ELECTRICITY POLICY
ELECTRICITY DAILY

Cybersecurity: IT vs. OT, and the Pursuit of Best Practices

In a cyber environment, where new threats to our power systems emerge daily, the processes, systems, and compliance frameworks we employ for protection, detection, and recovery must constantly evolve as well.

By Paul Feldman and Dan Hill

Electricity Policy – the website ElectricityPolicy.com and the newsletter Electricity Daily – together comprise an essential source of information about the forces driving change in the electric power industry.

Cybersecurity: IT vs. OT, and the Pursuit of Best Practices

In a cyber environment, where new threats to our power systems emerge daily, the processes, systems, and compliance frameworks we employ for protection, detection, and recovery must constantly evolve as well.

By Paul Feldman and Dan Hill

I. Introduction

Previously, we have written on the subjects of "A New Responsibility for Boards of Directors: Cybersecurity"[1], and on "Cyber-Risk, Standards, and Best Practices"[2]. The former was an effort to assist Boards of Directors in their thinking and approach to cybersecurity. The latter was a discussion of risk and the need for the industry to pursue cybersecurity best practices as a superior objective to simply being compliant. Here we offer thoughts related to future directions for compliance, as well as a specific best practice whose time has come.

Paul Feldman *is a director and past chairman of the Midcontinent ISO, where he chairs the Markets Committee and serves on the Information Technology and Governance Committees. Previously, Mr. Feldman served on the board of the Western Systems Coordination Council.* **Dan Hill** *is a board member of the New York ISO, where he chairs the Audit and Compliance Committee and serves on the Commerce and Compensation committee. Mr. Hill is retired from Exelon where he was Senior Vice President and Chief Information Officer. The views expressed here are Mr. Feldman's and Mr. Hill's and should not be attributed to any organization in which they serve.*

[1] See http://www.electricitypolicy.com/Articles/a-new-responsibility-for-utility-boards-of-directors-cybersecurity-2

[2] See http://www.electricitypolicy.com/articles/7926-cyber-risk,-standards,-and-best-practices

Before launching into the heart of the paper, it is useful to remember the importance of energy and electricity to our way of life. Presidential Policy Directive 21[3] named 16 critical infrastructure sectors. While a debate about which sector is most important may be interesting, we must realize that all sectors rely on the Electric Sector to perform. Electricity is central to our way of life and success as an economy.

The Northeast power outage of 2003[4] resulted in at least ten deaths and billions[5] of dollars in losses to the economy. A significant contributor to the blackout was a mere software bug that many believe was the primary cause of the blackout. While cyber-attackers as a group have a wide spectrum of goals, some pursue cyber-footholds for the purpose of causing damage to the grid. These groups, if successful in a highly coordinated attack, could potentially cause damage far beyond that caused by a simple, accidental software bug.

Since 2003, the U.S. has strengthened its capability to deal with cyber-attackers and its ability to manage the grid in the face of emergencies. If the 2003 event were to happen today, given today's set of RTOs and their capability, it is unlikely that it would be so widespread. New technologies have also been deployed to assist grid operators, such as visibility to energy flows beyond their own geography of responsibility, synchrophasors, and more. However, while the amount and complexity of software to manage the grid has greatly expanded (thereby growing the attack surface) the capabilities of attackers have also grown in strength and resolve.

Have our increased cyber-defenses moved at the same pace as the ability of the attackers? Probably not.

Have our increased cyber-defenses moved at the same pace as the ability of the attackers? Probably not. Attackers are far more sophisticated today and there are far more people and entities that can afford to launch cyber-attacks. Importantly, no electric utility CIO would believe that simply pursuing NERC compliance will accomplish the cybersecurity posture their company needs to be cybersecure. NERC compliance is a legal responsibility, while implementing cyber protections beyond the NERC standards are decisions based on a cyber-analysis and an understanding of best practices. The challenge for the industry is accomplishing best practices to be secure

[3] See White House site - http://tinyurl.com/q8pbbze and DHS site - http://www.dhs.gov/critical-infrastructure-sectors

[4] See Wikipedia at https://en.wikipedia.org/wiki/Northeast_blackout_of_2003

[5] See http://www.energycollection.us/Energy-Reliability/Economics-Impacts-2003.pdf an ELCON paper that also sites various references.

while also accomplishing compliance requirements.

NERC and FERC are trying

In the wake of the 2003 outage, Congress amended the Federal Power Act and directed FERC to select an Electricity Reliability Organization (ERO) to set standards and to audit against those standards. FERC selected NERC as the ERO. NERC was already doing that type of work, although the energy companies only participated on a voluntary basis. The amended Federal Power Act made compliance with the ERO's standards mandatory and a legal responsibility for the energy companies.

Much could be written about what has gone wrong and what is right about how NERC has performed to date. We choose to recognize some of the positive trends:

1. FERC and NERC have found a balance whereby FERC can strongly influence standards (which it must approve anyway), without dictating a standard.[6] This saves time and provides a balance to an industry-driven perspective.
2. The standards in general, and in particular the Critical Infrastructure Protection (CIP) standards, have evolved to be more encompassing and more protective.[7]
3. Standard development has included more expertise (including vendor expertise) over time as opposed to only energy company volunteers.
4. There is an understanding that more resources should be directed toward protecting more important assets, although the industry is still trying to develop strategies and tactics for doing so. Classical risk management principles are acting as a driver.
5. Executive Suites and boards have come to a more mature understanding of standards, compliance, threats, risk, etc. In a complex business with complex standards, there is little escape from an occasional standards violation. The chief focus is inclining toward being cyber-secure and understanding risk exposure.

Given the base now in place, there are other strategies that might be beneficial going forward for CIP Standards:

1. Utilize the regional auditors as semi-consultants. Instead of simply auditing against a set of fixed standards[8], provide a broader set of recommendations to the audited company related to what the auditor has seen in other places, and what the auditor knows about the subject area that might be helpful – i.e. share best practices.
2. Identify an entity/organization to develop and continuously maintain a set of best practices related to achieving a solid cybersecurity posture.

[6] The Federal Power Act does not authorize FERC to dictate a standard.

[7] We make this comment while observing that the development of CIP standards has arguably not kept pace with the ability of cyber-attackers.

[8] Which are generally 3-4 years old – unacceptable for critical infrastructure cybersecurity standards.

This would help to close the time gap between enforceable standards and cyber-attacker skills.

3. Continue the trend towards different levels of protection for assets having different value to grid reliability. Compliance standards that protect assets that are expendable at the expense of more protection for assets that are crucial is not a good trade-off.
4. Reduce delays in standards development through process improvement.
5. Moderate the legalese, financial fine-mentality, and other non-productive aspects of the current approach.
6. Spin the E-ISAC[9] out of NERC as a totally independent organization.
7. Identify an entity/organization to lead in the deployment of Information Sharing and Analysis Organizations.[10]

We recognize that #1 and #2 (if the regional auditors are the chosen entity) above are contrary to the traditional audit philosophy that auditors do not comment on how a company could accomplish a compliance element. While separating auditing from advising is a best practice in many places (e.g. financial controls), we believe better outcomes can be achieved by not following that practice in the NERC cybersecurity auditing.

Best Practice – Board Questions and Considerations

Recently we published our thoughts on what boards ought to be doing to fulfill their responsibility in an area where, typically, they have had little expertise. Many boards have recognized this deficiency and taken action. In some cases, board members have been added with knowledge in the field of cybersecurity. Others have beefed-up their interaction with the CIO and/or CISO[11], or added outside consultants to secure advice. These are positive trends.

Questions a board might pursue relate to: "What is the worst that could happen?" and "What kinds of attacks are we still potentially exposed to, given how we are deployed to protect the company?" The answers may be surprisingly elusive.

Hopefully, the days where the CIO or CISO assures the board that the company is totally protected are over. All companies have some level of exposure to a cyber-event. Given the many published high-profile breaches that have occurred, energy companies are exposed to various attacks that a CIO/CISO should understand and explain to the board. Boards may ask but should not expect definitive answers about the probability of such attacks. All companies of size have beefed-up their cybersecurity posture, so the risk of a breach may have been reduced. But the "bad guys" have improved their abilities as

[9] See - https://en.wikipedia.org/wiki/Information_Sharing_and_Analysis_Center

[10] See - http://www.dhs.gov/isao

[11] CIO is the Chief Information Officer; CISO is the Chief Information Security Officer

well, so we do not know who is winning the cyber-attack vs. cyber-defend race.

We do know that the loss a business could experience from a cyber-attack that interrupted electricity service for a period is very large. Considering a very small probability of a very large loss does not give a board much quantitative support to weigh when considering the advisability of more or less resources. And, let us not forget that, cybersecurity aside, the more software that is deployed the more software bugs are likely to be hiding under the surface. Even the ubiquitously deployed PI Server contained 56 vulnerabilities – likely a mix of bugs and cyber-vulnerabilities – announced as late as August 2015.[12]

It is unlikely any US company has been exposed to the most sophisticated attack possible. In the past such a sophisticated attack was less likely as only a nation-state could have assembled the resources needed to launch such an attack. Also, such an attack would likely have earned a proportional response by the US government. But today lesser actors have the funds and capability to launch sophisticated attacks with less fear of a proportional response, because often the attacker cannot be identified. The motivations and capabilities of such groups need to be factored into decisions as well. In the end, a board should weigh various inputs that have been rigorously collected, contemplated, and discussed with professionals.

An area on which a board can engage its advisors relates to the need to be compliant vs. the need to be secure. A CIO/CISO of a breached company that relies on proof that it implemented all the required compliance mechanisms should receive no great comfort from that fact alone, in fact may be about to undertake a job search. Compliance is not equivalent to being cyber-secure. Meeting compliance standards must be accomplished within the larger context of being secure.

As we know, the Department of Homeland Security has classified the energy sector as one of 16 critical infrastructure[13] industries, and the one all of the other critical infrastructure industries depend upon. Given that dependency, there are important elements of cybersecurity programs at energy sector companies that require special consideration and, at times, a deeper dive by their boards.

As an example of that special responsibility for utilities, we comment below on the use of a technology called “data diodes” or “unidirectional gateways.” This technology is superior to firewalls, but not required in any NERC CIP standards. Yet the Nuclear Regulatory Commission required this technology years ago for all nuclear plants to bridge between plant operations and company systems that were external to

[12] See copy here – http://www.EnergyCollection.us/Companies/DHS/OSIsoft-PI-Data.pdf - last accessed 8/19/2015 at https://ics-cert.us-cert.gov/advisories/ICSA-15-225-01

[13] See http://www.dhs.gov/critical-infrastructure-sectors

plant operations. The French have updated their standards to make much greater use of this technology beyond just protecting nuclear assets.

IT vs. OT (ICS) Systems and Support

IT is classic Information Technology – email, billing, Customer Information Systems (CIS), Work Management, Enterprise Resource Planning (ERP), and the normal systems found in any company. These traditional IT systems all reside on the business network of the company.

OT is Operational Technology – software and hardware systems, typically Industrial Control Systems, that are unique to a class of industries that require such systems to produce products and services. The Industries that most use OT/ICS systems are also generally the Industries defined by DHS as critical infrastructure sectors. At the core of the energy sector OT/ICS systems are SCADA[14] networks[15].

Many OT/ICS systems used in the energy business were not originally designed with security in mind, for two basic reasons: (1) Many are old and designed when cybersecurity was not the prevalent risk it is today and the known cyber risks/threats were significantly less sophisticated that those today; and (2) Many were designed with the thought that they would be "air gapped" from other systems – i.e. not connected physically (or wirelessly) to other systems that had a higher threat exposure and could be a carrier for an attack (i.e. other IT systems on the business network or the internet).

Today newer OT/ICS systems are being designed with cybersecurity in mind for many reasons, including: (1) Cyber-attacks are now a persistent and permanent threat; (2) OT/ICS systems are becoming more and more connected to general IT systems (i.e. IT/OT Convergence); and (3) It is now recognized that air-gapped systems are still vulnerable despite the air gap. (The most notable example is the Stuxnet[16] virus.)

It needs to be recognized that wholesale change-out of legacy OT systems that do not contain cyber protections as an integral part of the design may not be feasible. In these cases, other cyber protections are needed until newer systems are implemented. A mixed environment of legacy and new is likely to exist for several years.

From a cybersecurity standpoint, it is critical that a consistent and coordinated security approach is used across both IT and OT platforms. Historically, the teams that support IT and OT have similar, yet different, skill sets, with IT teams' core skills being typical IT skills (application development, application

[14] Supervisory Control and Data Acquisition systems monitor and control Transmission and Distribution systems.

[15] There is an ongoing debate about what is IT and what is OT. However, for a Board focused on risk and understanding the impact of a successful cyber-attack anywhere in the company – the debate is largely mute.

[16] Stuxnet - http://en.wikipedia.org/wiki/Stuxnet and http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet#

maintenance, infrastructure, operations, security, etc.) while OT teams typically have core engineering skills (control systems) and often less extensive IT skills.

In many utilities the IT and OT organizations have been merged/converged, while in others they remain in separate organizations. From a board governance standpoint, whichever officer is accountable for cybersecurity (CIO or CISO) should be accountable for the cybersecurity of both IT and OT systems to help ensure a consistent security approach across platforms.[17]

Best Practice: SCADA Network vs. Business Network

Utilities[18] utilize SCADA[19] networks to maintain the grid reliably. For electric utilities, SCADA networks take frequent measurements of demand and resources to meet that demand. The typical configuration in the industry today has an independent SCADA network that is segregated from the company's business network by firewalls[20]. Historically, some utilities have not segregated the SCADA and other business networks – a practice that in today's environment we view as simply unacceptable from a security standpoint, and hopefully non-existent given the extreme exposure that would allow. Efforts to expose such networks[21] have been ongoing for some time.

Some would argue that the SCADA network should be totally separate[22] from other business networks. That option is increasingly less attractive in today's world. The Internet of Things[23] grows exponentially and the need to compete requires real-time knowledge of the status of a company's industrial assets. Raw SCADA data is combined with other new data sources as input to emerging "big data" analysis methods. These tools help form a more complete picture of the state of the system, as well as identifying preventative maintenance opportunities. We take it as a given, therefore, that SCADA networks must be connected in some way to the business side of the company to properly derive value and be competitive. While many focus on a compliance solution to this dilemma, we focus on a more secure alternative below.

[17] We make this point while maintaining the CEO is not only ultimately responsible, but intimately responsible. Cybersecurity is a cross functional threat that requires CEO active involvement.

[18] Other industries use SCADA as well to control industrial processes.

[19] See - https://en.wikipedia.org/wiki/SCADA

[20] See - https://en.wikipedia.org/wiki/Firewall_(computing)

[21] See - http://www.shodanhq.com/

[22] Separating the SCADA network totally form everything else does not in any way guarantee cybersecurity. The famous Stuxnet attack targeted and penetrated a separate SCADA network.

[23] See - https://en.wikipedia.org/wiki/Internet_of_Things

It is important to put firewalls into perspective. Firewalls have historically been the norm to protect information from a would-be attacker. Firewall functionality is accomplished through software. Firewalls pass messages or data from one side to the other – often from the less secure side to the more secure side. The firewall software tries not to pass the dangerous messages/data. Because the kinds of dangerous messages/data quickly evolve over time, the firewall's software must be updated quite often. Firewalls are also becoming more sophisticated and more complicated to manage. It's an arms race between the firewall providers and attackers. Separate from the arms race, but related to whether the good guys or the bad guys can develop sophisticated software faster, there is also the bug issue. Firewalls are enabled by software, and software often contains bugs. Firewalls are difficult and expensive to manage; sometimes they don't work. Importantly, firewalls did not prevent any of the many successful attacks that have been disclosed.

> Firewalls are becoming more sophisticated and complicated to manage. It's a race between firewall providers and attackers.

In general, the OT/ICS side of the business needs greater protection than the IT side. If OT/ICS assets are damaged, there must follow a physical repair/replacement effort that could take from hours to weeks. A breach on the IT side normally just requires moving to a back-up copy of the software and databases. So, how do we connect OT/ICS to the IT side?

As we've said, a special methodology to bridge IT and OT/ICS systems is now required[24] in all nuclear plants. That methodology employs a hardware-based unidirectional gateway[25] ("data diode") to move data from the OT/ICS network to the IT/business network on a real-time basis. In this configuration it is impossible for the OT/ICS network to be infected or breached from the IT/business network through this connection, as the data can only flow one way.[26]

To avoid any confusion, unidirectional gateways are in common use by security organizations to pass information from a lower security level to a higher security level – e.g. Secret to Top Secret. It is the opposite use in the OT/ICS world, where we want to enable access to information produced by our most valuable assets

[24] By the Nuclear Regulatory Commission

[25] See - https://en.wikipedia.org/wiki/Unidirectional_network

[26] A LASER transmitter is on the OT/ICS side and transmits over a fiber to the IT side that only contains a photo-receiver. There is no receiver on the Nuclear OT/ICS side.

without putting those assets at risk. The term Unidirectional Gateway can also be problematic, as some software vendors will claim their firewalls can be configured for a one-way flow – but that configuration is enforced by software. The kind of Unidirectional Gateway we intend here is hardware-enforced, where the hardware is an optical fiber, with a transmitter at one end and a receiver at the other, making it physically impossible to pass information back from the receiver side.

We believe it's time for transmission and distribution companies to install unidirectional gateways between their SCADA/OT networks and their business networks. It is clear that our country's utility SCADA systems represent a target from a cybersecurity standpoint, given the criticality of our energy infrastructures. In addition, given the importance of maintaining the reliability and security of utilities' SCADA infrastructures, it takes longer to test security updates and anti-virus signature updates than for a business network, and during that time the SCADA systems are vulnerable to attacks that those updates are intended to prevent. We need to move to configurations in which it is physically impossible for our SCADA systems to be breached in real time from the Internet or directly from within a utility's business network. Even in so doing, breaches remain possible through mistakes within an air-gapped[27] system, or from malicious or compromised employees.

Moving to replace firewalls with physically-enforced security rather than software is not the total answer to protecting OT/ICS assets, but it does totally protect against the most dangerous exposure: that of a remote controlled attack which would require two-way communication. That said, OT/ICS networks are still subject to insider attacks and errors (employees, contractors, vendors), as well as Stuxnet-type attacks, and therefore need processes to address those vulnerabilities as well.

This technology example is one area where standards have not kept up with methodologies to thwart those that would do us harm by damaging our infrastructure. Mechanisms to identify these technologies and have them evaluated and deployed are needed more than ever as the amount of software used to manage our assets grows.

Conclusion

In a cyber environment with new threats and threat actors emerging daily, the processes, systems, and compliance frameworks we employ for protection, detection, and recovery must constantly evolve as well. In that spirit we have offered these ideas and suggestions that we believe should be considered. □

[27] Unidirectionally connected systems are generally considered "air-gapped" on the transmitting (LASER transmitter side).