Deloitte.

The cyber threat to grid reliability
6 action areas for protection of utility operations

Cybersecurity is at the top of our national agenda, and utilities are a foundational element of our national critical infrastructure. Until recently, the industry has tended to look at cybersecurity as IT's problem. Today, we know that cyber threats can impact the Bulk Electric System (BES) and become a serious business and public security problem.

Cyber attacks can lurk as invisible bits of code planted within substation devices – code that can be activated remotely to unleash system unreliability, outages, or in extreme cases, an impact to safety. Though IT professionals have been combating cyber attacks for more than two decades, this is a relatively new challenge in the Operational Technology (OT) domain. Addressing it requires new technology innovation, advanced monitoring operations, executive engagement, and a risk-oriented, multifaceted program to be secure, vigilant and resilient.

Skeptics of the impact of cyber threats on BES reliability may ask, "Isn't it easier to launch a physical attack?" In short, the answer is a resounding "No!" Physical protections are required at substations, control centers and other facilities, and there will always be the risk of a physical incident, but the digital transformation of power and water delivery has changed the business risk landscape.

Consider the ease with which a single individual or coordinated terrorist group or nation state could launch a cyber attack from 20,000 miles away -- without geographic limits, without the risk of physical harm to themselves, and shrouded by the relative anonymity of the Internet. It remains a critical regulatory and ethical obligation to protect consumer credit card and personal information; a data breach can have serious regulatory and reputational impact, but disruption to the BES could arguably cause far greater harm to business performance, national security, and public safety.

The roots of cyber risk

For as sophisticated and persistent as the cyber attackers can be, the risk is not all externally imposed. Yes, there has been an increase in the number of cyber incidents[i]. Yes, greater public awareness may be encouraging a brighter media spotlight on cyber incidents. Perhaps a greater number of companies are voluntarily reporting them. But utility companies themselves play an unintended, though active, role in the growing levels of cyber risk.

How? Through the things that businesses do to better utilize technology for cost reduction, greater operational efficiency, and improved customer service. The utility industry is driving more digital technology to the substation, adopting smart meters, modernizing grid systems, and reengineering back office operations to integrate metering, billing, and customer service systems. Behind the scenes, corporate office systems and OT networks are more tightly comingled and inter-dependent than ever before, opening new avenues for accidental or targeted, malicious disruption.

Some responsibility rests with the BES equipment and smart meters manufacturers themselves. These products were not necessarily designed with security in mind, and can be expensive, risky and cumbersome to keep up to date.

But there is a primary business factor at play. Cyber risk is the dark side of business-driven technology innovation. In the long run, the success of these innovations rests, in part, on how well companies manage the new risks they introduce, and maintain their regulatory and public service obligations.

What can happen?

Today's cyber attacks in any industry sector are rarely a single action or event. "Low-and-slow" style information collection or eavesdropping can go on for weeks or months unless the targeted company has adequate monitoring capabilities.

In today's competitive market, corporate espionage to gain an understanding of competitor's growth strategy is a real threat. What mergers and acquisitions are planned? In which energy market (nuclear, natural gas, alternative fuels, etc.) does a company plan to invest? While these attacks may not cause immediate impact to service delivery, they could potentially undermine competitive standing.

Having gathered the information they need, the objective of an ideologically-motivated attacker might be to plant malware in Supervisory Control and Data Acquisition (SCADA), Outage Management System (OMS), Energy Management System (EMS) and other devices that could be used, at the right time, with a few keystrokes, to launch an attack aimed at disruption of service or destruction of equipment – one that would likely be very difficult to trace. Such attacks, of course, might create unsafe facility conditions, threaten public safety, create regional havoc, and result in substantial capital costs, business losses and damage to public trust.

Is your environment a fertile ground for attackers?

Some malicious actors are highly skilled, well-organized, and well-funded; others are small groups or individuals who, utilizing an array of pre-built tools and infrastructure available in the cyber underground, can produce significant impact with a relatively low level of knowledge. They have all become more proficient at evading detection.

There are many potential points of entry into the BES environment, but they can generally be grouped into three categories. The first is exploitation of basic lapses in IT and physical security controls. Firewalls, intrusion detection systems or other perimeter devices may not be well-configured. One study showed an alarming number of ICS devices that had been left directly accessible to the Internet[ii]. Weak password practices or poorly defined user access policies make is easier for hackers to masquerade as legitimate users. Ill-designed segregation of networked corporate and OT assets can enable attackers, once inside the corporate environment, to make their way to substations and distribution systems. Physical security issues may literally leave doors open for intruders to plant malware into computer or OT systems.

> The utility industry is driving more digital technology, opening new avenues for accidental or targeted, malicious disruption.

A second major set of vulnerabilities stems from security flaws in the design of device software. While SCADA and OT equipment manufacturers issue software patches regularly, business operations typically limit how quickly or consistently they get applied. The problem can be exacerbated by reliance on legacy systems, or the sheer variety of equipment in some environments. Patching and upgrading can risk functional disruption – but as utility companies are increasingly targeted, the risk of unanticipated disruption caused by a cyber attack may significantly outweigh the risk of disruption caused by a relatively controlled, authorized change process.

[i] In the six months from October 1, 2012 to April 30, 2013, ICS-CERT responded to over 200 incidents across all critical infrastructure sectors, more than had been reported the entire previous year. (*ICS-CERT Monitor, April-June 2013*)

[ii] In 2012, a researcher identified over 20,000 ICS-related devices directly IP addressable and vulnerable to exploitation through weak or default authentication (*ICS-CERT Monitor, Oct.-Dec. 2012*.)

The third factor, and possibly the most difficult, is a human factor. Well-designed phishing emails can trick even well-trained readers into revealing proprietary information or installing malware on corporate systems. Although truly malicious "insider" attacks are few and far between, a disgruntled or distressed employee – particularly someone with authorized access to BES or other sensitive assets – can potentially exact damage far faster than an outsider. As the digital infrastructure and supplier ecosystem gets increasingly complex, the likelihood increases for accidents to be committed by employees, suppliers, contractors or vendors that are damaging in themselves, or create new avenues for attackers.

Cyber incidents will most certainly happen – to you

A number of sources point to the increase of cyber attacks against energy companies, and in particular the likelihood of attacks aimed at disruption[iii]. The operating assumption for utilities must be that attacks will happen; preparedness and preemptive measures give companies better ability to minimize the potential damages. To be in step with today's threat environment, utilities need to do more than beef up compliance programs and discipline around security controls. They need to become secure, vigilant and resilient to keep out what they can, and improve both the ability to detect threat activity, and to respond effectively when an incident does occur.

Six areas of action to get started on a BES cyber risk program

Achieve NERC CIP 5 compliance – but don't be blinded by it.

NIST standards and regulations such as NERC CIP are essential reference points for protection of the BES, based on what is known to date about threats and cyber risks. But to get ahead of emerging threats, nothing takes the place of a risk-based program to address each organization's unique conditions and environment. IT security teams and operations engineers remain on the front lines against BES threats, but business leaders must have enough understanding of the threat landscape and their risk environment to make sound decisions about how to shape the cyber risk program. Not all investments are equal in terms of risk management value. That many organizations are working with financial and other resource constraints makes it all the more important to focus first on areas of greatest business impact.

Institute a security lifecycle approach to managing the BES environment

IT security should not be an afterthought in the BES environment, or simply a set of technology-based controls. It should be an integral part of the design, operations, and ongoing maintenance routines. Important questions include: Have we limited access to BES-related resources to only the people who need access? Will third parties need access, and have we instituted the right policies and controls? Have we adequately considered security gaps when rolling out new initiatives? Do we have a well-disciplined process to upgrade BES devices? This cannot be an optional task; vulnerability management must become routine and executed with careful change management controls and pre-tested configuration standards.

Engage in cyber information-sharing

Most major cyber attacks, as discussed, occur not as single events, but as strings of events over time. If viewed in isolation, it can be impossible to see a big picture attack "campaign." One of the leading ways to know what to look for, and to develop preemptive strategies, is to engage in information-sharing. This can include opening relationships with local law enforcement offices, participating in self-defined peer sharing, or joining sharing organizations such as the Electricity Sector Information and Analysis Center (ES-ISAC) or The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Evaluate your monitoring capabilities

Many organizations have disparate monitoring components that provide visibility into particular types of devices, but few have the capabilities that enable cross-domain visibility and correlation. It's important to also integrate physical and IT monitoring systems. Without a single pane of glass and the ability to correlate seemingly disconnected events and activities, important symptoms or patterns of threat activity may be entirely missed, before it's too late to prevent major damage.

Undertake internal education and cyber awareness-building

Technology-driven security controls are only part of the picture. People are most commonly the weak link that attackers exploit. The entire organization must be on its toes, watchful for suspicious activity, and mindful of their part in protecting the company and the services they deliver to the public. Cyber security must be demystified for business leaders who, ultimately, need to guide risk alignment, investments and response in times of crisis. Effective collaboration must be established across the corporate and operational sides of the business. A cyber-aware workforce takes time to develop, but the time to get started is now.

Rehearse your incident response plans

Nothing will educate leaders and stimulate cyber collaboration better than rehearsing your incident response plans and engaging in cyber war-gaming exercises. Most organizations have crisis response plans, but the scope may not be adequate for BES threats, or may segregate

[iii] See, for example, *The Verizon 2014 Data Breach Investigations Report* – Energy and Utilities, which notes that in 2013 the energy sector was hit by significantly greater numbers of web application attacks, crimeware, Denial-of-Service attacks, and cyber espionage than the all-industry averages. 38% of energy and utilities incidents were web application attacks, almost two-thirds of which were enacted by groups with an ideological agenda to disrupt, rather than to commit a financial crime.

the corporate and OT aspects. While IT and OT teams will be essential in the technical work of analyzing and stopping the bleeding, a business leader needs to be at the helm, able to engage other senior leaders to make business continuity decisions, and rapidly interact with the public, local government, safety organizations, the media, law enforcement, vendors, industry groups, and others. The rehearsal is not a one-time pass/fail event. It is an opportunity to identify and remediate weak areas, both human and technical.

While hopefully full-blown malicious attacks impacting the electric grid itself will be few and far between, the complexity of the technical and business environment, and the larger global climate, makes some form of cyber attack virtually inevitable. Today's organizations must strive for consistently and methodically applied security controls, but they must also become better at detecting threats in their early stages, and be as prepared as possible to respond effectively. It's not just about "security" anymore – it's about being ***secure, vigilant and resilient***.

Today's organizations must strive for consistently and methodically applied security controls, but they must also become better at detecting threats in their early stages, and be as prepared as possible to respond effectively.

For more information, please contact:

Ed Powers
National Managing Partner
Cyber Risk Services
Deloitte & Touche LLP
epowers@deloitte.com

Steve Livingston
Principal
Cyber Risk Services
Deloitte & Touche LLP
slivingston@deloitte.com

Sharon Chand
Director
Cyber Risk Services
Deloitte & Touche LLP
schand@deloitte.com

David Nowak
Senior Manager
Cyber Risk Services
Deloitte & Touche LLP
dnowak@deloitte.com

For further information, visit our website at www.deloitte.com

This piece is based on an article originally published in *Electricity Today Magazine*, available on the web at www.electricity-today.com