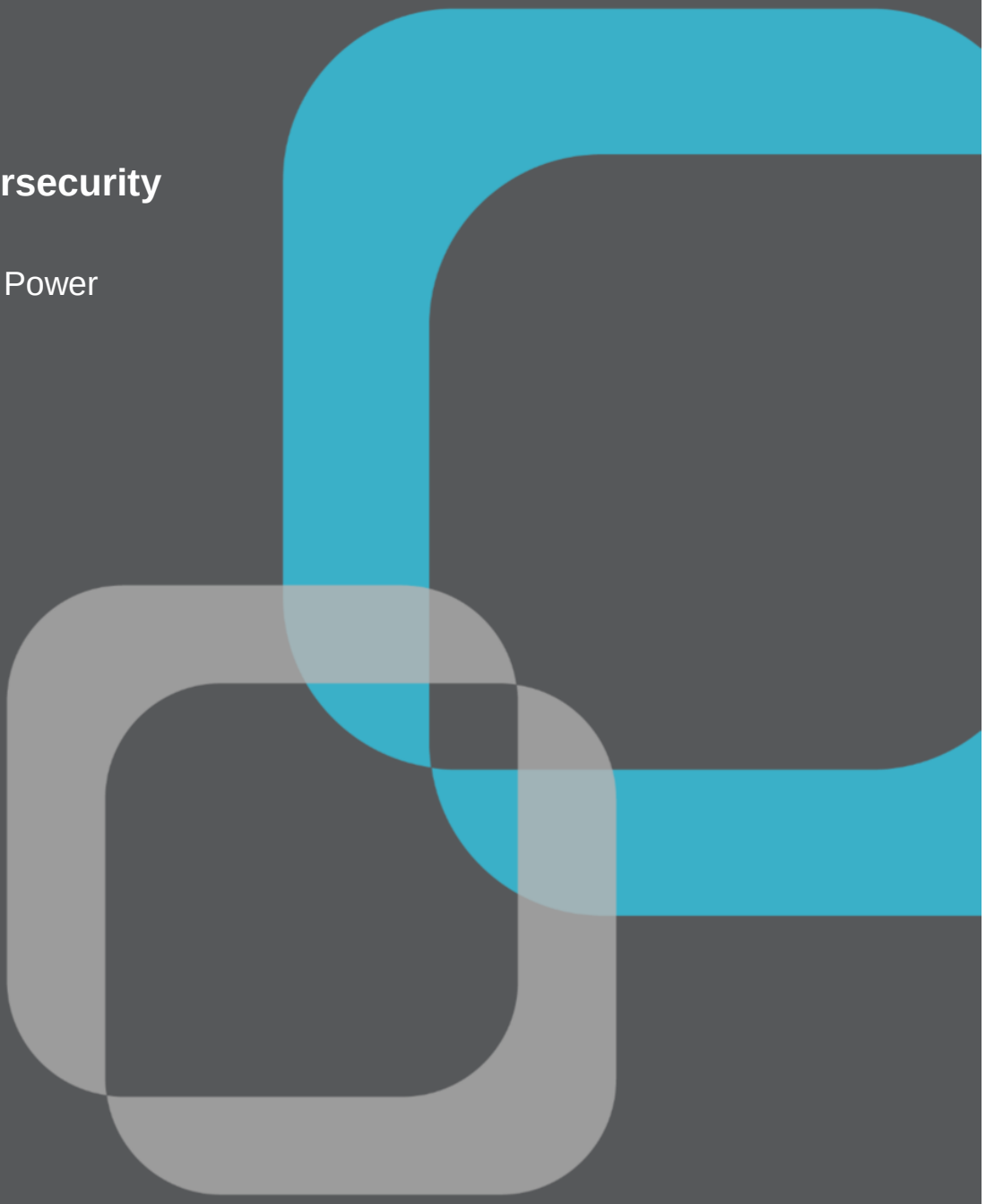
Enhancing Cybersecurity

A Briefing for Public Power

December 2016



Smart. Focused. Done Right.®

scottmadden
MANAGEMENT CONSULTANTS

INTRODUCTION

Thanks to an evolving landscape of technology, our world has never been more connected. The use of complex systems to manage our infrastructure and share tremendous amounts of data has improved operations and customer response times. However, despite the benefits of these technologies, it is becoming increasingly difficult to keep up with the real and growing danger of cyber attacks they bring. Vulnerabilities in your IT and OT systems can expose your operations and customers to significant risks. As a member of the power generation community, you have a special responsibility to secure your infrastructure by implementing controls to both prevent cyber attacks and mitigate their impact.

Concerns over cybersecurity stem from the potentially wide-ranging impacts caused by any disruption to customer service or the reliability of the grid. The resulting cost to a targeted company's reputation and bottom line from these types of cyber attacks can be significant. No executive wants to read the headlines that follow a successful breach, like Target's admission that hackers compromised 40 million customer records or the unplanned power outage in Ukraine that caused a six-hour outage for almost 225,000 customers[1]. More and more, companies have felt the impact of cyber attacks on the bottom line. This year, the cost of cybercrime for organizations in the utility and energy sectors has risen to $14.8 million, an 18% increase over 2015.[2] Perhaps most alarming for the industry, the energy sector accounted for 35% of cybersecurity incidents reported against critical infrastructure in the last three years, though none so far have caused power outages in the United States.[3]

> ***"The modern electric utility in the United States is a target for many who see an opportunity to destabilize the American economy or harm American citizens via malicious attacks on utility assets."***
>
> Puesh Kumar
> Director of Engineering and Operations
> American Public Power Association

As the potential for damaging, coordinated attacks against the energy industry continues to increase, enhancing your cybersecurity programs should be a top strategic priority for your business.

IMPACT OF CYBERSECURITY ON PUBLIC POWER

Public power represents a significant part of the energy industry, accounting for roughly one-third of electricity sales revenues while providing services to more than 80 million people[4]. Despite their large impact on the industry, public power has remained insulated from early attempts to provide cybersecurity

[1] ICS-CERT. (2016, February 25). Cyber-Attack against Ukrainian Critical Infrastructure. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
[2] Ponemon Institute LLC. (October 2016). 2016 Cost of Cyber Crime Study & the Risk of Business Innovation
[3] NCCIC/ICS-CERT. (FY 2012 - FY 2015). Year in Review. Department of Homeland Security
[4] American Public Power Association. (2015). 2015-2016 Annual Directory & Statistical Report. http://www.publicpower.org

regulation to the industry. Regulators are beginning to take notice of infrastructure vulnerabilities, and customers and members have a growing awareness of the serious risks associated with cyber attacks.

Back in 2009, the federal government enacted standards to help utilities defend themselves from cyber attacks. The recent updates to the NERC Critical Infrastructure Priorities standards (CIP V5) have expanded the coverage from generation facilities designated by their operators as critical assets to all assets included in the bulk electric system.[5] Energy distributors that operate under 100 kV and local distribution facilities, which includes most public power utilities, are exempt from CIP V5 compliance requirements.

After three years of struggling with their implementation efforts, the industry requested an extension to meet the CIP V5 standards. If large utilities and system operators are struggling with compliance, public power should take note. NERC and other regulators may develop future standards to encompass public power assets, and if history is any indication, it is never too early to start your compliance efforts.

In addition to taking note of expanded regulation, public power members are becoming more aware of cybersecurity risks. In a recent consumer cybersecurity survey, 73% and 69% of respondents identified making an online purchase and accessing online accounts, respectively, as activities that generate the most concern.[6] Smart metering devices, demand reduction, energy efficiency initiatives, and online billing all contribute to the digital interaction that your members expect from a utility, and they're concerned about security. Nearly 50% of respondents to the survey said they're taking more precautions compared to last year. While you could view cybersecurity as an internal IT and OT issue, cybersecurity is a concern for members and employees throughout your organization, and it deserves a comprehensive perspective.

IMPLEMENTING A STRATEGY FOR CYBERSECURITY

ScottMadden has decades of experience helping energy industry leaders navigate business challenges in uncertain regulatory environments. Recently, we have noticed that many energy utilities are struggling to keep pace with policy makers and shifting consumer sentiment with regards to cybersecurity. ScottMadden found that more than 50% of energy leaders classify the magnitude of cybersecurity threats as high or severe, but only a quarter (26%) agreed that their organization effectively managed cybersecurity risks.[7]

In response to concerns that not all cybersecurity investments are adequate or effective, ScottMadden has developed a methodology to help energy and technology leaders take a more programmatic approach to cybersecurity. We've aligned our process with industry standards, including NIST[8] and ES-C2M2[9], so you can take a proactive stance toward future regulation. Our methodology will guide you through a series of steps, starting with risk identification and ending with a clear road map that contains objectives, metrics, and change management capabilities.

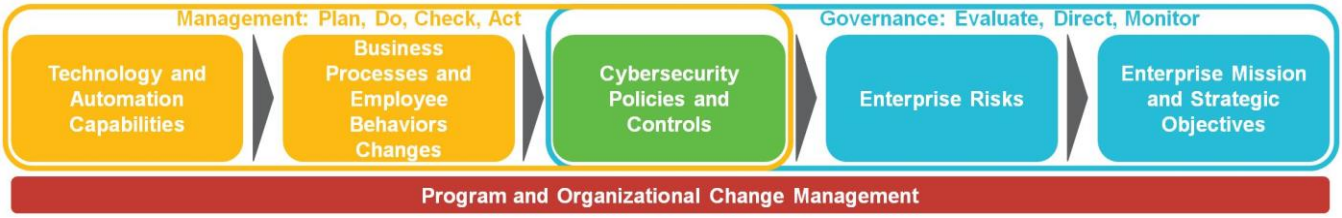
The first phase of the process focuses on evaluating your enterprise risks and requires that you characterize your most important information assets. Our strategic framework will ensure that managers

[5] NERC. (April 2014). Bulk Electric System Definition Reference Document. North American Electric Reliability Corporation
[6] Experian. (Jan 2016). Consumers find balance between cyberspace risks and benefits [Press Release]. http://www.prnewswire.com/news-releases/consumers-find-balance-between-cyberspace-risks-and-benefits-300210286.html
[7] Kerner, J. (July 2015). Energy Industry Cybersecurity Report. http://www.scottmadden.com/insight/energy-industry-cybersecurity-report/
[8] NIST. (February 2014). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. National Institutes of Standards and Technology. https://www.nist.gov/cyberframework
[9] DOE. (February 2014). Electricity Subsector Cybersecurity Capability Maturity Model, Version 1.1. Department of Energy. http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program

prioritize their assets based on business impact, not what is easiest to secure. Identifying which information assets support mission critical business processes, end-to-end, provides the context required to support a meaningful risk discussion.

Once you have identified critical assets, you should engage business stakeholders in an enterprise risk discussion–- this makes cyber threats real. Your business community may not have deep knowledge of cyber risks, but the discussion doesn't need to be overly technical or scientific. Educating business leaders will provide context for the cybersecurity program and create a starting point for a more detailed understanding of specific risks.

Identifying your critical assets and risk areas allows you to start managing cybersecurity as a business process. You can accomplish this by defining your targets and desired capabilities using industry-standard maturity models and then managing those targets as you would any other business process with the help of continuous improvement practices. ScottMadden has helped clients evaluate their cybersecurity maturity levels, prioritize gaps, and implement improvement programs through a framework depicted below.



Finally, you can build out your decision-making capabilities and show the value of cybersecurity by developing key metrics. Cybersecurity metrics can reduce uncertainty and build confidence in improvement efforts. We recommend a structured approach to selecting effective metrics, which will answer key questions about your organization's progress.

This programmatic approach will deliver strategic outcomes by coordinating individual efforts that address the entire system. Often, organizations attempt to build cybersecurity capabilities through a series of individual projects, but this can lead to siloed or disjointed efforts. Our programmatic approach allows you to step back and see the big picture while helping you achieve your target security posture.

CONCLUSION

Public power has an opportunity to manage the risk of cybersecurity concerns through the implementation of programs that address these threats head-on. If you, like other energy leaders, are concerned about upcoming regulations, the growing interconnectedness of your data, or the bottom-line impact of electronic vulnerabilities, please contact us. We can share with you how other utilities have been able to secure their assets and their reputations. ScottMadden has experience-based knowledge that can help you decide what you should do to protect your assets, employees, and members and how to do it.

ABOUT THE AUTHORS

Jon Kerner (jkerner@scottmadden.com) is a partner and leads the firm's technology practice area. Marc Miller (mdmiller@scottmadden.com) is a partner and leads the firm's public power and electric cooperatives practice. Henry Bell (henrybell@scottmadden.com) is a director, Ryan Smith (ryansmith@scottmadden.com) is a senior associate, and Ben Thayer (bthayer@scottmadden.com) is an associate with the firm.