


Insights on IT risk  
Technical briefing  
January 2012



# Bringing IT into the fold

## Lessons in enhancing industrial control system security



# Executive summary

Power and utility companies, as well as other enterprises with industrial operations, such as oil and gas and many manufacturing companies, are facing increasing risk of cyber attacks as they converge their real-time operational technology (OT) environments with their enterprise information technology (IT) environments.

Because companies need improved visibility into process and control information, as well as better data collection and distribution capabilities, their OT environments are increasingly adopting standard IT technologies, including connectivity to enterprise IT networks and the internet. Leveraging standard IT technologies rather than the closed protocols and software allows for this increased data exchange; however, as a result, the OT environment is now exposed to threats and vulnerabilities that it often is not sufficiently prepared to handle. Beyond the IT network, initiatives such as the smart grid and advanced metering technology are further complicating the threat and vulnerability landscape now being encountered.

To address the risks of a more cyber-exposed OT environment, companies need to undertake a reasonable level of due diligence to gain assurance that they are appropriately protected. As a minimum, they should protect the OT environment in a manner that is on a par with the resources invested to protect the enterprise IT environment, and in many cases, the criticality of the OT environment warrants even greater investment. The convergence of OT and IT environments dictates the need for a more thorough approach to OT security designed to prevent attackers, both external or internal. Specifically, it needs to protect against such issues as malware that is able to penetrate the perimeter and improve its capability to detect and respond to security incidents.

Although the concepts of least privilege and limiting access seem to oppose the key OT environment objectives of accessibility and availability, the traditional perimeter-based, "security through obscurity" posture needs to give way to practices that embrace the principle of defense in depth, which traditionally has been viewed as a contradiction to leading practices in the OT community.

It's time for companies to adjust their cybersecurity strategies to defend against the risks associated with a rapidly evolving OT environment that is increasingly vulnerable to potentially disruptive cyber attacks.

The following recommendations will help build a foundation for an enhanced cybersecurity program:

1. Co-develop and implement an ICS cybersecurity program that focuses on identified risks – not just regulatory compliance
2. Build a cross-functional cybersecurity team to develop and manage the cybersecurity program
3. Create and maintain an OT environment asset inventory
4. Develop security policies and standards specific to ICS devices and IT systems connected to the OT environment
5. Understand and validate all connection points between the IT and OT environments
6. Use predictive threat modeling driven by the OT environment asset inventory to identify and assess threats and vulnerabilities
7. Apply controls or countermeasures to complicate an attacker's ability to achieve their objectives, detect their activity and effectively respond to discovered attacks
8. Perform production systems and network security reviews of the OT environment, including penetration tests
9. Consider ICS security requirements in the vendor management process
10. Develop and implement training and awareness programs that link safety and availability with good cybersecurity practices



## Introduction

OT networks containing industrial control systems (ICS) – supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and programmable logic controllers (PLC) – have traditionally operated in isolated or “air gapped” networks using proprietary hardware, software and communication protocols. The OT environment’s proprietary and isolated nature has historically been its primary means of protection against the cyber attacks that have plagued enterprise IT environments for years. However, business demands for improved input into process and controls, visibility of process and control information and the need for better data collection and distribution capabilities are challenging the continued effectiveness of this “security through obscurity” posture.

Electric utility companies are leading this movement for improved visibility with their transition to smart grid technology and advanced metering infrastructure (AMI). Although these advances offer many benefits for the utilities, their customers and the natural environment, they also increase the risk of cyber attack. As OT environments become more interconnected with enterprise IT networks, they create additional access vectors and greater exposure to internet-based threats. In addition, OT environments are moving beyond their proprietary models. As they adopt standard commercial off-the-shelf (COTS) hardware and IT technologies such as Windows- and Red Hat Linux-based operating systems, web services, ethernet, Wi-Fi, Bluetooth and TCP/IP, their risk grows.

## Threats and vulnerabilities

The evolution of the OT environment exposes it to threats and vulnerabilities – some new and specific to OT and others that are similar to the IT environment.

The growing prevalence of standard IT technologies in OT environments, coupled with the increase in access vectors, provides attackers with the opportunity to exploit well-known vulnerabilities – “low-hanging fruit.” For example, operator workstations running Windows in the OT environment often are not hardened as they would be in the enterprise IT network, making them highly susceptible to viruses, worms or other attacks. These Windows systems are often logically and physically segmented off from the rest of the enterprise network but they still present attack vectors, such as use of a USB flash drive, to introduce malware. This was believed to be the method used for introduction of the Stuxnet malware.

COTS components, such as Windows workstations and servers within or connected to the OT environment, are not the only devices at risk. ICS system vulnerabilities are well established and documented and it is reasonable to assume that malicious actors are aware of these vulnerabilities and the opportunity they present. Recent headline-grabbing events, such as Stuxnet and the publishing of security flaws in the Kingview software prevalent in China’s critical infrastructure, raise awareness of the opportunities available to exploit vulnerabilities in the OT environment. In addition, security industry conventions such as Black Hat and DEF CON include SCADA vulnerability presentations, further eroding the technical barrier to entry into ICS device vulnerability exploitation.

Threats can originate from malicious insiders as well as external people, ranging from organized crime, nation states and terrorist organizations targeting a nation’s critical infrastructure to the individual hacker with an agenda. Legitimate threats are not limited to sophisticated attackers using advanced techniques. Free web-based tools can be used to discover internet-facing SCADA devices and the Agora SCADA+ add-on for the canvas penetration testing framework can identify and exploit vulnerabilities in discovered SCADA devices. Such tools can make even an amateur, opportunistic attacker a real threat.

### A malware first

Stuxnet is a Windows computer worm discovered in July 2010 that targets industrial software and equipment. While it is not the first time that hackers have targeted industrial systems, it is the first discovered malware that spies on and subverts industrial systems, as well as the first to include a PLC rootkit.

The worm initially spreads indiscriminately, but it includes a highly specialized malware payload that was designed to target only Siemens SCADA systems that are configured to control and monitor specific industrial processes. Stuxnet infected PLCs by subverting the Step-7 software application that is used to reprogram these devices.



## Challenges to secure the OT environment

The reality of the threat and vulnerability landscape is further complicated by both the technical and cultural challenges to secure the OT environment.

OT environments can contain a mix of specialized software running on standard computers and control systems with custom-built operating systems. ICS devices, especially legacy systems, were not

designed to operate in untrusted environments and therefore lack the security features more common to IT systems. ICS devices, such as field instrumentation and control systems, often have proprietary operating systems and limited computing resources available to accept traditional IT security countermeasures such as anti-virus software, intrusion detection and prevention systems (IDS and IPS), patching or vulnerability scanning to compensate for their lack of inherent security features. Table 1 below demonstrates some of the characteristics of ICS devices that increase the challenge in securing the environment.

**Table 1: Unique characteristics of ICS devices that increase the challenge in securing the environment**

Security topic	Information technology (IT)	Industrial control systems (ICS)
Antivirus and mobile code	Very common; easily deployed and updated	Can be very difficult due to impact on ICS; legacy systems cannot be fixed
Patch management	Easily defined, enterprise-wide remote and automated	Very long runway to successful patch install; OEM-specific, may impact performance
Technology support lifetime (outsourcing)	2-3 years, multiple vendors; ubiquitous upgrades	10-20 years, same vendors
Cybersecurity testing and audit (methods)	Use modern methods	Testing has to be tuned to system; modern methods inappropriate for ICS; fragile equipment breaks
Change management	Regular and scheduled; aligned with minimum-use periods	Strategic scheduling; nontrivial process due to impact
Asset classification	Common practice and done annually; results drive cybersecurity expenditure	Only performed when obligated, critical asset protection associated with budget costs
Incident response and forensics	Easily developed and deployed, some regulatory requirements, embedded in technology	Uncommon beyond system resumption activities; no forensics beyond event re-creation
Physical and environment security	Poor (office systems) to excellent (critical operating systems)	Excellent (operations centers, guards, gates, guns)
Secure systems development	Integral part of development process	Usually not an integral part of systems development
Security compliance	Limited regulatory oversight	Specific regulatory guidance (some sectors)

Source: "Improving ICS Security with Defense in Depth Strategies," National Institute of Standards and Technology, October 2009.

Standard IT technology is subject to public scrutiny and vulnerabilities are identified on a daily basis. One of the key foundations of a security program for IT environments is a routine patch management process that occurs frequently (i.e., at least once a month). However, the disproportionate need for availability and accessibility of OT networks compared to traditional IT networks, coupled with the mix of proprietary software and specialized operating conditions, complicates the process of patching vulnerable software.

Security patches for IT technology, such as the Windows operating system, are not designed to account for special operating environments like OT networks. As a result, OT technology vendors often need to adapt security patches released by IT technology vendors to their proprietary software. This introduces an additional layer of complexity and delay to the patch management process, leaving OT network administrators at the mercy of the vendors, awaiting the release of OT-specific patches in a timely manner.

Cultural challenges are another factor. OT networks traditionally are managed by operators and engineers rather than someone with an IT or information security background. As these individuals are trained to focus on safety and operating efficiency, cybersecurity awareness is often secondary – it is not linked to its role in maintaining safety and process operation effectiveness. This culture of safety and operating efficiency often prioritizes redundant access over the security concept of least privilege. For example, it is not uncommon for a single user to have administrator privileges on every machine in the OT environment. And when personnel change roles within the organization or leave it entirely, their accounts may not be subjected to typical IT procedures, such as adjustment of permissions or disabling of accounts.

In addition, a focus on compliance (e.g., NERC CIP or non-US equivalent) for companies in the critical infrastructure sector often trumps a more comprehensive, risk-based approach to the design and implementation of effective cybersecurity controls. However, the impetus to implement effective cybersecurity should be most evident in organizations that manage critical infrastructure where the ramifications can put health and human safety at risk.

## Smart grid considerations

Smart grid advances are a significant driving force in the transformation of the ICS environment. Key considerations related to smart grid include:

- ▶ Increasing complexity could introduce vulnerabilities and increase exposure to potential attackers and unintentional errors.
- ▶ Removing physical or logical borders between network segments increases impact and potential propagation of malware or other attacks.
- ▶ Interconnection of ICS and enterprise networks introduces common IT vulnerabilities to the ICS environment.
- ▶ Introduction of malicious software or firmware or compromised hardware could result in denial of service (DoS) or other attacks.
- ▶ Increased number of entry points and paths are available for potential adversaries to exploit.
- ▶ Increased use of, and rapid implementation of, new technologies can introduce vulnerabilities.
- ▶ Expansion of the amount of data that will be collected can lead to the potential for compromise of data confidentiality, including the breach of customer privacy.
- ▶ Implementation of wireless technology in an AMI may permit undetectable interception of wireless traffic.



## Recommendations

Within the US, existing publications such as NIST 800-52 and 800-53 provide guidance on specific controls that can improve OT environment security. However, detailed risk mitigation activities and controls should be chosen based on the results of a thorough risk assessment and their ability to mitigate risks specific to each organization. The following recommendations can provide a solid foundation for a cybersecurity strategy within an OT environment.

### 1

#### Co-develop and implement an ICS cybersecurity program that focuses on identified risks – not just regulatory compliance

To address this evolving threat and vulnerability landscape, organizations should develop a formal cybersecurity program that applies defense-in-depth principles. The cybersecurity strategy should include short-term, mid-term and long-term goals aimed at transforming the security posture of the OT environment. Companies need to do more than aim to achieve compliance, especially with regulations that are more focused on documentation and ideas of “electronic security perimeters” that are becoming more and more blurred in today’s increasingly borderless world.

At the program level, progress should be monitored and reported to executive management and, as much as possible, to an independent governing body like the audit committee. The program must be based on a sound business case that effectively addresses common misconceptions of ICS security – security based on obscurity and OT environment isolation. Risk analysis processes also should be reviewed to make sure there is an appropriate balance or weighting of likelihood and impact given the potentially devastating nature of ICS incidents.

Given the complex nature and high availability demands of OT networks, implementing an extensive defense-in-depth strategy may take years to achieve. Companies should develop a risk-based strategy that provides a road map and framework for prioritizing and addressing existing challenges while also providing a mechanism for building security into future initiatives. As with any initiative, especially those that have a transformational impact, it is imperative to obtain executive support for the program’s establishment and ongoing activities.

### 2

#### Build a cross-functional cybersecurity team to develop and manage the cybersecurity program

An effective cybersecurity program will require collaborative relationships between IT, Information Security and OT to be successful, so any existing silos within these organizations must be addressed.

While IT and Information Security can bring their experience and understanding of threat and vulnerability management, as well as their technical expertise, a thorough understanding of the ICS environment is also required. A cybersecurity team should include individuals from several areas of the business such as executive leadership, IT and Information Security, ICS operators, OT engineers and Physical Security, as well as trusted external advisors (e.g., vendors).

When building a cybersecurity team, the following guidelines should also be considered:

- ▶ The cybersecurity team should not be tasked with leading a compliance program (e.g., NERC CIP).
- ▶ While the team should be cross-functional, members of the cybersecurity team should be cross-trained in information security and OT networks and devices.
- ▶ Roles and responsibilities that provide clear direction and accountability should be defined.
- ▶ A cybersecurity council should be formed, consisting of cross-functional leaders with oversight responsibilities to foster enterprise accountability for the cybersecurity program.

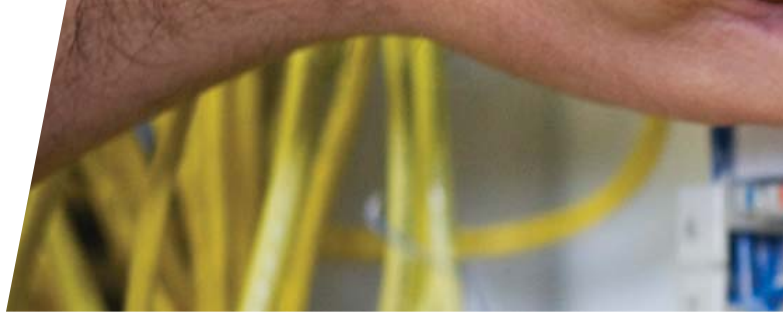
### 3

#### Create and maintain an OT environment asset inventory

By nature, ICS environments are disparate and consist of multiple device types. Maintaining an accurate inventory of technologies in place is an important first step in securing the OT environment. A thorough asset inventory should include:

- ▶ **ICS devices** – hardware, software, firmware, vendor
- ▶ **IT platforms** – operating system type (e.g., Windows, Linux) version, service pack level, host names
- ▶ **Communication mechanisms** – remote access vectors (e.g., RDP, Wi-Fi, Bluetooth), network accessibility (e.g., connected to corporate network, internet, air gapped).

An OT asset inventory management process should include roles and responsibilities for updating the inventory as changes are made and for periodically reviewing the inventory for accuracy and completeness.



## **4** Develop security policies and standards specific to ICS devices and IT systems connected to the OT environment

While OT environments are changing to look more and more like traditional IT environments, they continue to have their own characteristics and requirements that need to be considered when developing policies and standards. It's important to develop security policies and standards specific to ICS devices and those IT systems that connect to the OT environment. If an OT environment's requirements make it impossible to implement certain technical controls, compensating controls should be identified.

When creating ICS-specific policies and standards, it is important to address identified risks. Existing standards, like NIST 800-52, provide guidance on how common controls can be tailored to an ICS device. Security recommendations in ICS vendor documentation can also serve as input into ICS-specific policies and standards.

## **5** Understand and validate all connection points between the IT and OT environments

Securing the OT network traditionally has relied on a strict demarcation or boundary between the OT environment and the IT environment. But this boundary is becoming harder to define, due to the increasing use of traditional IT platforms and protocols; wireless technology, including portable and mobile devices; and smart grid advances. Moreover, advanced metering technologies now provide users the ability to take actions such as remote shutoff that directly affect distribution activities.

As a result of this transformation, it is critical to develop a process that allows you to identify and maintain a complete and accurate understanding of all entry points to the OT environment. Consider how business partners and vendors access the OT environment, how information is transferred between the OT and IT environments (e.g., SAP), what exposure the OT environment has to the internet and how field workers connect mobile devices.

After these connection points are identified, the OT environment must be segmented sufficiently from other internal and external networks. Unfortunately, segmentation is often not as effective as companies perceive it to be. The effectiveness of the OT boundary security should be tested periodically, and additional controls should be implemented when needed to achieve the necessary level of segmentation.

## **6** Use predictive threat modeling driven by the OT environment asset inventory to identify and assess threats and vulnerabilities

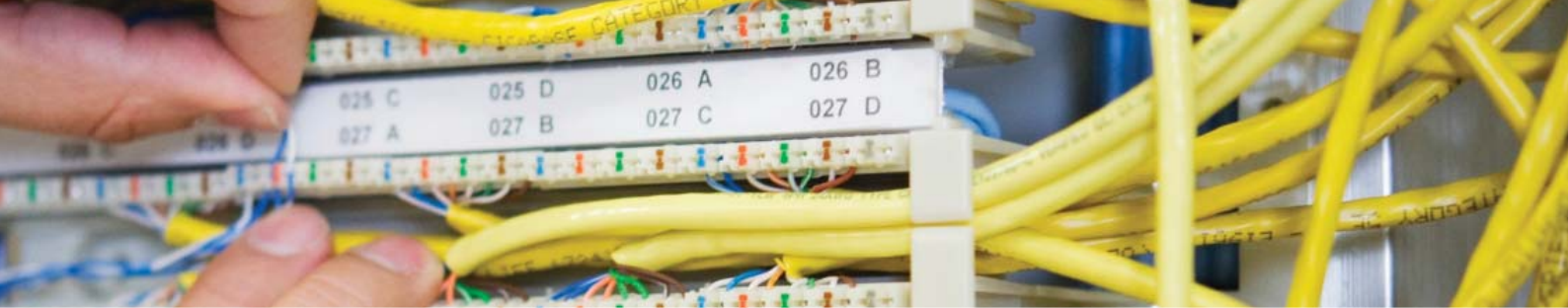
Knowing the threats and vulnerabilities for relevant technologies is critical to securing the OT environment. One approach to accomplishing this objective is to use predictive threat modeling as part of a formal threat and vulnerability management framework that accounts for the uniqueness of an ICS environment. Predictive threat modeling is most effective when a cross-functional team applies a business and operational process-driven view to define threats and create a prioritized remediation road map.

A broader risk framework should be implemented to rank the risk of each item in the asset inventory to known threats and vulnerabilities. Individuals should monitor emerging threats to the ICS environment, including understanding the results of controlled lab tests and real-world events and their applicability to each company's OT environment. The cybersecurity team should be regularly updated on threats and vulnerabilities and report on the company's posture to senior management.

## **7** Apply controls or countermeasures to complicate an attacker's ability to achieve their objectives, detect their activity and effectively respond to discovered attacks

The threat and vulnerability management program should feed into prioritized and proactive device hardening activities across the OT environment based on a device's criticality to production, its pervasiveness on the network and the ease or extent of real-world exploit potential. When evaluating controls or countermeasures to implement, generally accepted IT security system hardening techniques should be considered where standard IT platforms are in use (e.g., Windows operator workstations and servers, Windows-based PLC supervisory systems). A control strategy should include a multi-layered approach designed to complicate an attackers' ability to achieve their objectives and detect mechanisms (people, process, technology) that will alert an incident response team to effectively respond to the attacks.

Controls that result in configuration or architecture changes should only be implemented after extensive testing in a non-production environment followed by a closely monitored, gradual deployment to production. Above all, controls should not put an environment at greater risk than the threat they are intended to prevent or detect. However, countermeasures should be restrained only if careful analysis and testing finds that the measure will negatively affect the availability or integrity of process control activities. Where technical measures cannot be implemented, organizations should consider compensating controls that will allow for better management of the identified risks.



## 8 Perform production systems and networks security reviews of the OT environment, including penetration tests

Once controls and countermeasures have been put in place, the OT environment should be assessed as a whole to validate that the implementation was performed correctly and that no gaps exist between controls. In addition to performing the assessment directly in the OT environment, it is important to identify access paths into the OT, which could include direct contact with the internet, dial-up or wireless access and connections to the corporate network. Penetration testing helps to identify such gaps and demonstrate their impact on the entire environment. This all-inclusive perspective differentiates penetration testing from vulnerability assessments and can help illustrate how devices unrelated to the OT network can lead to compromise of OT assets.

In contrast, vulnerability assessments are vital in detecting specific vulnerabilities in operating systems and software. They play an important role in patch management of individual systems but they fall short of providing insight into what would happen if the vulnerabilities identified were exploited by an attacker. Penetration testing leverages the additional access gained by exploiting the vulnerabilities to progress deeper into the environment and determine the overall impact. This approach most effectively determines to what extent the OT environment adheres to defense-in-depth principles and where there may be weaknesses that are not evident on the surface. Given the high availability requirements for systems in an OT environment and the potential impact of a service disruption, testing must be planned and managed carefully. It is critical to use a highly experienced team to conduct penetration testing that could potentially access critical components within the OT environment. Where the risks of penetration testing, even when using a highly experienced team, outweigh the benefits, other mechanisms for performing a thorough and holistic assessment of the production OT environment should be identified. These alternative assessment options should be used for an interim period while protocols for reducing the risk of performing penetration testing are explored.

The broad perspective of a penetration test will also help to quantify the risks identified during the risk analysis. The end result of a complete attack path to an established target can provide evidence of whether a particular vulnerability, for example, causes temporary disruption on a noncritical system or enables an attacker to gain access that eventually leads to the “keys to the kingdom.”

## 9 Consider ICS security requirements in the vendor management process

Vendors play a critical role in securing control systems. As ICS equipment can potentially remain in production for much longer than traditional IT systems, it is even more critical to address security as new equipment is deployed. For example, new equipment purchases and upgrades to support strategic initiatives such as smart grid provide an opportunity to incorporate security considerations into the procurement processes.

The cybersecurity team needs to be involved in the procurement process for ICS equipment so that security expectations can be included within contracts and associated service level agreements. The cybersecurity team should also assess the vendor and its product against the established ICS security policies and standards. In addition, the cybersecurity team should establish processes for managing vendor access. Processes for granting access according to the least-privilege principle, along with processes for removing access when vendor employees no longer require it, are important areas to consider.

An effective vendor management program should also include understanding and evaluating how vendors manage security risks when their network or end points (e.g., laptops, mobile devices) are connected to your environment. Security expectations should be communicated to the vendors and, over time, incorporated into service level agreements.

## 10 Develop and implement training and awareness programs that link safety and availability with good cybersecurity practices

ICS cybersecurity should be viewed as an enabler of the “safety first” and availability goals of an OT environment. A training and awareness program should aim to make those responsible for ICS aware of the changing risk profile within OT environments. The program also should be leveraged to expose IT and Information Security personnel to the particular requirements of an OT environment. Both actual and thwarted incidents should be used to communicate lessons learned that reinforce good behavior and discourage undesirable behavior.

Training and awareness should be required as part of orientation and updated periodically. In addition to these formal training events, targeted awareness campaigns should be conducted as necessary and should include practical tips on appropriate responses to real-life scenarios, especially in areas where technical controls cannot be enforced and risk mitigation relies primarily on sound user judgment.

**Table 2: Repercussions from ineffective cybersecurity practices in OT environments**

Event	Location	Impact
Gasoline pipeline failure exacerbated by control systems not able to perform control and monitoring functions	North America	Three fatalities, total property damage > US\$45m
Sewage spill caused by wireless hacking of sewage discharge valves	Australia	> 1m liters of sewage spilled
Substation communication failure from Slammer work traffic	North America	SCADA failed, resulting in loss of control
Targeted SCADA hack from internet	North America	No SCADA servers for two weeks; no mapping system for two weeks; four man-months to recover
Control center communication failure from unpatched Cisco router by worm	Europe	Loss of communication to almost half of the distribution substations for almost three days; inability to diagnose for 24 hours; approximately 40 man-weeks to clean up
Aurora experiment at the Idaho National Laboratory demonstrated a large diesel generator malfunctioning due to a remote attack	North America	Remote destruction of a large diesel generator
Control system workstation failures caused by IT penetration testing	North America	Slowdown or shutdown of all power plant control system workstations
Loss of power plant control from hackers	North America	For a brief period of time, a hacker played with the level control on a deaerator control system
Stuxnet attack targeting Siemens SCADA systems resulting in significant setbacks to the Iran nuclear program	Iran	Damage to the controllers handling the centrifuges at Iran's Natanz facilities

Source: Joseph Weiss, *Protecting Industrial Control Systems from Electronic Threats*, page 145.

# Conclusion

The dynamic nature of cybersecurity and the rapidly changing OT environment continue to reshape the threat and vulnerability landscape. A coordinated, strategic response that addresses this new reality demonstrates responsible risk management. However, developing a mature, multi-layer defense that effectively leverages both preventive and detective countermeasures takes time and resources. As such, the cybersecurity program's success and continued effectiveness will rely heavily on strong executive leadership.

The impetus for a comprehensive approach to OT security need not be based on fear, uncertainty and doubt – what the IT world calls "FUD." Real-world incidents, the increase in attack vectors and vulnerabilities resulting from the convergence of IT and OT, along with the growing sophistication of ICS-targeted malware and threat actors, legitimize cybersecurity in the OT environment. The potential impact of cyber attack, particularly in the critical infrastructure sector, is too great to continue to rely on a static security strategy based on a strong perimeter defense and the proprietary nature of ICS devices and networks. It's time to adopt the lessons of the IT world and develop a defense-in-depth strategy that better protects the OT environment – while acknowledging its distinct issues.

**Table 3: Potential ineffective cybersecurity ramifications for critical infrastructure companies**

Impacts	IT environments	OT environments
Revenue and profitability	▲	▲
Reputation	▲	▲
Regulatory and fines	▲	▲
Health and human safety		▲
Environmental damage		▲
National security		▲



**About Ernst & Young**

Ernst & Young is a global leader in assurance, tax, transaction and advisory services.

Worldwide, our 152,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity.

Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit [www.ey.com](http://www.ey.com).

**About Ernst & Young's Advisory Services**

The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 20,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and superior client experience. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential as an organization you require services that respond to your specific issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.

© 2012 EYGM Limited.  
All Rights Reserved.

EYG no. AU1077



In line with Ernst & Young's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

# How Ernst & Young makes a difference

**At Ernst & Young, our services focus on our individual clients' specific business needs and issues because we recognize that each is unique to that business.**

IT is a key to allowing modern organizations to compete. It offers the opportunity to become closer to customers and more focused and faster in responses, and can redefine both the effectiveness and efficiency of operations. But as opportunity grows, so does risk. Effective ITRM helps you to improve the competitive advantage of your IT operations, by making these operations more cost efficient and managing down the risks related to running your systems. Our 6,000 IT risk professionals draw on extensive personal experience to give you fresh perspectives and open, objective advice – wherever you are in the world. We work with you to develop an integrated, holistic approach to your IT risk or to deal with a specific risk and information security issue. We understand that to achieve your potential you need tailored services as much as consistent methodologies. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

For more information on how we can make a difference in your organization, contact your local Ernst & Young professional or a member of our team listed below.

## Contacts

### Global

<b>Norman Lonergan</b> (Advisory Services Leader, London)	+44 20 7980 0596	<a href="mailto:norman.lonergan@uk.ey.com">norman.lonergan@uk.ey.com</a>
--	------------------	--

<b>Paul van Kessel</b> (IT Risk and Assurance Services Leader, Amsterdam)	+31 88 40 71271	<a href="mailto:paul.van.kessel@nl.ey.com">paul.van.kessel@nl.ey.com</a>
--	-----------------	--

### Advisory Services

<b>Robert Patton</b> (Americas Leader, Atlanta)	+1 404 817 5579	<a href="mailto:robert.patton@ey.com">robert.patton@ey.com</a>
--	-----------------	--

<b>Andrew Embury</b> (Europe, Middle East, India and Africa Leader, London)	+44 20 7951 1802	<a href="mailto:aembury@uk.ey.com">aembury@uk.ey.com</a>
--	------------------	--

<b>Doug Simpson</b> (Asia-Pacific Leader, Sydney)	+61 2 9248 4923	<a href="mailto:doug.simpson@au.ey.com">doug.simpson@au.ey.com</a>
--	-----------------	--

<b>Naoki Matsumura</b> (Japan Leader, Tokyo)	+81 3 3503 1100	<a href="mailto:matsumura-nk@shinnihon.or.jp">matsumura-nk@shinnihon.or.jp</a>
---	-----------------	--

### IT Risk and Assurance Services

<b>Bernie Wedge</b> (Americas Leader, Atlanta)	+1 404 817 5120	<a href="mailto:bernard.wedge@ey.com">bernard.wedge@ey.com</a>
---	-----------------	--

<b>Manuel Giral Herrero</b> (Europe, Middle East, India and Africa Leader, Madrid)	+34 91 572 7479	<a href="mailto:manuel.giraltherrero@es.ey.com">manuel.giraltherrero@es.ey.com</a>
---	-----------------	--

<b>Troy Kelly</b> (Asia-Pacific Leader, Hong Kong)	+852 2629 3238	<a href="mailto:troy.kelly@hk.ey.com">troy.kelly@hk.ey.com</a>
---	----------------	--

<b>Giovanni Stagno</b> (Japan Leader, Tokyo)	+81 3 3503 1159	<a href="mailto:stagno-gvnn@shinnihon.or.jp">stagno-gvnn@shinnihon.or.jp</a>
---	-----------------	--