From compliance to risk management:
Defending against emerging cyber threats at power and utility companies

December 2011

At a glance

Standards have not kept pace with evolving cyber threats and can include sophisticated new malware that poses tremendous risk to operational IT systems

A risk management framework enables companies to proactively address cyber risks and avoid a reactive over-reliance on compliance

A comprehensive risk-based approach will put power and utility companies in a stronger position to ensure the security of operational systems

pwc

The American electric power industry has changed enormously over the past two decades. One area not keeping pace with this change is the mitigation of cyber security risks in operational IT environments, especially within control systems infrastructure. To help protect the integrity and reliability of the power system, companies have long separated their operational IT from commercial and administrative IT. The prevailing mindset is oriented to regulatory compliance rather than risk management. As consumer markets drive more real-time data and its associated interconnectivity, and cyber threats become ever more sophisticated, traditional approaches to cyber security in operational IT are becoming badly outdated.

Understanding the problem

History shows there are compelling reasons for separating operational IT from IT in the rest of the company. Achieving a reliable, continuous flow of power to a diverse and dispersed customer base requires sophisticated, highly specialized and isolated control systems. Operators have made sure to cloister such systems away from the commercial and corporate sides of the business—areas where flexibility and openness have become increasingly vital to efficient IT service.

At the same time, a long history of regulation, coupled with the continuous necessity of ensuring high reliability and safety, has led operations managers to focus on complying with regulatory mandates. This somewhat "check-the-box" approach has worked well for requirements such as vegetation management or preventing transmission path congestion. Yet cyber security does not lend itself well to this historical compliance-based approach.

Since the 1990s, deregulation has broken down formerly isolated and closed operations environments, requiring more system and network interconnections between the operational and the administrative side of the business. Industrial control systems now provide real-time information to other systems that they were not designed to provide. Unlike typical general purpose systems in administrative IT environments, control systems such as Supervisory Control and Data Acquisition (SCADA) and programmable logic controllers (PLC) are designed to interface with and control physical processes and equipment. These environments utilize both public and proprietary

purpose-built protocols to support distinct, engineered specifications for controlling equipment like generators, electric switches and protective relays.

Many of these protocols are not designed with security features and do not leverage security functions commonly found in administrative IT environments, such as network access control or device and user authentication. Other common security functions, such as vulnerability assessment tools for network firewalls, can disrupt or inhibit the high reliability and safety functions necessary in control environments, and must be implemented with extreme care.

Operational IT personnel have worked very hard to protect against many cyber threats, although awareness of threats and vulnerabilities taken for granted in administrative IT is somewhat low across the industry. Many have built layered defenses such as de-militarized zones (DMZs), which are protected regions between networks that by design do not trust each other. Some have also implemented protective monitoring technology such as intrusion detection and prevention systems. But these can be difficult to deploy effectively due to the unique nature of control system environments.

The Energy Policy Act of 2005 introduced new cyber security requirements onto the bulk power industry. Under this law, bulk power entities must comply with the Critical Infrastructure Protection (CIP) cyber standards issued by the North American Electric Reliability Corporation (NERC). Companies have become increasingly burdened with the time and expense of complying with these standards. Even so, the standards have not kept pace with evolving cyber threats, and they exclude some important cyber threat vectors altogether. Newer malware and other exploit techniques are so invasive and opportunistic that they cannot simply be engineered away through compliance rules.

The Federal Energy Regulatory Commission (FERC) issued Order 706 to address these limitations and others in the standards. FERC also urged NERC to consider adopting the risk management framework (RMF) issued by the National Institute of Standards and Technology (NIST), which is a thorough set of security controls and processes for reducing information and system risks across an organization.

The benefits of holistic cyber risk management

There's a better way to address cyber risks and avoid an over-reliance on compliance. Agencies in the Energy, Interior and Defense departments are already implementing the NIST RMF to reduce cyber risks and comply with a variety of information security regulations, while still complying with the NERC CIP standards. The NIST RMF is comprised of a series of Special Publications, Federal Information Processing Standards, and related guidelines. Some private power and utility companies have shown a growing interest in adopting the framework to manage their cyber risks holistically. Other frameworks gathering interest include the International Organization for Standardization (ISO) 27001, and ISACA COBIT.

Generally, adopting a RMF involves developing a thorough roadmap and capability metrics that the framework would support. In this way, companies can be sure to avoid gaps in their security capabilities and governance processes, while minimizing complexity and gaining the ability to define the level of residual risk that executives are willing to tolerate.

A major objective of a RMF is to identify risks remaining after making security investments, and also define a structure for formal acceptance of those residual risks. This risk-based approach recognizes the impossibility of preventing all possible security problems. Instead, such frameworks enable cost-effective, repeatable processes and continual vigilance to mitigate likely risks to the point where an organization can confidently go about its business.

Unlike compliance-focused approaches, a RMF establishes continuous monitoring and disciplined risk-reduction processes throughout an organization. An essential component is to identify and deploy common controls—key processes and mechanisms that have cross-organizational impact in mitigating security risks. RMFs also integrate physical and cyber security processes. By assessing the entirety of interconnected systems, for example, the processes highlight overlapping protections and shine a spotlight on weak spots, rather than passively relying on mandated protections alone that might not be effective.

Indeed, while NERC's CIP standards incorporate certain assumptions about cyber risk, these assumptions are not based on real-world assessments of the systems being protected. For example, the standards exclude communication links between what are known as electronic security perimeters, or boundaries, between two geographically separate locations. An entity can be fully compliant with the CIP standards and yet be vulnerable to cyber threats from the excluded links. A RMF such as NIST would automatically include all applicable communication circuits, connections and protocols as potential cyber threat vectors. Because of this more flexible and real-world approach, a RMF can enable power and utility companies to achieve both improved security and compliance at the same time—and add greatly to the integrity and reliability of the overall bulk electric power system.

The organizational challenge

The drivers for adopting a holistic, forward-looking risk management framework are only growing. Ongoing smart grid investments are intensifying the desire for increased connectivity between operational and administrative IT, further breaking down traditional barriers. Virtualization and the general move toward cloud computing, while bringing much-needed flexibility to IT, are adding to the risk. Today's power and utility CIOs are frequently being asked to ensure that cyber threats are addressed across their entire enterprise, and that means working with operations personnel to develop thorough risk mitigation strategies. Stuxnet and other highly advanced malware have awakened industry and governments to the threat of major disruptions to critical infrastructure control systems. Companies will find it harder to maintain a compliance-oriented approach to operational IT.

A number of sizeable power and utility companies are studying RMFs or beginning to implement them, but others aren't sure where to begin. In companies where the compliance mindset runs especially deep, managers may not even realize there could be a better way to address their cyber risks. Given the traditional bifurcation in IT and the sway of regulators, shifting from segregated compliance activities to integrated risk management is one with potential cultural and organizational impediments as well.

Operational and administrative IT professionals can learn much from each other. The latter have dealt with cyber threats for many years, and most of these personnel have extensive experience with risk management. At the same time, they have the opportunity to understand the highly specialized systems and networks that are the norm in operational IT environments. Some of the cyber mitigation methods common in administrative IT environments don't necessarily translate to operational environments. For example, control systems are very specialized and sensitive to communication anomalies. IT diagnostic tools, if not run carefully and tuned specifically for such equipment, can be highly disruptive and even cause physical damage and bodily harm.

By working together, operational and administrative IT personnel can implement a holistic RMF while effectively addressing their unique needs and capabilities. A RMF would allow a power or utility company to assess the impact of its corporate policies, standards and procedures within both contexts, and plan for any potential negative impacts they may cause.

For example, suppose a company mandated a single-laptop policy for all its employees. Under the compliance-based framework, such a company might merely require that its operations users take their annual compliance training. A RMF process, by contrast, would likely identify the risk of malware infection stemming from operations users having a single laptop for accessing both control system networks and administrative email and web browsing. The company could avoid this vulnerability by a policy exception for its operations staff to use separate laptops in each of these environments, even though it might require more capital investment. The trade-off of increased cost would come with reduced risk of enterprise network and system infection and loss of business revenue, customer service, or mission-critical capabilities.

Going forward

While the timing is better than ever for a shift toward RMFs, most companies will need a good amount of time to get there. They will want to move conservatively in order to maintain existing compliance with standards like NERC CIP. While RMFs are thorough, they can be introduced iteratively and in parallel with existing security and compliance measures.

For some power and utility companies, the CIO's office is the right place to spearhead such a move. Yet because of the numerous differences between operational and administrative IT, CIOs must proceed carefully. A CIO must be familiar with the unique characteristics of operational IT systems and networks and how those relate to cyber security. When operations management and the CIO develop a mutual understanding and trust, they will achieve a level of cooperation necessary to make this work. Each team will be an equal partner throughout the process and ultimately succeed.

There's no magic bullet for keeping our critical electric power assets secure against today's evolving cyber threats. But shifting toward thorough, risk-based approaches and away from compliance-driven security will put power and utility companies in a stronger and more sustainable position for dealing with tomorrow's cyber landscape.

www.pwc.com/us.utilities

PwC is a leading professional services organization, assisting power and utility clients with strategies for security policy, regulatory compliance, risk management, security architecture, control systems security, threat and vulnerability management, identity management and governance, and training and awareness programs. For a deeper discussion on these issues, please contact:

Brad Bauch
Power and utilities principal
(713) 356-4536
brad.bauch@us.pwc.com

Jon Stanford
Power and utilities director
(971) 544-4325
jon.stanford@us.pwc.com