

# **Managing Cybersecurity Threats to the Smart Grid**

Prepared for

The Maxwell School of Citizenship and Public Affairs

Syracuse University

PAI 752: Capstone Workshop

By

Megan O'Connor, Mark A. Nicholas,  
Satoshi Nakamura, and Tom Kaczmarek

June 13, 2014

## Acknowledgements

This project was sponsored by Rochester Gas & Electric, New York State Electric and Gas Corporation, and Central Maine Power Company, subsidiaries of Iberdrola USA. The authors would like to thank the Maxwell School, the Syracuse University College of Law, and the Syracuse University Institute for National Security and Counterterrorism for providing in-kind contributions including meeting space, telephones, and ongoing support and guidance for the project. We would also like to thank our faculty advisor, Keli Perrin, who provided us with guidance and advice along the way.

This report contains a literature review of smart grid technology, smart grid and cybersecurity issues, and an overview of influential documents from the government, research institutions, and nonprofits. It is supplemented with interviews from smart grid cybersecurity practitioners and experts. The appendices are comprised of training materials for electric utility lineworkers on their role regarding smart grid cybersecurity.

The authors accept responsibility for the accuracy of the information in this report. The content of this report does not necessarily represent the views of Iberdrola USA, RG&E, NYSEG, CMP, the Maxwell School of Citizenship and Public Affairs, or Syracuse University.

## About the Authors

This report was compiled by four Master of Public Administration students in the 2014 class of the Maxwell School of Citizenship and Public Affairs. The research was conducted as part of the required MPA Capstone Project, which grants MPA candidates the opportunity to utilize practical skills developed throughout the program on real world issues.

*Tom Kaczmarek*

*Satoshi Nakamura*

*Mark A. Nicholas*

*Megan O'Connor*

# Table of Contents

Purpose of Research	4
Methodology	4
Introduction	6
Overview of Smart Grid Technology	6
Cybersecurity Threats to Electric Utilities	10
Utility and Government Efforts to Prevent and Mitigate Threats	14
Conclusion	19
Appendix A: Awareness Campaign	23
Appendix B: Cybersecurity in a Smart Grid World: Lineworker Training	24
Appendix C: Lineworker Quick Reference Guide	44

## Purpose of Research

Iberdrola USA is responsible for training its fieldworkers on information security and privacy standards necessary for the protection of their critical assets and infrastructure. This team is responsible for developing an Information Security and Privacy Training module for Iberdrola fieldworkers, specifically lineworkers. The following literature review provides the fundamental components for understanding the basics of smart grid technology, cybersecurity, and other information necessary for outlining training scenarios and recommendations. The appendices include a guideline for developing a training session on an online learning platform, content, and visuals to be included in the training session, and a reference guidebook for lineworkers on cybersecurity.

## Methodology

Our analysis focuses on the cybersecurity threats against smart grid technology and the cybersecurity framework necessary to mitigate such threats. In conducting our analysis, we collected information from governmental guidelines, through interviews with experts, and from a review of cybersecurity and smart grid literature.

### Identification of Relevant Research and Guidelines

To develop a comprehensive understanding of cybersecurity threats on smart grid technology, we researched issues pertaining to the smart grid and cybersecurity both separately and collectively. We identified academic studies, journalistic contributions, think tanks, nonprofit advocacy groups, and other reputable sources.

Recognizing the importance of government and public sector organizations and their guidelines for overcoming the threats of cyber attacks, we identified key guidelines produced by the energy, security and defense industries. We utilized resources produced by the US Department of Energy (DOE), the US Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST) and North American Electric Reliability Corporation (NERC), the Federal Energy Regulatory Commission (FERC), and the International Organization of Standardization (ISO) and International Electrotechnical Commission (IEC).

### Selection of Interviewees

The introduction of smart grid technology poses unique cybersecurity threats in a new and evolving frontier and requires highly expertized knowledge of technology; thus, we interviewed smart grid cybersecurity practitioners and experts. Interviews included those with:

- ❖ *Jeri Teller-Kanzler (Director of Cybersecurity at Iberdrola USA Management Corp), who provided insight into where the most crucial cybersecurity challenges permeate on the smart grid, what the priorities for utility companies are, and how utility companies try to deal with this problem from a managerial perspective.*
- ❖ *Kevin J. Kumpf (Security Architect of Operations Technology at Iberdrola USA Management Corp), who offered his perspective on where technical difficulties in implementing cybersecurity on the smart grid exist and how utility companies try to deal with this problem from an IT and OT perspective.*
- ❖ *John Reynolds (Owner of Integrated Architectures and Chief Architect of the Security Fabric Alliance), who assisted in the development of federal guidelines on ICS cybersecurity, explained the key points that a utility company needs to address for preventing cyber attacks.*
- ❖ *Kevin Du (Professor in Department of Electrical Engineering and Computer Science of Syracuse University), who provided us with several examples regarding potential access points for hackers and other entities seeking to take advantage of the smart grid, helping us to formulate examples for other sections of the project.*
- ❖ *George Theoharis (Associate Dean for Urban Education Partnerships at School of Education of Syracuse University), who offered his guidance on adult education techniques to help us better formulate plans on how to best address target populations to smart grid cybersecurity training.*
- ❖ *Peter J. Wilcoxon (Associate Professor of Public Administration and International Affairs, and Economics, and Senior Research Associate at the Center for Policy Research and Administration of Syracuse University), who offered his time to help review materials and progress, providing insight and critical feedback for areas of concern.*
- ❖ *Steve Chapin (Associate Professor of Computer Science at Syracuse University), who offered his time to help review and provide critical feedback on the content and delivery of the training modules.*
- ❖ *Keli Perrin (Adjunct Professor and Assistant Director at the Institute for National Security and Counterterrorism at Syracuse University), whose constant guidance and advice, both practical and technical, gave us the ability to formulate this report and enhance our understanding of the complexities regarding privacy and cybersecurity concerns in the smart grid. She provided us with the critical support needed throughout the process that ultimately led to the formulation of this report and other materials associated with the project.*

## Introduction

The smart grid is the next step in the evolution of energy distribution, moving antiquated electricity infrastructure into the 21st century by combining power system and IT communication system domains.<sup>1</sup> The smart grid revolutionizes electricity delivery by integrating cutting-edge technologies that increase the reliability, efficiency, and security, of the United States' electrical system. Upgrading the electrical grid will reduce greenhouse gas emissions, increase integration of alternative energy and electric cars into the electric grid, and allow consumers to actively monitor and regulate their energy usage. But with these new benefits come new risks.

The smart grid introduces technological advances that have more interfaces, more information, more interactions, and therefore more vulnerable access points than ever before. This forces utility companies to consider security precautions more common in industries such as banking and defense. Private consumer and critical infrastructure information are transported throughout the smart grid and can be compromised by cyber attacks at multiple access points. This capstone report addresses:

- a) Smart grid technology
- b) Cybersecurity threats to electric utilities;
- c) Utility and government resources to prevent and mitigate threats

## Overview of Smart Grid Technology

The current electric grid was designed over a hundred years ago to serve a smaller population with a lower energy demand. Originally, the grid focused on providing power to small communities with local generation plants, which led to personalized power needs and delivery in each region.<sup>2</sup> In the past, the typical household used low energy appliances such as lighting, radios, and televisions, a distant model from the current structure of energy demand. Today, the typical household includes power-intensive technology that requires large amounts of electricity. Faced with an increased energy demand, energy companies have shifted to regional power infrastructure instead of community-based models. As there is no central planning system for transforming the grid, the evolution of the electric grid is not surprisingly hampered by poor infrastructure planning, structural inabilities in technologies implemented to grow with demand, and a general lack of investment in the grid infrastructure. As Otto J. Lynch, vice president of Wisconsin-based Power Line Systems explains,

---

<sup>1</sup> NISTIR 7628 Guidelines for Smart Grid Cybersecurity v1.0 – Aug 2010, Chapter 1 P. 4.

<sup>2</sup> U.S. Department of Energy, "What is the Smart Grid?" Smartgrid.gov, [https://www.smartgrid.gov/the\\_smart\\_grid](https://www.smartgrid.gov/the_smart_grid)

*“[O]ur grid [is] much like a water system, and basically all of our pipes are at full pressure now. If one of our pipes bursts and we have to shut off that line, that just increases the pressure on our remaining pipes until another one bursts, and next thing you know, we’re in a catastrophic run and we have to shut the whole water system down.”<sup>3</sup>*

This is exactly what happened in the massive Northeast blackout on August 14, 2003. An error in a computer system at FirstEnergy Corp in Ohio triggered the largest blackout in North American history, leaving 50 million people from Ohio to Ontario powerless.<sup>4</sup> Events like this one magnify the need for the next evolution in electricity production and transmission systems, the smart grid. This section will focus on two main components:

- a) Development of the smart grid
- b) Challenges to smart grid implementation

## Development of the Smart Grid

Envisioning the needs of a more energy-intensive consumer base, the concept of the smart grid was developed. The development of smart grid technology is driven by the desire to renovate energy infrastructure to be proactive in meeting energy demands. This section will address innovation in demand response, distributed generation, increased resilience, and efficient management.

In this technological era, many consumers want more control over their energy consumption and more information, at an almost instantaneous rate. This requires utilities to have more efficient demand response capabilities. Currently, one of the largest issues that stymies these demand response capabilities is the structure of the traditional electrical grid with its one-way communication and energy flow design. Without the ability to sense power usage in the grid, operators are often tasked with estimating power loads, requiring excess power generation, often from inefficient energy sources, to meet potential spikes in demand.<sup>5</sup> When these estimates fail, blackouts are triggered, leading to extremely costly infrastructure repairs.

To combat blackouts, the smart grid will incorporate diversified sources of energy production to build resilience and allow for easily scalable electricity supplies. In the traditional grid, solar and wind energy are difficult to integrate due to antiquated

---

<sup>3</sup> Ashley Halsey III, “Aging power grid on overload as U.S. demands more electricity,” Transportation, The Washington Post, [http://www.washingtonpost.com/local/trafficandcommuting/aging-power-grid-on-overload-as-us-demands-more-electricity/2012/08/01/gjQAB5LDQX\\_story.html](http://www.washingtonpost.com/local/trafficandcommuting/aging-power-grid-on-overload-as-us-demands-more-electricity/2012/08/01/gjQAB5LDQX_story.html)

<sup>4</sup> Scott DiSavino, “RPT—Ten Years After Northeast Blackout, Experts Say Similar Event Is Far Less Likely To Happen,” Reuters, <http://www.reuters.com/article/2013/08/12/blackout-anniversary-idUSL2N0GCO6R20130812>

<sup>5</sup> Robert Lamb, “Smart Grid Integration: Out with the Old,” *How the Smart Grid Will Work*, How Stuff Works, <http://science.howstuffworks.com/environmental/green-science/smart-grid1.htm>

transformers and difficulties with intermittency of these energy sources. By upgrading transformers on the grid to allow for two-way energy distribution, consumers who utilize solar or wind energy can potentially sell energy back to the grid, keeping track of their contributions to the grid through net metering. This distributed generation will help ease the burden of unexpected spikes in energy consumption. In addition, large scale energy storage options can be utilized, helping to provide immediate influxes of energy to combat times the grid is strained.

With nationwide implementation, the smart grid would eliminate the need for up to 2,000 dirty and inefficient power plants, saving consumers billions of dollars.<sup>6</sup> By combining this with self-monitoring capabilities built into many critical components of the smart grid, blackout frequency and severity can be reduced. One such self-monitoring device, the smart switch, can automatically trigger the localized shutdown of damaged components. Increased automation combined with constant feedback from monitoring stations can increase resilience, saving consumers and utilities \$150 billion dollars annually in costs associated with outages and damage to grid infrastructure.<sup>7</sup> With a 5% improvement in grid efficiency, the greenhouse gas emission equivalent of 53 million cars could be eliminated.<sup>8</sup>

At the consumer level, the smart grid is most visible in the presence of smart meters, a fundamental difference between the smart grid and traditional grid. By fitting every consumer with smart meters as opposed to the traditional analog or digital meters, consumers can get constant readings regarding their electricity consumption and utilities can get constantly updated information regarding such energy usage.<sup>9</sup> Managing smart appliances within the home would give energy companies the ability to communicate with consumers requesting the strategic shut off of appliances to ease electricity demand loads.

Another improved component of the smart grid that leads to increased grid reliability are phasor management units (PMU). These PMUs sample currents and voltages at transformers, taking measurements several times per second as opposed to previous technology that provided measurements every 2 or 4 seconds. These new dynamic measurements will lead to much less electricity loss during distribution (currently estimated

---

6 Environmental Defense Fund, "What consumers need to know about the smart grid and smart meters," *Energy*, [http://www.edf.org/sites/default/files/EDF-smart-grid-benefits-fact-sheet\\_0.pdf](http://www.edf.org/sites/default/files/EDF-smart-grid-benefits-fact-sheet_0.pdf)

7 U.S. Department of Energy, "The Smart Grid: An Introduction,"

[http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE\\_SG\\_Book\\_Single\\_Pages\(1\).pdf](http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf)

8 Wipro Council for Industry Research, "Achieving Sustainability through Smart Meter & Smart Grid," [http://www.wipro.com/Documents/Achieving\\_Sustainability\\_Through\\_Smart\\_Meter\\_Smart\\_Grid.pdf](http://www.wipro.com/Documents/Achieving_Sustainability_Through_Smart_Meter_Smart_Grid.pdf)

9 Baltimore Gas and Electric Company, "Smart Meters," Smart Energy, <http://www.bge.com/smartenergy/smartgrid/smartmeters/Pages/smart-meters.aspx>



to be 6% of all electricity produced<sup>10</sup>), ultimately reducing the amount of energy produced and lowering costs for both utilities and consumers.

The smart grid also outperforms the traditional electric grid in the ability to rapidly pinpoint and remedy causes of power outages. Industrial Control Systems (ICS), such as Supervisory Control and Data Acquisition (SCADA) systems, enable the utility to centrally monitor and control many of its processes. Through SCADA, operators can utilize advanced location information provided by outage management systems (OMS), and Geographic Information Systems (GIS) Asset Management Systems, to pinpoint malfunctioning infrastructure components. This information allows for immediate deployment to components causing the outage, instead of having lineworkers drive up and down electricity lines to find the outage.<sup>11</sup> These management systems will also allow for immediate automated rerouting of electricity to critical assets in the case of a blackout, such as hospitals, emergency services, and national defense systems, reducing their reliance on potentially faulty backup generators on site.

## Challenges to Smart Grid Implementation

While smart grid innovations and positive developments are numerous, there is still considerable opposition to widespread implementation of the technology. Lack of consensus among many stakeholders on how to introduce smart grid technologies to utilities and the public has created the lack of a unified message, leading to confusion and hesitancy by utilities to fully embrace smart grid technologies.<sup>12</sup> Another pervasive concern is the complexity of the smart grid, specifically the integration of new energy sources. Predicting wind and solar generation to forecast electricity loads depends on strong weather prediction capabilities. To combat the intermittency of such technologies, energy storage technologies must be deployed. Currently, these technologies are cost prohibitive to many companies.<sup>13</sup> Nonetheless, many electric utilities across the country are beginning to upgrade grid technology to reap the efficiency, resiliency, demand, and distribution benefits the smart grid provides.

---

10 U.S. Department of Energy, "Frequently Asked Questions," U.S. Energy Information Administration, <http://www.eia.gov/tools/faqs/faq.cfm?id=105&t=3>

11 U.S. Department of Energy, "What the Smart Grid Means to Americans," Consumer Advocates, <http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/ConsumerAdvocates.pdf>

12 Adam James, "Marketing The Smart Grid: The Complex Challenge of Selling Complexity," Climate, Climate Progress, <http://thinkprogress.org/climate/2012/10/09/975161/marketing-the-smart-grid-the-complex-challenge-of-selling-complexity/>

13 Antonello Monti and Ferdinando Ponci, "The Complexity of Smart Grids," *IEEE Smart Grid*, IEEE, <http://smartgrid.ieee.org/may-2012/579-the-complexity-of-smart-grids>

## Cybersecurity Threats to Electric Utilities

With the new benefits of the smart grid come additional security responsibilities to protect it – known as “cybersecurity.” Cybersecurity refers to the mechanisms, processes, devices and individuals used to prevent unauthorized access or use of technological systems for the purposes of alteration, theft, or destruction.<sup>14</sup> With the advent of advanced and integrated smart grid technologies, cybersecurity threats against utilities are not only more likely, their effects are more substantial. In the past, hackers were only able to get minimal information regarding power distribution from various components of the electrical grid. Now the scope of attacks and the potential impact of such attacks has been amplified exponentially under a smart grid system. Each new layer of technology gives hackers access to much more damaging information. To better understand cybersecurity concerns for electric utilities, this section will identify:

- a) Risks associated with cyber attacks
- b) Who conducts cyber attacks
- c) Where vulnerabilities exist

### Risks Associated with Cyber Attacks

The potential damage caused by the theft, manipulation or destruction of smart grid data can be extensive. The capacity to capture, exchange, and process more information to improve the efficiency and reliability of the grid simultaneously adds to three dimensions of risk: threats to utility operations, threats to national security, and threats to privacy.<sup>15</sup>

Utility operations can be adversely affected by cyber attacks. By losing operations information to theft, such as trade secrets that keep utility companies providing high quality services, utility companies can be incapacitated by a competitor through loss of competitive advantage. Cyber attacks resulting in the destruction of operations information can be costly to restore or redevelop essential data. Because more systems are automated and run by computers, cyber attacks can alter system protocols managing work crew schedules, meter readings and billing; reactivate power lines; and threaten the lives of lineworkers addressing them.

National security can also be threatened by cyber attacks on the smart grid, as critical functions of the United States depend on the proper operation of the power grid. Since electricity is an essential element for almost all activities in modern society, cyber attacks on the smart grid can not only affect homes, businesses and their occupants, they can threaten

---

<sup>14</sup> U.S. Department of Homeland Security, “Explore Terms: A Glossary of Common Cybersecurity Terminology, *National Initiative for Cybersecurity Careers and Studies*, <http://niccs.us-cert.gov/glossary>  
<sup>15</sup> NISTIR 7628 Guidelines for Smart Grid Cybersecurity v1.0 – Aug 2010, Chapter I PI

the operations of hospitals, prisons, traffic lights, air traffic control, and national defense systems.<sup>16</sup> For instance, the manipulation of operations data can be used to cause system-wide blackouts, or threaten the lives of thousands of people by opening floodgates at inopportune times. What's more, the manipulation of data by a cyber attacker can damage utility operations or informational technology systems. By altering the information processed on the grid, critical systems, like those at nuclear power facilities, can be pushed beyond their intended limits and put lives at risk. As the former Chairman of the Joint Chiefs of Staff General Martin Dempsey recently urged the United States Senate, addressing the cybersecurity of the nation's power grid is of utmost importance because "the uncomfortable reality of our world today is that [cyber attacks] can be as threatening as bullets and bombs."<sup>17</sup>

Cyber attacks against smart grid technology also pose significant threats to individual privacy. Sensitive personal information, such as social security information, credit card data, and even when a customer is home or away, can place both customers and employees at risk.<sup>18</sup> Attacks such as the recent Target breach or "Heart Bleed" bug confirm how privacy breaches affect far more than the individuals. While theft of private, personal customer and employee information from the smart grid can result in the loss of millions of dollars, such identity theft can result in massive government fines for the utility and loss of public trust in the utility, as well as more serious forms of identity theft for purposes of committing non-financial crimes.

### Who Conducts Cyber Attacks?

Cyber attacks on the smart grid can be conducted by several different types of attackers and for several reasons, making it all the more essential to have a complex cybersecurity framework in place:

- ❖ Insiders, such as employees or contractors, may use their access to sensitive information for personal financial gain. Additionally, disgruntled employees may conduct an attack to damage the organization's image.
- ❖ Customers with access to smart meters may similarly seek to steal information for personal gain.
- ❖ Criminal organizations may seek to commit credit card theft for financial gain, or use company information for purposes of blackmail.
- ❖ Other utility companies may similarly steal operations data to be more competitive or to identify vulnerabilities in competitors' operations, as other

---

<sup>16</sup> National Infrastructure Protection Plan: Partnering to enhance protection and resiliency, Department of Homeland Security, 2009, P.1

<sup>17</sup> Gen. Martin E. Dempsey, "Letter to Senator John D. Rockefeller IV," U.S. Department of Defense, <http://www.hsgac.senate.gov/imo/media/doc/CYBER%20letter%20Dempsey.pdf>

<sup>18</sup>Data Access and Privacy Issues Related to Smart Grid Technologies, Department of Energy, October 5, 2010, Pp. 2-3

organizations may seek to steal customer information for marketing purposes.

- ❖ Nations and terrorist organizations may conduct cyber attacks on the smart grid to inflict damage or incite fear in their enemies. Independent phishers, hackers and spammers may conduct attacks for any of the reasons previously listed.
- ❖ Independent hackers. Whether for personal malicious purposes or because they have been contracted by insiders, organizations, nations, or terrorist groups, the presence of independent hackers highlights the concern that cyber attackers can come from anywhere.<sup>19</sup>

## Cybersecurity Vulnerabilities

Advancements in smart grid technology make it possible for cyber threats to penetrate more access points on the grid. Vulnerabilities on older ICS were confined to physical access points on central consoles. But with the integration of data management systems on newer ICS, the number of access points, and the number of vulnerabilities, increases.<sup>20</sup> Cyber attacks can thus be conducted with physical access to any interface, including power generation systems, grid monitors, smart homes, transmission points, and even electric vehicles. Attackers can then gain access through physical modes such as USB drives, by cracking employee passwords, or remotely by phishing techniques through e-mail servers.<sup>21</sup> With the increased use of wireless communication, the potential for more remote cyber attacks against the smart grid highlight the need for protection against attacks at multiple layers. Since the smart grid is the combination of power systems and IT communication system domains, cybersecurity in the smart grid needs to address vulnerabilities in technologies as well as organizational processes and governance structures to mitigate threats.<sup>22</sup> The greatest potential cybersecurity vulnerabilities in the smart grid thus are at the following levels:<sup>23</sup>

- a) Policies and Procedures
- b) Platform
- c) Network Vulnerabilities

### *Policy and Procedural Vulnerabilities*

The first such organizational level smart grid SCADA systems may be vulnerable is at the policy and procedural level. Any level of “incomplete, inappropriate, or nonexistent security documentation” introduces vulnerabilities to SCADA.<sup>24</sup> This can manifest itself through

---

19 Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, P. 3-6

20 Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, P. 1

21 Risley, Allen and Roberts, Jeff. Electronic Security Risks Associated with Use of Wireless, Point-to-Point Communications in the Electric Power Industry, Schweitzer Engineering Laboratories, Inc., pp. 4-5

22 NISTIR 7628 Guidelines for Smart Grid Cybersecurity v1.0 – Aug 2010, Chapter 1 P. 4

23 Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, P. 3-5

24 Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, P. 3-7

inadequate cybersecurity policies and procedures specific to SCADA systems, enabling cyber attackers to identify weak points on the smart grid. Even with comprehensive policies and procedures specific to SCADA, the system is vulnerable without comprehensive and routine staff trainings. The smart grid is also vulnerable if security audits are not conducted or if procedures are not in place to maintain the integrity of SCADA systems while hardware, firmware or software modifications are made. Finally, a lack of mitigation or disaster recovery plans may not be vulnerabilities in and of themselves, but may lead to longer and more significant downtimes after an attack.<sup>25</sup>

### *Platform Vulnerabilities*

Vulnerabilities may also exist in SCADA hardware, operating systems, and applications. Misconfigurations are the source of many of these vulnerabilities. Due to the complexity of modern ICS and IT, the potential for flaws is high. When flaws are identified, it often takes time for software patches to be developed, leaving a system vulnerable. Since SCADA systems are essential to maintain operations, the lack of adequate testing of security updates or the time between security updates may render security systems less prepared for attacks.<sup>26</sup> SCADA systems with unique capabilities may be vulnerable when default configurations are used.

With more distributed access to the smart grid SCADA systems than traditional grid technology, several additional vulnerabilities exist at the user level. Unprotected data on cell phones and tough books can give cyber attackers direct access to sensitive information. Additionally, poor password policies or procedures render system information vulnerable. The smart grid is vulnerable if any device does not require a password, does not require a complex password, does not require the routine updating of passwords, or passwords are shared either intentionally, accidentally, or maliciously such as by “shoulder surfing.”<sup>27</sup>

Poor maintenance of hardware platforms may pose significant cybersecurity risks. Unauthorized personnel may pose a threat by having physical access to SCADA equipment, by having remote access to unprotected wireless systems, or if they have access to undocumented assets. A system is rendered vulnerable as well without hardware redundancies and backup power generation should components or systems fail.<sup>28</sup>

Software and malware vulnerabilities permeate the smart grid SCADA security systems as well. Software threats can come from simply failing to enable installed security and

---

25 Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, Pp. 3-7, 3-8

26 Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, P. 3-3

27 Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, P. 3-9

28 Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, P. 3-10

intrusion detection software or running unnecessary and easily exploitable software. The smart grid is also vulnerable if proper authentication is not established for access to certain software and if logs of software changes are not maintained. Inadequate software can also lead to denial-of-service attacks, rendering authorized personnel unable to perform their duties. Lacking up-to-date and tested malware protection can leave the smart grid open to undetected attacks. But some instances are far less commonsense, and in fact may be counterintuitive. For instance, common industry-wide SCADA protocols are highly insecure, leaving systems accessible to cyber attackers.<sup>29</sup>

### *Network Vulnerabilities*

Finally, vulnerabilities may exist at the network level of the smart grid SCADA. Network configuration and hardware vulnerabilities similar to those already listed may exist. But the network comes with a unique set of vulnerabilities as well. For instance, the network can be vulnerable to attacks if a security perimeter is not clearly defined, including adequate firewalls. Unprotected or unauthenticated data exchanged over wireless networks becomes open to attacks. Protected networks can then pose a risk if they are used for unprotected and unnecessary purposes, potentially introducing new threats or simply consuming too many system resources. Serious threats can also be posed through communications channels. And SCADA protocols may lack authentication processes or communications integrity checks, leaving cyber attackers free to manipulate emails and other communications undetected.

As this section makes evident, there are countless cybersecurity threats that require complex systems and processes to identify, prevent, and mitigate cyber attacks. In the next section, we explore the tools available to provide cybersecurity for the smart grid.

## **Utility and Government Efforts to Prevent and Mitigate Threats**

The need to overcome cybersecurity threats and vulnerabilities that have the ability to affect critical infrastructure, public safety, national security, the economy, and the everyday functioning of the country, is recognized by government and public sector organizations and regulated through the guidelines they distribute nationally. The following institutions are key players in influencing public and privately owned utilities to comply with cybersecurity policies and standards.

---

<sup>29</sup> Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, Pp. 3-10, 3-11

## National Institute of Standards and Technology (NIST)

NIST is an agency within the US Department of Commerce that works to promote innovation and competitiveness by providing up to date standards for industries including the electric industry. NIST is one of the key players in promoting the growth of the smart grid by providing a forum for stakeholders across the market to develop “interoperable standards” so that all components of the grid will be able to work together. The current level of interaction of the grid has prompted NIST to develop a research plan to address industry standards pertaining to cybersecurity threats. These standards pull from already implemented standards in industries like banking and defense networks, which face similar cybersecurity threats.<sup>30</sup>

The Smart Grid Interoperability Panel (SGIP), founded by NIST, supports the creation of these standards by gathering input from public and private stakeholders, identifying new areas for testing, and extensively working on smart grid outreach and educational programs. SGIP maintains the Catalog of Standards, which includes all of the standards and guidelines for the development of the smart grid.<sup>31</sup>

The following three NIST documents are crucial reference tools for a utility developing their smart grid technology, as well as maintaining their organization’s ability to combat cybersecurity threats.

- a) *Framework for Improving Critical Infrastructure (NIST February 2014)*:<sup>32</sup> This document is a result of the President’s Executive Order 13636 “Improving Critical Infrastructure Cybersecurity,” that set a standard for the United States to improve security measures for critical infrastructure and protect individual privacy and civil liberties of its citizens. The proposed framework is voluntary for industries and organizations to follow and addresses key components for assessing risk management processes. The lack of specificity and strict guidelines for implementation within the document allows it to be a platform for outlining best practices that may be used within any organization.

The three components of the Framework are (1) the Framework Core, (2) the Framework Implementation Tiers, and (3) the Framework Profile. The core presents a set of activities identified by the industry that are key in effectively managing cybersecurity risk. To assist the organizations that choose to use this document, the core breaks down the activities into functions (Identify, Detect, Respond, and Recover), categories (tied to activities that achieve the functions), subcategories (technical breakdown of activities), and informative

---

<sup>30</sup> U.S. Department of Commerce, “NIST and the Smart Grid,” *Smart Grid*, NIST, <http://www.nist.gov/smartgrid/nistandsmartgrid.cfm>

<sup>31</sup> U.S. Department of Commerce, “Smart Grid Interoperability Panel (SGIP),” *Smart Grid*, NIST, <http://www.nist.gov/smartgrid/sgipbuffer.cfm>

<sup>32</sup> U.S. Department of Commerce, “Framework for Improving Critical Infrastructure Cybersecurity,” *Cybersecurity Framework*, National Institute of Standards and Technology, <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>



references (links to best practice documents and standards). The implementation tiers are designed to allow an organization to assess itself and where its current risk management practices fall. Lastly, the profile helps to indicate what cybersecurity outcomes the organization already has and reveals gaps where threats against cybersecurity need to be addressed.<sup>31</sup>

- b) *Guidelines for Smart Grid Cybersecurity (September 2010)*: This advisory document, drafted by a SGIP working group, presents guidelines and tools found within the NISTIR 7628 document for organizations working to develop their smart grid cybersecurity. NISTIR 7628 is divided into three volumes: (1) Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements, (2) Privacy and the Smart Grid, and (3) Supportive Analyses and References. Volume 1 includes a risk management process that can be used to identify high-level security requirements within an organization and also outlines 22 key logical interfaces, detailing the technical and management issues associated with the smart grid networks. Volume 2 looks more closely at privacy issues within individual citizen's dwelling following the implementation of smart grid technology, and provides best practice recommendations for organizations associated with this component of the smart grid. Lastly, Volume 3 provides users with identified vulnerabilities, security analyses, and references.<sup>33</sup>

While this document is very inclusive, it is unwieldy and unorganized in its attempt to represent such crucial information. It does however, present electric utilities with seven tenets to follow, briefly summarized below:<sup>32 34</sup>

- i. Identity management: The utility assigns each device and each individual at the utility a unique and strong ID and/or digital certificate.
- ii. Mutual authentication: The utility provides a reasonable mechanism for each person to identify the entity/person they are communicating with.
- iii. Authorization: The utility assigns permissions for each person to access depending upon job function.
- iv. Audit: The utility will record, backlog, and encrypt what occurs on the grid, including work done by employees.
- v. Confidentiality: The utility will determine what level of confidentiality each type of information has and protect it with the appropriate privacy measures.
- vi. Integrity: The utility will ensure that no one has changed information, not even a single character, between collection and transmission.
- vii. Availability: The utility will ensure that communication pathways will not fail and will prevent denial of service attacks.

From the interview with John Reynolds regarding this document, it is acknowledged that in order to minimize the possibility and damage of cyber attacks, a utility company needs to abide by these tenets as much as possible when building organizational structure and utilizing IT communication technology. A utility company should formulate a cyber assets management policy which requires each division of the organization to take responsibility of protecting critical assets.

---

<sup>33</sup> The Smart Grid Interoperability Panel Cyber Security Working Group, "Introduction to NISTIR 7628," National Institute of Standards and Technology, [http://www.nist.gov/smartgrid/upload/nistir-7628\\_total.pdf](http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf)

<sup>34</sup> John Reynolds, "Security Fabric," The Smart Grid Security Innovation Alliance, [http://www.kerberos.org/events/2011conf-interop/2011slides/2011kerberos\\_john\\_reynolds.pdf](http://www.kerberos.org/events/2011conf-interop/2011slides/2011kerberos_john_reynolds.pdf)



- c) *Guide to Industrial Control Systems Security (NIST 800-82, May 2014)*: This document focuses security and risk management for industrial control systems (ICS), including sensory control and data acquisition (SCADA), which is a crucial component the smart grid. NIST focuses on ICS because these systems predominantly have a direct impact on physical infrastructure, human lives, and the environment. The interconnectedness and interoperability of smart grid technology presents serious threats to the cybersecurity of these systems, such as blocked information flow, inaccurate information flow, viruses, or tampering with system to directly impact some other component. This document assists organizations in risk management assessments and understanding their cybersecurity architecture.

## International Organization of Standardization (ISO) & International Electrotechnical Commission (IEC)

ISO's focus is primarily concerned with developing voluntary international industry standards. ISO collaborates with IEC when developing standards related to electrical utilities.<sup>35</sup> Collectively, the two organizations act as a medium for the advancement of international industries and innovation. As smart grid technology has developed worldwide, ISO/IEC has published standards on relevant issues including:

- ❖ *Information security management guidelines (ISO/IEC TR 27019)*: This document, written by an ISO/IEC joint technical committee that specializes on informational technology, outlines standards for energy utility companies in regards to information control in process control systems. These standards highlight the difference between traditional IT and process control systems, namely, differences in security features, system architecture, maintenance, and equipment resources. As the smart grid becomes more digitized, utility management needs to become more aware of best standards of practice to ensure private company and customer information is secure.<sup>36</sup>

## North American Electric Reliability Corporation (NERC)

NERC works to maintain the reliability of bulk power systems in North America. The organization develops and enforces standards, annually reviewing the reliability of more than 1,900 bulk power companies that serve approximately 334 million people. NERC's Smart Grid Task Force (SGTF) seeks to promote reliability of the smart grid by outlining risks and vulnerabilities, including cybersecurity that bulk power companies need to consider when implementing components of the grid.<sup>37 38</sup>

---

<sup>35</sup> International Organization for Standardization, "About ISO," *About us*, <http://www.iso.org/iso/home/about.htm>

<sup>36</sup> ISO/IEC 27019 Informational technology, Security Techniques, Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

<sup>37</sup> North American Electric Reliability Corporation, "About NERC," <http://www.nerc.com/AboutNERC/Pages/default.aspx>

<sup>38</sup> North American Electric Reliability Corporation, "Reliability Considerations from the Integration of Smart Grid," [http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/SGTF\\_Report\\_Final.pdf](http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/SGTF_Report_Final.pdf)

## Federal Energy Regulatory Commission (FERC)

FERC regulates interstate transmission, distribution, and wholesale sales of energy produced by United States utilities. The organization regulates and enforces standards regarding safety, privacy, reliability, and environmental issues. FERC often has regulatory overriding powers for standards created by NERC, especially those pertaining to national security, which may include cybersecurity attacks. During the modernization of the grid, FERC is working on establishing regulations that promote interoperability and reliable functioning of the interstate energy systems.<sup>39</sup>

These organizations, along with state public commission organizations, work to ensure all utilities are provided the information and standards to ensure the security and privacy of the consumers and of critical infrastructure. As the grid advances, these organizations will need to continue to collectively work on maintaining standards that address current and future cybersecurity threats. Their efforts show that it is crucial to establish a risk management process with organizational measures and up-to-date technological precautions.

## Utility Worker Training

According to the *Framework for Improving Critical Infrastructure*, one of the Framework Core's primary components is Awareness and Training. This component suggests that "the organization's personnel and partners are provided Cybersecurity awareness education and are adequately trained to perform their information security duties and responsibilities consistent with related policies, procedures, and agreements."<sup>40</sup> To provide comprehensive cybersecurity management as well as to comply with recommended industry guidelines, electric utilities are expected to ensure that all users are informed and trained about their roles and responsibilities in physical and information security matters.

The training within this capstone project (Appendix A) specifically targets lineworkers, a division of fieldworkers, who are responsible for the maintenance of the physical transmission and distribution systems. Lineworkers are equipped with devices that are linked back to the overall SCADA system and must take the necessary steps and precautions to ensure that these devices are not stolen, hacked into, or tampered with in a way that could allow hackers to permeate the utility's larger network. Developing a training module

---

<sup>39</sup> Federal Energy Regulatory Commission, "Smart Grid," *Industry Activities*, <http://www.ferc.gov/industries/electric/industry-act/smart-grid.asp>

<sup>40</sup> U.S. Department of Commerce, "Framework for Improving Critical Infrastructure Cybersecurity," *Cybersecurity Framework*, National Institute of Standards and Technology, <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>

for lineworkers provides them with pertinent knowledge to avoid, identify, and mitigate potential cyber threats.

## Conclusion

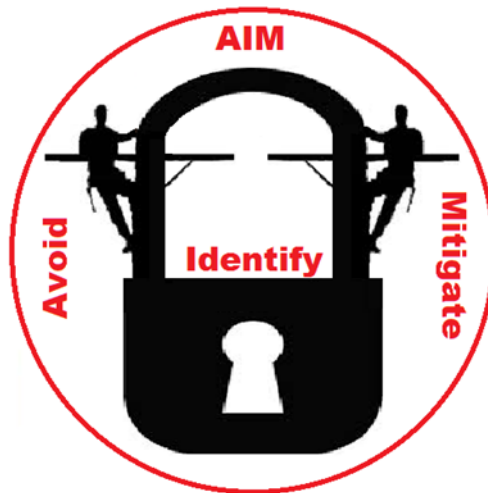
The smart grid will bring with it myriad benefits, yet cyber attacks will be more plentiful than ever. Using the precautions and resources outlined in our research paper, utilities will be in a strong position to combat these ongoing threats. However, even though a utility company makes its best efforts with these organizational and technological measures, it will be impossible to eliminate completely the possibility of destructive cyber attacks.

Due to the cat-and-mouse structure of cyber attacks and cybersecurity, utility companies need to continuously develop their organizational and technological measures while remaining vigilant in identifying new cybersecurity threats. Utility companies also need to estimate human actions and errors, putting an onus on the importance of continued training and monitoring. Regardless of the level of automation present, it will be critical to keep human interaction with the smart grid. The benefits of a fully integrated smart grid system will be readily evident, however, losing sight of the omnipresent cybersecurity threats the grid will face can ultimately not only undermine all the good inherent in the smart grid, it can potentially devastate critical infrastructure in ways never before perceived.

## Appendices

### Appendix A: Awareness Campaign

An awareness campaign focused around the most pertinent message from the lineworker training should be developed to keep lineworkers ever cognizant of their responsibilities to prevent and mitigate cybersecurity attacks on the smart grid. Our team identified several potential messages and solidified it under one simple and easy to remember acronym and concept: A.I.M. (Avoid, Identify, Mitigate).



The utility wants to first advise lineworkers to avoid a cyber attack by protecting their passwords, assets, and avoiding sources of infection. Second, the utility wants lineworkers to be able to identify potential warning signs of a cyber attack against their passwords and assets. And lastly, lineworkers should take the appropriate steps to mitigate the effects of an attack by following the utility's protocol.

This logo should trigger the lineworkers to remember this training module and should be placed in multiple locations around the office and in their trucks. Our team recommends purchasing stickers or magnets, as well as placing the logo on documents that are regarding the lineworkers' work in smart grid cybersecurity.

## Appendix B: Iberdrola Lineworker Cybersecurity Modules

### Training Guidebook

#### *Proposed Process*

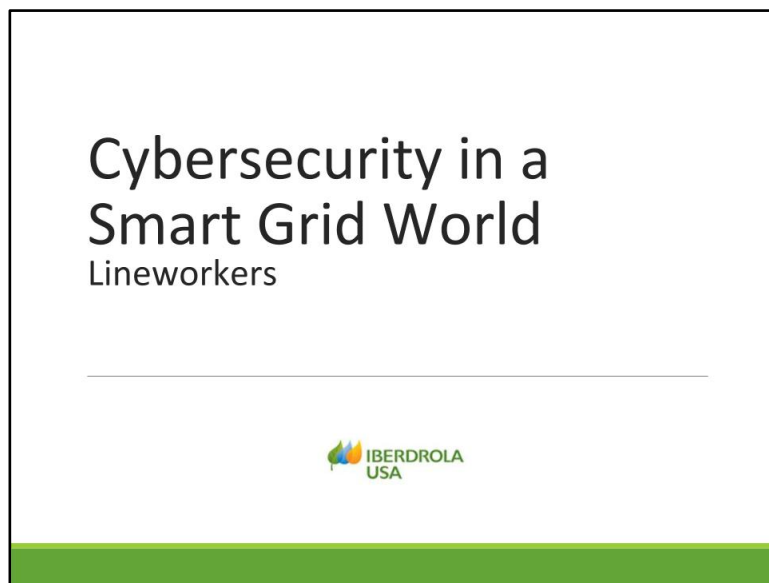
The training should be designed for an online learning platform that can host both video and informational slides for the lineworkers to work through. The total content should take the average lineworker no more than two hours to finish, but they will have the ability to stop and start at their convenience. The proposed platform to use is Moodle (<https://moodle.org/>). This platform can be accessed via the Toughbook and can present the information visually, audibly, and also include a fun, interactive game to “quiz” the lineworkers upon completion. We recommend you hire an instructional designer to set up the course.

- ❖ Information in this overview document is aligned with a powerpoint presentation
- ❖ Each slide should have an audio component to relay the information

#### *Pre-Module Recommendations*

- ❖ Distribute information about training sessions to lineworkers via email and/or fliers. In the email include:
  - By completing the modules and the game, they will receive a \$25 gift card.
  - Each lineworker will be provided with electronic copies of a quick reference guide and awareness campaign posters.
  - Instructional designer should be given adequate time to become familiar with all this information, especially if they are not familiar with the industry.

#### *Slide 1: Title Slide*




### ***Cybersecurity in a Smart Grid World: Lineworkers***

*Audio: Welcome to the training module for Iberdrola USA lineworkers on cybersecurity in a smart grid world. Each slide contains information or video based scenarios that will later be assessed in an interactive game. The training is not timed and you can stop and start at your convenience through completion.*

#### *Slide 2: Disclaimer about images*

**Disclaimer**

- The sole intent of this presentation is to serve as a framework for adaptation into an interactive, online platform and should not be viewed otherwise
- All images in this presentation need to be sourced or reproduced for training purposes




#### *Slide 3: Introduction*

**What is the reason for this training?**

- To comply with new industry standards created from a market shift to Smart Grid technology where there are increased privacy and cybersecurity risks.
- To educate you on the changing landscape of security in the electrical grid and how it relates to the work you do.

**What do I get for completing it?**

Not only will you be armed with a greater understanding of cybersecurity, but you also earn a **\$25 gift card** when you successfully complete the training and interactive quiz!



**Overview of why this training is occurring:**

- ❖ *Comply with new industry standards created from a market shift to Smart Grid technology where there are increased privacy and cybersecurity risks.*
- ❖ *To educate you on the changing landscape of security in the electrical grid and how it relates to the work you do.*
- ❖ *\$25 gift card as an incentive to complete the training*

Slide 4: Outline of module

**What's in store?**

1. Cybersecurity and the smart grid
2. Threats against access points
3. The company's responsibility
4. Your responsibility: AIM to be a cybersecurity pro
5. Testing your knowledge: Scenarios and Quiz

Slide 5: Cybersecurity: What is it, and what is it good for?

- ❖ *Protects against unauthorized access or use of technological systems for alteration, theft, or destruction.*
- ❖ *Cybersecurity threats matter for national security, privacy, and protection of our critical infrastructure*
- ❖ *Technology has the potential to improve the productivity, efficiency and responsiveness of the power grid – essential for keeping our schools and businesses open, our hospitals functional, and our military operational.*
- ❖ *But with added capabilities comes greater security threats to this critical infrastructure as well...*



**Cybersecurity: what is it, and what is it good for?**

- Protects against unauthorized access or use of technological systems for alteration, theft, or destruction
- Cybersecurity threats matter for national security, privacy, and protection of our critical infrastructure
- Technology has the potential to improve the productivity, efficiency and responsiveness of the power grid – essential for keeping our schools and businesses open, our hospitals functional, and our military operational.
- But with added capabilities comes greater security threats to this critical infrastructure as well...

*Slide 6: Traditional Grid vs. The Smart Grid*

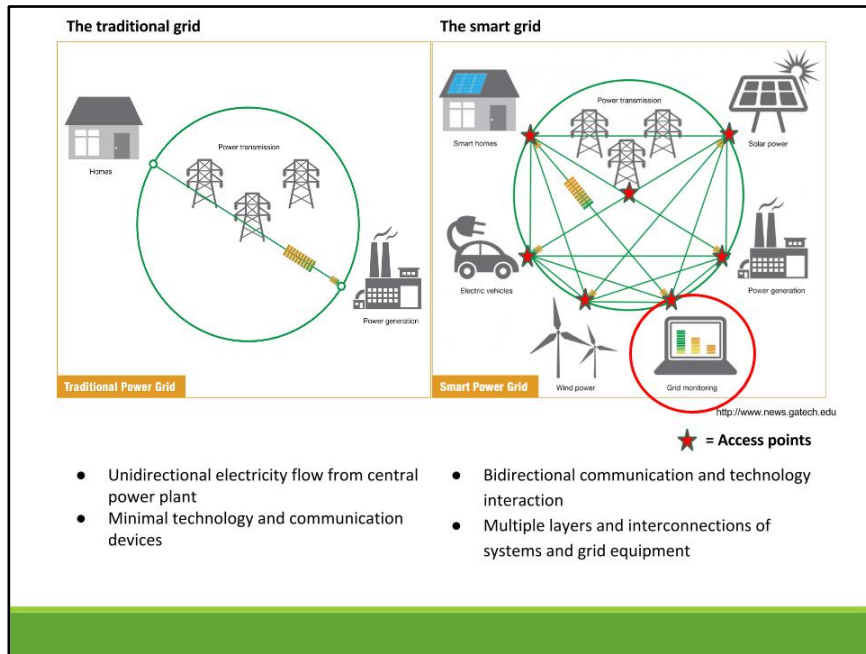
*Audio: Technology, specifically smart grid technology, has changed how utilities communicate and distribute electricity. On the left, you can see the traditional grid. With unidirectional electricity flow from a central power plant and minimal technological or communication devices, the traditional grid is what we are all used to working with. However, on the right, is an example of a smart grid. The smart grid introduces the concept of bidirectional communication and technological interaction with multiple layers and interconnections of systems and grid equipment.*

*<click forward and stars will appear>*

*The interconnectivity of smart grid technology allows for more accurate monitoring and reduced electricity consumption on behalf of the consumer but also introduces significantly more access points for cyber attacks. Therefore, advancing cybersecurity protocols have been a key focus of utilities and regulatory agencies throughout the world. The access points, interconnected through internet technologies provides hackers with entry points to potentially compromise large components of the smart grid.*

*<click forward and circle appears>*

*In this training module, you will focus on the grid monitoring access points.*



Slide 7: Grid Monitoring Access Points

**Grid Monitoring Access Points**

These new hardware technologies increase the potential vulnerabilities at each point. Within each hardware component, several software interfaces are present that give hackers even more potential access points, software such as:

- GIS asset management systems
- Customer information systems (CIS)
- Outage management systems (OMS)
- Workplace management systems (WMS)

This software can be accessed on any of your devices (phone, Toughbook) that is connected wirelessly to the larger network. **Physically protecting these critical assets is extremely important!**






Slide 8: The consequences have changed

**The consequences have changed**

	Old grid	New smart grid
<b>Lose a piece of your equipment</b>	Cost to replace equipment (\$800)	Cost to pay for privacy breach (\$10m)
<b>People get access to your password</b>	Access to personal and work files	Access to grid infrastructure
<b>Install bad software on a device</b>	Annoying pop ups due to a virus	Annoying critical system failures due to a virus

Slide 9: How can an access point be compromised?

**How can an access point be compromised?**

- Hackers and viruses can gain access through you and your equipment:
  - USB thumb drive
  - CD installation
  - SIM/microSIM card
  - Wireless connection
  - Corrupted bar code
- Direct access to technology and interfaces
  - Weak passwords 
  - Stolen or lost equipment 
  - Accidental actions by employees 
  - Intentional actions by employees 
  - Viruses spreading from your home computer to work systems 


Slide 10: Who conducts cybersecurity attacks and why?

<b>Hacker profiles</b>	
<b><u>Who conducts cybersecurity attacks?</u></b>	<b><u>Why do they attack?</u></b>
Insiders (employees, contractors)	Fear factor
Customers	To damage a company's image
Independent hackers, phishers, and spammers	To identify vulnerabilities in a security system
Organizations	For personal/organizational gain (theft, fame, personal attacks)
Criminal groups	National/regional attack
Nations	
Terrorists	


Slide 11: What can happen if an access point is compromised?

**What can happen if an access point is compromised?**


**Matters to national security**

- Alter or destroy critical power infrastructure (necessary for hospitals, air traffic control, national defense systems, etc.) 
- Manipulate data (open floodgates, overheat nuclear plant, etc.)

**Matters to privacy**

- Customer information 
- Your information as an employee

**Matters for utility operations**

- Manipulation of daily operations (False signals, change in work orders, etc.)
- Loss of competitive advantage (stolen operations information) 
- Destruction of data (Costly restoration)
- Personal safety risk (reactivated line while working on it)

Slide 12: Example of Cybersecurity Threats

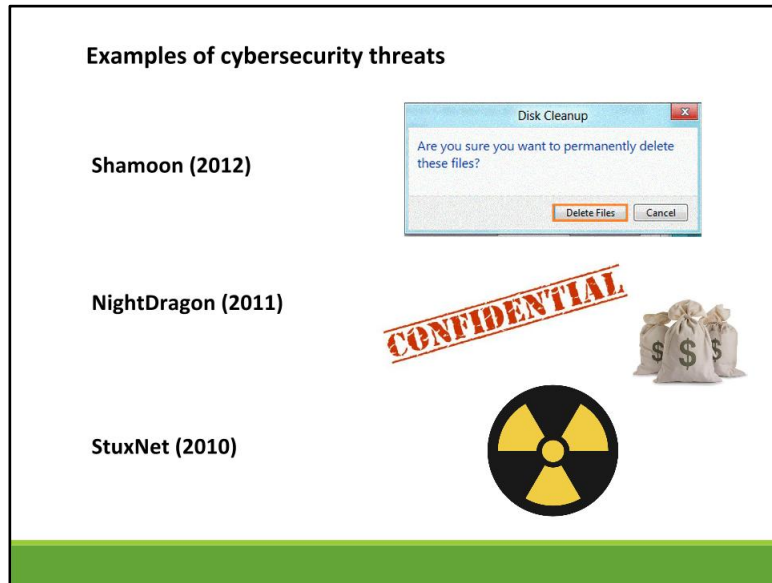
*Audio:*

*Three major attacks show how hackers finding vulnerabilities in programs can lead to devastating results.*

- ❖ *Shamoon - This attack was done to an energy company by a coder with very rudimentary hacking skills. The hacker was able to enter a system and get access to internal controls, infecting 30,000 company computers. The hacker received information on all the hard*

drives from these 30,000 computers and then wiped all drives clean, forcing the company to completely disconnect its IT system to deal with the threat, causing massive damage.

- ❖ *NightDragon* - The *NightDragon* attack was done by foreign entities to western energy companies by accessing mobile laptop computers through email phishing. They were able to steal gigabytes worth of sensitive material, such as financial transaction, and information on field operators, causes upwards of \$40 billion in damage to the companies.
- ❖ *StuxNet* - This attack was on nuclear power facilities and installed on computers through a USB connection. The virus displayed incorrect information regarding the statuses of each nuclear centrifuge. Ultimately the virus was able to do each damage to the centrifuges that approximately 1,000 were completely destroyed and needed to be replaced.



Slide 13: What impact does the smart grid have on your job?

*It benefits the utility as well as the customers, and impacts your job as a lineworker. It is beneficial for lineworkers to understand the impacts - especially for protecting critical infrastructures.*

- ❖ *The utility requires each division of the organization to take responsibility in order to protect critical assets under the cyber asset management policy.*
- ❖ *It is the responsibility of lineworkers to manage and control the cyber assets they own, including cell phones, toughbooks, papers, and any other asset potentially containing valuable, sensitive or critical information.*

**What impacts do access point vulnerabilities have on my job?**

It is beneficial for you to understand the impacts - especially for protecting critical infrastructure.

- The utility requires each division of the organization to take responsibility in order to protect critical assets under the cyber asset management policy.
- It is your responsibility to manage and control the cyber assets you own, including cell phones, Toughbooks, papers, and any other asset potentially containing valuable, sensitive or critical information.



[www.oregon.gov](http://www.oregon.gov)



[www.wsau.com](http://www.wsau.com)

Slide 14: Cybersecurity buster slide



[imageShots.com](http://imageShots.com)

**Cybersecurity Busters:**

You are a critical part of the team!

Slide 15: Your company's responsibility


*Audio: The increase in cybersecurity measures is at all levels of the utility, including management. Management is committed to ensuring these seven guidelines are followed to provide the best cybersecurity precautions for you.*

- ❖ Identity management
- ❖ Mutual authentication
- ❖ Authorization
- ❖ Audit
- ❖ Confidentiality

- ❖ Integrity
- ❖ Availability

**The Team's Responsibility**

1. Identity management
2. Mutual authentication
3. Authorization
4. Audit
5. Confidentiality
6. Integrity
7. Availability

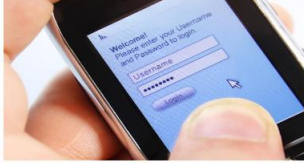


Slide 16: What does this mean for you?


- ❖ **Identity management:** You and your devices are all assigned a unique and strong ID
- ❖ **Mutual authentication:** Mechanism for each person to identify the entity/person they are communicating with

**What does this mean for you?**

1. **Identity management:** You and your devices are all assigned a unique and strong ID



2. **Mutual authentication:** Mechanism for each person to identify the entity or person they are communicating with



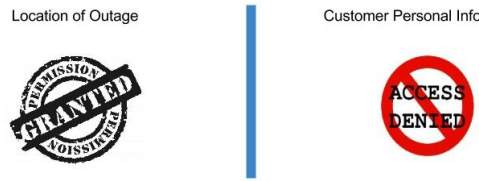
Slide 17: What does this mean for you?

- ❖ **Authorization:** Permissions assigned to each person to access the information you need for your job.
- ❖ **Audit:** Record, backlog, and encrypt what occurs on the grid, including work done by employees


**What does this mean for you?**

**3. Authorization:** Permissions assigned to each person to access only the information you need

Location of Outage      Customer Personal Information



**4. Audit:** Record, backlog, and encrypt what occurs on the grid, including work done by employees



Slide 18: What does this mean for you?


- ❖ **Confidentiality:** Determination of how sensitive information is and protecting it appropriately
- ❖ **Integrity:** Ensure no one has changed information between collection and transmission

**What does this mean for you?**

**5. Confidentiality:** Determination of how sensitive information is and protecting it appropriately


Are the potential threats high? Then expect stronger security

Potential Impact	Vulnerability			
	Very High	High	Moderate	Low
Devastating	Red	Red	Red	Red
Severe	Red	Yellow	Yellow	Yellow
Noticeable	Yellow	Green	Green	Green
Minor	Yellow	Green	Green	Green



**6. Integrity:** Ensure no one has changed information between collection and transmission

Data Collection      Data Transmission



Slide 19: What does this mean for you?


- ❖ **Availability:** Ensures timely and reliable access to and use of information



**What does this mean for you?**

**7. Availability:** Ensures timely and reliable access to and use of information

Do you need access to secure information for your job? If you're authorized, your utility company will make it available to you.



unlocked


Slide 20: Things to worry about

*Audio: As a lineworker, you have three main things to worry about. The first is losing your device, whether that is your company cell or your Toughbook. The second is if someone steals your username and password, or any information that could allow them to sign into the network as you. The third is if someone installs corrupt software or viruses on your devices.*

*This could occur if you download something, if you physically lose your phone, or could occur remotely without your knowledge at all of it occurring.*

**You have three primary things to worry about...**

1. Theft of your username or password
2. Losing your devices
3. Someone installing corrupt software on your devices



www.dilbert.com


Slide 21: Cybersecurity responsibilities for lineworkers:

Audio: If the utility is providing you with all of the support just mentioned, then you are equipped with what you need to be the first line of defense in the field. It is important for you to:


- a) Avoid
- b) Identify
- c) Mitigate

**Responsibilities for Lineworkers:**  
**AIM to be a Cybersecurity Pro!**


**Step 1. Avoid**



**Step 2. Identify**



**Step 3. Mitigate**



www.illustrations.com 127

Slide 22: Avoid

**1 Avoid: Steps you can take to avoid a cyber attack**

**A. Protect your username and password**

- Do comply with company standards on length, strength, expiration dates
- Don't share your username or password with anyone
  - Be aware of "shoulder surfers"
  - Be aware of phishing attacks through downloaded apps, emails, and embedded links
  - Be aware of individuals posing as help agents
  - Iberdrola will NEVER ask you for your username or password

**B. Protect your assets**

- Do keep all assets secure and limit access to trucks and field crew tools
- Do be vigilant in checking all field infrastructure
- Don't share devices with anyone - coworkers and family included

**C. Avoid Infection**

- Do maintain all software in the most up-to-date version as possible
- Don't exchange emails between personal and work devices
- Don't open suspicious emails

Slide 23: Identify

**2 Identify: Potential Warning Signs of a Cyber Attack**

A. Password warning signs

- Your coworker was looking over your shoulder after you log into your laptop
- Your password no longer works

B. Asset warning signs

- Your device is not how you remember leaving it
  - Device is out of place
  - Device is powered on or logged in
  - Device is missing


C. Infection warning signs

- You are redirected to a suspicious page after clicking on a link
- You receive confusing orders from WMS, OMS or GIS system

Slide 24: Mitigate (information needed)

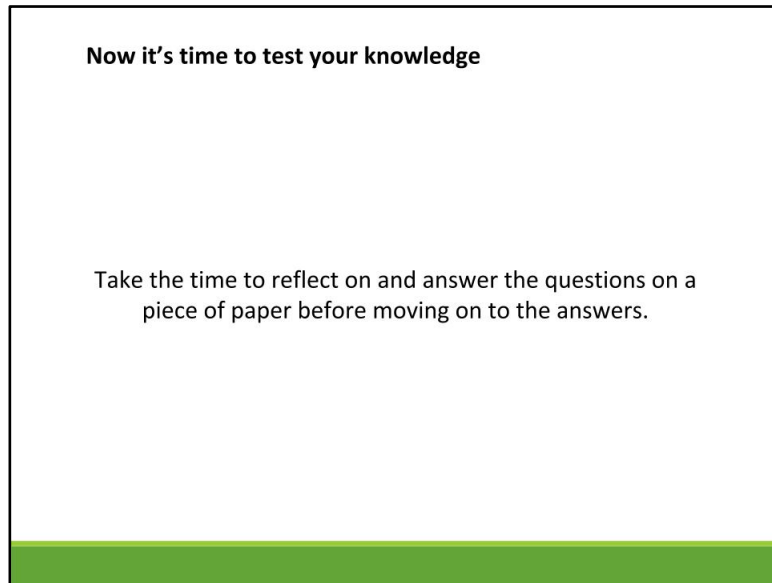
**3 Mitigate: Limit the damage of a potential cyber attack**

- Follow Iberdrola protocol



Slide 25: Scenario time

***\*\*Ideally these scenarios will be produced in short video clips for the lineworker to watch.\*\****



*Slide 26: Scenario 1: Phishing email at home*

*Play audio or video.*

*Imagine you are sitting at home on your personal computer, you get an email from Iberdrola. You open it and see it is directly addressed to you, discussing errors that were present within the work logs for the last month because there were discrepancies in hours worked. It requests that log into the Iberdrola portal to confirm your work hours.*


*You get this email, what are your immediate reactions? Do you reply? Why or why not?*

*Answer: This is called a phishing email. If you think this couldn't happen to you, think again. 38% of cyber attacks are done through phishing emails. If you gave that information out, people could access your work system, where they could access not only your personal information including banking information, social security number, home address, and phone number, but because of advancements in Smart Grid technology, they can attack critical infrastructure logged in as you.*

**Scenario 1**

Imagine you are sitting at home on your personal computer, you get an email from Iberdrola. You open it and see it is directly addressed to you, discussing errors that were present within the work logs for the last month because there were discrepancies in hours worked. It requests that you log into your worker account through this provided link to double check the discrepancies.


- You get this email, what are your immediate reactions?
- Do you open the link?
- Why or why not?



To: Dan Johnson  
 From: Iberdrola IT Department ([IT@iberdrolausa.com](mailto:IT@iberdrolausa.com))  
 Subject: URGENT - Hours reported issue

Dan,  
 This is your IT department. There are errors in the work logs from last month relating to the hours you worked. Please log into the Iberdrola portal to confirm your work hours reported.

<http://www.iberdrolausa.com/employees/login>

Thanks,  
 Information Technology Staff 

Slide 27 & 28 Scenario 2: Phone

*Audio OR video could be made to depict each of the three iterations and answers.*

*Your crew is addressing an outage in a remote, rural area on a hot summer day. You are preparing to go into the bucket and check out the transformer. Your phone is in your pocket. A young woman is walking down the road past the truck. She asks you if she can borrow your phone because her car broke down and she's several miles away from the closest store.*

- a) You decide not to engage with the person. You continue working without surveying the scene. What could happen?  
*Answer: The person discreetly reaches into the truck and tampers with/steals technology.*
- b) You decide to engage with the person by giving her the use of your phone (this includes personal and company phones). What could happen?  
*Answer: Stolen phone, virus, hacked for data/access*
- c) You decide to engage with the person by calling for help for the person. What could happen?  
*Answer: Risk of unidentified number that can connect third party hackers to the information. The person could stand close enough to the lineworker to "shoulder surf" the password information.*


*What are the appropriate steps for the lineworker to take?*

- a) Acknowledge that the person is there.
- b) Survey surroundings to ensure nothing is out of place/unusual.
- c) Ie. Other non-utility individuals walking around.
- d) Secure all critical equipment, including van.

- e) Ensure all crew members are aware that a person is there.
- f) Follow company protocols based on engaging an emergency response in the field.


*Key information: Keep your phone secure at all times and do not let outside parties use it for calls, texts, or internet for any reason. When engaging, be aware of surroundings at all times.*

**Scenario 2**



Your crew is addressing an outage in a remote, rural area on a hot summer day. You are preparing to go into the bucket and check out the transformer. Your phone is in your pocket. A young woman is walking down the road past the truck. She asks you if she can borrow your phone because her car broke down and she's several miles away from the closest store.

**Scenario 2**



**Iteration 1:** You decide not to engage with the person. You continue working without surveying the scene. What could happen?

**Iteration 2:** You decide to engage with the person by giving her the use of your phone (this includes personal and company phones). What could happen?

**Iteration 3:** You decide to engage with the person by calling for help for the person. What could happen?

*Slide 29 & 30 Scenario 3*

*The following simulation will incorporate all three aspects of your role as a lineworker in addressing cybersecurity threats and to please keep them in mind as you proceed through this exercise.*

*You and your crew stop at a local diner to take your usual one hour lunch break.*

*Three iterations of the scenario. Prompt the lineworkers with an iteration.*

- *Before you head into the diner for lunch, what steps should you take to avoid a cybersecurity incident?*

*Possible responses:*

- ❖ *Lock all phones, laptops and other technology*
- ❖ *(Is there protocol for alerting HQ when away from technology?)*
- ❖ *Secure all technology on your person or in a secure location on the vehicle*
- ❖ *Lock vehicle*
- ❖ *Maintain line of site with vehicle while at lunch*

- *When you return to your vehicle after lunch, what are some basic red flags that indicate you should be concerned about the security of the vehicle while you were away?*

*Possible responses:*

- ❖ *Door is unlocked*
- ❖ *Contents have shifted*
- ❖ *Laptop or other technology is open, turned on, logged on, generally tampered with, etc.*

- *Now imagine that when you return from lunch you notice that the passenger side door is unlocked and the laptop you left in your vehicle is slightly open. What immediate steps should you take?*

*Possible responses:*

- ❖ *Follow Iberdrola incidence response plan, likely including:*
- ❖ *Contact supervisor through secure channel such as your radio or personal phone to alert them*
- ❖ *NOTE: Facilitator should encourage trainees to consider security risks associated with using system-integrated communication devices to accomplish this task*
- ❖ *Once any device integrated with a work network is potentially compromised, any other device on the network could be compromised as well*
- ❖ *Survey rest of scene and take inventory of all devices*



### Scenario 3

Scene: You and your crew stop at a local diner to take your usual lunch break.

- A. Before you head into the diner for lunch, what steps should you take to avoid a cybersecurity incident?
- B. When you return to your vehicle after lunch, what are some basic red flags that indicate you should be concerned about the security of the vehicle while you were away?
- C. Now imagine that when you return from lunch you notice that the passenger side door is unlocked and the laptop you left in your vehicle is slightly open. What immediate steps should you take?



Slide 30: Avoid, identify, mitigate

#### 1 AVOID

- Lock all phones, laptops and other technology
- (Is there protocol for alerting HQ when away from technology?)
- Secure all technology on your person or in a secure location on the vehicle
- Lock vehicle
- Maintain line of site with vehicle while at lunch

#### 2 IDENTIFY

- Door is unlocked
- Contents have shifted
- Laptop or other technology is open, turned on, logged on, generally tampered with, etc.

#### 3 MITIGATE

- Follow Iberdrola incidence response plan, likely including:
- Contact supervisor through secure channel such as your radio or personal phone to alert them
- Survey rest of scene and take inventory of all devices



Slide 31: Quiz

<http://www.wolfscience.com/byojeopardy/play.php?id=52325>

**That's a Wrap!**

Now you should know:

- Why cybersecurity matters to the electric grid
- How **you** play an integral role

If you have any additional questions, please contact your supervisor for more resources.

**Now take the quiz and win a \$25 gift card!**

