EFFECTIVE APPROACHES TO CYBERSECURITY FOR UTILITIES

TERRY M. JARRETT

HEALY & HEALY ATTORNEYS AT LAW, LLC

OCTOBER 24, 2013

AGENDA

- Why Cybersecurity?
- A Few Helpful Cybersecurity Concepts
- Developing Expertise: Cybersecurity Resources

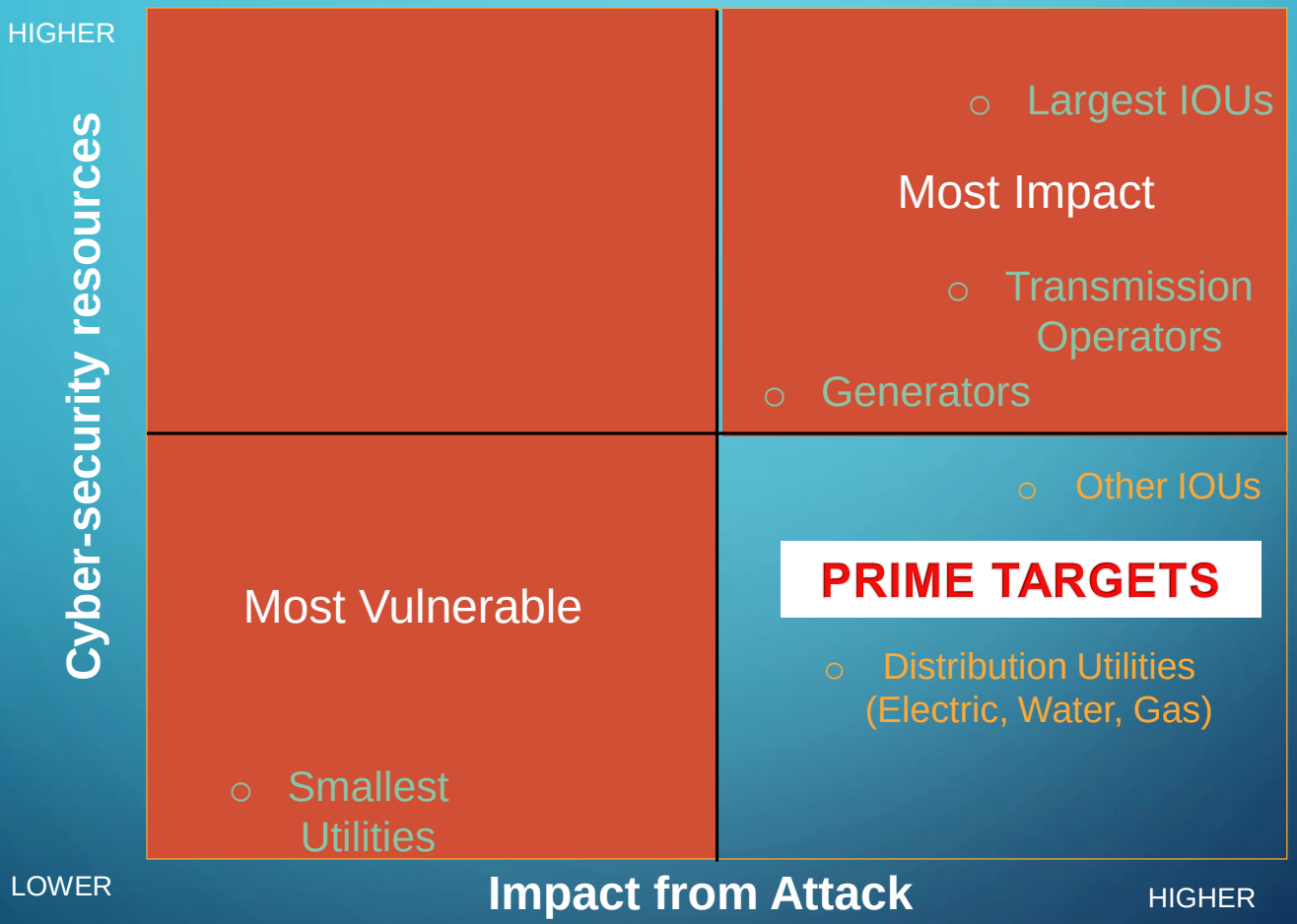
WHY CYBERSECURITY?

JUST LOOK AT RECENT HEADLINES IN THE NEWS . . .

- "State-Sponsored Cyber Attacks – This is Only the Beginning: Survey," securityweek.com, September 4, 2013
- "Syria's cyberattack: First wave of a bigger war?," cnn.com, August 30, 2013
- "Exclusive: Cyberattack Leaves Natural Gas Pipelines Vulnerable to Sabotage," csmonitor.com, February 27, 2013
- "Chinese Hackers Seen as Increasingly Professional, Experts Say," FoxNews.com, February 25, 2013
- "Hackers Take Aim at Key U.S. Infrastructure," money.cnn.com, February 20, 2013
- "US Says Iranian Hackers Behind Electronic Assaults on US Banks, Foreign Energy Firms," Wall St. Journal, October 12, 2012

ANOTHER KEY REASON CYBERSECURITY MATTERS

- According to NERC's monthly Key Compliance Trends publication, there are about 100 CIP violations per month
- Fines for compliance violations can be up to $1 million/day, and in the past four years, actual fines assessed have totaled more than $150 million


HIGHER
Cyber-security resources
LOWER
Largest IOUs
Most Impact
Transmission Operators
Generators
Other IOUs
PRIME TARGETS
Distribution Utilities (Electric, Water, Gas)
Most Vulnerable
Smallest Utilities
Impact from Attack
HIGHER

CYBER THREATS

- The power grid is transitioning from a previously isolated environment to a complex interconnected one
- Smart grid may be vulnerable to cyber attacks because it has extensive information systems and communications systems components
- As new smart grid technologies are deployed, new vulnerabilities and risks increase

THREAT SOURCES

- Hackers
  - Alone or in a group (like Anonymous). They are doing it primarily for fun, to cause embarrassment, or to make a political statement.
- Disgruntled Employees
- Organized Criminal Elements
  - Industrial Spies
  - These are malicious actors interested in stealing information for financial gain
- Nation-states
  - Malicious actors interested in taking down the grid as part of a larger attack or cyber warfare
  - This is increasing

WHAT IS THE GOAL OF CYBERSECURITY?

- Goal is not to have a response to a cyber threat that is piecemeal, reactive, or fragmented
- Aim is to encourage proactive and strategic action on the part of utilities, rather than a patchwork response

A Few Helpful Cybersecurity Concepts

CONCEPTS THAT SHOULD INFORM AN ASSESSMENT OF A UTILITY'S CYBERSECURITY PERFORMANCE

- Prioritizing systems and networks over components
- Ensuring that human factors are considered
- Deploying defense-in-depth
- Promoting system resilience

SECURING SYSTEMS AND NETWORKS VS. DEVICES ON THE NETWORK

- Cybersecurity may call for securing entire networks, in addition to devices on that network.
- For example, the meters within a smart grid system can be fortified against attack, but in order to ensure that the entire network of the smart grid system is secure, the components linking those meters, as well as every other component in between, must be secured as well.

SECURING SYSTEMS AND NETWORKS VS. DEVICES ON THE NETWORK

- Another example: An employee brings a thumb drive infected with malware to work and plugs it into his or her computer. You want a security system that can isolate and quarantine the malware before it infects the entire system.

PERSONNEL SURETY: SECURING PEOPLE AS WELL AS SYSTEMS

- A system is only as secure as the people who run and operate it.
- Training is essential to ensure that in the event of a cyber attack, personnel are skilled in identifying and responding to the impacts.
- Personnel can also be “insiders” involved in a deliberate or accidental cybersecurity breach. Identifying key personnel and using background checks is a potential strategy to mitigate this, but once they have been hired, policies that limit an individual’s ability to inflict harm may also be important.

DEFENSE-IN-DEPTH

- Achieving defense-in-depth requires placing multiple, diverse barriers in front of a potential attacker
- An overall cybersecurity policy that calls for multiple measures and employs cybersecurity strategies such as identifying authentication and authorization, admission control, encryption, integrity checking, detections of policy violations, data logging and data auditing
- Effective cybersecurity often encompasses physical as well as technological measures – restricted access to server rooms, locks on smart meters, security fencing and cameras at key substations, for example

RESILIENCE AND RECOVERY

- Resilience ensures that the unexpected will not persist indefinitely
- A resilient system will not only be prepared for deterring, defending against and mitigating attacks, but also for ensuring quick and efficient restoration in the event that an attack compromises the system, through disaster recovery planning

REGULATORY OVERSIGHT

- Regulatory role is increasing
- More cyber attacks to business processes and NERC CIP Standards compliance are driving new cybersecurity expenditures by utilities
- Deployment of smart grid adds new cost and reliability elements

Developing Expertise: Cybersecurity Resources

FOUR KEY AREAS THAT MOTIVATE AND INFORM UTILITY INVESTMENTS IN CYBERSECURITY

- Good business practices by the utilities
- Laws
- Enforceable standards
- Voluntary best-practice guidance

GOOD BUSINESS PRACTICES

- It's good business for utilities to avoid power outages
  - Customer complaints
  - Regulatory, political and public scrutiny
- So, its good business to prevent cyber attacks on their systems

LAWS

- State laws require that utilities must provide safe and adequate (reliable) service
  - In Missouri, statute is § 393.130.1, RSMo
- Federal Law
  - FERC regulates the interstate transmission of electricity, natural gas, and oil. FERC also reviews proposals to build liquefied natural gas (LNG) terminals and interstate natural gas pipelines as well as licensing hydropower projects.

ENFORCEABLE STANDARDS

- North American Electric Reliability Corporation Critical Infrastructure Protection Reliability Standards (*NERC CIP)* http://www.nerc.com/page.php?cid=6|69
- These standards already drive a good deal of cybersecurity investments and, as greater coverage is applied to protection of the electric grid, this process will only become more important.
- NERC's CIP efforts include standards development, compliance enforcement, and supporting and providing technical subject matter expertise to the program.

VOLUNTARY BEST PRACTICE GUIDANCE

- National Institute of Standards and Technology (*NIST) Smart Grid Interoperability Panel and Cyber Security Working Group* http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG
- NIST Interagency Report (NISTIR) 7628, Guidelines for Smart Grid Cyber Security, available here: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628

VOLUNTARY BEST PRACTICE GUIDANCE

- National Electric Sector Cybersecurity Organization (NESCO)/National Electric Sector Cybersecurity Organization Resource (NESCOR)
  - Formed by DOE, NESCO creates a "comprehensive public private partnership to coordinate the efforts in the industry to meet the growing challenge of securing the electric sector."
  - Formed by EnergySec and the Electric Power Research Institute (EPRI), NESCOR is intended to strengthen the cyber security posture of the electric sector by establishing a broad-based public-private partnership with the Department of Energy (DOE) for collaboration and cooperation.
  - The two organizations bring together experts to strengthen the cybersecurity posture of the electric sector by working with the DOE Electricity Sector Information Sharing and Analysis Center and industry.

AMERICAN PUBLIC POWER ASSOCIATION (APPA)

- www.publicpower.org

CONCLUSIONS

- Cyber security is a process, not an end goal
- Absolute cybersecurity is neither attainable, nor is it the end goal
- Cybersecurity is best approached through a nimble and complex balance of functionality, security and cost
- Planning for, protecting against, detecting and responding to cyber attack must take into account a dynamic relationship of systems, physical components, people and their function

QUESTIONS?

Terry M. Jarrett

Healy & Healy Law Offices, LLC

573-415-8379

terry@healylawoffices.com