides seamless protection of critical infrastructure, systems and data, continuously monitoring for threats in real time, and putting in place the necessary defenses. A trusted partner to government at all levels, CGI supports high-intensity cyber engagements for military and intelligence nerve centers and high-profile multi-national defense programs.

The more IT is used to improve the business of government, the greater the public demand that personal data and critical infrastructure be managed safely and securely. From initial risk assessment to incident response, cybersecurity is a huge job that is only getting bigger. CGI can help. Learn more at **www.cgi.com/cyberguide**.

https://t.me/learningnets

SHUTTERSTOCK.COM