Life Is On | Schneider Electric

Cybersecurity by Design:
Building a Company Culture to Strengthen a Digital Business

by Schneider Electric

Executive summary

Cyber risks are heightened as industries and enterprises transform operations through digital channels, automation technologies, and data sharing. Today's cyberattacks are numerous, frequent, and existentially more threatening than ever before. Attackers aim to infiltrate and manipulate not just an individual company but the entire ecosystem to which it belongs. To this end, decision-makers need to feel confident that their integrated cyber strategy, defenses, and recovery capabilities will protect their business and support their growth strategies.

Aligned to the NIST framework, Schneider Electric's approach illustrates how cybersecurity can be accounted at the very front-end of development lifecycles.

A comprehensive digital risk strategy that incorporates "Cybersecurity by Design" principles helps companies to deploy strategies that account for industrial cybersecurity, and to build resiliency across a company's whole digital ecosystem, including supply chain and beyond.

Drawing on practical use cases, this white paper suggests a pragmatic approach to a digital risk strategy.

Contents

Introduction: The business imperative for a digital risk strategy with cybersecurity building blocks

The Internet of Things (IoT) is driving significant investment in projects that integrate smart devices, big data, analytics, and other digitization-related tools. The connectivity of Information Technology (IT) systems is now migrating at an accelerated rate into the Operations Technology (OT) layer, which represents a vast collection of physical infrastructure systems such as power, control, automation, heating, cooling, and ventilation systems. Without question, these environments are converging at an unprecedented pace as IoT business strategies mature.

With the increasing power of embedded electronics, connected intelligence will migrate down to the lower levels of the automation hierarchy: to the control level and to the sensors and actuators, for example. As a result, the merged IT and OT systems will enable a much flatter, responsive, and information-driven architecture. Businesses will benefit from this advanced and intelligent connectivity through increased efficiencies, lower cost, and faster time-to-market. Yet this IT/OT convergence raises the concerning question: What is the cybersecurity risk of creating this merged digital environment?

Figure 1

Effective cybersecurity involves modifications to technology, process, and human work habits.

Balancing digital risk and the benefits of smart connectivity

78%
of Board decisions are regularly influenced by risk data

Gartner Annual Security and Risk Survey, February - March 2017

One of the perceived challenges of a more connected landscape, particularly within critical buildings and industrial sites, is the exposure of control systems that once were closed to such open, connected networks. Machines and devices that support factories, oil & gas operations, and healthcare facilities now produce much of the data that organizations count on for streamlining operations, enabling better business decisions, and developing new digital business models. Even non-critical environments have the same bottom-line concerns about cyberattacks such as maintaining business continuity, upholding brand reputation, and preserving customer trust.

Everyone agrees that *not* being connected, however, presents a greater business risk. With advancements in IoT, connectivity, and mobility, intelligent devices can be mon-

itored across the infrastructure. These devices can flag anomalies and real-time information, thereby accelerating detection, response, and recovery. Building a clear digital risk strategy that simulates and weighs different classes of risks, therefore, is an essential first step toward driving cyber resilience in this converged landscape, and it must be an organization-wide framework communicated and upheld at every level of the organization. After all, 78% of Board decisions are regularly influenced by risk data.[1]

"For any company, a perimeter defense is not enough in today's digital world. Everyone is connected constantly — from our homes, smartphones, and across the distributed enterprise network. A layered approach is essential as we cannot just rely on a moat — as wide as it is — in today's hyper-connected world."

Hervé Coureil,
Schneider Electric
Chief Digital Officer

Within this digital risk framework, it is worth noting the cost of threats to OT infrastructure: both loss of business continuity and the impact on human/public safety. According to the State of Industry Cybersecurity 2018 survey, 14% of sampled companies experienced at least one security incident related to OT/Industrial Control System (ICS) and/or control system networks within the prior 12 months (with 17% of those surveyed experiencing two or more incidents).[2] The survey cited causes of those incidents as: 64% conventional malware/virus outbreaks, 30% ransomware attacks, and 27% employee errors/unintentional actions.

The business imperative therefore is clear: identifying and balancing digital risk is essential in order to realize the benefits of data-driven decision-making, enhanced efficiency and productivity, new digital business models, and an enriched customer experience. Only 30% of organizations leverage CIOs/CISOs to take steps to ensure a business-led approach to digital risk, however.[3] Now is the time to drive cybersecurity efforts as a strategic priority for digitally transformed companies. As worldwide spending is projected to reach $133.7 billion on security-related hardware, software, and services in 2022, according to IDC (versus $92.1 billion forecasted for 2018),[4] approaching cybersecurity as a business decision — *instead of an IT issue* — is mandatory.

Aligning end-to-end cybersecurity strategy to the NIST framework

Figure 2

National Institute of Standards and Technology (NIST)

To drive a clear digital risk strategy supported by a holistic approach to cybersecurity, Schneider Electric has aligned its efforts with the framework of the National Institute of Standards and Technology (NIST),[5] a non-regulatory agency of the United States Department of Commerce. The NIST framework encompasses five concurrent and continuous functions to advance a secure digital ecosystem beyond the company to encompass its supply chain, product delivery process, and deployment to customer sites. These five steps are *Identify, Protect, Detect, Respond, and Recover*.

This layered Defense in Depth approach is how Schneider articulates its defense against kill chains and risk scenarios, modeling and continuously fortifying its ongoing cybersecurity posture and resilience:

1. **IDENTIFY** cyber risks with a register that includes the high-value assets
2. **PROTECT** with capabilities implementation and digital locks (that is, enforcing mechanisms) to mitigate threat
3. **DETECT** incidents and monitor events through a Security Operations Center
4. **RESPOND** to threats immediately following tested plans and protocols
5. **RECOVER** from any issue by gathering learnings garnered by ongoing Reality Checks, revisiting and adapting our cybersecurity posture accordingly, including faster and better emergency and improvement plans across the company

IDENTIFY: Scrutinize cyber risk using a register that prioritizes high-value assets

"A cybersecurity strategy cannot be a reactive one. A proactive, end-to-end approach is a business opportunity for digitally transformed organizations. It is a business conversation that spans the entire organization, supply chain, and digital ecosystem of partners and customers."

Christophe Blassiau, Schneider Electric Chief Information Security Officer

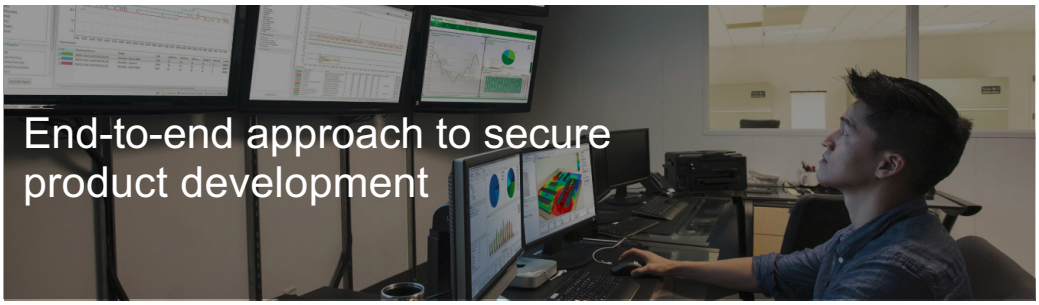
In order to identify and close security gaps, Schneider recognizes the criticality of a digital risk strategy that includes cybersecurity not just as a "feature" of a hardware or software product but as a fundamental business practice that affects *people, process,* and *technology*. Today's technology deployments must account for the safe, widespread rollout of connected devices across the IT and OT layers. Security, therefore, is integrated at the beginning of the product development lifecycle — that is, *a Cybersecurity by Design approach* —within the proactive digital risk framework.

Three main factors influence this landscape for identifying digital risk and attack paths for products, solutions, services, and software during the R&D lifecycle, and, in turn, deploying ways to mitigate the security gaps:

- **People –** All employees, from new recruits to the C-suite, need to realize how a cyberattack can erode trust in the organization, and just how damaging and far-reaching the consequences may be. Intertwining security practices with business operations and ongoing training to improve an organization's security posture is not a function relegated to the IT department. Instead, companies must cultivate a cyber-resilient culture company-wide. In addition, more and more attention needs to be paid to the identification of potential insider threats.
- **Process** –The Schneider Electric Security Operations Center monitors incidents, driving an incident response process. From there, recovery includes learning as much as possible from every incident, passing along lessons learned through the digital ecosystem and customer installed base. To drive forward a holistic cyber process, Schneider requires its best-in-breed partners to pass certifications while supporting its secure product development lifecycle approach from product design, to integration into customer systems, and through to value-added services that monitor potential threats and that neutralize incidents if they occur.
- **Technology –** R&D ecosystems, global supply chain, and solution deployment channels all play an important role in bolstering the overall cyber posture. Solutions must be based on secure designs, and they must adjust quickly to correct identified vulnerabilities. This means that attention is required both at a product level and at a system level, as a perfectly secure product can become a threat vector if exposed via a flawed system design. Prioritizing high-value asset protection is key; Schneider has ongoing Reality Checks against metrics and targets and evolves them against the threat landscape to fortify its ongoing cyber posture. McKinsey notes that companies can realize 20% cybersecurity ROI savings by prioritizing these crucial assets alone.[6]

Schneider shares processes, skills, and expertise with its partners and customers. In addition to driving cybersecurity as a core part of its business strategy, product devel-opment (see "Cybersecurity at Schneider Electric" White Paper), supply chain, and solution deployment, Schneider has invested in developing cybersecurity-specific

consulting and training solutions for its customers. The goal is to help customers identify and address the human and technology aspects of their own cybersecurity posture and, accordingly, design and implement cybersecure solutions and systems that meet their specific business needs. These consulting teams enable Schneider customers to bridge the two worlds of IT and OT in a secure, proactive way.



PROTECT: Implement Cybersecurity by Design capabilities and digital locks to mitigate threats at every step

Within the Schneider product development process, teams embrace a “security at the beginning” posture, focusing on threats and establishing a cyberattack prevention mindset. To this end, business stakeholders are trained to become owners of the cybersecurity risk. Such ownership has provided business value in the form of more efficient processes and more robust products and systems.

Schneider has adopted many of the cybersecurity principles developed by NIST for certifying development centers and integrating security management for hardware and software development processes and critical sites. In addition, as more and more customers require secure product development lifecycle processes, these core elements serve as fundamental Cybersecurity by Design building blocks for Schneider to:

- Establish a clear Secure Development Lifecyle process
- Adhere to industry standards and government cybersecurity-related regulations
- Certify product cybersecurity levels through qualified third-party organizations

Secure Development Lifecycle process

Cybersecurity prevention is never an absolute across today’s digital landscape. A clear, end-to-end lifecycle approach to secure product development and deployment is essential. Digital enterprises must strike a delicate balance between investment, threat mitigation, and technology innovation.

Schneider embraces this lifecycle process as a framework that establishes product security from the beginning of development through the lifecycle with incident and vulnerability reporting and management.

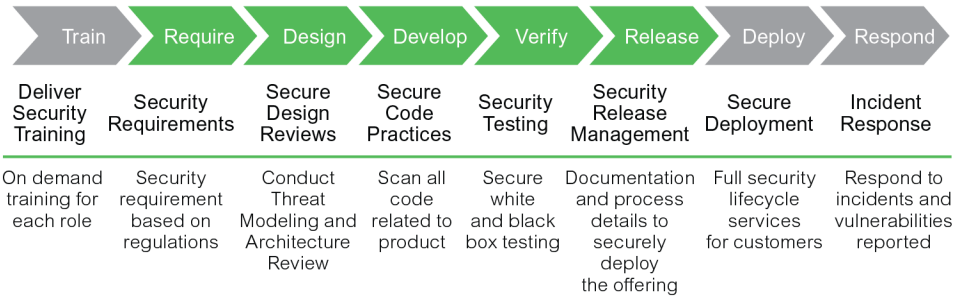


Figure 3

The Secure Development Lifecycle process makes products more resilient. As new products replace old, entire systems evolve to become more cybersecure.

"To successfully deploy cybersecure systems in OT environments, it is important to understand what is mission critical and consider this in the design from the beginning. Security needs to be considered through the whole lifecycle of a product or system, and it is key to being aware of emerging threats and to adequately react to them."

Klaus Jaeckle,
Schneider Electric Chief Product Security Officer

During this process, the following steps occur:

- Secure architecture reviews are performed
- Threat modeling of the conceptual security design is created
- Secure coding rules are followed
- Specialized tools are used to analyze code
- Security testing of the product is completed

These actions help to "harden" products, making them more resilient against cyberattacks. In this way, as new products replace old ones, entire systems can evolve to become more cybersecure. The Secure Development Lifecycle process helps product developers to determine how much security a particular product requires, versus what might be optional. It is a risk-based approach that takes into consideration relevant industry standards and proper testing (e.g. penetration tests, vulnerability scans, secure code analysis) before a product is released to the public. This framework also offers strategies for addressing vulnerabilities and for handling incident response situations.

New devices continually undergo a Schneider security review. Engineers test the cybersecurity and physical robustness of the devices. In addition, functions such as secure boot and firmware signing are gradually getting added to new devices. There also is a precedent for all R&D cybersecurity-related activities to follow a specific set of internal standards to be validated during development. The adherence to both international and internal standards allows for consistently secured product development.

IoT-enabled EcoStruxure architecture

A Cybersecurity by Design development process guides secure product development across Schneider's vendor-neutral, open, IoT-enabled architecture and platform: EcoStruxure™. This architecture includes an open but tailored stack of connected products; edge control level solutions and software; and cloud-based apps, analytics, and services. End-to-end cybersecurity supports applications and data analytics, em-bedded across these layers, which converge IT and OT equipment and solutions, software, and services within six domains of expertise.

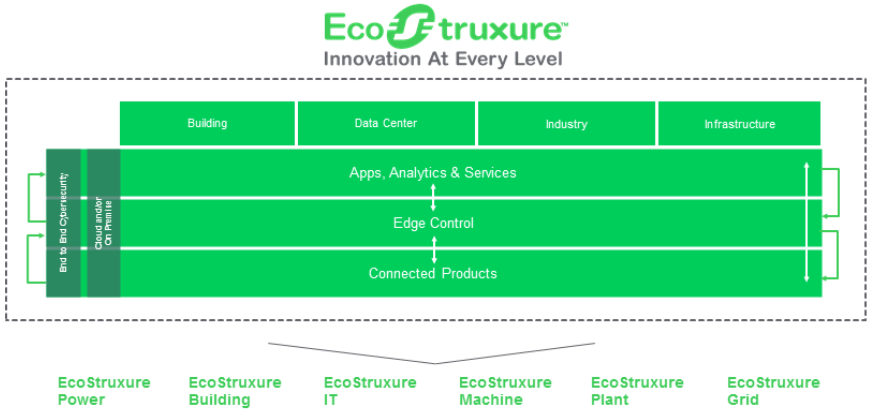


Figure 4

End-to-end cybersecurity across EcoStruxure architecture

With EcoStruxure, enterprises have easier management of core processes across the key elements of cloud, edge, and on-premise. Operators view cloud-connected critical data anytime, anywhere from any device. Resiliency and visibility are improved

through live sensor data, predictive analytics, and smart alarming. Operators also have access to experts monitoring connected assets 24/7.

Schneider can support customers' robust cybersecurity stance with dedicated cybersecurity services, secure EcoStruxure digital offers and solutions.

Indeed, attention is critical at both the product level and the system level; after all, a perfectly secure product can become a threat vector if exposed by an improper system-level design.

Given that EcoStruxure solutions are deployable both on-premise and in the cloud with built-in cybersecurity at each architectural level, users perform real-time corrective actions in the short term and optimize their whole ecosystem in the long term. This capability results in better decisions that directly increase business productivity and efficiency, and reduce downtime.

EcoStruxure improves the agility of organizations by enabling key process owners to respond more quickly to market dynamics. By providing a collaborative workspace that connects applications and analytics to the field systems/devices, the architecture allows teams to view combined intelligent dashboards in real-time, enabling fast and accurate decisions.

Secure global supply chain

200+
factories in
40+
countries
90+
distribution centers

Protection extends to the Schneider Electric global digital ecosystem that includes the supply chain.

Protecting the holistic digital ecosystem includes the global supply chain delivery and deployment to customers from two angles.

- First, the scope of Schneider's Cybersecurity by Design framework includes internal operations of plants and distribution centers, customer base installations, and its vast network of partners and suppliers. Schneider works with partners — such as Claroty — leading in OT infrastructure security to secure its factories (e.g., by monitoring the production line, OT infrastructure, and controls, alongside enterprise IT infrastructure).
- Second, the goal is also to protect products so that they emerge from the supply chain secured downstream for delivery and deployment to customers. For example, if Schneider chooses to use a real-time operating system in a particular product and testing reveals a vulnerability, it expects that the provider be responsible for issuing a timely patch to protect the product. In this way, having the supply chain engaged in the overall Cybersecurity by Design process is a critical facet of being able to deliver secure products.

Secure partner ecosystem

Schneider places a high priority on strengthening cybersecure digital innovation through an extended enterprise approach that includes strategic partnerships with best-in-breed technology providers, customers, startups, universities, and developers. This ecosystem advances co-innovation and the development of secure EcoStruxure solutions while also providing an open community for developers.

Examples of this digital ecosystem approach include a partnership between Schneider and Claroty, a specialist in providing visibility and security to OT networks; collaborative development and management of a Security Operations Center (SOC) with IBM; and the creation of incident response teams that strengthen resilience and responsiveness capabilities.

In addition, Schneider engages in numerous public and private partnerships in order to actively engage in cybersecurity topics globally to complement Schneider's own internal cybersecurity expertise to make both legacy and new products more cybersecure. For example, Schneider is an active member of the Cybersecurity at MIT Sloan (CAMS), formerly IC^3, an interdisciplinary, confidential forum that brings together MIT faculty/researchers and C-level cybersecurity experts on cyberspace, cybercrime, and cybersecurity as applied to critical infrastructure.

Cybersecurity standards and certification

Extended enterprise security imperative

Many suppliers and partners undergo a cybersecurity certification.

By adhering to published cybersecurity standards and testing to those standards, products are externally validated. Organizations such as the ISA Security Compliance Institute (ISCI) offer ISASecure® EDSA certification specifications using the framework of the IEC62443 standards. ISASecure® EDSA focuses on the security of embedded devices and tests and evaluates software development security, functional security and communication robustness.

Schneider follows local regulations and uses additional industry established frameworks to conform to cybersecurity standards, such as ISO2700x suite and other standards, for its products, solutions, and services. Schneider also takes an active part in the evolution of today's industrial cybersecurity standards, contributing to the standards and frameworks.

Protecting legacy systems

~37 years old

average age of nuclear power plants in the U.S.

U.S. Energy Information Administration

The Secure Development Lifecycle process and certification alignment ensure that new products and solutions follow rigorous security checks and balances. One of the major challenges for securing both IT and OT equipment is how to address the cybersecurity hurdles of pre-digital legacy systems, especially infrastructure with a capital expenditure with a projected 30+ year lifespan or longer (e.g., from heavy processing industries). Although the new generations of physical infrastructure products and solutions are far more cybersecure, a "rip and replace" approach to legacy systems is rarely practical or economically feasible.

Several best practices can bolster the security of these legacy assets, and cybersecurity services play a significant role in helping to execute these practices:

- **Proper segmentation of the network** – Network segmentation can separate groups of systems or applications from each other, making it more difficult for a hacker to perpetrate an attack throughout an entire network.
- **Locking down the current installed base of products and systems** – Performing an assessment of critical systems will identify communication paths and potential external access points.
- **Endpoint protection** – A comprehensive Defense in Depth strategy can mitigate risks from access through devices on the periphery of the OT network.
- **Patch management** – Often taken for granted, management and control of the implementation of patches for operating systems and anti-virus tools are critical lines of defense.
- **Tested backup and recovery procedures** – Backups of critical systems and data not only need to be performed at frequent intervals, but recovery procedures also need to be tested as well and managed in different locations.
- **Authentication, authorization, accounting** – Along with a secure network design, role-based access controls with multi-factor authentication must be implemented and managed to provide access only where necessary and to log access activity.

120 million

new malware variants every year

McKinsey Cybersecurity and Cyberrisk Service Line

- **Closer monitoring of systems** – This practice includes 24/7 monitoring and auditing of system events and intrusion detection prevention systems to detect anomalous traffic on the network, with real-time alerting.
- **Specific management of remote access, if any** – Specifically, this step requires all remote users to connect and authenticate through a single, managed interface before conducting software upgrades, maintenance, and other system support activities.

Though no single one of these approaches provide a cybersecurity "silver bullet," together, they significantly reduce the collective cybersecurity risk to legacy systems.

DETECT & RESPOND: Monitoring incidents with a 360° and 24/7 lens and responding according to fast, tested plans

In the digital economy, every corporation is tasked with managing variable levels of risk driven by adopting new digital business models, enriching digital experiences, and ever-increasing IoT integration to drive productivity and efficiency. A prevention posture against cyberattacks is no longer sufficient. Ramping up a Detect & Respond strategy, in addition to preventive measures, is critical for being able to counterattack breaches and threats immediately.

99 days
on average to detect a covert attack
McKinsey & Company

By 2020, 60% of enterprise information security budgets will be slated for rapid detection and response approaches (vs. just 20% in 2015).[7] According to McKinsey & Company, "companies still need about 99 days on average to detect a covert attack."[8] Although new products will be designed with cybersecurity protections in mind, it is every company's responsibility to place those products in a secure environment, managed by people at every level who understand the responsibility of maintaining cyber vigilance.

More robust detection

The smarter connected devices become, the greater the potential variety of behaviors. Analytics and artificial intelligence (AI) models can flag which behaviors are acceptable and which constitute an anomaly (hence reducing the number of false positives). An anomalous behavior may be noticed regarding a particular device, but this also may be noticed on a certain percentage of devices in the field. This richer detection allows for a much more robust data set that suggests, with more accuracy, if aberrant behavior is occurring.

Schneider's detection strategy incorporates the latest technology and detection and machine learning to monitor and manage minor and critical incidents. When technology flags a critical incident, or the potential for one, an expert investigates and validates whether the alert was justified, in turn deciding on the appropriate response and the proactive, tested response plan. This convergence of analytics/AI with the contextual understanding of a domain expert is essential for detecting real threats and responding quickly to lessen the impact.

Schneider monitors threats across its extended ecosystem, which encompasses both people and technology. The people component includes customers, partners, customer care and sales representatives, field services, cybersecurity partners, and suppliers. The technology component includes EcoStruxure digital assets under management, OT networks' monitoring systems, and intrusion detection systems.

Schneider continues to invest in strengthening its resilience, detection, and responsiveness capabilities with its Security Operations Center and Incident Response teams.

Testing incident response plans proactively

The response to an incident must be based on a proactive, tested incident response plan to minimize risk, protect customer trust, and strengthen customer assurance.

$1M saved
by companies that contained data breaches within 30 days of detection v. 30+ days to resolve

Ponemon Institute

Companies that contain data breaches within 30 days of detection can save over $1 million in impact (versus resolving in 30+ days).[9] More important, a quick response can protect the safety of factory and industrial site workers, and/or the public at large, e.g., when it comes to heavy processing industrial sites and nuclear power plants.

At Schneider, the goal is early containment and proactive remediation, ensuring clear incident ownership to respond to threats at the convergence of OT/IT. Across the industry, if a broad attack is detected, new configurations and updates can be pushed out in order to eliminate the vulnerability that the attacker is attempting to exploit. This approach provides industrial players with a transparent response that does not inconvenience the user.

RECOVER: Lessons learned from ongoing Reality Checks for faster, stronger emergency response and improved plans

Should an incident occur, Schneider takes every step to learn as much from the incident as possible, and to revisit and adapt its cybersecurity posture accordingly. Ongoing cyber resiliency includes a recovery plan to act on emergencies as well as proactive improvement plans to manage cybersecurity incidents and vulnerability reports. A dedicated Vulnerability Management process is based on ISO 30111, and all product vulnerability disclosures are posted to the corporate global cybersecurity website, accessible here.

A best practice is to learn as much as possible from any incident that occurs through root cause analysis: 1) uncovering key learnings related to people, process, and technology and 2) the mapping of issues roadblocking prevention. Schneider's cybersecurity organization leads the response investigation, evaluation, and subsequent mitigation planning of future internal and external cyberattacks based on these learnings.

The lessons learned are passed on across its digital ecosystem, and a portfolio of Schneider Electric Cybersecurity Services enables customers to become more resilient — via identification, protection, detection & response, and recovery.

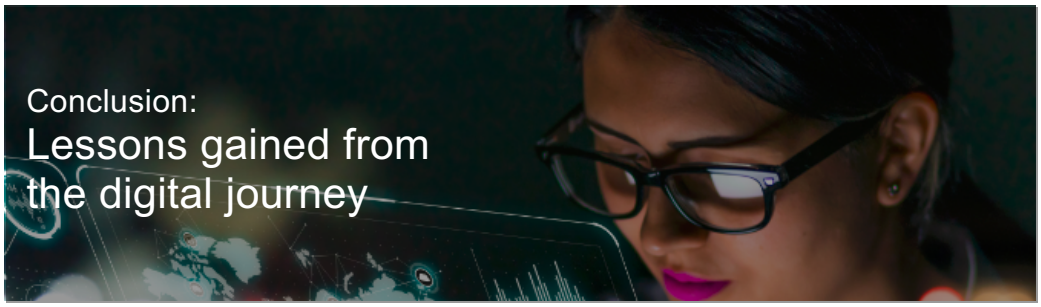
Strengthening the ability to monitor threats

While well understood protocols exist for monitoring and protecting computers and data centers, cybersecurity monitoring of OT systems, until now, often was not prioritized. These systems are increasingly connected to other information systems and to the Internet. While this advancement in technology improves automation and enables remote operations, it also exposes these systems to possible cyberattacks.

Tools such as Security Incident and Event Management Systems (SIEM) provide 24/7 real-time alarming so that system events can be both audited and monitored by the appropriate teams. Third-party monitoring services can also furnish regular reports regarding the nature and volume of threats and the actions that have been taken to neutralize those threats.

Maintaining ongoing cybersecurity updates

Maintenance of secure industrial control system technology deployments can be supported by the organizational and operational processes that manage the critical infrastructures. In much the same way that software updates are provided on a regular basis to computer users, the regular updating of all critical OT assets helps to ensure cybersecurity resiliency. In this way, all stakeholders (e.g., industrial site local teams, suppliers, site maintenance and commissioning teams) are well trained and sensitized to those security measures that are in place. In addition, these stakeholders must be made to use and maintain the secured system baseline while performing daily operations.



38%
of companies
integrate the Chief Information Security Officer into initial discussions of new business opportunities

Accenture

In today's highly connected environments, cybersecurity is now an inherent part of digital business culture, processes, and innovation. Schneider has taken lessons from its digital journey to develop a digital risk strategy and proactive secure framework for developing new products, solutions, and services. This framework extends beyond its boundaries to include the extended ecosystem of partners and customers. In turn, Schneider passes along its lessons learned to partners and customers as a foundation to accelerate digital transformation in a secure way. Cybersecurity services, support customers' efforts to safeguard R&D centers, plants, buildings distribution centers, data centers, and other critical environments.

In a digital world, no company can become a castle. Every organization is exposed to the threat of cyberattacks in the age of the rapid convergence of IT/OT. And at this convergence, the technology aspect of cybersecurity only partially addresses the issue of ongoing cyber threats. Organization-wide changes, processes, and employee training must inform and bolster any company's cybersecurity stance for mitigating digital risk. Cybersecurity strategy must be an ongoing business conversation for every company engaged in digital transformation, and the Chief Security Officer must have a regular seat the table. Digital innovation depends on it.

References

Margin statistical references

Board decisions / risk data: Survey reported in Rob McMillan and Paul E. Proctor, Gartner, "Cybersecurity and Digital Risk Management: CIOs Must Engage and Prepare." Published 17 January 2018 - ID G00349114 https://www.gartner.com/document/3846477

Average age of U.S. nuclear power plants: U.S. Energy Information Administration, https://www.eia.gov/tools/faqs/faq.php?id=228&t=21

Malware variants: McKinsey Cybersecurity and Cyberrisk Service Line, cited in "Digital and Risk A new posture for cybersecurity in a networked world," March 2018. https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world

Days to detection: Thomas Poppensieker and Rolf Riemenschnitter, McKinsey & Company, "A new posture for cybersecurity in a networked world," March 2018. https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world

Cost savings from rapid detection: Ponemon Institute, "The 2018 Cost of a Data Breach Study," July 2018

CISO / new business decision making: Accenture Security, Cyber Resilient Business, "Building pervasive cyber resilience now," June 26, 2018. https://www.accenture.com/us-en/insights/security/securing-future-enterprise-today

Body copy references

[1] Gartner, Annual Security and Risk survey in five countries between 24 February and 22 March 2017. Cited in "Cybersecurity and Digital Risk Management: CIOs Must Engage and Prepare," Published: 17 January 2018 ID: G00349114 Analyst(s): Rob McMillan, Paul E. Proctor. https://www.gartner.com/ngw/eventassets/en/conferences/sec24/documents/gartner-security-risk-management-summit-us-research-note-cybersecurity-digital-risk-management-2018.pdf

[2] Wolfgang Schwab and Mathieu Poujol, "The State of Industrial Cybersecurity 2018 White Paper," commissioned by Kaspersky Lab, June 2018. https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf

[3] "Cybersecurity and Digital Risk Management: CIOs Must Engage and Prepare." Published: 17 January 2018 ID: G00349114 Analyst(s): Rob McMillan, Paul E. Proctor https://www.gartner.com/document/3846477

[4] "New IDC Spending Guide Forecasts Worldwide Spending on Security Solutions Will Reach $133.7 Billion in 2022." October 4, 2018. https://www.idc.com/getdoc.jsp?containerId=prUS44370418

[5] https://www.nist.gov/cyberframework

[6] Thomas Poppensieker and Rolf Riemenschnitter, McKinsey & Company. "Digital and Risk: A new posture for cybersecurity in a networked world Leading in a disruptive world." March 2018. https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world

[7] Ayal Tirosh and Paul E. Proctor, Gartner, "Shift Cybersecurity Investment to Detection and Response," Refreshed: 3 May 2017' Published: 7 January 2016 ID: G00292536. Statistic cited at https://www.gartner.com/newsroom/id/3337617

[8] Thomas Poppensieker and Rolf Riemenschnitter, McKinsey & Company, "A new posture for cybersecurity in a networked world," March 2018. Available at https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world

[9] Ponemon Institute, "The 2018 Cost of a Data Breach Study," July 2018