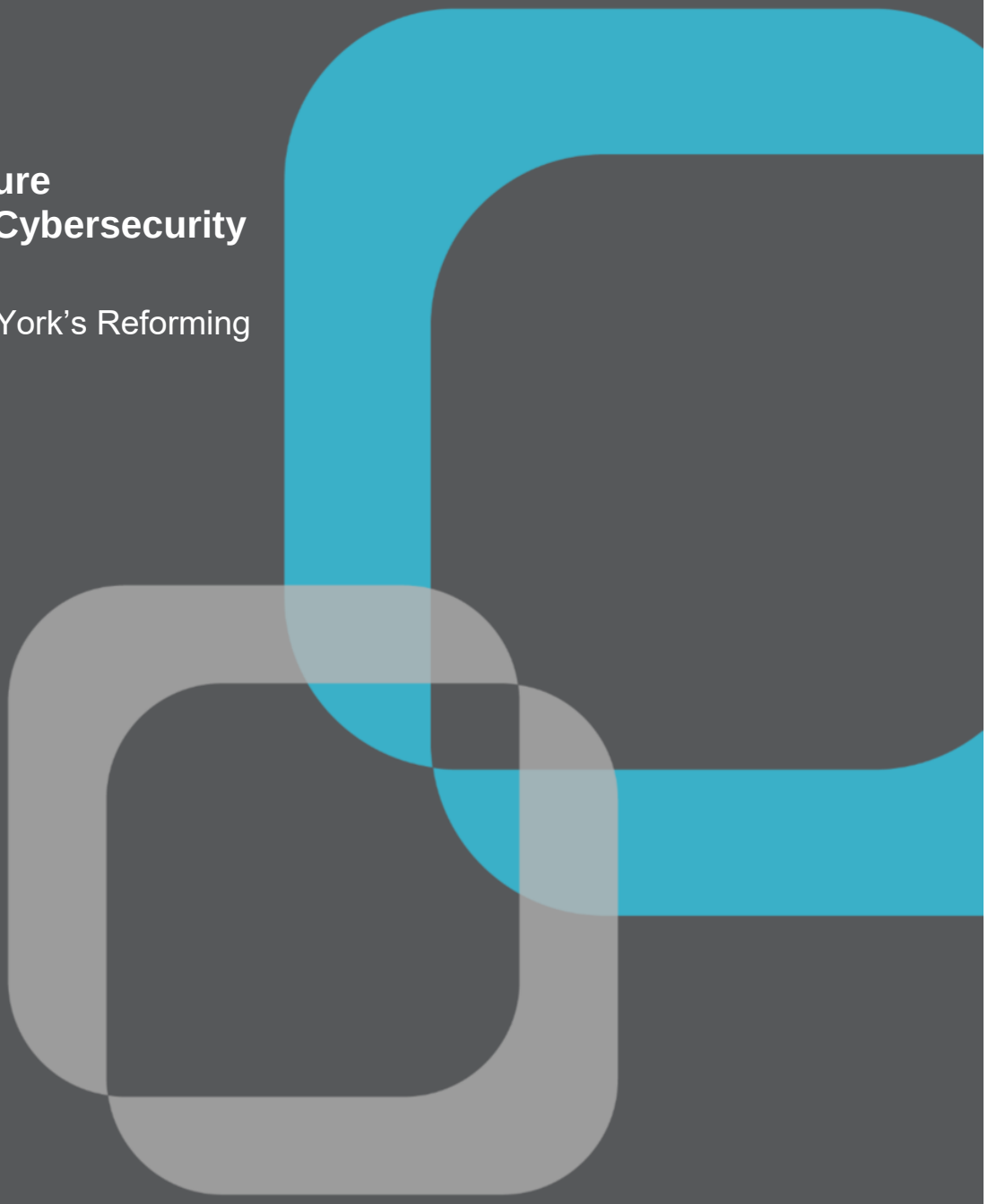
Utility of the Future
Implications on Cybersecurity

A Spotlight on New York's Reforming the Energy Vision

March 2016



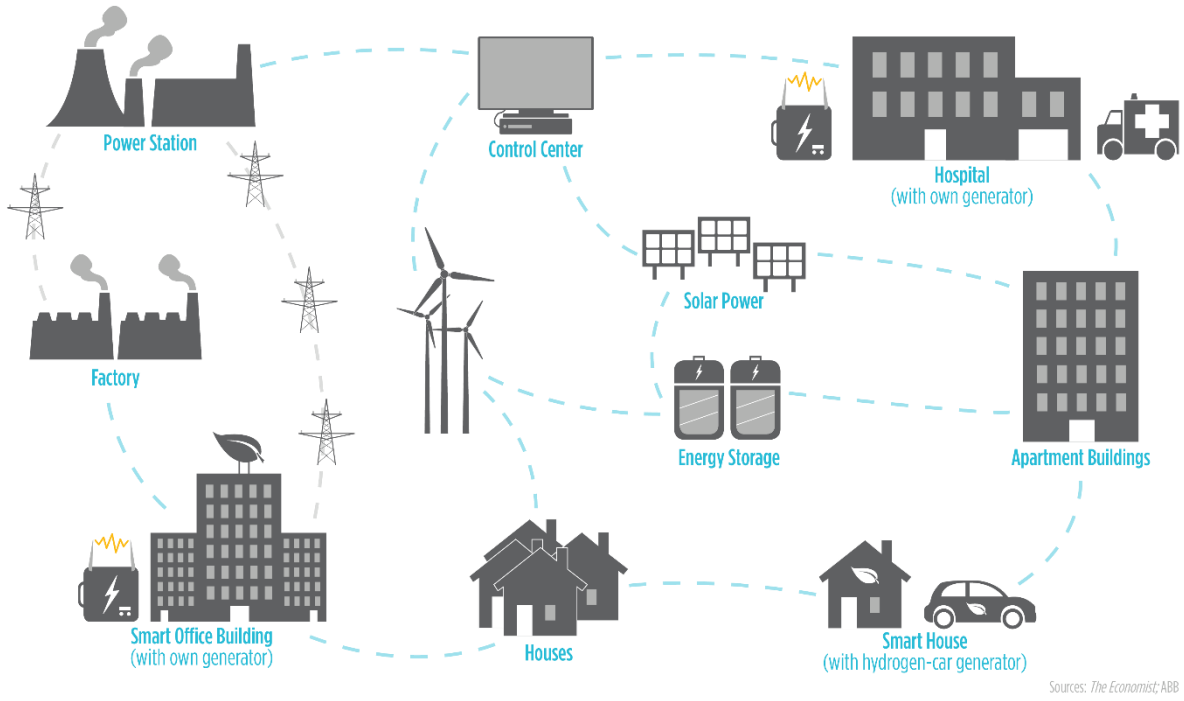
Smart. Focused. Done Right.®

scottmadden
MANAGEMENT CONSULTANTS

INTRODUCTION

The utility grid of the future is starting to emerge from a confluence of technology, economic, and regulatory developments that are leading to increased interconnectivity and data exchange amongst stakeholders. While these new technologies have the ability to revitalize aging energy infrastructure, executives and regulators are becoming increasingly concerned with the resulting cybersecurity implications. Many of the new cybersecurity risks facing smart grids are related to the interconnection of once-static assets via smart devices and an increasing number of two-way data flows between utilities, vendors, and customers. In today's world where sophisticated hackers are rapidly and continually enhancing their tools and techniques, large energy corporations responsible for securing billions of dollars in assets are having a hard time keeping up.

Figure 1: Utility of the Future Grid Interaction



This article will present the growing threat of cybersecurity issues for the energy industry, highlighting the effort in New York to support Reforming the Energy Vision (REV) proceedings as a representative case for states at the forefront of grid modernization. In general:

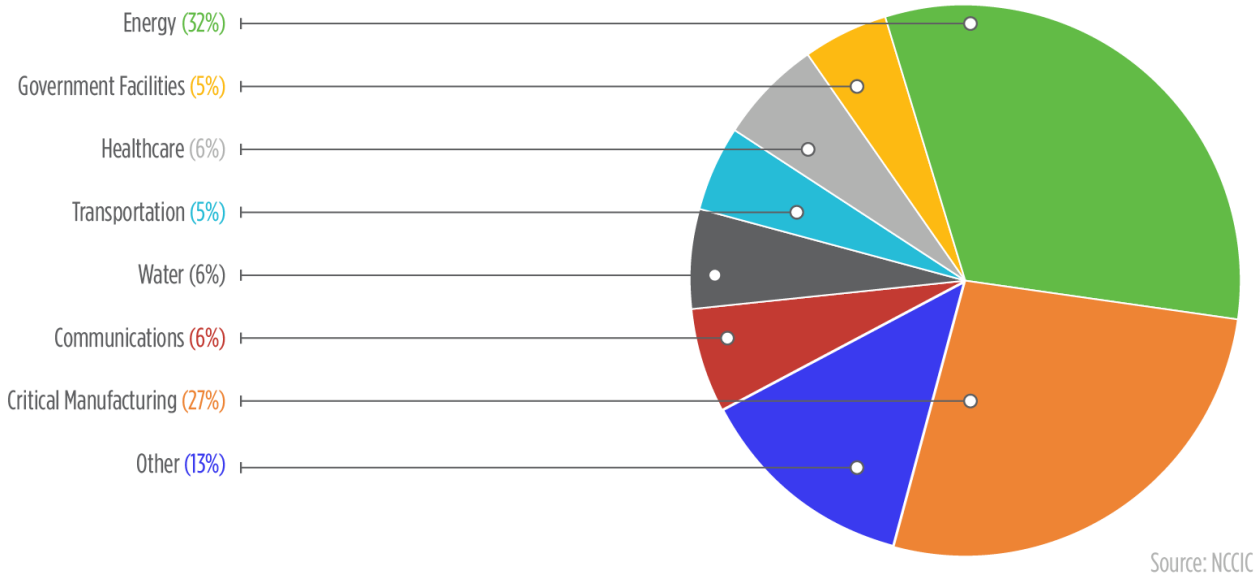
- There are significant changes to the grid taking place in certain parts of the country
- To realize the potential of these changes, there will need to be significant exchanging of confidential information—information that has traditionally remained within the control of the utility

- This represents a cybersecurity risk—particularly since the energy industry is a frequent cybersecurity target
- The federal government has provided industry regulation and guidance but has not provided a focus in some of the new risk areas being exposed by grid transformation
- Ultimately, states are left to fill this gap

THE GROWING CYBERSECURITY THREAT

According to the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the energy industry was the most commonly targeted industry in the United States for cyberattacks in the fiscal year 2014 with 32% of all attacks being directed against the energy sector. By some estimates, the vulnerability of the grid to cyberattack is in the billions of dollars.[1] SCADA devices, programmable logic controllers (PLCs), as well as other control systems, which are linked and transfer data across third-party networks, are often the targets of cyberattack against the energy industry.

Figure 2: Cybersecurity Incidents by Sector



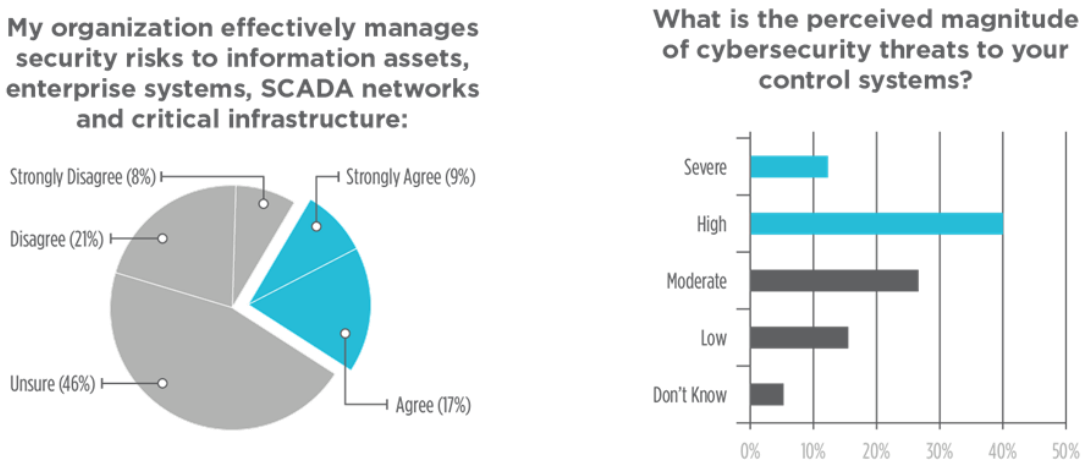
The hardware and software components that make up these systems are produced by a globally distributed supply chain that has no common incentive or guidance to compel suppliers to design components to an agreed-upon security standard, which falls outside of U.S. regulatory authority. Federal Energy Regulatory Commission (FERC) is proposing modifications to existing standards to improve upon the current FERC-approved, CIP Version 5; however, a more comprehensive update would also include changes to supply chain security standards for data flowing across unsecured third-party networks (click here for a link to ScottMadden's Wires Minute on this topic). In addition to the new supply chain standards, utilities and state regulators are independently pursuing standards to safely operate the grid and enable

[1] Lloyd's "Business Blackout" Report, May 2015

greater Distributed Energy Resources (DER) penetration, such as ISO 27002 for cybersecurity, OpenADR as a data formatting standard, and IEEE 1547 for the DER hardware itself.[2]

Energy executives have also taken note. In a recent study by ScottMadden, more than 70% of energy executives professed minimal confidence in their organization's ability to effectively manage security risks to information assets, enterprise systems, SCADA networks, and critical infrastructure. Moreover, more than 50% of these executives perceived the magnitude of cybersecurity threats to their control systems to be high to severe. The increasing volume and severity of cyberattacks combined with an inadequate ability to respond poses a significant challenge for the energy industry.

Figure 3: Select Results from the 2015 Energy Industry Cybersecurity Report



SPOTLIGHT ON NY REV

> "Issues relating to the sharing of customer data for the purpose of stimulating customer engagement and increasing DER deployment are currently the subject of Commission inquiry and include consideration of the mechanisms for the collection and dissemination of data and strengthening privacy, cyber security, and protection of customer rights."
>
> *-New York Public Service Commission*

In the absence of an overarching federal policy addressing cybersecurity for DER and other smart grid innovations, these issues have begun to be taken up at the state level. In states where DER penetration and smart grid technology employment are advancing more quickly as a result of progressive regulatory policy incentivizing innovation, the alignment of cybersecurity policy toward the future state needs to begin immediately. One such state making a swift and comprehensive push toward innovation is New York with its REV.

[2] Both the ConEd AMI business case and the SCE DRP (http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId=%7B075E822D-4286-4A63-9AD5-E3BC36B95D21%7D)

The New York Public Service Commission's (PSC) proposition to move toward market-based pricing at the distribution level, with a utility acting as Distribution System Platform Provider (DSPP), presents a unique set of cybersecurity challenges. Namely, the deluge of sensitive data that will be transferred between the DSPP, energy consumers, DERs, smart utilities, and third-party entities will be much more substantial than other current utility grids. In order to adequately protect the privacy of those involved in these data transactions, the DSPP and all relevant third-party entities will have to implement well-thought-out cybersecurity policies and solutions. Moreover, with this data being analyzed and acted upon in real time by the DSPP, the integrity of the data and the system in which it is transferred is of the utmost importance.

Figure 4: New York State Electric Utility Service Areas

The New York PSC will soon release final guidance for the utilities' Distributed System Implementation Plans (DSIP), which will guide utilities in conducting a focused self-assessment as they begin to design a DSIP. The draft of that guidance includes a specific reference to the concerns regarding striking a balance between enabling customer engagement and maintaining cybersecurity and privacy protections, cited below.

Considering the trend of progressive regulatory policy pushing smart grid innovation and DER integration in multiple states, it seems that concerns surrounding the implications for cybersecurity are valid and will need to be addressed in the near future. New York is far from being alone in considering how to ensure cybersecurity and personal privacy protections as more data is transmitted across the grid. In their distribution resources plans, the California investor-owned utilities define the need for updated risk assessments, cybersecurity and privacy standards, and system designs.[3] Texas has also passed rules mandating compliance with cybersecurity standards in order to maintain grid reliability.[4]

[3] SCE DRP

[4]http://www.puc.texas.gov/industry/projects/electric/40128/puct_project_40128_electric_grid_cybersecurity_in_texas.pdf

HOW SCOTTMADDEN CAN HELP

Cybersecurity developments are occurring quickly. As a result, many capital projects have been launched, introducing new monitoring, detection, protection, and security management capabilities. Gartner estimates cybersecurity spending will grow by 8.2% this year. Even as spending increases, energy leaders are becoming less confident in their ability to secure their critical assets from cyberattack. They struggle to engage business leaders in security direction-setting and decision-making. These professionals are charged with securing assets, yet they complain that security is not a priority for the rest of the business. Operations managers are more concerned about the productivity and reliability impacts of the security practices being introduced. Executives are worried about cybersecurity's return on investment.

ScottMadden understands that electric utilities' core missions remains the same—delivering safe, reliable power to their customers—but, industry innovation and customer expectations have created a new class of risks to this mission. ScottMadden helps our clients deal with these types of issues by changing how they manage and govern their cybersecurity efforts by providing a strategic, outcome-driven approach that addresses the following four areas: identify the biggest cybersecurity risks for an enterprise; determine the appropriate response to the cybersecurity risks; establish how to measure the success of a cybersecurity program; and determine how to get to the desired state.

ScottMadden has undertaken numerous consulting projects in the management and governance of cybersecurity for energy companies throughout North America. Leveraging institutional knowledge, our cybersecurity experts can help you achieve your cybersecurity goals.

ABOUT SCOTTMADDEN'S ENERGY PRACTICE

We know energy. Since 1983, we have been consulting to the energy industry. We have served more than 300 clients, including 20 of the top 20 energy utilities. We have performed more than 2,400 projects across every energy utility business unit and every function. We have helped our clients develop strategies, improve operations, reorganize companies, and implement initiatives. Our broad and deep energy utility expertise is not theoretical—it is experience based.

ABOUT THE AUTHORS

Henry Bell (henrybell@scottmadden.com) and Mike Morley (mfmorley@scottmadden.com) are managers in the Atlanta office. Josh Kmiec (joshuakmiec@scottmadden.com) and Chris Sturgill (chrissturgill@scottmadden.com) are senior associates in the Raleigh office. Chase Bebout (chasebebout@scottmadden.com) is a senior analyst in the Atlanta office.

FOR MORE INFORMATION

Please visit www.scottmadden.com to learn more about the services we offer. Visit www.gridcybersec.com and subscribe to our newsletters to receive daily cybersecurity research. Also, follow us on twitter @gridcybersec.

Sources

- Explosion in DERs + good graphics – http://www.utilitydive.com/news/grid-edge-live-2015-the-trends-behind-the-explosion-in-distributed-resourc/401417/
- Smart grid + AMI – https://www.smartgrid.gov/recovery_act/deployment_status/sdgp_ami_systems.html
- NYC REV – http://www3.dps.ny.gov/W/PSCWeb.nsf/All/CC4F2EFA3A23551585257DEA007DCFE2?OpenDocument
- Smart Grid – http://energy.gov/oe/services/technology-development/smart-grid
- AMI security RECs – http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/14-AMI_System_Security_Requirements_updated.pdf
- NY Energy Plan – http://energyplan.ny.gov/
- Robust three-part article on market-driven solutions – http://aceee.org/blog/2015/02/why-we-don%E2%80%99t-have-choose-between-ener
- Article on ESCOs, billing, consumer protections, etc. – https://www.cga.ct.gov/2015/rpt/pdf/2015-R-0109.pdf
- New York state senate cybersec hearings – http://www.nyiso.com/public/webdocs/media_room/press_releases/2015/NYISO_Addresses_New_York_State_Senate_Hearings.pdf
- DERs cybersecurity excerpts/paragraph, book – https://books.google.com/books?id=H6ISH6uTOCwC&pg=PT210&lpg=PT210&dq=DERs+cybersecurity&source=bl&ots=TvMHeE0doh&sig=alaOuyUNBe4y5qpJSP6TzyswjH4&hl=en&sa=X&ved=0CDUQ6AEwA2oVChMIl9PS5LrcxwIVWBmSCh1JyQ8o#v=onepage&q=DERs%20cybersecurity&f=false
- http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html
- http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf
- https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/energy-at-risk.pdf