

Getting real about cyber threats: where are you headed?

Energy, utilities and power generation companies that understand today's cyber threats will be in the best position to defeat them

June 2011

At a glance

As energy, utilities and power companies increase their use of innovative technologies such as smart grid, advanced metering infrastructure, and modern control systems, cyber threats and their associated risks grow.

The true cost of a security breach goes beyond initial data loss or service disruption. It can result in financial losses, intellectual property theft, fraud, diminished shareholder value, and reputational damage.

The mark of a mature cyber security program reflects the necessity of unceasing vigilance against the continuous threat of compromise.



Introduction

Nearly every reported incidence of cybercrime is motivated by financial gain or economic espionage. It could be hackers who are intent on selling compromised customer information or competitors looking to steal intellectual property, get inside intelligence on financial dealings, or gain details on sensitive internal operations. Regardless of motive, advanced cyber threat actors are organized, patient, and willing to make significant investments to accomplish their objectives. Threats are varied, often highly complex, and continually evolving. For these reasons, companies need to embrace a philosophy that recognizes the realities of today's cyber threats and protect their businesses accordingly.

So what's the problem?

It's an unfortunate condition seen all too often—had digital evidence and breach indicators been recognized at the time of an event, victims of cybercrime could have taken positive action and minimized their risk. Contrary to popular opinion, cybercrime is a risk to all industries and not just among companies dealing with payment cards or personal customer information.

Recent reports confirm that cyber attacks on several multinational energy companies resulted in security breaches long before the victims became aware that their systems had been compromised. In each case, it was a situation of not knowing until it was too late. Energy companies are targets because they possess valuable, proprietary data on reserves and discoveries, including intellectual property on how to access resources

and financial information about related transactions. According to published reports, state-sponsored foreign attackers have used highly sophisticated methods to compromise these types of targets.

Professionals who support cybercrime investigations have noted that energy, utilities and power generation companies share a concern that direct cyber attacks have the potential to disrupt or damage their business and critical information technology (IT) infrastructures. And for good reason. The nation's critical infrastructures, including those of the energy, utility and power generation industries, are of keen interest to various adversaries.

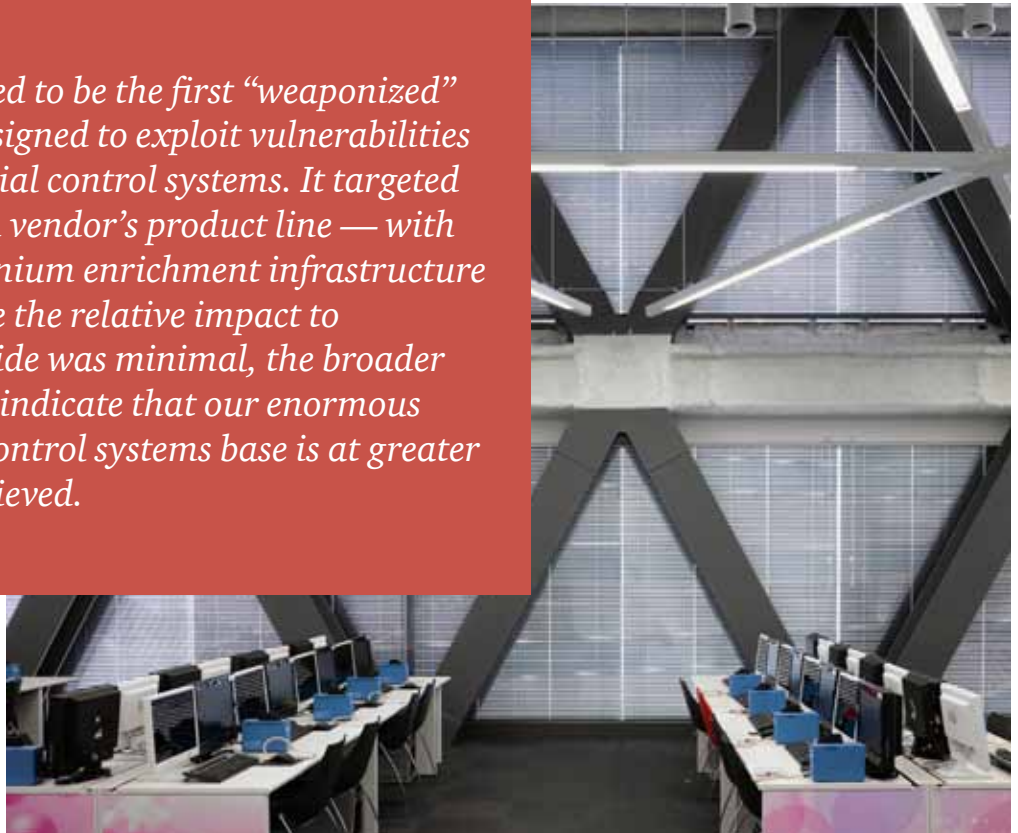
In light of the fact that smart grid systems collect valuable data about utilities and power customers, legacy privacy and security issues take on

a new and perplexing dimension. Computerized smart meters are typically connected to large networks needing protection with a rigorous suite of security protocols against malware infiltration, physical tampering, or data snooping. A security breach could result in unauthorized access to energy usage data or the corruption of smart meter settings, with the goal of disrupting power delivery to a single customer, neighborhood, or entire city.

To protect themselves and their customers, energy, utilities and power companies must adopt a fresh and modern cyber security philosophy—one accepting of the ongoing state of cybercrime and committed to appropriate levels of preparation and incident response capability.

Stuxnet

Stuxnet is widely believed to be the first “weaponized” malware specifically designed to exploit vulnerabilities in and sabotage industrial control systems. It targeted a specific control system vendor’s product line — with disruption of Iran’s uranium enrichment infrastructure likely its key goal. While the relative impact to control systems worldwide was minimal, the broader implications of Stuxnet indicate that our enormous critical infrastructure control systems base is at greater risk than previously believed.



Today's cyber threat landscape

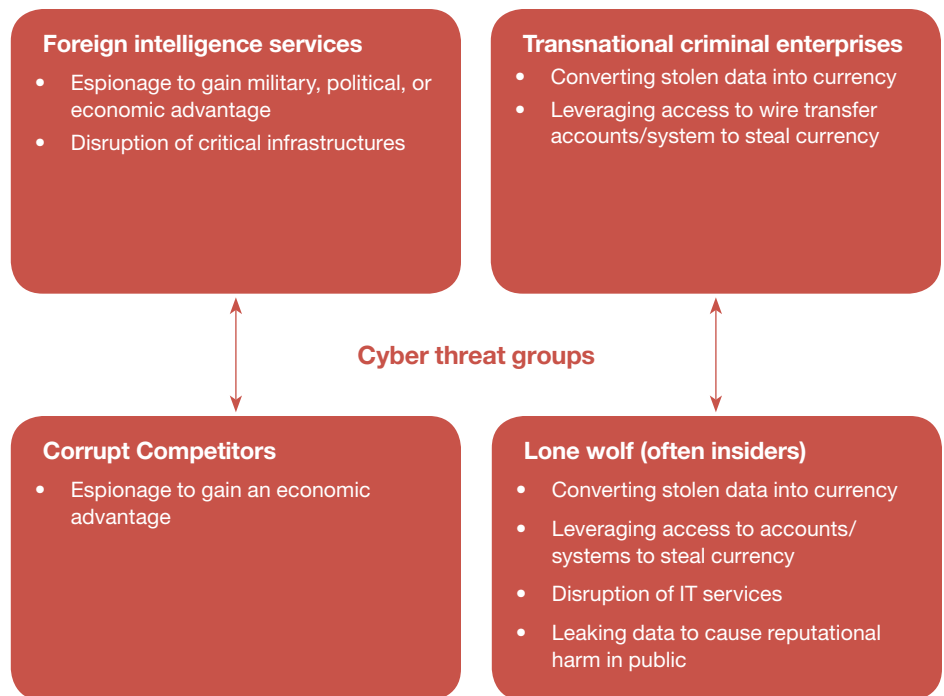
Why does a typical in-house cyber security program—people, processes, and technology—fail to detect the advanced threats that can lie in wait for months or years before executing their final stages of attack? The short answer is that most security programs are not organized to fully take such threats into account. They are mainly focused on threats that generate detectible and recognizable patterns, looking for signs of malicious intent. Today's cyber criminals are keenly aware of the typical defensive measures taken by most companies.

Cybercrimes are committed by a multitude of offenders with diverse motives:

- Trusted insiders who abuse their authorized access to enable a security breach
- Competitors seeking advantage
- Foreign governments committing espionage for military, political or economic gain
- Transnational criminal enterprises stealing and extorting to generate income

Today's advanced criminal techniques present a bigger challenge than monitoring for malicious code patterns or changes to system configurations with intrusion detection technology. The technical and intelligence capabilities of potential adversaries increase daily. Evidence shows that preventive and detective measures can effectively reduce risks pertaining to

Figure 1: Groups of cyber criminals



acceptable use policy violations and some types of computer and network intrusions, data loss/leakage, and asset sabotage. However, adversaries that target specific companies and industries are keenly aware of these limitations and have developed sophisticated methods to exploit both human and technological weaknesses.

Many of these adversaries operate among highly organized, global groups and underground networks. They are often categorized as “transnational criminal enterprises” with a pure profit motive, and are patient, persistent, and extremely determined.

The intelligence services of foreign governments are the most sophisticated, organized, and well-funded. These entities steal commercial intellectual property (IP) and business transaction data to gain an economic advantage and abscond with classified government information to gain military or political advantage. Establishing and maintaining unauthorized remote access for as long as possible is a primary objective of state-sponsored groups in order to execute future malicious actions.

Historical perspective

Many of the security technology investments made over the past decade can help combat cybercrime, but only if companies have the right technical knowledge and experience to use them. A cursory review of recent cyber security history illustrates the need to tighten security by increasing the awareness, use, and capabilities of technological security applications. Energy, utilities and power companies need people with experience investigating advanced cyber intrusions that can also employ the right technology to enable advanced warnings of security breaches. This experience should address threats against smart grid components and networks, industrial and process control systems infrastructure, nuclear facilities, and also take highly sophisticated attacks like the Stuxnet malware into account.

Figure 2 outlines the evolution of technology and threat response capability during the previous decade.

Figure 2: Cybercrime evolution 2000-2010



Recognizing breach indicators

Cyber security breaches characterized by undetected intrusions may include the following types of event indicators.

- Unauthorized web pages posted on an Internet-facing web server
- Outbound data transmissions using unknown, unauthorized, or unlikely protocols or ports
- Outbound transmission of large compressed files
- Unusual connections between user systems using native operating system networking features
- Log entries on domain controllers indicating the execution of unauthorized programs

Based on real-world cases at organizations experiencing a cyber intrusion, indicators such as these were typically available for days, months, or in some cases, even years. To best protect your own company, you must become familiar with these and

other types of breach indicators. Your company should be able to determine whether systems either have been or are actively being compromised through methods such as network- or media-based data ex-filtration or e-mail.

Post-event cybercrime investigations can help improve your operational cyber security posture and reduce related organizational risks. When our clients engage us to apply the mindset of the cyber criminal and use our world-class cybercrime investigation methods, we have found that, on average, 3% to 5% of the client's computer systems are compromised.

Incident recovery and initial steps toward an improved cyber program

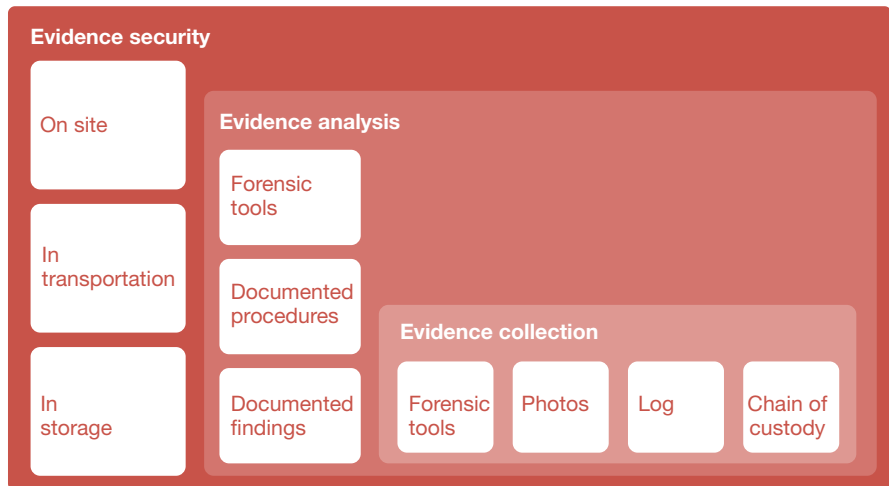
Recognizing the importance of our clients' business operations and that of their partners, we recommend they adopt a mature and innovative response capability that reflects the continuous threat of compromise.

As security issues are identified and resolved during an investigation, an independent and objective security assessment should be conducted to confirm successful remediation.

After an incident is contained and security remediation has begun, a formal review of the incident response effort should be conducted to assess the team's performance. Results of this review can be used to strengthen training and improve responses.

The major functional activities and areas for assessment are outlined in Figure 3.

Figure 3: Functional activities and areas for assessment



Characteristics of a mature cyber security program

Mature cyber security programs are typically marked by several complementary elements, including security management, operations, and architecture; regular testing for compliance with regulations; established policies and procedures; privacy; education and awareness; identity and access management; threat and vulnerability management; physical security; and incident response.

In addition to virus detection, intrusion detection, and prevention technologies, application “white listing” should be implemented on critical computer systems. White listing provides a mechanism such that only software known to be safe is allowed to run on systems—all others are blocked by default. This is an effective way to prevent the introduction of new viruses and malware.

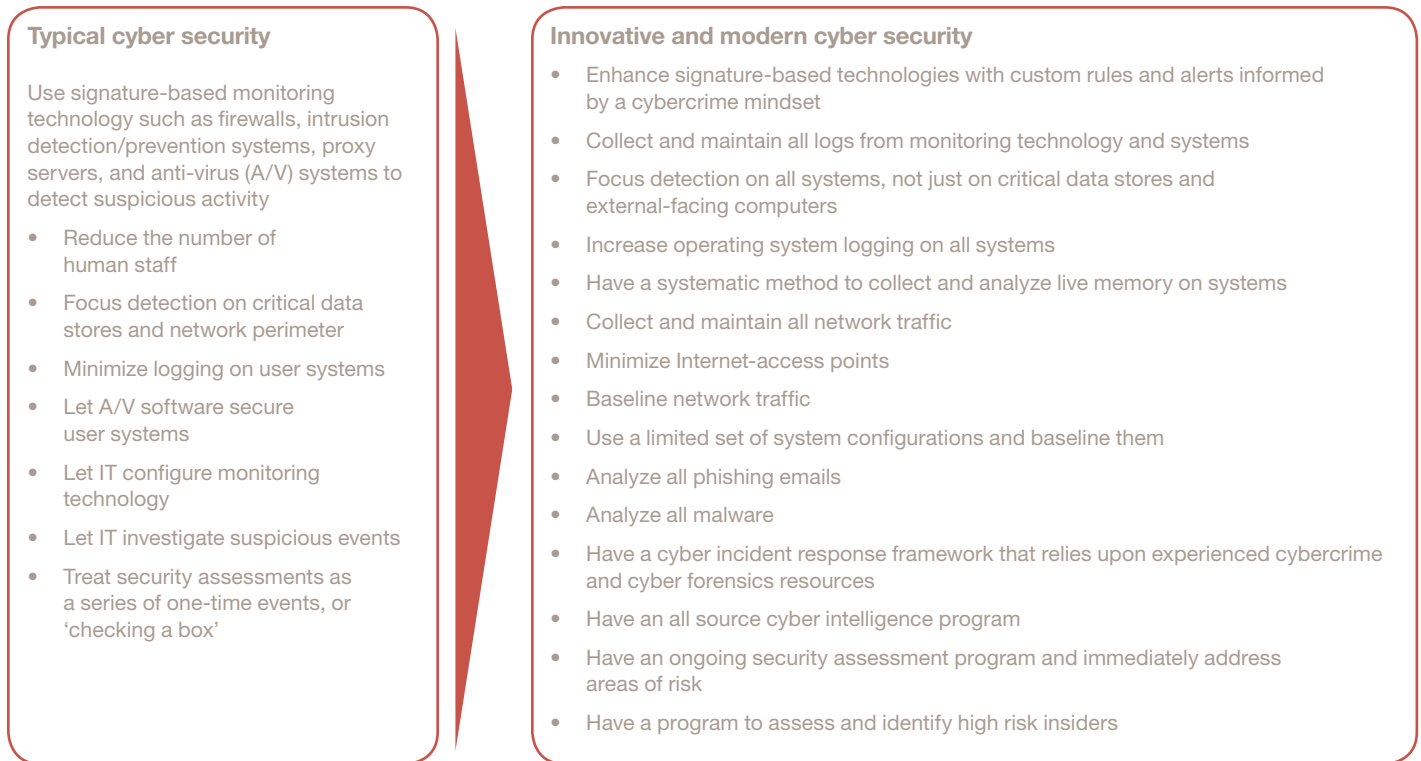
Regardless of an organization’s perception of the strength of its control environments, it should consider performing tailored forensic analysis procedures on the network and key servers to determine whether there is

evidence that a breach has occurred. This process is more difficult to accomplish because of the nature of today’s advanced threats. The signatures that companies would be looking for are not in the public domain, and the attacks are often company-specific, so commercial software such as virus protection or intrusion detection systems will not identify these programs or the existence of a breach.

Companies will need to team with a service provider that has in-depth experience responding to such threats. The network traffic analysis is relatively nonintrusive; however, assessing a system may require a full forensic image of the server. Due to the real-time and always-available nature of these systems, acquiring these images requires careful coordination and a skilled project team.

Even mature cyber security programs can benefit from a fresh cyber security perspective to improve the security of data and the IT infrastructures that contain it. This includes the recognition that there are no

Figure 4: Key characteristics of legacy and innovative cyber security programs



technological silver bullets. Rather, the approach assumes an active and perpetual state of compromise, seizes all opportunities to gather cyber threat intelligence, transforms the IT environment into a treasure trove of digital evidence, assesses the state of security of its interconnected vendors, recognizes the authorized insider as a cyber threat, has a forensic incident response capability, and understands and overlays business operations needs—all in an effort to fuel an enhanced state of cyber security.

Figure 4 outlines key characteristics of legacy and innovative cyber security programs.

As we have seen, cyber criminals are continuously evolving their techniques to access sensitive information and maintain unauthorized access to systems and networks for as long as they possibly can. Cyber threat actors are fully committed to understanding your company's IT or operations environment to achieve their malicious objectives. Companies wanting to better protect themselves and their stakeholders from advanced cyber threats need to adopt a new cyber security philosophy that acknowledges the realities of cybercrime and features the flexibility needed to meet changing security demands for years to come.

.....
:
***For a deeper discussion of these issues,
please contact:***

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

Shane Sims
Advisory forensics services director
(703) 918- 6219
shane.sims@us.pwc.com

Jon Stanford
Energy and utilities and power generation director
(971) 544-4325
jonathan.k.stanford@us.pwc.com

Less Stoltenberg
Energy and utilities and power generation director
(713) 356-4469
less.j.stoltenberg@us.pwc.com