PAPUC

CYBERSECURITY BEST PRACTICES FOR SMALL & MEDIUM PENNSYLVANIA UTILITIES

FIFTH EDITION

THE PUBLIC UTILITY COMMISSION (PUC) PROVIDES THIS AS A COURTESY TO BE USED FOR INFORMATIONAL PURPOSES ONLY. THIS IN NO WAY CONSTITUTES LEGAL ADVICE OR COUNSEL NOR IS IT A SUBSTITUTE FOR OBTAINING LEGAL ADVICE FROM YOUR OWN PRIVATE ATTORNEY.

Revised 05/2022

CYBERSECURITY BEST PRACTICES FOR SMALL AND MEDIUM PENNSYLVANIA UTILITIES

1. ASK QUESTIONS

Cybersecurity is the responsibility of every employee; however, there are basic questions to which executives and employees should know the answers. For example:

- Who in my organization is responsible for cybersecurity?
- What are the rules that govern my use of company resources (computers, smartphones, tablets)? How can I become aware of updates to these rules?
- If I suspect I have a cybersecurity issue (malware, spyware, etc.), who should I contact within my organization?
- Does my organization have a policy on bringing personal devices into the workplace?
- What devices am I allowed to connect to my company's network, and could my personal device infect the system?
- What staff in my organization are responsible for contacting the following agencies if the organization experiences a cybersecurity incident: local police, Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency (CISA), Pennsylvania Criminal Intelligence Center, and/or the Pennsylvania Public Utility Commission?
- Has our organization taken advantage of any of the free resources available to assist with performing a cybersecurity assessment?
- How are third-party vendors vetted in order to ensure they do not pose any risk to my company's Information technology infrastructure or sensitive data?

There are any number of questions a company may wish to add to this list. Use the resources mentioned in or attached to these best practices to find additional ideas.

2. CYBER ESSENTIALS

The Cybersecurity and Infrastructure Security Agency's (CISA's) Cyber Essentials is a guide for leaders of small businesses and leaders of small and local government agencies, which assists those organizations with developing an actionable understanding of where to start implementing organizational cybersecurity practices. For a deeper look and greater insight, consider utilizing the Cyber Essentials Toolkits, which are a set of modules designed to break down the CISA Cyber Essentials into bite-sized actions for IT and C-suite leadership to work toward full implementation of each Cyber Essential. More information about CISA's Cyber Essentials is available here: https://www.cisa.gov/cyber-essentials

3. COVER SOME OF THE BASICS

There are some basic rules all companies should follow in practicing good cybersecurity.

- Every user should have their own account with specific rights and restrictions based on what the employee needs in order to perform their job duties.
- Users should have strong password requirements and receive prompts to update those passwords at regular intervals.
- Job descriptions, policy statements and other company documents (e.g., procedures manuals) should clearly identify employees' cybersecurity responsibilities.
- Companies should update their employees' and contractors' security credentials as they move through the organization. Often, employees will still have access to systems despite moving to new areas that do not require such access or even upon leaving the company. Long after work is completed, contractors may retain remote access to systems or sites; companies should make concerted efforts to limit and prevent this remote access once outside vendors' contracts are complete.
- Companies should regularly patch software, maintain updates to security patches on software, and remove outdated versions of software.

The U.S. Department of Homeland Security, Cybersecurity Infrastructure Security Agency (CISA) provides additional detailed advice on maintaining safe computer networks and systems. This information can be found at: www.cisa.gov.

4. RISK MANAGEMENT

Managing risk is a priority shared by industry and government. As the Agency's planning, analysis, and collaboration center, the National Risk Management Center (NRMC) brings the private sector, government agencies, and other key stakeholders together to identify, analyze, prioritize, and manage the most significant risks to our critical infrastructure. The NRMC's dynamic, cross-sector risk management process transforms private-public engagement into collective action by defragmenting how the government and industry develop response and security plans, risk-reduction activities, and share information. Visit the NRMC Initiatives to learn more about each initiative: https://www.cisa.gov/national-risk-management.

5. USE AN ASSESSMENT TOOL

If your company is not sure where to begin on a risk assessment, CISA has created a Cybersecurity Evaluation Tool to guide users through a step-by-step process to assess their cybersecurity readiness. Companies can download this free tool at: www.cisa.gov/ics.

6. MANAGING VENDORS AND CONTRACTORS

Protecting your company's information in a digitally connected world requires understanding not only of your company's immediate supply chain, but also the extended supply chains of third-party vendors, service providers, and customers. The following essential steps will assist your organization in managing supply chain risks and building an effective Supply Chain Risk Management (SCRM) practice:

- **Identify the people**: Build a team of representatives from various roles and functions of the company (e.g., cybersecurity, information technology, physical security, procurement/ acquisition, legal, logistics, marketing, and product development). Ensure personnel at all levels are well-trained in the security procedures of their role or function.
- **Manage the security and compliance**: Document the set of policies and procedures that address security, integrity, resilience, and quality. Ensure they are based on industry standards and best practices on how to conduct SCRM such as those from the National Institute of Standards and Technology (NIST).
- **Assess the components**: Build a list of Information and Communications Technology (ICT) components (e.g., hardware, software, and services) that your organization procures to enable your business. Know which internal systems are relied upon for critical information or functions, and which systems have remote access capability that must be protected to prevent unauthorized access.
- **Know the supply chain and suppliers**: Identify your suppliers and, when possible, the suppliers' sources. In today's world of increased outsourcing, it is important to understand your upstream suppliers as part of the larger supply chain ecosystem.

- **Verify assurance of third parties**: Verify that your suppliers maintain an adequate security culture and SCRM program to appropriately address the risks that concern your organization. Establish the protocols your organization will use to assess the supply chain practices of your suppliers.

- **Evaluate your SCRM program**: Determine the frequency with which to review your SCRM program, incorporate feedback, and make changes to your risk management program. This may also include auditing suppliers against practices and protocols established by your organization.

You can download the ICT SCRM Essentials for more detailed information on how companies and organizations can effectively implement organizational SCRM practices at: https://www.cisa.gov/sites/default/files/publications/ict_scrm_essentials_508.pdf

You can also download the Internet of Things (IoT) Acquisition Guidance Document for SCRM and cybersecurity factors to consider before purchasing or using IoT devices, systems, and services. The guide can be found at: https://www.cisa.gov/sites/default/files/publications/20_0204_cisa_sed_internet_of_things_acquisition_guidance_final_508_1.pdf

7. SECURITY AS A STARTING POINT

Decades of familiarity with antivirus programs have conditioned people to think of cybersecurity as a separate tool added on top of other products. From the outset, today's development and design of software and control systems should begin with security in mind while constructing networks to minimize possible intrusions which allow a company to recognize quickly when it is under attack.

- When possible, speak with vendors about the security characteristics of their products and incorporate cybersecurity as a key component in any new specifications your company develops.

8. DON'T OVERLOOK THE PHYSICAL

Discussions of cybersecurity tend to focus on firewalls, network infrastructure, and control systems. It is important not to forget about protecting your company's physical assets as well. For example, if your company has a computer on its network in a remote location, ensure that access is controlled and monitored. Employees or contractors who log in to your system remotely may inadvertently compromise your security by misplacing their devices.

- Understand the physical attack vectors that exist and may grant access into your network; restrict access to those points.

9. TESTING

Training, assessment, and system hardening are good, but each needs to be tested regularly. In the same way utilities conduct exercises focused on physical security and disaster response, they should also test cybersecurity scenarios. These exercises might range from sending a phishing email to employees to identify whether they click the link to hiring a third party to attempt to penetrate your company's cyber defenses. CISA's website offers some helpful tips for planning your own cybersecurity exercise.

10. LEARN FROM YOUR PEERS

Some of the best resources out there for small and medium sized utilities are peers. Trade associations and other forums can provide beneficial outlets for sharing best practices and learning measures that other companies are undertaking. National and state organizations, like the National Association of Water Companies and the Energy Association of Pennsylvania, have actively engaged their members on issues of cybersecurity. These groups can be a great resource on everything from the latest threat information to sample questions for vendors within your industry.

11. SO YOU'VE BEEN HACKED...

In today's world, it is not a question of whether your company will have a cyber incident, it is a matter of when. When cyber incidents occur, CISA can provide assistance to critical infrastructure companies to:

- Analyze the potential impact from the incident.
- Investigate those responsible.
- Work with law enforcement partners to conduct criminal investigations.

CISA works in close coordination with owners and operators of critical infrastructure, to ensure greater unity of effort and response to cyber incidents. To request assistance, contact CISA at: https://www.cisa.gov/cyber-incident-response

12. VIGILANCE

Your company's cybersecurity defenses are only as good as they are timely. State of the art technology and techniques for both attackers and defenders change constantly. Be sure your company is keeping up with and is aware of the latest threats and issues. Government agencies, trade organizations, and your company's own vendors can be excellent resources in ensuring that your organization is on top of the latest cybersecurity developments.

13. REPORTING INCIDENTS

If your company has been the victim of a cybercrime, notify the appropriate regional FBI office. The FBI has two field offices in Pennsylvania, one in Pittsburgh and the other in Philadelphia. The FBI may be able to assist critical infrastructure owner/operators when there is a cyberattack or suspected cyber incident. The FBI regional offices are located in Pittsburgh and Philadelphia. The Pittsburgh Office number is 412-432-4000 and the Philadelphia Office number is 215-418-4000.

14. DEVELOPING AND MAINTAINING APPROPRIATE WRITTEN CYBERSECURITY, EMERGENCY RESPONSE AND BUSINESS CONTINUITY PLANS PURSUANT TO 52 PA. CODE §§ 101.1-101.7

According to state regulations, most utilities are required to develop and maintain written security, emergency response and business continuity plans. In addition, utilities are required to file an annual self-certification form with the Public Utility Commission that affirms their compliance with this requirement. Information about the self-certification as well as the form are available on the Commission's website at www.puc.pa.gov.

15. POTENTIAL BENEFITS OF ENGAGING A LAW FIRM IN ADVANCE OF A CYBERSECURITY INCIDENT BREACH

Because cybersecurity incidents are inevitable, a company needs to plan on how it responds in the first hours and days after the incident occurs. If a company waits until after an incident has occurred to plan its response, the company is at risk of greater financial and reputational consequences. During such a crisis, time is critical and it is imperative to quickly determine the cause and extent of a cybersecurity incident, as well as implement established procedures to timely notify and educate key internal and external stakeholders.

This response will impact whether the company gains or loses support from its customers, regulators, and the public. Engaging a law firm to assist during a cybersecurity incident and to facilitate the implementation of mitigation procedures could provide substantial benefits, from the following services:

- Preparation of written breach response plans that will address cybersecurity incidents.
- Retaining a forensics firm that can develop tools to monitor and assess threat levels, as well as respond to any suspected cybersecurity attack. Law firms can assist in preparing the Request for Proposals (RFPs) for forensic firms and then engage a forensics firm directly to afford legal advice and protection to the company, both prior and subsequent to a breach.
- Assistance with RFPs for other third-party vendors, including crisis communication firms, call center assistance, credit service providers, etc. A law firm also may partner with the company to help ensure that these vendors satisfy various regulatory and legal requirements.
- Ensuring that a company has an effective governance structure in place with respect to cybersecurity, which not only meets regulatory and legal requirements, but also helps ensure that key stakeholders are kept well-informed.
- Advice in scoping and obtaining cyber insurance coverage.
- Assistance in the classification and protection of confidential information and/or privileged information.
- Development of training materials and exercises.
- Terms and conditions for vendor contract management that obligate a vendor to maintain adequate information security safeguards, as well as allow the company to perform periodic inspections and audits of the vendor.

As demonstrated by these prospective services, law firms may be able to provide broad assistance to a company to both prepare for and respond to a cybersecurity incident. However, to be successful and mitigate risk, the law firm needs to be engaged and the scope of services established well in advance of a crisis. While engaging a law firm for the aforementioned services may certainly be considered a best practice to combat cyber threats, a utility must consider its financial capabilities in seeking out or retaining the services of a law firm. For some utilities, it may be cost prohibitive to keep a law firm on retainer; these utilities may have to rely on in house counsel and prudent cyber protection practices to mitigate the financial and operational risks of a cybersecurity incident.

FEDERAL RESOURCES

DEPARTMENT OF HOMELAND SECURITY (DHS)

The U.S. Department of Homeland Security (DHS) has several offices that address cybersecurity matters. They are set forth below.

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

CISA helps organizations better manage risk and increase resilience using all available resources, whether provided by the Federal Government, commercial vendors, or their own capabilities. CISA also coordinates cybersecurity and resilience efforts using trusted partnerships across the private and public sectors and delivers technical assistance and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide.

CISA enhances public safety interoperable communications at all levels of government to help partners across the country develop their emergency communications capabilities. For more information on the CISA and its services go to its website: www.cisa.gov.

ICS CYBER EMERGENCY RESPONSE TEAM

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and United States Computer Emergency Readiness Team (US-CERT) work to mitigate cybersecurity incidents in close coordination with public and private sector partners.

ICS-CERT provides onsite support to owners and operators of critical infrastructure, ICS-CERT services include incident response, forensic analysis, and site assessments. ICS-CERT also provides tools and training designed to increase stakeholder awareness of the threats posed to industrial control systems.

The ICS-CERT website provides various resources for owners and operators of critical infrastructure and the industrial control systems that operate many of the key functions of their facilities, such as SCADA system. The website contains links to resources such as alerts, advisories, newsletters, training, recommended practices, as well as a large list of standards and references. The ICS-CERT website can be found here: https://www.us-cert.gov/ics

FEDERAL BUREAU OF INVESTIGATION (FBI)

The Federal Bureau of Investigation (FBI) has two field offices in Pennsylvania, one in Pittsburgh and the other in Philadelphia. The FBI may be able to assist critical infrastructure owner/operators when there is a cyberattack or suspected cyber incident. The FBI encourages reporting of suspected cyberattacks by critical infrastructure owners.

The Pittsburgh Office number is 412-432-4000 and the Philadelphia Office number is 215-418-4000.

INFRAGARD

InfraGard is an FBI program that began as a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. It is now a national program under the responsibility of the FBI's Cyber Division. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters. InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector.

The goal of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI. InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes. Membership is free and open to all critical infrastructure owners and operators.

More information, including information on membership, can be found here: https://www.infragard.org/.

DEPARTMENT OF HOMELAND SECURITY PROTECTIVE SECURITY ADVISORS (PSA) AND CYBER SECURITY ADVISORS

DHS's Protective Security Advisor (PSA) program offers critical infrastructure owner/operators a conduit to many free services such as security training, site assessments, and assistance with local exercise coordination. More information about PSA can be found at: https://www.cisa.gov/protective-security-advisors.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY FRAMEWORK

In 2013, the Obama Administration directed the National Institute of Standards and Technology (NIST) to work with cybersecurity and critical infrastructure stakeholders to develop a voluntary framework that would enable organizations to assess their cyber-risk based on existing NIST standards, guidelines, and best practices. The objective of this assessment is to reduce cyber risks to an organization's critical infrastructure.

Since releasing the Framework, NIST has been educating a broad audience about the Framework's use and value. The Framework is being employed across the country, in a host of sectors, and by organizations ranging from multinationals to small businesses. The proposed value of the Framework has been validated through a large volume and breadth of interactions between NIST and industry. The Cybersecurity Framework and information on its applicability can be found here: https://www.nist.gov/cyberframework.

STATE RESOURCES

PENNSYLVANIA GOVERNOR'S OFFICE OF HOMELAND SECURITY (OHS)

Pennsylvania Governor's Office of Homeland Security (OHS) coordinates homeland security functions among federal agencies, state government, regional task forces, local government, and the private sector. OHS is a source for general information about cybersecurity in the state. More information is available at: www.homelandsecurity.pa.gov.

PENNSYLVANIA CRIMINAL INTELLIGENCE CENTER (PaCIC)

The Pennsylvania Criminal Intelligence Center (PaCIC) was formed by the Pennsylvania State Police with the goal of proactively addressing the threats posed to our citizens from criminal and terrorist acts by sharing state police intelligence resources with criminal justice agencies in Pennsylvania and nationwide. The PaCIC's mission has expanded to include providing information bulletins to critical infrastructure partners as well as providing a means to report suspicious activities or emerging threats.

For more information on PaCIC, including applying to receive informational bulletins, please email SP-ProtectPA@pa.gov, or call 855-772-7768.

PENNSYLVANIA OFFICE OF ADMINISTRATION (OA) – INFORMATION SECURITY OFFICE

The Pennsylvania Office of Administration (OA) is responsible for ensuring the cybersecurity of the Commonwealth network systems. OA has a website with information and resources related to cybersecurity that is available to the public. The website can be accessed here: www.cybersecurity.pa.gov.

PENNSYLVANIA PUBLIC UTILITY COMMISSION (PUC)

Utilities are responsible for managing cybersecurity as part of their overall security planning and readiness. Jurisdictional utilities are required to self-certify that they have developed and maintained their security plans on an annual basis. Utilities cybersecurity plans are subject to audit by the Commission. See 52 Pa. Code §§ 101.1 101.7

For more information on the Commission's self-certification forms, visit: www.puc.pa.gov/documents/utility-files/279/Security_Planning_Self-Cert_Checklist2021-F.pdf

To download a Commission self-certification form, visit: www.puc.pa.gov/documents/utility-files/367/FAQ_PUSPR_Self_Certification.pdf.

updated 6/22

The Pennsylvania Public Utility Commission balances the needs of consumers and utilities; ensures safe and reliable utility service at reasonable rates; protects the public interest; educates consumers to make independent and informed utility choices; furthers economic development; and fosters new technologies and competitive markets in an environmentally sound manner.

Pennsylvania Public Utility Commission

www.puc.pa.gov

1-800-692-7380