WaterISAC
Security Information Center

10 Basic Cybersecurity Measures:
Best Practices to Reduce Exploitable Weaknesses and Attacks

October 2016

Developed in partnership with the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the FBI, and the Information Technology ISAC. WaterISAC also acknowledges the Multi-State ISAC for its contributions to this document.

About WaterISAC

The Water Information Sharing and Analysis Center, established in 2002 by the water and wastewater industry, is the designated communications and operations arm of the United States water and wastewater sector. With an all-hazards focus, WaterISAC provides its members with threat alerts and analysis as well as best practices and training on reducing risk, mitigating vulnerabilities, improving resiliency, and recovering from natural and manmade emergencies.

WaterISAC members are in the U.S., Canada, and Australia. They include water and wastewater utilities; federal, state, and local government agencies involved in security, law enforcement, intelligence analysis, emergency response, and public health; and engineering and consulting firms.

WaterISAC members have access to the world's largest and richest source of information and tools for strengthening water and wastewater utility security, resilience, and emergency management.

For more information about WaterISAC, visit https://www.waterisac.org or email service@waterisac.org.

If your organization has experienced a cybersecurity breach or suspects a breach has occurred, please contact WaterISAC and ICS-CERT:

WaterISAC
Email: analyst@waterisac.org
Call: 866-H20-ISAC
Online Incident Report form: https://www.waterisac.org/report-incident

ICS-CERT
Email: ics-cert@hq.dhs.gov
Call: 877-776-7585

Introduction

In partnership with the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the FBI, and the Information Technology ISAC, WaterISAC has developed a list of 10 basic cybersecurity recommendations water and wastewater utilities can use to reduce exploitable weaknesses and defend against avoidable data breaches and cyber attacks. Each recommendation is accompanied by links to corresponding technical resources. This document is an updated version of the *10 Basic Cybersecurity Measures to Reduce Exploitable Weaknesses and Attacks* guide that WaterISAC published in June 2015.

In reviewing its incident reports for 2014, ICS-CERT noted that implementation of the first three recommendations likely would have detected the issues, prevented the vulnerabilities, and averted the resulting impacts related to those incidents. In its review of 2015 assessments, ICS-CERT noted that over one-third of weaknesses found were related to six security practices. Although risks remain and threat actors will continue to change their capabilities and methods, ICS-CERT advises that the first three recommendations be implemented as soon as practical.

For further measures to reduce cyber risks, consult the *Framework for Improving Critical Infrastructure Cybersecurity* by the National Institute of Standards and Technology (NIST) and the American Water Works Association's (AWWA's) *Cybersecurity Guidance and Tool*. The NIST Cybersecurity Framework is a set of voluntary practices, standards, and guidelines created to help critical infrastructure owners and operators manage cyber risks. The AWWA Guidance and Tool is a sector-specific approach for adopting the NIST Cybersecurity Framework.

Also, download WaterISAC's *Cybersecurity Resource Guide* for more information on key resources to help water and wastewater utilities and the government agencies that support them mitigate risks and resolve vulnerabilities.

1) Maintain an Accurate Inventory of Control System Devices and Eliminate Any Exposure of this Equipment to External Networks

Never allow any machine on the control network to talk directly to a machine on the business network or on the Internet. Although some organizations' industrial control systems may not directly face the Internet, a connection still exists if those systems are connected to a part of the network – such as the corporate side – that has a communications channel to external (non-trusted) resources (i.e., to the Internet).

Organizations may not realize this connection exists, but a persistent cyber threat actor can find such pathways and use them to access and exploit industrial control systems to attempt to create a physical consequence. Therefore, organizations are encouraged to conduct thorough assessments of their systems, including the corporate enterprise segments, to determine where pathways exist. Any channels between devices on the control system and equipment on other networks should be eliminated to reduce network vulnerabilities.

- ICS-ALERT-12-046-01A Increasing Threat to Industrial Control Systems (ICS-CERT)
- ICS-ALERT-11-343-01A Control System Internet Accessibility (ICS-CERT)
- Targeted Cyber Intrusion Detection and Mitigation Strategies (ICS-CERT)

2) Implement Network Segmentation and Apply Firewalls

Network segmentation entails classifying and categorizing IT assets, data, and personnel into specific groups, and then restricting access to these groups. By placing resources into different areas of a network, a compromise of one device or sector cannot translate into the exploitation of the entire system. Otherwise, cyber threat actors would be able to exploit any vulnerability within an organization's system – the "weakest chain in the link" – to gain entry and move laterally throughout a network and access sensitive equipment and data. Given the rise of the "Internet of Things" – whereby many previously non-Internet connected devices, such as video cameras, are now linked to systems and the web – the importance of segmenting networks is greater than ever.

Access to network areas can be restricted by isolating them entirely from one another, which is optimal in the case of industrial control systems (as described in recommendation #1 above), or by implementing firewalls. A firewall is a software program or hardware device that filters the inbound and outbound traffic between different parts of a network or between a network and the Internet. For connections that face the Internet, a firewall can be set up to filter incoming and outgoing information. By reducing the number of pathways into and within your networks and by implementing security protocols on the pathways that do exist, it is much more difficult for a threat to enter your system and gain access to other areas.

Creating network boundaries and segments empowers an organization to enforce both detective and protective controls within its infrastructure. The capability to monitor, restrict, and govern communication flows yields to a practical capability to baseline network traffic (especially traffic traversing a network boundary), and identify anomalous or suspicious communication flows.

These boundaries also provide a means to practically detect potential lateral movement, network footprinting and enumeration, and device communications attempting to traverse from one zone to another.

- Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies (ICS-CERT)
- Why You Need to Segment Your Network for Security (CSO)
- Firewall Deployment for SCADA and Process Control Networks (UK Centre for the Protection of National Infrastructure via ICS-CERT)
- Beginners Guide to Firewalls: A Non-Technical Guide (MS-ISAC)
- Guide to Industrial Control Systems Security – Special Publication 800-82 (NIST)
- Guidelines for Application Whitelisting in Industrial Control Systems (ICS-CERT)

3) Use Secure Remote Access Methods

The ability to remotely connect to a network has added a great deal of convenience for end users, but a secure access method, such as a Virtual Private Network (VPN), should be used if remote access is required. A VPN is an encrypted data channel for securely sending and receiving data via public IT infrastructure (such as the Internet). Through a VPN, users are able to remotely access internal resources like files, printers, databases, or websites as if directly connected to the network. This remote access can further be hardened by reducing the number of Internet Protocol (IP) addresses that can access it by utilizing network devices and/or firewalls to specific IP addresses and/or ranges and from within the U.S. Note that a VPN is only as secure as the devices connected to it. A laptop computer infected with malware can introduce those vulnerabilities into the network, leading to additional infections and negating the security of the VPN.

- Configuring and Managing Remote Access for Industrial Control Systems (ICS-CERT)
- Extending Your Business Network through a Virtual Private Network (SANS Institute)
- Virtual Private Networking: An Overview (Microsoft)

4) Establish Role-Based Access Controls and Implement System Logging

Role-based access control grants or denies access to network resources based on job functions. This limits the ability of individual users – or attackers – to reach files or parts of the system they shouldn't access. For example, SCADA system operators likely do not need access to the billing department or certain administrative files. Therefore, define the permissions based on the level of access each job function needs to perform its duties, and work with human resources to implement standard operating procedures to remove network access of former employees and contractors. In addition, limiting employee permissions through role-based access controls can facilitate tracking network intrusions or suspicious activities during an audit.

Implementing a logging capability allows for the monitoring of system activity. This enables organizations to conduct thorough root cause analyses to find the sources of issues in the system, which may have been the activities of an employee or an outsider. Monitoring network traffic also allows organizations to determine if a user is making unauthorized actions or if an outsider is in the system, which provides an opportunity to intervene before problems are manifested.

- Role Based Access Control and Role Based Security (NIST)
- An Introduction to Role Based Access Control (NIST)
- Extending Role Based Access Control (SANS Institute)
- Targeted Cyber Intrusion Detection and Mitigation Strategies (ICS-CERT)

5) Use Only Strong Passwords, Change Default Passwords, and Consider Other Access Controls

Use strong passwords to keep your systems and information secure, and have different passwords for different accounts. Hackers can use readily available software tools to try millions of character combinations to attempt an unauthorized login – this is called a "brute force attack." Passwords should have at least eight characters, but longer passwords are stronger, because of the greater number of characters to guess. Also, include uppercase and lowercase letters, numerals, and special characters. Change all default passwords upon installation of new software, particularly for administrator accounts and control system devices, and regularly thereafter. Implement other password security features, such as an account lock-out that activates when too many incorrect passwords have been entered. Organizations may also consider requiring multi-factor authentication, which entails users verifying their identities – via codes sent to devices they previously registered – whenever they attempt to sign-in.

- Choosing and Protecting Passwords (US-CERT)
- Supplementing Passwords (US-CERT)
- Strong Passwords (Microsoft)

6) Maintain Awareness of Vulnerabilities and Implement Necessary Patches and Updates

Most vendors work diligently to develop patches for identified vulnerabilities. But even after patches and updates have been released, many systems remain vulnerable because organizations are either unaware of or choose to not implement these fixes. In its *2016 Data Breach Investigations Report*, Verizon found that in most industries, three quarters of incidents and breaches are covered by only three patterns. For utilities, these patterns were cyber espionage, crimeware, and denial of service. Among its recommendations, understanding the building blocks of an attack (e.g., a kill chain) can help construct defenses and detect a breach. Effective patching can also stop a large portion of attacks considering the top 10 cyber vulnerabilities accounted for 85% of successfully exploited. traffic.

Cisco's *2016 Annual Security Report* stated that security professionals must rethink their defense strategies as cyber criminals have refined their infrastructures to carry out attacks in more efficient and profitable ways. The report also covered global threat intelligence and insights on possible future criminal behavior, ransomware, risks of aging IT infrastructure, and geopolitical concerns for internet governance.

To protect one's organization from these opportunistic attacks, a system of monitoring for and applying system patches and updates should be implemented. WaterISAC regularly posts information on vulnerabilities and patches, which it receives from its partners at the U.S. Department of Homeland Security's ICS-CERT and United States Computer Emergency Readiness Team (US-CERT), other ISACs, and cybersecurity firms, among others. Where possible, organizations should also consider setting systems and software to auto-update to avoid missing critical updates. These updates are designed to fix known vulnerabilities and are encouraged for any Internet-connected device.

- Recommended Practice for Patch Management of Control Systems (ICS-CERT)
- Software Update Management Guidelines (Microsoft)
- Index of Advisories by Vendor (ICS-CERT)
- Top 30 Targeted High Risk Vulnerabilities (US-CERT)

7) Develop and Enforce Policies on Mobile Devices

The proliferation of laptops, tablets, smartphones, and other mobile devices in the workplace presents significant security challenges. The mobile nature of these devices means they are potentially exposed to external, compromised applications and networks and malicious actors. Further contributing to this challenge is the increasing trend of organizations allowing employees to use their personal electronic devices for work purposes, known as the "Bring Your Own Device (BYOD)" phenomenon.

Therefore, it's important to develop policies on the reasonable limits of mobile devices in your office and on your networks. These measures should be strictly enforced for all employees, as well as for contractors. Devices should also be password protected to ensure only authorized users can log-in. Otherwise, an unauthorized user can gain access to restricted networks and files using an authorized user's device. Similarly, employees should avoid or be cautious about using devices that do not belong to them as they cannot be sure these are properly protected or comply with established policy. Such devices may actually be infected, and using them could put the information and networks you access at risk.

- Cybersecurity for Electronic Devices (US-CERT)
- Guidelines on Cell Phone and PDA Security (NIST)
- Guidelines for Managing the Security of Mobile Devices on the Enterprise (NIST)
- Guide to Enterprise Telework, Remote Access, and BYOD Security (NIST)
- User's Guide to Telework and BYOD Security (NIST)
- Bring Your Own Device (BYOD) Design Considerations Guide (Microsoft)

8) Implement an Employee Cybersecurity Training Program

Cybersecurity for critical infrastructure sectors that operate industrial control systems, such as the water and wastewater sector, is extremely important given that these systems are increasingly being targeted. When employees aren't involved in cybersecurity, not only can vulnerabilities and threats go unnoticed but the employees themselves can become conduits through which attacks are executed. Therefore, employees should receive initial and periodic cybersecurity training, helping to maintain the security of the organization as a whole.

While cybersecurity is an expansive field, there are certain topics that should be emphasized for general awareness. One such topic is social engineering, which continues to be a popular means for cyber criminals to prey upon unsuspecting employees. These methods involve emails ("phishing"), phone calls, or other types of personal interactions in which malicious actors attempt to entice employees into providing sensitive personal or corporate information, such as account passwords or details about information technology infrastructure. Alternatively, these actors might attempt to make employees perform specific actions, such as pay for alleged services, download infected attachments, or visit malicious websites. Unsolicited emails, phone calls, and other correspondence from unknown senders should be viewed with particular caution.

Among the key points in Booz Allen Hamilton's *Industrial Cybersecurity Threat Briefing* for 2016, one-third of ICS operators around the world were breached in 2015 and spear phishing was the primary method of attack. In spear phishing incidents, the vulnerabilities were the users who were comprised through social engineering. According to its survey, the water and dams sectors totaled 31 incidents in 2015. The primary threats included nation-states (specifically China, Russia, North Korea, and Iran), ransomware targeting ICS operators, the sale of access to SCADA systems as a service, freely available attack resources, attacks against the supply chain, and improper access control. The briefing included detailed descriptions of incidents per sector, and mitigation practices.

Training should also incorporate the importance of smart Internet browsing practices. Visiting suspicious websites may expose users to infection by malware embedded on the site (a "drive-by-download" attack). Even legitimate websites, as well as the files on them, may be compromised. Cyber attackers employ a variation of this type of tactic, a "watering-hole" attack, to target the employees of a company they know will visit the website. Therefore, caution should be exercised no matter where a user navigates and the materials that are downloaded.

- Avoiding Social Engineering and Phishing Attacks (US-CERT)
- Recognizing and Avoiding Email Scams (US-CERT)
- Securing Your Web Browser (US-CERT)
- Preparing for Cyber Incident Analysis (ICS-CERT)
- Best Practices for Dealing with Phishing and Ransomware (Osterman Research)
- Five Tips to Help Execute an Employee Training Program (Help Net Security)

9) Involve Executives in Cybersecurity

Despite the continued proliferation of cyber threats and the far-reaching effects cyber attacks can have, researchers have found that organizational leaders often lack sufficient awareness of cybersecurity threats and needs. Cyphort and the Ponemon Institute published a study in March 2016 titled *The State of Malware Detection and Prevention* that identified serious challenges organizations face in preventing and detecting cyber attacks and prioritizing and investigating malware alerts. Only 36 percent of respondents say IT security and others who are responsible for security have the necessary information to make the C-suite aware of advanced threats. The report also notes that 34% of respondents say C-level executives are never updated on security incidents.

While organizations are increasingly elevating cybersecurity to the executive level by adding the role of Chief Information Security Officer (CISO), many organizations remain unprepared for cyber threats. IBM's paper, *Securing the C-Suite*, surveyed 700 executives worldwide to assess non-technical executives' understanding of cyber threats. According to the results, there are four signs that an organization is not prepared for cybersecurity threats. These involve the misidentification of the actual threats, the lack of a chief information security officer (CISO), not including all C-suite members in cybersecurity planning, and a reluctance to share information about cybersecurity threats with external organizations.

- Cybersecurity Questions for CEOs (US-CERT)
- ICS Cybersecurity for the C-Level (ICS-CERT)

10) Implement Measures for Detecting Compromises and Develop a Cybersecurity Incident Response Plan

Despite the many preventative measures organizations implement, many still experience compromises. Indeed, many cybersecurity experts have noted that experiencing a compromise is not really a question of "if," but more of a question of "when." When a compromise occurs, the organizations that fare the best will be those that quickly detect the issue and have a plan in place to respond.

Implementing such measures as intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), anti-virus software, and logs (previously described in recommendation #4) can help to detect compromises in their earliest stages. Most IDSs and IPSs use signatures to detect port scans, malware, and other abnormal network communications. New viruses are discovered every day, and anti-virus programs are oftentimes set to automatically update themselves to look for the latest threat signatures. Still, administrators should not rely solely on anti-virus software for detecting infections. Logs from firewalls, intrusion detection and prevention sensors, and servers should be monitored for signs of infections.

Incident response plans are a critical yet underutilized component of emergency preparedness and resilience. An effective cybersecurity response plan will limit damage, increase the confidence of partners and customers, and reduce recovery time and costs. Plans should include measures for reacting to destructive malware in an ICS environment. In such situations, organizations should be prepared to "island" their ICS environments by disconnecting from non-ICS networks. They should also

be capable of going to "manual operations" if network conditions impact visibility from the SCADA system, or if malware potentially renders control devices inoperable via an automated means.

Rather than being developed by a single entity, the plan should be a product of collaboration between all departments that would be stakeholders in a cybersecurity incident. This will ensure a cooperative and unified response that leverages all of an organization's resources to the greatest extent possible. For enhanced responsive capability in the event of a cybersecurity incident, organizations should consider forming a Computer Security Incident Response Team (CSIRT).

This task is not complete once the plan has been developed; it needs to be operationalized as well. It is critical that plans be routinely reviewed and updated to ensure they remain relevant and useable for when they are actually needed. Furthermore, to truly understand their cybersecurity incident response plan, organizations must practice them through regular exercises. This will ensure that all stakeholders understand the procedures that would be implemented in the event of a significant cyber disruption or breach, enabling a more effective and efficient response.

- Malware Threats and Mitigation Strategies (US-CERT)
- Developing an ICS Cybersecurity Incident Response Capability (ICS-CERT)
- Nine Steps For A Successful Incident Response Plan (CSO Online)
- Ten Steps to Planning an Effective Cyber-Incident Response (Harvard Business Review)
- Create a CSIRT (CERT)
- Best Practices for Continuity of Operations (ICS-CERT)
- Five Useful Tips to Build a Successful and Mature Security Operations Center (IBM)
- How Incident Response Fails in ICS Networks (Dark Reading)