WHITE PAPER

JUNE 2017

PHOENIX CONTACT
INSPIRING INNOVATIONS

Cybersecurity: Going Beyond Protection to Boost Resiliency

By Don Dickinson

Senior Business Development Manager – Water Sector, Phoenix Contact USA

Executive summary

It's a fact of life in the digital age. Managing cyber-threats is the new norm. The challenge of protecting sensitive data and cyber-assets becomes even more daunting as tens of billions of devices are connected globally, creating the Internet of Things (IoT). Cyber-threats take on an even greater significance when the target is critical infrastructure such as the electrical grid, a transportation system, or a water/wastewater utility.

Although security professionals continue to expand and strengthen security profiles, cyber-criminals continue to find ways to exploit vulnerabilities in even the best security plan. As a result, a comprehensive security plan for a water or wastewater utility must go beyond protection strategies and include provisions for detecting and responding to a potentially harmful cyber-event in order to minimize its immediate impact on operations and public health and safety. Further, a security plan must include measures to recover from a cyber-event to minimize the long-term impact on business continuity. Going beyond protection boosts a utility's resiliency, enhances

INSIDE:

sustainability, and ensures the availability and reliability of essential water and wastewater operations.

In February 2014, the National Institute of Standards and Technology (NIST) issued the Framework for Improving Critical Infrastructure Cybersecurity. The purpose of the Framework is to help organizations manage cybersecurity risks in a cost-effective way based on the business needs of the critical infrastructure sectors, including Water and Wastewater Systems.

A key part of the NIST Cybersecurity Framework is the Framework Core. The Framework Core is a set of cybersecurity activities segmented into five functions: Identify, Protect, Detect, Respond, and Recover. These functions organize basic cybersecurity activities at their highest level.

This paper, "Cybersecurity: Going Beyond Protection to Boost Resiliency," will provide an overview of the NIST Cybersecurity Framework and the five functions of the Core that must be addressed as part of a comprehensive utility-wide security plan. Although protecting critical cyber-assets is the first order of business, this paper will emphasize the need for utilities to look beyond protection strategies to boost resiliency and bolster sustainability.

The new normal

Recent high-profile cyber-attacks and security breaches are a reminder that managing cyber-risks is now the norm in the digital age. On the cyber battlefield, there is both good news and bad news. Per the SonicWall 2017 Annual Threat Report,[1] the good news is that in 2016, security teams leveraged groundbreaking technologies to fend off attacks that would have devastated their organizations in years past. The bad news is cyber-criminals proved to be exceptionally innovative as well, wreaking havoc in the cyber world with attacks on targets ranging from hospitals to the CIA. Despite the endless string of cyber-events that have been reported – and countless others that were not – there are several trends worth noting.

Attacks get bigger

In September 2016, Yahoo reported that data associated with at least 500 million user accounts had been stolen in late 2014.[2] The event was considered to be one of the largest cybersecurity breaches ever – until December 2016, when Yahoo announced that more than one billion accounts were compromised in a 2013 attack! The two attacks are the largest known security breaches of one company's computer network.[3] Not only have attacks increased in scale, but they continue to evolve, presenting new and more challenging threats for security professionals.

Botnets

In October 2016, an automated attack using IoT devices caused a tremendous disruption to large portions of the internet. Malicious software (malware) known as Mirai was used to create a botnet – a network of Internet computers (robots or "bots") being controlled as a group without the owners' knowledge. A botnet can overwhelm targeted devices or websites with communications that ultimately shut down the device or website. This type of attack is known as a distributed denial of service (DDoS) attack.

The target of the attack was Dyn, an Internet infrastructure firm. The attack was one of the largest ever seen and impacted web services for some of the best known online sites that use Dyn's services. Interestingly, the botnet was mostly IoT devices such as DVRs, webcams, and routers. A troubling aspect of this and other DDoS attacks is that perpetrators do not need extensive knowledge to carry out such an attack – even on a large scale. Perhaps the good news is that the result of the attack was only a disruption of Internet service – albeit a significant one. Other types of cyber-threats can have much more harmful results.

Ransomware

Ransomware is malware that blocks access to a computer or computer system until a sum of money is paid. In May 2017, the WannnaCry ransomware attack crippled more than a quarter million computers in 150 countries. The attack was unprecedented in scale. Its victims range from critical health care systems to automotive manufacturing plants. It is fortuitous that a web security researcher identified a way to dramatically slow the spread of the ransomware. Although the attack was highly disruptive on a global scale, its impact was relatively low, as most systems were able to recover within days of the attack. Had this been an attack that specifically targeted critical infrastructure, the outcome could have been devastating.

In April 2016, Michigan's third-largest electric and water utility, Lansing Board of Water & Light (BW&L), was a victim of a ransomware attack. The utility's IT systems, including administrative systems and online customer services, had to be taken offline for a week – including the online system for reporting power outages.[4] Lansing BW&L reportedly paid ransomware attackers $25,000 to regain control of their system. However, administrators have since reported that the actual cost of the attack is $2.4 million when considering all costs related to the attack.[5]

The use of ransomware has increased dramatically. Per the SonicWall report, there was an exponential increase in the number of ransomware attacks during 2016, from nearly 4 million attacks in 2015 to 638 million in 2016.[6] Losing access to a utility's IT network due to a ransomware attack is a dire problem. Losing control of a critical process would be disastrous.

Although this attack did not cause an interruption in service, it may be a harbinger of things to come, and a reminder of how a cyber-event can negatively impact utility operations. A security plan that reduces both the likelihood and the potential impact of a cyber-event enables business continuity and sustainability.

Social engineering

Even the best security plan can be compromised by the click of the mouse. The ransomware malware that took control of the Lansing Board of Water & Light business system was part of a phishing attack. Phishing is a form of social engineering, which is the use of deception to manipulate someone to willingly provide confidential information. Cyber-criminals are always looking to exploit human weaknesses to gain unauthorized access to a network. This is much easier than finding vulnerabilities in the network.

Spear phishing is an email that targets a specific individual or organization and appears to be a legitimate communication from a trusted source. When the receiver opens the email or clicks on a link, malware, such as ransomware, is introduced. Once a threat actor has access to the network, it is not difficult to acquire information that will aid in a future attack. Typically, when that attack occurs, it is too late to do anything about it. If the target of that attack is a water/wastewater utility, the results could be potentially catastrophic.

Cybersecurity going forward

Cybersecurity will become only more challenging in the future, as the demand for more data drives more interconnectivity. The IoT will change our personal lives in ways that we can only yet imagine. Already, there are several billion IoT devices connected to the Internet. It is predicted that tens of billions of devices will be connected to the Internet in just a few years.

The Industrial Internet of Things (IIoT) will change our professional lives, as we usher in the fourth industrial revolution driven by dramatic technological advances in IoT technologies and embedded intelligence. Within the water sector, there are numerous variations on the IIoT theme such as the Smart Water Grid, Intelligent Water, Advanced Metering Infrastructure (AMI), and Asset Management, to name just a few. The common denominator is data.

"Big Data" is already transforming our world, and it will transform our industry. Data analytics has the potential to identify significant opportunities for process improvements, increased efficiencies, lower life-cycle costs, enhanced regulatory compliance, and improved customer service. But more interconnectivity will make cybersecurity all the more challenging, as evidenced by the Dyn cyber-attack referenced earlier.

Protecting critical infrastructure

A key component in protecting critical infrastructure from cyber-attack is protecting the automated systems used to monitor and control critical processes. Systems that control water and wastewater processes are known by many names. Industrial control system (ICS), supervisory control and data acquisition (SCADA), distributed control system (DCS), and process control system (PCS) are just a few of the terms that fall under the general category of Operational Technology (OT).

Increasingly, OT systems and networks are coming under attack. Malware such as Stuxnet, Havex, and BlackEnergy that specifically target OT systems and networks have been developed and used to attack critical infrastructure. Along with specialized malware, threat actors can employ a variety of tactics to penetrate defenses for critical infrastructure.

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-1300 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
E-mail: info@phoenixcon.com • Website: www.phoenixcontact.com

One example is the December 2015 attack on the Ukrainian power grid that left hundreds of thousands without power. It was the first publicly acknowledged cyber-attack to result in a power outage.[7] In addition to BlackEnergy malware, the attackers used spear phishing emails to gain access to the target's business system and harvest credentials to gain access to the OT network via a virtual private network (VPN). Once the attackers were in the OT network, they employed multiple tools and technology to alter OT devices and process functions. Finally, a telephone denial-of-service attack on the target's call center prevented customers from reporting outages. It is clear that the perpetrators of this attack were motivated and highly skilled. This attack should serve as a powerful reminder that the threat to critical infrastructure cannot be ignored.

Owners and operators of OT systems controlling critical infrastructure must be aware of these threats and take steps to manage cyber-risks. Although the primary goal of an OT security plan is to prevent a cyber-event from impacting critical infrastructure, even the most secure systems can be and have been compromised. A comprehensive security plan must go beyond the implementation of OT protection strategies. By planning its response to and recovery from a cyber-event, the utility increases its resiliency while reducing the likelihood of potential fines and litigation.

NIST Cybersecurity Framework

In February 2014 the NIST issued the Framework for Improving Critical Infrastructure Cybersecurity (Version 1.0)[8] to help organizations manage cyber-risks within the critical infrastructure sectors, including water and wastewater systems. The Cybersecurity Framework (CSF) is available as a download from the NIST web site (www.nist.gov/cyberframework).

The CSF is a voluntary, risk-based approach for managing cybersecurity risks for critical infrastructure. It references industry standards, guidelines, and best practices known as informative references to help organizations manage cybersecurity risks. Because there are no specific directives for securing OT in the water sector, the CSF is a useful resource for identifying relevant resources. The CSF is not meant to replace an existing program but can be used as the foundation for a new cybersecurity program or as a means to improve an existing program.

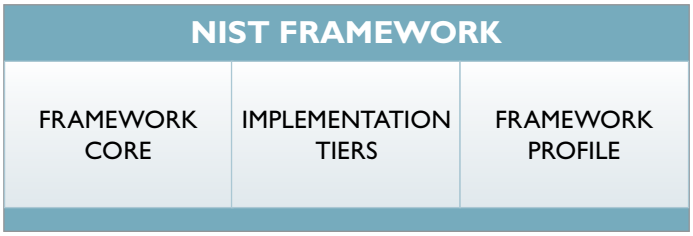

Figure 1: NIST Cybersecurity Framework

The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profile, as shown in Figure 1.

Framework Implementation Tiers characterize the organization's risk management practices as defined by one of four tiers, with Tier 1 having the least amount of risk management and Tier 4 the highest. Each organization must determine which tier is appropriate for them to work toward, given the organization's unique goals, feasibility of implementation, and acceptable level of cybersecurity risk.

The Framework Profile helps an organization define a road map for moving from a "current" profile that defines current risk management practices to a "desired" profile that defines the outcomes needed to achieve the desired cybersecurity risk management goals. A comparison of the current profile and the desired profile provides a gap analysis that can be used to establish a plan defining actions required to meet organizational goals, and prioritization of activities to ensure cost-effective allocation of resources.

Cybersecurity Framework Core

A key part of the Cybersecurity Framework is the Framework Core. The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references common across all critical infrastructure sectors and segmented into five functions as shown in Figure 2: Identify, Protect, Detect, Respond, and Recover.

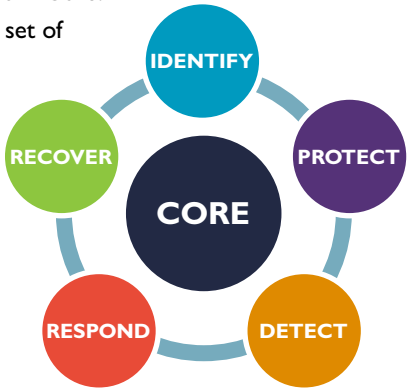

Figure 2: Cybersecurity Framework Core

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-1300 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
E-mail: info@phoenixcon.com • Website: www.phoenixcontact.com

These functions organize basic cybersecurity activities at their highest level. The Core functions are divided into categories and then into subcategories that are linked to key industry standards and best practices referred to as "Informative References," which provide specific guidance for each of the Core functions. The five core functions as defined by the NIST Framework are:

Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Figure 3 illustrates how a function (Identify in this example) is broken down into a category (Asset Management), and then to a subcategory (Devices & Systems Inventoried), and then linked to a specific entry or entries in one or more of the Informative Reference (ISA-62443 security standard in this example).

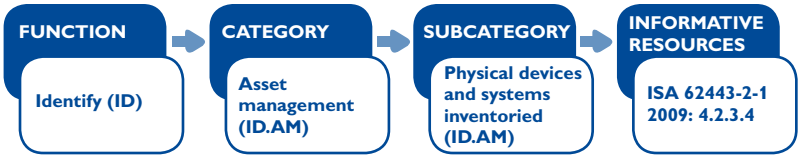

Figure 3: Linking Cybersecurity Function to Informative References

The Informative References provide useful information on all aspects of cybersecurity and valuable guidance for developing a security program. When a utility's security plan covers all aspects of security, not just protection, the utility increases its resiliency and improves sustainability as illustrated in Figure 4.

Figure 4: Increasing Resiliency & Sustainability

Sustainable infrastructure

A comprehensive security plan is essential for increasing a utility's resiliency and, ultimately, its sustainability. It's important to put OT security into the broader context of sustainability.

The U.S. Environmental Protection Agency (EPA) promotes sustainable infrastructure within the water sector. Sustainable water infrastructure is critical to providing the American public with clean and safe water. The EPA's Clean Water and Drinking Water Infrastructure Sustainability Policy encourages a range of practices that support sustainable water and wastewater systems. These practices include asset management, energy management, and Effective Utility Management. In many cases, OT security is a foundational element of a utility's overall resilience and sustainability. For more information on the EPA's Sustainable Water Infrastructure initiative, go to: https://www.epa.gov/sustainable-water-infrastructure.

Asset management

Asset management is maintaining a desired level of service for what you want your assets to provide at the lowest life cycle cost.[9] Traditionally, we think of assets as being pumps, motors, pipes, or other types of equipment with predictable probabilities of failure. The consequences of equipment failure and the cost to replace a failed asset are rather straightforward. OT cyber-assets are now a fundamental part of water and wastewater processes and should be considered critical assets essential to sustained

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-1300 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
E-mail: info@phoenixcon.com • Website: www.phoenixcontact.com

performance. Asset management includes protection of critical assets. As a result, cybersecurity is an important facet of asset management and essential to meeting commitments of a desired level of service to customers, regulators, and stakeholders.

Effective Utility Management

Effective Utility Management (EUM) is an initiative started in 2008. It is supported by a coalition of major water sector associations, including the EPA. EUM is the most widely recognized water sector utility management program in the U.S.[10]

This approach for utility management is based around the Ten Attributes of an Effectively Managed Utility and Five Keys to Management Success. Effective Utility Management: A Primer for Water and Wastewater Utilities outlines the initiative and is available at www.epa.gov.

The ten attributes of an effectively managed utility listed in the EUM Primer are:

1. Product Quality
2. Customer Satisfaction
3. Employee/Leadership
4. Operation Optimization
5. Financial Viability
6. Infrastructure Strategy/ Performance
7. Enterprise Resiliency Development
8. Community Resiliency
9. Water Resource Sustainability
10. Stakeholder Understanding/Support

A common theme throughout the ten attributes is resiliency and sustainability. Cybersecurity is directly relevant in several of the attributes such as Enterprise Resiliency and Infrastructure Strategy and Performance. However, cybersecurity and protection of OT cyber-assets play a role in many of the other attributes as well. Regardless of one's role, it is beneficial to understand how cyber-events can impact a utility's overall resilience and sustainability.

Summary

Cybersecurity is a critical facet of protecting critical infrastructure, and one that will become more challenging as the Internet of Things and the Industrial Internet of Things become an everyday reality. Now is the time to establish and implement a comprehensive, utility-wide security plan that focuses on resiliency and sustainability – not just protection.

List of acronyms

CSF	Cybersecurity Framework
DDoS	Distributed Denial of Service
EPA	Environmental Protection Agency
IIoT	Industrial Internet of Things
IoT	Internet of Things
IT	Information Technology
NIST	National Institute of Standards and Technology
OT	Operational Technology

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-1300 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
E-mail: info@phoenixcon.com • Website: www.phoenixcontact.com

References

[1, 5, 6] SonicWall. "2017 SonicWall Annual Threat Report." Web. https://www.sonicwall.com/whitepaper/2017-sonicwall-annual-threat-report8121810/

[2] Seth Fiergerman, "Yahoo Says 500 Million Accounts Stolen." CNN Tech. September 23, 2016. Web. http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/

[3] Vindu Goel, Nicole Perlroth, "Yahoo Says 1 Billion User Accounts Were Hacked." New York Times. December 14, 2016. Web. https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=1

[4] John Zorabedian, "Electric Utility Hit by Ransomware Shuts Down IT Systems for a Week." Naked Security. May 04, 2016. Web. https://nakedsecurity.sophos.com/2016/05/04/electric-utility-hit-by-ransomware-shuts-down-it-systems-for-a-week/

[7] Electricity Information Sharing and Analysis Center (E-ISAC). "Analysis of the Cyber Attack on the Ukrainian Power Grid, Defense Use Case." March 18, 2016. Web. http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[8] National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0." February 12, 2014. Web. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[9] Environmental Protection Agency. "Asset Management: A Best Practices Guide." April 2008. Web. https://nepis.epa.gov/Exe/ZyPDF.cgi/P1000LP0.PDF?Dockey=P1000LP0.pdf

[10] Environmental Protection Agency. "Effective Utility Management Primer." January 2017. Web. https://www.epa.gov/sites/production/files/2017-01/documents/eum_primer_final_508-january2017.pdf

About the author

Don Dickinson has more than 30 years of sales, marketing, and product application experience in industrial automation and control systems, involving a wide range of products and technologies in various industry segments. Don is the senior business development manager for Water Management, Phoenix Contact USA. He is a past chair of the NC American Water Works Association – Water Environmental Association (AWWA-WEA) Automation Committee. Don served on the AWWA Project Advisory Committee for development of Process Control System Security Guidance for the Water Sector. He is a member of the International Society of Automation (ISA) and the Water Environmental Federation (WEF) Automation and Information Technology Committee.

ABOUT PHOENIX CONTACT

Phoenix Contact develops and manufactures industrial electrical and electronic technology products that power, protect, connect, and automate systems and equipment for a wide range of industries. Phoenix Contact GmbH & Co. KG, Blomberg, Germany, operates 50 international subsidiaries, including Phoenix Contact USA in Middletown, Pennsylvania.

For more information about Phoenix Contact or its products, visit **www.phoenixcontact.com,** call technical service at **800-322-3225,** or email **info@phoenixcon.com.**

PHOENIX CONTACT • P.O. BOX 4100 • HARRISBURG, PA 17111-0100
Phone: 800-888-1300 • 717-944-1300 • Technical Service: 800-322-3225 • Fax: 717-944-1625
E-mail: info@phoenixcon.com • Website: www.phoenixcontact.com