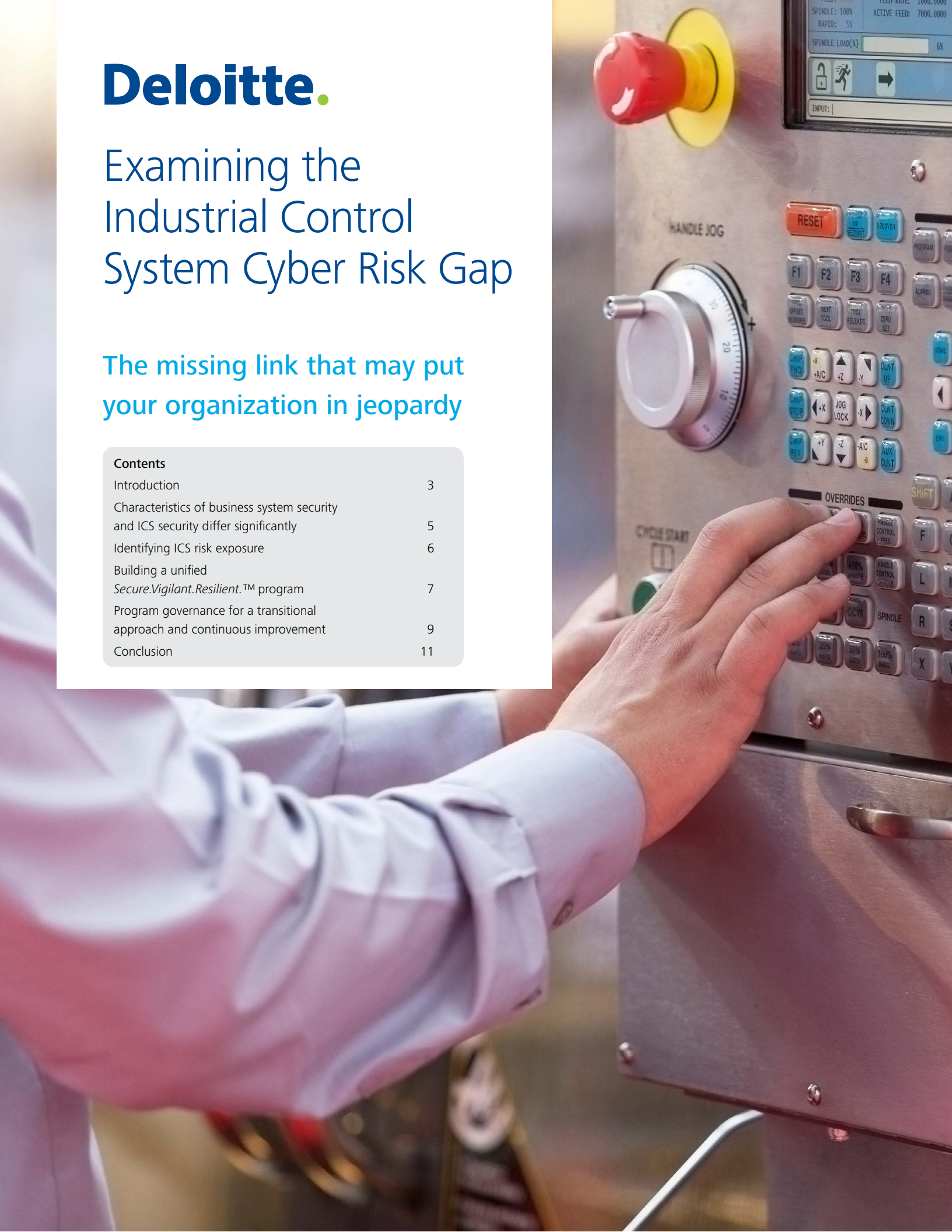
Deloitte.

Examining the Industrial Control System Cyber Risk Gap

The missing link that may put your organization in jeopardy

Contents



Introduction

Industrial Control Systems (ICS) are command network and systems devices designed to monitor and control industrial processes. The ICS family includes supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations. ICS were initially designed for, and deployed in, isolated networks, running on proprietary protocols with custom software. As a result, the exposure of these systems to cyber threats was limited.

Today, as an enabler of business innovation and efficiency, more ICS systems are connected to the Internet, either directly or through the corporate networks, and are remotely accessible to allow remote process monitoring, system maintenance, process control and production data analysis. Accordingly, the threat of exposure has risen and so have the corresponding business and compliance risks.

These business needs have led to the convergence of Enterprise Resource Planning (ERP) systems, Manufacturing Execution Systems (MES) and SCADA systems. By providing increased access to industrial process data, these innovations allow manufacturers to make better business decisions. In addition, manufacturers have extended their manufacturing and supply chain processes and systems beyond their own organization to include supplier and customer processes and systems.

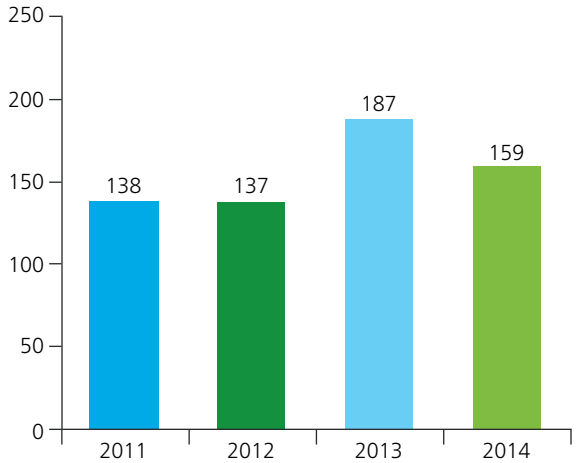
Although these developments improve business productivity, they have also made companies more reliant on the security posture of their suppliers and consumers. In addition, disruption to these systems can directly impact the process flow between the supplier and consumers. IT security specialists often do not fully understand the industrial processes supported by ICS, and ICS specialists do not always fully understand modern IT security risks. As a result, companies are often not aware of, or prepared to address, the full range of security and business-related risks that stem from the connected ICS environment.

This lack of security awareness and safeguards can have serious consequences. While years of effort may be invested in reaping the benefits of convergence, a serious cyber incident—in a matter of minutes, hours or days—could erode these gains by causing revenue loss, brand damage and loss of customer trust, theft of intellectual property, safety issues, and even loss of life. These costs can be far-reaching. While the direct costs of analyzing and repairing technical damage can be significant, the ongoing litigation and loss of operational productivity can be even greater. This paper will discuss common ICS cyber risks in greater detail, and presents important steps companies may need to take toward a more broad cyber risk program.

We have found it highly effective to think about cyber risk management using the following paradigm:

- **Secure**: Effective risk management begins by preventing system breaches or compromises. This may include controls of many layers, types, and approaches, because the potential attacks are quite effective at exploiting weaknesses never imagined by their creators. We lock our doors because thieves might enter through them. Similarly, we physically "harden" sensors on power plants to protect them from accidental or deliberate assaults, and install software firewalls to keep out hackers.
- **Vigilant**: The nature and intensity of attacks can change in ways that render previously effective security measures obsolete. No degree of security is perfect. Best efforts still leave any system vulnerable. Consequently, security must be complemented by vigilance—monitoring to determine whether a system is still secure or has been compromised.
- **Resilient**: When a breach occurs, limiting the damage and reestablishing normal operations are much more easily and effectively done when there are processes in place to quickly neutralize threats, prevent further spread, and recover.

Frequency of ICS Cyber Incidents



According to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), ICS incidents increased in the past couple of years.

Cyber risk programs built on this framework can help manufacturing companies innovate with greater confidence by giving balanced attention to the cyber risks inherent in a connected ICS environment.

The threat is real

Specific risks vary from one company to another, but several current factors and worldwide trends make ICS more susceptible to cyber threats:

- Systems have become networked;
- Unmanned and remote workforce models and management practices have developed;
- Use of wireless communications in process control has increased;
- Use of mobile devices has increased;
- Commodity IT solutions and open design protocols —whose vulnerabilities are widely known to adversary communities—are more widely used;
- The IT global workforce is growing and becomes highly skilled;
- Use of third parties to manage and maintain systems is more widespread; and
- Cybercrime-related activities have increased.

Not all vulnerabilities stem from the technologies themselves; some gaps are essentially talent, process, and organizational issues. As previously noted, although IT and ICS networks are increasingly intermingled, the specialists on either side often do not fully understand each other's operating concerns. This may result in a wide range of policy and controls gaps, and change and asset management processes that have not matured to match the degree of integration that exists.

Who are the attackers that would exploit these weaknesses? Broadly speaking, companies face two types of potential attacks: targeted and non-targeted.

Targeted attacks are ones that are directed against a particular organization, usually with a very specific motive. Attackers may be politically-or ideologically-driven groups trying to cause disruption or public embarrassment, nation-state actors aiming to undermine the victim's financial health or market position, disgruntled insiders, organized criminals seeking financial gain, or industry competitors. Targeted attacks are usually "low-and-slow" in style: an initial infiltration may go unnoticed; over weeks or months, the attackers quietly move from system to system, gaining the access and collecting the information they need to carry out their intent.

Non-targeted attacks are more opportunistic. Attackers spread malicious software via email, websites, USB sticks, or other means. The aim is to breach systems wherever possible to steal data that can be converted to value in underground markets, or, as in the case of the 2013 Cryptolocker campaigns, encrypt users' files to coerce organizations into paying ransom for the return of their data. In some cases, a non-targeted attack can become a stepping stone for a subsequent—and potentially more damaging—targeted attack.

Characteristics of business system security and ICS security differ significantly

To establish a unified cyber risk program incorporating the ICS environment, it is important to acknowledge and address the differences in the way security has typically been handled between the business side and the ICS operational side, illustrated in Table 1.

ICS security is not typically governed by the corporate IT security function, nor is it generally integrated into an organization's security management processes. The term "Industrial Control System" implies systems and applications that are generally implemented and managed by departments outside the business IT (often referred to as 'enterprise IT') function, such as production, engineering, and maintenance. Technical automation is often performed by a department other than IT, adding further complexity to the issue of ownership.

The technical ICS environment also has inherent security challenges. Decisions about ICS software are often not made centrally by corporate IT, but rather at the plant or departmental level, resulting in products from different vendors, based on different technologies, and with different IT security strategies. Mergers and acquisitions have also led to significant diversity in IT systems and security at the ICS level. Older industrial control systems may not have advanced security protection features. The diversity and criticality of ICS devices makes it especially challenging to upgrade systems frequently.

Table 1

Category	Business system security	ICS security
Risk management requirements	• Data confidentiality and integrity are paramount • Fault tolerance is less important; momentary downtime is not typically a major risk • Major risk impact is delay of business operations and financial reporting	• Human safety is paramount, followed by protection of the process • Fault tolerance is essential; even momentary downtime may not be acceptable • Major risks can include loss of life, production interruption, product integrity and safety, equipment damage or loss
Architecture security focus	• Primary focus is protecting IT assets and the information stored on or transmitted among these assets	• Primary goal is to protect process control devices managed by computing devices
System and process lifecycle	• Reboots of systems are frequent, and availability is not as essential • Latency is not a primary focus • System capacities allow for the deployment of security tools	• Requirement for 24/7 availability is critical and poses challenges to patching, upgrade and maintenance procedures • Driven by end-to-end manufacturing lifecycle of products • Highly customized processes based on manufacturing requirements and materials • Real-time capabilities are essential; latency issues must be avoided at all costs
Software maintenance	• A variety of maintenance procedures, such as emergency patches, can be applied • Unavailability of services causes only marginal cost	• Downtime due to maintenance procedures must be kept to an absolute minimum • Unavailability can cause substantial financial and reputational losses
Component lifetime	• Typically 10 to 15 years	• Typically 15 to 25 years
Access to components	• Components are usually local and easy to access	• Components can be isolated and remote, and can require extensive physical effort to gain access to them

Identifying ICS risk exposure

Whether or not a company is likely to face targeted ICS attacks, safeguards to address malware, viruses and common threats that target networked systems should be put in place. Beyond that, risk management practices should be proportionate to the risks present.

The first step is to move beyond the initial question of "Is the risk real?" to "What risks do we face, how big is it, and what level of investment is warranted to mitigate it?" Establishing risk appetite is fundamentally a business issue that needs to be addressed at the executive level. Many factors should be considered, including the following:

- **Are there factors that make the company a particularly attractive target?** The size, complexity, or value of an organizations' products could be significant factors. Examples of potential targets include an industrial products manufacturer with valuable intellectual property; a company with recent large, public capital investments in manufacturing processes; or an organization that provides goods or services that falls within the scope of critical infrastructure.
- **Are all ICS assets subject to appropriate corporate IT standards, governance, and monitoring processes?** It is not uncommon to distribute ICS IT support and related security and change management responsibilities to professionals who may not be aware of the latest IT security policies and strategies.
- **Have the full range of potential cyber incidents been considered, and have the potential consequences and costs been thoroughly identified?** Consequences could include IP loss, reputation and brand damage, loss of human life, and other potential risks that would need to be defined through an analysis of the industrial process. Some questions to ask about potential incident scenarios include:
  - What would the impact to the organization be if the MES and SCADA systems were penetrated by hackers?
  - How would the business impact of a denial-of-service attack differ in the ICS environment?
  - Is there a risk of catastrophic failure if any ICS or production device is compromised?

A detailed review of the ICS environment is likely warranted. Management should give appropriate strategic consideration to the business risks by leveraging a multidisciplinary team of operations, engineering, and IT security professionals to:

- **Inventory critical devices and systems** and determine if they are subject to well-known and exploitable vulnerabilities.
- **Assess ICS environment safeguards that often contain weaknesses** such as credential management, network design, firewall rules, event monitoring, support documentation, privileged access management, and access controls.
- **Understand the difference between the security considerations** for business systems and industrial control systems and devices. IT security standards and processes should address both back-office systems and ICS to confirm that an appropriate level of governance and security is being applied and implemented across all systems.
- **Understand the interaction of the different levels of ICS** to identify and evaluate the exposure, risk, and impact of penetration at each level or component. This includes understanding the baseline security profile of the ICS and defining security standards to apply consistently to the ICS environment. This may reveal security limitations inherent in the ICS environment, which the organization should evaluate to establish appropriate mitigating procedures.
- **Understand third-party dependencies.** This is increasingly critical as manufacturers increase the supply chain integration and systems integration they achieve with customers and suppliers.

Common assumptions about ICS security

Some companies may conclude that their ICS cyber risks are sufficiently small and do not need major mitigation. Some common assumptions and viewpoints, however, can prevent companies from realistically assessing their level of exposure.

- "My industrial control system is isolated, and therefore doesn't pose a risk."
- "Security is the responsibility of the integrator."
- "Our organization is not a likely target."
- "Security does not help us to sell more products."
- "Firewalls separate the IT and OT networks."
- "My systems and processes work perfectly, so let's not touch them."
- "Security audits and assessments may be important, but we don't have budget for them."

Building a unified Secure.Vigilant.Resilient. program

The starting point for a risk-centric program is to understand the cyber threats to which the organization is exposed, as discussed, and to set realistic goals that can be achieved using a *Secure.Vigilant.Resillent.* program depicted in Figure 1—Key program considerations.

Additionally, well-defined governance processes enable organizations to continually adjust the program as both the business and threat environments change. Efforts to implement a *Secure.Vigilant.Resilient.* program would likely not be effective without addressing the organizational disparity between the business technology environment and the ICS side, as previously discussed. The program is not simply an expanded set of technical requirements—it may also require cultural shifts, re-engineering of processes, and new collaboration and accountability mechanisms.

Figure 1 shows some of the most urgent questions that arise in designing a cyber risk program for ICS environments.

Figure 1—Key program considerations

Starting points

The International Electrotechnical Commission (IEC) assessment framework describes some of the most important foundational elements of a mature program[1]. These can form a starting point for a tailored *Secure.Vigilant.Resilient.* program.

Secure

Asset inventory: An inventory of all ICS components is maintained, containing information about each component's configuration and connections, to estimate corresponding security levels and to select mitigating controls;

- Governance, Roles and Responsibilities: Governance policies & procedures as well as roles & responsibilities for ICS security are clearly defined and assigned for everyone contractually, from employees in the management layers to the process operators to third-parties;
- Training: Employees and contractors working in or with ICS environments, are trained to assure process continuation in safe and secure manner;
- Access Control: Physical and logical access to ICS environment (e.g., hardware components, applications, networks) is only assigned after formal authentication and authorization;
- Change Management: Changes to the ICS environment, either in hardware or software, are formally authorized and implemented in accordance with written, periodically tested procedures;
- Operating System Security Patches: Patches for operating systems and application software are managed in accordance with written, periodically tested procedures;
- System Hardening: ICS component software, services, accounts and configurations are limited at a bare minimum as required for business continuation;
- Network Security: Access to wired and wireless networks within the ICS environment is limited and secured in accordance with leading practices;
- Portable Media: Use of portable media within the ICS environment is disabled. When not disabled, written, periodically tested procedures must ensure portable media is cleaned from malicious software before connecting to the ICS components;
- External Access: All remote access traffic to/from ICS components (i.e., to/from other network domains) is controlled and processed via a Process Control Access Domain (PCAD);
- Portable Computers: All portable devices such as laptops and tablets must be formally authorized before accessing the ICS network or its components and
- Network Segregation: The ICS network is segregated, differentiating on ICS component's functions and risks.

Vigilant

- Anti-virus: Where feasible, each ICS component is featured with anti-virus software which is running by default and updated periodically;
- Threat Management: Periodic testing of infrastructure and applications are performed; and
- Security Log Collection and Management: Written procedures are in place which ensure security events within the ICS environment are logged, enabling traceability and accountability. The logfiles are collected, correlated, stored and reviewed in accordance with the procedures in order to detect security incidents within the ICS environment timely.

Resilient

- Backup and Restore: A "time-to-restore" is defined for each ICS component (software and data) and appropriate back-up and restore procedures are implemented accordingly and
- Incident Response: A written, periodically tested incident management procedure is implemented, which is part of the overall incident response process.

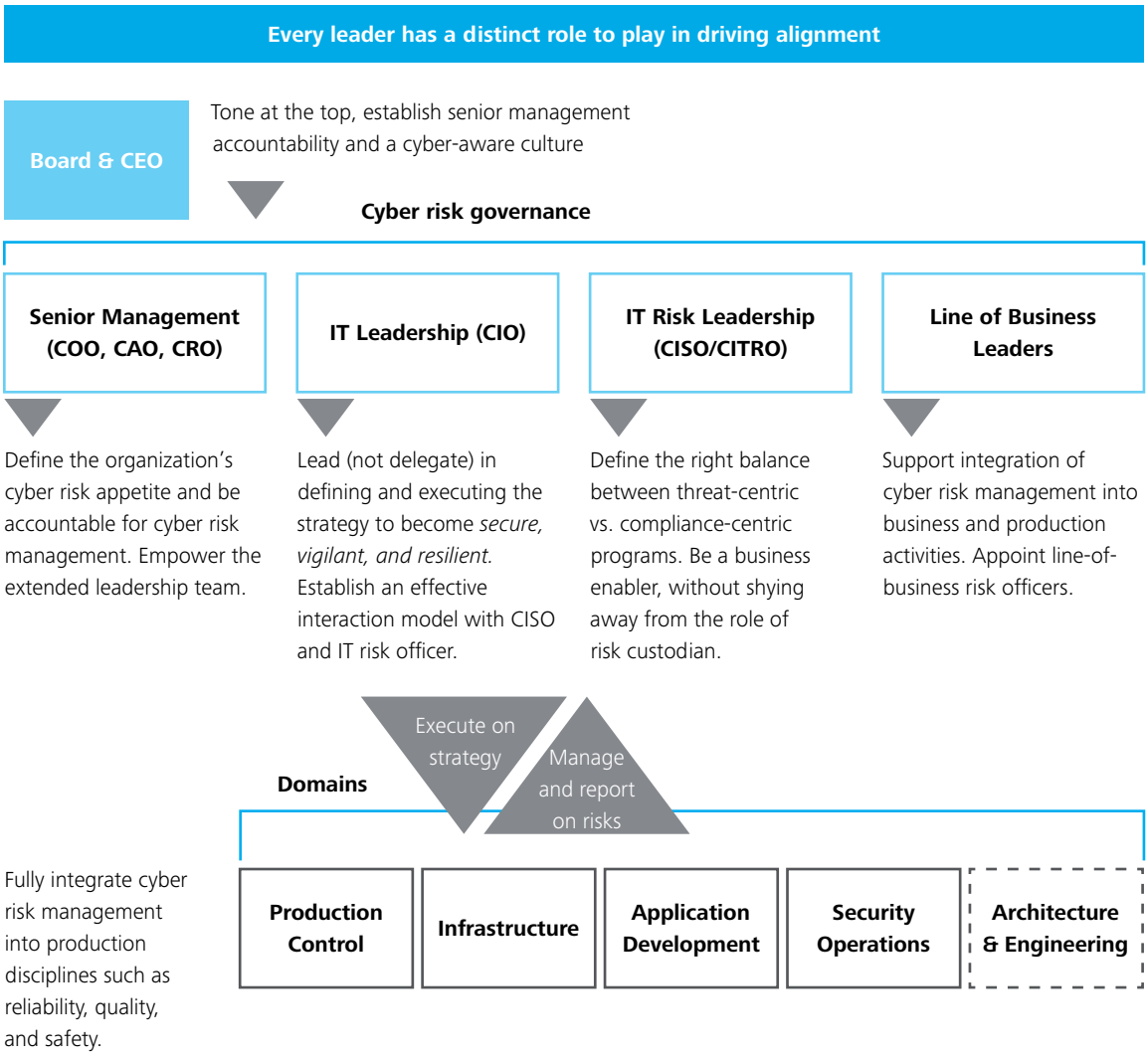
1 See IEC 62443-2-1:2010 "Industrial communication networks—Network and system security—Part 2-1: Establishing an industrial automation and control system security" and IEC 62443-3-3:2013

"Industrial communication networks—Network and system security—Part 3-3: System security requirements and security levels"

Program governance for a transitional approach and continuous improvement

Although it's essential to integrate the technical aspects of the IT and OT cyber risk program—security architecture, policies and ongoing management—the cyber risk program is not just the domain of technical teams. A risk-focused approach requires full engagement of the business and the establishment of a cyber-aware culture throughout the organization. Leaders at multiple levels have vital roles to play, as illustrated in Figure 2.

Figure 2—Addressing cyber risk requires business alignment



It may seem daunting to make the transition from where your organization is today to where you need to be, but remaining focused on top cyber threats to the business—your core cyber risk areas—provides a set of priorities to guide a phased approach. You may determine that some components of your business process, cutting across a subset of both IT and OT components, are especially critical. You may determine that gaps in basic ICS device controls throughout the ICS environment are a priority to shore up basic security capabilities, but in any case, the four-phase approach described in Table 2, incorporating considerations in all three of the secure, vigilant, and resilient areas, can be applied to drive ongoing improvements.

Table 2—ICS security transition approach

Phase 1	Phase 2	Phase 3	Phase 4
What are my vulnerabilities and where are my greatest risks? What is our risk appetite? Are we adequately prepared to address the comprehensive environment?	What are our strategic risk priorities? What is a realistic plan to achieve our objectives?	How do we effectively implement our strategy? What processes and procedures should be in place?	How do we develop an ongoing process to mitigate ICS cyber risks and maintain and integrated program?
Diagnostic Analysis	Strategy and Program Design	Program Development	Continuous Improvement
• Conduct a risk assessment: – Interviews to assess maturity of security processes – External security test – Internal security test – Configuration security test • Conduct asset analysis • Document process and data flow with key interaction requirements • Compare governance procedures • Conduct Human Resources (HR) capability assessment • Evaluate exposure risk • Develop and evaluate ICS security risk profile • Develop diagnostic report and report	• Develop charter and enterprise-wide strategy, including objectives and scope • Determine roles and responsibilities • Develop program design and governance	• Establish policies, standards and protocols • Develop malware and advanced persistent threat (APT) detection capability • Establish escalation chains and communication channels • Develop procedures and refine workflows • Develop scenarios and conduct case testing	• Establish a continuous improvement program • Monitor the ever-evolving threats and the effectiveness corresponding implemented ICS security controls • Use analytics to evaluate resource implications on detect, prevent and react activities

Conclusion

As traditional corporate IT perimeters have disappeared, as corporate and operational systems have become more thoroughly integrated, and as organizations leverage the continuing emergence of new technologies, cyber threats will continue to evolve. Cyber risks are often changing faster than companies can react, and cyber attacks are more frequent, sophisticated, and malicious. To achieve their growth and innovation potential, company executives, business leaders, and IT management need to make integral investment in cyber risk capabilities.

Among ICS-dependent organizations, there is a growing cyber readiness gap. As there have been rapid increases in the sophistication of our technology environments and the sophistication and persistence of cyber adversaries, there has often not been a parallel advance in organizations' cyber risk capabilities. Despite broad public awareness and greater government action on the problem of cyber threats, many organizations have been slow to close this readiness gap.

Companies with an increasing dependence on integrated ICS systems should transform how they handle ICS cyber risk, considering the following:

- Vulnerabilities exists, the threats are real, and the risk is high.
- Knowing what you have, and the state of your cyber risk posture, is vital.
- Preventive controls to better protect ICS assets are essential. However, because cyber attackers will sometimes succeed in penetrating the environment, situational awareness and detection capabilities are essential to shorten the time it takes to discover an intrusion. Once they've infiltrated, adversaries will sometimes successfully execute an attack. It is therefore equally important to strengthen cyber incident preparedness and response capabilities.
- Taking actions such as these are both a business and a technology challenge; leadership sponsorship and governance are must-haves for success.

By building a comprehensive *Secure.Vigilant.Resilient.* program, an organization can improve its security profile, enhance its ability to thrive in the face of disastrous attacks on its manufacturing base, and therefore gain greater confidence in leveraging the benefits offered by an integrated ICS environment.

About the authors

Ed Powers
National Managing Principal, Advisory
Deloitte & Touche LLP
epowers@deloitte.com

Sean Peasley
National Managing Principal, Advisory
Deloitte & Touche LLP
speasley@deloitte.com

Rene Waslo
Principal, Advisory
Deloitte & Touche LLP
rwaslo@deloitte.com

Byron Fletcher
Senior Manager, Advisory
Deloitte & Touche LLP
bfletcher@deloitte.com

David Dinh
Senior Manager, Advisory
Deloitte & Touche LLP
ddinh@deloitte.com