Best practices for cyber security in the electric power sector

Abstract

With rare exceptions, utilities do an excellent job of managing traditional types of risks facing their operations. However, cyber security is the one category of risk that remains stubbornly opaque and resistant to attempts to manage, monitor, and measure. Determining the likelihood and severity of cyber security risks, as well as the efficacy of an organization's approaches to mitigate them, continues to be a challenge.

IBM believes there are now practical ways to greatly improve management and execution of enterprise-wide cyber security. To help stakeholders understand the landscape of cyber security threats currently facing utilities, IBM introduces "best practices" that any utility organization can implement including:

I. View security as risk management
II. Create a fully integrated security enterprise
III. Implement security by design
IV. Use business-oriented security metrics and measurements
V. Understand that change begins at the top
VI. Take action on the top 10 recommended security actions from IBM

Cyber security for energy and utilities organizations

Cyber security is one of the most important policy and technology topics an organization must address. Critical infrastructure for energy and utilities is vital to personal safety, economic growth and national defense. There is growing interest in the topic from senior utility executives, regulators and customers around the world. But there are also legitimate concerns about ensuring that adequate resources and focus are directed to the task of securing critical infrastructure. One senior executive recently asked the question: "Based on everything IBM knows from its wide experience with clients and technology, how would you run security at a utility these days?" Here's how.

The security environment

As the planet becomes smarter and increasingly interconnected, critical infrastructure systems that were previously isolated from other networks are now connected with both critical and non-critical systems—many of which are not under the direct control of infrastructure operators. This interconnectedness can enable many new efficiencies and conveniences. But it also means that, while every business must continue to refine and improve its security capabilities, critical infrastructure industries—like electric utilities and associated providers of technology and services—must adopt best practices in policy and controls. These best practices should be infused into the culture of the organization, while still enabling the kind of information-sharing and analysis that can lead to new efficiencies and innovation.

Whether motivated by international competition, corporate espionage, political ideology, organized crime, a grudge against an employer or even idealism (for example Anonymous, LulzSec), malicious hacking continues to expand. Thanks to the proliferation of "how to hack" materials online, as well as free or affordable high-powered tools, it has never been easier for a hacker to succeed. Social networking also makes sharing both information and successful techniques just as easy for these hackers as it is for the rest of us. The combination of complex network connections that no one fully owns, a largely opaque software supply chain and the vulnerabilities inherent with human operators provide a ripe environment for hackers and those with malicious intent.

Security and compliance challenges

Whether assessing the threat of equipment failure or the potential for employee injuries, energy and utilities organizations have long been accustomed to managing operational risk. Now, as the transition to advanced communication, control and computing technologies accelerates, a new kind of operational risk is emerging. Traditionally, a single-direction flow of power and data on isolated systems was the norm. That is now giving way to more dynamic and integrated electricity production and delivery systems along with advanced metering infrastructure. Sensitive operations and personal data are now moving over common or integrated communications infrastructure, flowing in multiple directions within a dense, multi-nodal system.

By definition, a smart grid has more access points and multiple networked systems. As this positive transformation of operations continues, there is an impact on cyber security—namely in a marked increase in the risks of cyber breaches. To address this, a host of industry and government standards and regulations, such as the North American Electric Reliability Corporation—Critical Infrastructure Protection (NERC-CIP) standards, have been developed. Even so, significant societal and industry concerns remain.

Regulations covering data privacy and information security protections are becoming the norm around the world. Therefore, policy-making bodies have developed an increased interest in what utilities are doing to meet the following challenges:

- Integrating information technology (IT) and operational technology (OT) networks due to grid modernization and other business initiatives
- Exposing both IT/OT networks to the Internet—either directly or indirectly, whether intended or not
- Mitigating threats to IT and OT systems from the widespread use of mobile devices, social media and easily portable USB drives, and lack of governance for the use of these tools in critical environments
- Eliminating internal threats posed by disgruntled employees and human error by authorized technicians
- Countering recent OT threat events, such as the emergence of Stuxnet, Flam and their variants as well as the 2012 "Project Basecamp" release of packaged OT attacks on E&U programmable logic controllers (PLCs) and other control system equipment

There are increased expectations for the reporting of compliance with security and privacy directives. Scrutiny by federal agencies such as the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), and the Department of Energy (DOE) is likely to expand. Future versions of the NERC-CIP standards promise to expand the scope and depth of utility compliance requirements. There is also a sustained and targeted effort from the regulatory and policy-making communities in key markets around the world to push the industry toward full preparedness.

Ultimately, the market will need to bear the costs of assuring compliance. In addition to the direct cost of any failures during compliance audits, the less obvious costs of mitigating a security breach must also be managed.

Security is a key operational domain

Current utility governance and oversight plans must be adapted to meet the new requirements for compliance. Senior leaders need to be able to answer some basic questions:

- How can we objectively measure the current cyber risk level within our organization?
- What is the current status and adequacy of our existing security policy and controls?
- How do we estimate and prioritize security expenditures, and what improvements do we expect from those expenditures?
- Where should responsibility within our organization rest for security policy, operations, enforcement, compliance and reporting?
- What are the responsibilities of our Board of Directors, the CEO and other senior leaders for complying with SEC disclosure requirements?

Quantifying the benefits of managing cyber security in the energy and utilities industry can be challenging. It is common to hear, "I spend a lot of money on security, but have absolutely no idea what I am getting for it!"

In any organization, senior executives may view cyber security as a confusing and highly technical domain, one perhaps best left to experts. Cyber security is also a function that usually only costs money, rather than an obvious source of savings or revenue. Thus, at best, it may be viewed as a "cost of doing business," similar to insurance. But in a fast-changing world, cyber security needs to be managed proactively as a key part of overall operations. An organization cannot assume its current cyber security policies and funding are adequate, simply because they have not experienced a recent attack.

Without proper security management, it is almost impossible to determine the current state of preparedness. Measuring the effectiveness of cyber security is still a developing science, and hard to quantify with traditional business metrics. But waiting for an attack to reveal a cyber security program weakness is like waiting for bankruptcy to expose a vulnerability in a financial management system.

For executives accustomed to managing operational risk using readily available performance metrics, cyber security can cause great uncertainty and frustration. Despite the challenges, energy and utilities organizations can apply a number of fairly simple, cost effective, and easy-to-understand best practices.

Best practices for energy and utilities

IBM recommends energy and utility organizations adopt the following six key security strategy and policy elements:

I. View security as risk management
II. Create a fully integrated security enterprise
III. Implement security by design
IV. Use business-oriented security metrics and measurements
V. Understand that change begins at the top
VI. Take action on the top 10 recommended security actions from IBM

I. View security as risk management

Two focus areas for all utilities are: safety for utility customers and employees, and maintaining a high degree of power quality and reliability. Historically—apart from dealing with economic and regulatory risks—utility risk management professionals have focused on anything and everything that could interfere with those critical areas of safety and reliability. Until fairly recently, cyber threats had not been considered a significant threat to either.

For calculating risk, utilities have traditionally used the following formula:

Risk = Threat x Vulnerability x Impact

This same formula can be used for measuring the risks posed by cyber threats with the following explanations for the variables:

- **Threat:** The proliferation of cyber attacks is expected to continue to increase across all sectors of the digitally connected economy. As noted, the more electric power systems become interconnected with each other and with other domains, the greater the exposure to potential attack.
- **Vulnerability:** There have always been plenty of vulnerabilities in grid systems, but in the past most were adequately shielded by physical security protections and procedures. With the advent of smart grid and other information and communication improvements, attackers no longer need to bypass physical security protections or risk personal injury. Highly networked systems provide new pathways for hackers to reach critical operational systems. Vulnerability is no longer specific to locations and equipment used by the utility, and attacks can be launched from anywhere in the world with an Internet connection.
- **Impact:** Given the fact that electric power enables much of modern life, electric utilities have focused on reliability, and the potential impact from any kind of security threat has always been quite high. In the past, cyber threats were not much of a concern since attackers would have been unable to reach important operational systems. Today, the impact to critical systems from a cyber security breach increases exponentially as electrical system operations become more instrumented and interconnected.

Strategies used to mitigate the impacts of threats such as severe storms and natural disasters, which can draw on historical data and well-documented experiences, can provide metrics that senior management can use to evaluate return on investment. But developing similar metrics for the efficacy of cyber security investments continues to be a challenge.

Many utility executives continue to be confused by cyber security. As a result, it is often understood only by a small, secluded cadre within their organizations. This cyber security team, which is tasked with the performance of security and compliance functions along with dozens of other duties, is generally separated from senior executives and decision-makers by multiple layers of management. Without a senior-level advocate, the inability of a cyber security team to articulate risks and requirements clearly and in business-friendly terms often keeps them at the periphery of the organizational culture.

The best way to address this and increase the adequacy and effectiveness of security strategy is to apply the risk management principles that have worked well for managing the traditional risks faced by electric utilities. Most utilities already have mature methods and metrics for estimating and preparing for other types of risks, including fires, hurricanes, ice storms, audit failures, fuel price volatility or macroeconomic changes. These same proven methods can and should be applied to cyber security risk to gain a similar level of understanding and control over this increasingly-important aspect of operations.

II. Create a fully integrated security enterprise

Working with clients around the world as well as in its own operations, IBM has demonstrated that the best way to improve visibility and gain operational control is to integrate previously disparate, disconnected business processes and take a centralized approach to managing security. Happily, this approach aligns well with work already underway in many utility organizations to integrate their core IT and OT systems.

One example of how this integrated approach could enhance security is access to facilities. Select employees might have card-key access control to the gates of major substations. If the utility also has an asset-management and maintenance system, it could be integrated with the access control system. Once integrated, the two systems could do a cross-check whenever an authorized employee enters a substation to ensure that there is an "open ticket" for maintenance work—and generate a security alert if there is not. This type of cross-referenced, security-related data could be aggregated and analyzed to determine appropriate actions to improve operations and reduce risk.

Integration also applies to cyber security policy. Like other business processes, cyber security policies that are formulated, promulgated and enforced by multiple independent groups within an organization tend to be ineffective. At best, they tend to be optimized for outcomes at the group level, rather than for the enterprise as a whole. At worst, they lack the basic business logic that links them to the desired business outcomes. This can result in an inconsistent, incoherent and contradictory mix of security actions.

Therefore, the first step to achieving better security outcomes is centralizing the authority and accountability for improving cyber security strategy and execution. This centralization will inevitably require the integration of previously disparate organizations and processes.

Just as financial risk management must apply across investments, accounts payable and purchasing to develop an integrated view of financial risk, cyber security risk management must also connect the dots across domains to provide a complete view of key indicators and failures. Applying analytics to an integrated view of both historical data and near-real-time operational data can allow organizations to discover, investigate and thwart suspicious activity before it becomes a full-fledged attack.

One approach that helps some utilities accelerate the integration and centralization of security is borrowed from the US Department of Defense—developing a security operations center (SOC). Establishing a centralized operations center can help drive process and organizational integration. When sponsored by the CEO and senior leadership, an SOC becomes the nerve center for cyber security visibility and control. It also can demonstrate to auditors that the organization is taking serious and concrete steps to improve its security position.

III. Implement security by design

It is generally understood that any important feature required for a new system or service should be incorporated from the earliest stages of planning and design. Yet security is often left out of the early stages of planning. In many cases, security professionals are only brought in to "harden" the system or service after the system is deployed and proves to be vulnerable.

As IBM Chief Information Security Officer (CISO), Kris Lovejoy, says in her article, "Security Essentials for CIOs":

"One of the biggest vulnerabilities in information systems—and wastes of money—comes from implementing services first, and then adding security on as an afterthought. The only solution is to build in security from the beginning, and to carry out regular automated tests to track compliance. This also saves money. If it costs an extra $60 to build a security feature into an application, it may cost up to 100 times as much—$6,000—to add it later."

In the view of IBM, the principle of security by design should be applied both to utility organizations and their cultures. Senior leaders need to make it clear to the organization that cyber security competence is a core value, and the organization chart should reflect it. Again, according to Lovejoy:

"An enterprise's culture of security must extend beyond company walls, and establish best practices among its contractors and suppliers … Security should be infused in the entire ecosystem. The ruinous effects of carelessness in one company can convulse entire sectors of society."

The utility's suppliers and partners should know that its security policy applies to them as well. This may mean that projects don't proceed until the provider updates or improves some aspect of how its product handles important security functions such as authentication, authorization and encryption.

IV. Use business-oriented security metrics and measurements

Capturing data is only a first step, one that needs to be followed by the use of analytics to turn raw data into useful, actionable information. In order to run cyber security as a true enterprise function, management needs a framework with which to establish a baseline for current security programs, understand the context and critical interdependencies, and set priorities accordingly. The framework also is used to identify gaps and monitor progress in filling them, and achieve other strategic security objectives while ensuring security programs are fully coordinated with the utility's core business objectives and initiatives.

While there are numerous security-related maturity frameworks and models to choose from, perhaps one of most promising is still in development. Sponsored by the US DOE, with assistance from Carnegie Mellon University, the Electricity Subsector Cyber security Capability Management Maturity Model (ES-C2M2) team is working to build a common tool utilities can use to measure their current security programs and to develop objectives for the future.

Here's what White House Cyber security Coordinator Howard A. Schmidt said about it in early 2012:

"This effort will be focused on performance-based strategies and concrete steps to measure progress of cyber security in the electric sector … It is important to understand the sector's strengths and remaining gaps across the grid to inform investment planning and research and development, and enhance our public-private partnership efforts."

Frameworks and maturity models can help organizations identify their strengths and weaknesses and compare them against current industry best practices. Such approaches are widely used to improve performance, efficiency and quality. One existing example is the Smart Grid Maturity Model, a strategic framework designed to help your company develop business cases and explicit plans to move toward a smart grid infrastructure. With the advent of the first version of the ES-C2M2, the electric sector should have a much-needed, common cyber security scorecard that will help utilities gauge how they are doing in key aspects of security, and determine where they want or need to focus next to manage their business risks.

Utilities' business and organizational structures vary widely, and not all frameworks, maturity models or metrics will be appropriate. To account for the unique requirements of individual utilities, some customization is required. When new cyber security metrics are being considered, there are three characteristics IBM considers essential for the metrics to be of maximum value to senior utility leadership. Cyber security metrics must be:

1. **Easy to obtain** with no expensive tools or overly labor-intensive processes needed to acquire data.
2. **Easy to understand** so a business person can easily understand the connection between what is being measured and what it indicates about the organization's risk management, reliability, safety or other performance objectives.
3. **Easy to share** such that the information gathered should not be so sensitive that it can't be shared among internal organizations and depending on the metrics, outside the utility with oversight and stakeholder organizations.

V. Understand that change begins at the top

The security and compliance challenges facing utilities today have critical implications for all parts of the enterprise, and addressing them requires organizational, cultural and technological change beyond the control of any single division or department. IBM believes that no other single action will do more to galvanize a new approach to security in an organization than the appointment and empowerment of a Chief Security Officer (CSO) responsible for enterprise-wide cyber security and compliance. The CSO must have ultimate control and responsibility for securing IT and OT across all lines of business, and as needed, into the extended supply chain. Regulators, governments, investors, employees and customers will notice and appreciate the strong signal a CSO appointment sends about how seriously the organization takes security and privacy.

To be most effective, IBM recommends the CSO position report directly to the corporate CEO, COO or CFO and have responsibility and authority for:

- Implementing and monitoring the performance of the best practices described in this paper.
- Setting and maintaining all cyber and physical security policies.
- Ensuring proper business and technical controls are implemented, tested and kept current.
- Translating security challenges and opportunities into business language for regular consumption by the CEO, the Board of Directors and other key senior leaders.
- Guaranteeing enterprise-wide compliance with any policies and regulations that cover the protection of critical infrastructure and other key systems.
- Ensuring security personnel and assets are available to support corporate privacy policies which typically are created and maintained outside of a security organization.
- Directing security audits and other validations of vendor compliance, from procurement through acceptance and commissioning.

IBM CISO Lovejoy calls for a "new breed of security leader," and describes the change in organizational behavior the CSO is expected to lead:

"The only answer is to change, at a fundamental level, the way companies operate. It starts with expanding the mission of enterprise security, from the tech staff and their machines to every person within the company, and everyone who does business with it … In the end, success hinges upon creating a strong and persistent awareness: a risk-aware culture … It represents a new way of thinking, one in which a pragmatic approach to security informs every decision and procedure at every level of the company. This must recast the way people handle information, from the "C-suite" to summer interns."

A handful of the largest US utilities currently have CSOs, Chief Information Security Officers (CISOs) or equivalent leaders in place. If this becomes the norm rather than the exception in the electrical and utility sector, implementing the other best practices will be much easier. Overall, the industry will not only be demonstrably more secure, but will better communicate the business benefits of security improvements to regulatory agencies, investors, customers, employees and other stakeholders.

VI. Take action on the top 10 recommended security actions from IBM

Similar to organizations in other sectors, many utilities empower a comparative handful of employees to select and implement isolated, single-purpose security technology solutions without having a set of business and risk-management metrics in place to optimize these resource-intensive investments. Having security best practices in place before implementing technology-based security programs—or any other security initiatives—will help ensure that the programs are measurable and manageable in terms of efficacy, cost and value.

While there is no easy checklist that absolutely ensures security for an organization, if the recommendations already set forth in this document are followed, then these 10 complementary actions can have a tremendously positive impact on security. Originally developed with the IT department in mind and proven through successful application in organizations worldwide, these 10 actions apply to OT as well:

1. **Perform regular third-party external and internal security audits.** Your networks are constantly changing. When new security problems are introduced, you need to find them before the hackers do. Regular third-party security audits coupled with constant vulnerability assessments and scanning are the best ways to understand the complete landscape of your networks and where the weaknesses are located.
2. **Control your endpoints.** Do you know what systems you have in your networks, what software is running on them, and what patch levels and configurations you have? The closer you can get to total endpoint awareness and control, the more secure your infrastructure should become. Do you keep up with security fixes? Or do you struggle to patch systems due to lack of resources, legacy code or custom code that is incompatible with the latest technologies? Legacy systems and long patch deployment cycles can become a security liability.
3. **Segment sensitive systems and information.** In environments where people work with particularly sensitive information, such as operations centers or classified data centers, employees are typically given separate desktop systems for web surfing and doing email versus the work of managing the system. You may not be working with classified information in your office, but it still makes sense to eliminate unnecessary interconnectivity between sensitive data and insecure networks, particularly if your organization is targeted by sophisticated attacks. It is important to keep in mind that interconnectivity takes many forms, such as USB tokens.
4. **Protect your networks.** You need to understand what resides in your networks, and you also need to understand who has access. Breaches often happen in areas where intrusion prevention systems were not deployed or were not carefully monitored. When breaches occur, successful investigations depend upon having access to extensive data logs. The more you monitor your networks and the more you know about what has previously occurred to them, the better prepared you are for breaches.
5. **Audit your web applications.** Web application vulnerabilities continue to be a common gap that is targeted by attackers of every motivation and skill level. Whether a web application was developed in-house, purchased from a software vendor or downloaded from the Internet, if it is running on one of your networks, you need to check it for vulnerabilities. If you don't, someone else will find those vulnerabilities for you.
6. **Train end-users about phishing and spear phishing.** Many sophisticated attacks involve social engineering or a spear phishing element. Attacks may target personal as well as business accounts and systems. Savvy users may suspect that something is out of the ordinary. If your organization knows that it could potentially be targeted, employees are more likely to report something suspicious instead of ignoring it.

7. **Search for bad passwords.** Even after decades of experience, bad passwords remain a common security weakness. Cyber security audits may make cursory attempts to find bad passwords, but constant, proactive efforts to find and fix bad employee passwords are much more effective, particularly when coupled with comprehensive policies and user education.
8. **Integrate security into every project plan.** The cyber security team should not be constantly chasing down projects that have just been rolled out, because that can introduce massive security gaps into networks that will show up on a vulnerability assessment report. Security must be applied to new projects from the beginning. Achieving this requires political finesse, with the security organization enabled to succeed and not simply seen as another bureaucratic barrier. The security team must constantly demonstrate its value to the rest of the business at all levels.
9. **Examine the policies of business partners.** In this world of cloud computing and complex outsourced relationships, many of the systems you are responsible for may be operated by other companies. Many insider attacks come from employees who work for business partners of the targeted firm. Has your security team audited the practices of your partners? Are their practices consistent with yours? How confident are you in their execution?
10. **Have a solid incident response plan.** Managing sophisticated, targeted attacks is an ongoing process that involves not just being able to identify that a breach has occurred, but being able to respond and investigate, learn and adapt. If you are a strategic target and you are not aware of any breaches, it may mean that you are not looking carefully enough.

IBM and cyber security

IBM is a well-recognized leader in cyber security, particularly in the energy sector. Over the past several years, industry analysts have consistently identified IBM as a top provider of cyber security products and services to electric utilities. IBM has worked with individual clients around the globe to help ensure the security and privacy of utilities and their customers during smart grid development and other critical projects. IBM is also active in advancing security standards and best practices across the industry. Proof of the extensive cyber security experience of IBM brings includes:

- Working with the US DOE national labs to apply wide-area situational and security to projects, and educate regional grid-balancing entities.
- Participating in designing, securing and deploying dozens of advanced metering infrastructure (AMI) networks and smart grid projects around the world.
- Performing supervisory control and data acquisition (SCADA) and control-system cyber security assessments and remediation.
- Delivering NERC-CIP compliance assessments and software to help meet CIP requirements.
- Designing information and security governance systems, data security controls and privacy programs for utilities seeking to secure customer and utility data.
- Showing utilities how to apply advanced analytics to develop security insights and derive business value from Big Data.
- Securing utility customer web portals.
- Actively contributing to industry cyber security standards bodies, including: the US National Institute of Standards and Technology (NIST) Cyber security Working Group, the GridWise Interoperability and Security working group, the US National Bureau of Information Security Examiners (NBISE) electric sector, the US DOE Risk Management Maturity Model development team, Institute of Electrical and Electronics Engineers (IEEE) 2030, and other organizations.

In 2012, IBM established two dedicated security divisions: IBM Security Systems and IBM Security Services. These divisions bring together the security consulting, product and managed services capabilities from across IBM to help clients solve security problems. With more than 6,000 dedicated security engineers, researchers and consultants worldwide, the new divisions include the award-winning IBM® X-FORCE® threat and response research team, and house the largest vulnerability database in the industry.

IBM supplements energy and utility sector expertise with security best practices developed for clients in other industries such as financial services, telecommunications, and aerospace and defense. IBM security experts have helped protect international banks and brokerages as they modernized their IT and Internet operations, and have ensured telecommunication systems and traffic were safe from attack as that industry moved from analog to digital. In addition, IBM has played a leading and trusted role in military and government information-assurance efforts in countries throughout the world. Finally, the IBM Research division ensures our clients across all sectors continue to receive cutting edge cyber security technology and practices.

For more information

To learn more about the IBM best practices for cyber security in the electrical power sector, please contact your IBM marketing representative or IBM Business Partner, or visit the following website: **ibm.com**/energy

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: **ibm.com**/financing

IBM Corporation
IBM Sales and Distribution Group
Route 100
Somers, NY 10589

Produced in the United States of America
August 2012

EUW03064-USEN-00