Building a Cybersecurity Strategy for the Life Sciences Industry

se.com

Life Is On | Schneider Electric

Table of contents

Strengthen digital trust:

1

Controlling risks to safety, efficiency, reliability, and profitability

Identify ecosystem threats:

2

Securing your digital supply chain, including partners, integrators, and other providers

Protect the end-to-end ecosystem:

3

Safeguarding efficiency, safety, reliability, and uptime at the convergence of IT/OT

Detect and respond quickly:

4

Monitoring threats 24 / 7 and lessening their impact with proactive plans

Recover and share lessons learned:

5

Learning from each and every incident to strengthen resilience

Improve security at IT/OT convergence

6

Leveraging three IT security practices for the digital ecosystem

Strengthen digital trust

Controlling risks to safety, efficiency, reliability, and profitability

Cyber threats and incidents are a major operating and business risk for every digital enterprise. In age the of digitisation, creating and executing a strategy that allows you to see, reduce, and respond to cyber threats and risks is critical for achieving your financial objectives.

Scrutinising digital risk

642 Bn

Predicted loss from Life Sciences companies over the next five years (globally, USD)

Life Sciences companies are likely to lose 642 billion USD globally to direct cyber attacks over the next 5 years, according to a recent Accenture report.[2]

Scrutinising digital risk

Data, analytics, Iand artificial intelligence create a significant growth opportunity for Life Science organisations: real world data and artificial intelligence are expected to completely change R&D operations. With this, data becomes more criticial for the success of Life Sciences Orgnisation. Executing a holistic cybersecurity strategy is an urgent business imperative and competitive — it's not just a technology issue. As your digital footprint expands, a result of rapid IoT integration, strengthening your company's security posture is essential for establishing the digital trust you need to compete. But where do you begin?

The purpose of this e-guide

This e-guide will help you establish a pragmatic approach for creating a multi-layered cybersecurity strategy to help you reduce your business and digital risks. It focuses on developing an end-to-end approach that considers people, process, and technology; is aligned to the NIST framework; and uses ISA / IEC 62443 and ISO 2700x standards (and others) to help you safeguard your entire digital ecosystem. The guide draws on Schneider Electric use cases and other experience to illustrate how, through our Cybersecurity Services and offers, we can help you deploy your strategy.

Securing your end-to-end digital ecosystem

Today, understanding digital risk means looking well beyond a sole connected object or database, identifying risk across your full extended digital enterprise.This end-to-end ecosystem includes supply chain and partners. Just as important, you must be able to communicate a clear digital risk strategy across your company and to your Board, as these organisations also host sensitive information about patients, patented drugs, clinical trials, research projects, and advances in technology.[3]

We recommend leveraging the five-part National Institute of Standards and Technology (NIST) Cybersecurity Framework for securing your digital enterprise and fortifying the resilience of your critical infrastructure. You can look to it as a good practice for integrating cybersecurity building blocks in a digital world that knows no perimeter.

Schneider Electric itself has adopted this approach

See the “Cybersecurity at Schneider Electric” white paper for a full view of our own cybersecurity strategy. Discover more

“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.”

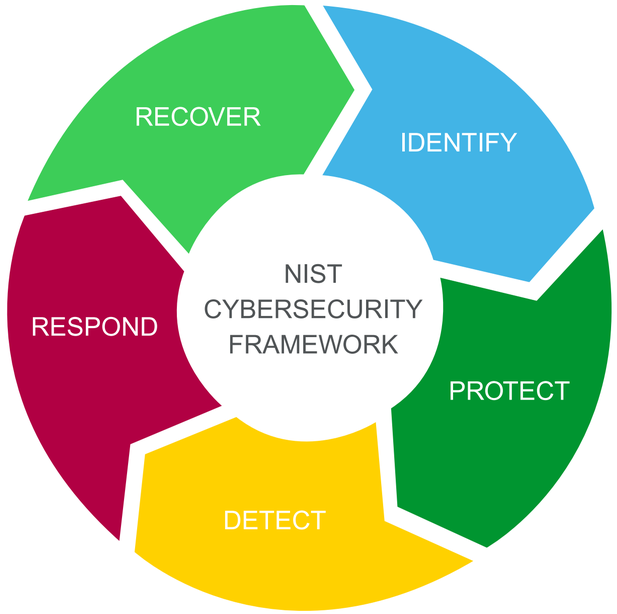
Hervé Coureil, Chief Digital Officer, Schneider Electric

A closer look at the NIST Cybersecurity Framework

In a connected, always-on world, just protecting the perimeter is no longer enough. No one is isolated, nor can we afford to be. To keep pace with real-time market dynamics and competitive pressures, every organization needs to take advantage of new trends in digitization. But implementing new technology often expands your attack surface. However, the five functions of NIST's layered approach enable you to push onward with your digital transformation journey while reducing your business and digital risks.

1. Identify

The goal is to develop an organizational understanding of managing cybersecurity risk to systems, people, assets, data, and capabilities.



2. Protect

The goal is to outline safeguards that facilitate delivery of critical infrastructure services and to limit / contain the impact of a potential cybersecurity event.

3. Detect

The goal is to define the appropriate activities to identify when and where a cybersecurity event occurs, enabling a timely discovery of incidents.

4. Respond

The goal is to be able to take immediate action regarding a detected cybersecurity incident, supporting your ability to contain its impact.

5. Recover

The goal is to map out clear recovery plans for resilience and to restore any capabilities or services impaired by a cybersecurity incident.

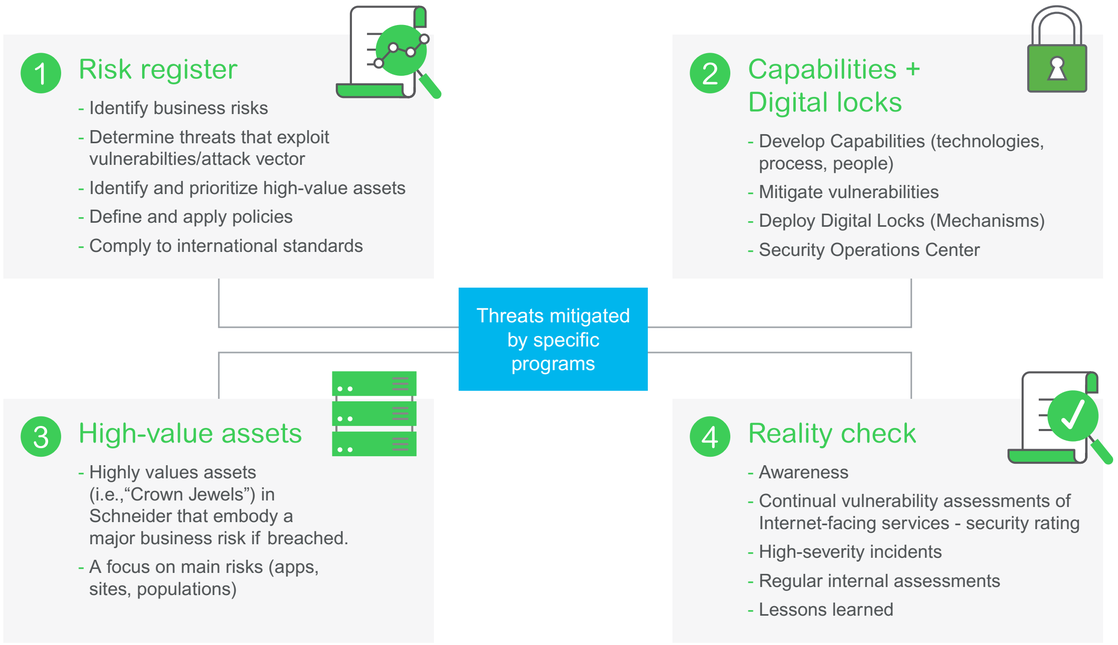
Mapping out your secure enterprise strategy

The benefit of the NIST framework is that you do not have to re-create the wheel for your own adaptation and adoption. The five high-level pillars of the NIST framework are meant to be flexible guideposts for your own holistic cybersecurity strategy.

What are high-value assets?

These include your most sensitive corporate assets and populations, such as your R&D, your IP, your data, and your mission-critical equipment. Assuring maximum security for your high-value assets requires specific and different levels of protection, for example identity and asset management, as well as dedicated training and specialized processes and tools, for example when working in remote locations and being connected to customers assets. The goal is to prevent any durable impact on your business continuity and the quality of service you provide your customers. McKinsey notes that companies can realize 20% cybersecurity ROI savings by prioritizing high-value assets (e.g., R&D) alone.[4]

An adaptation example Schneider's own Digital Security Approach



Identify ecosystem threats

Controlling risks to safety, efficiency, reliability, and profitability

600%

increase in overall IoT attacks in 2017.[5]

In today's hyperconnected world, approaching cybersecurity as a business enabler — instead of as a technology issue — is mandatory. That's how you will ensure business continuity, while protecting your people, your assets, and the communities you serve.

Three areas of identification

A strong digital risk strategy recognizes that cybersecurity is not just a “feature” of a your hardware and software components. Instead, it is a fundamental, ongoing business practice that helps you identify, mitigate, and reduce risks by applying standards and good practices to your people, processes, technology and research.

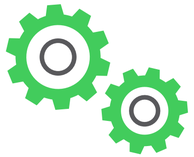
Need to know where you stand?

Understanding where your systems are vulnerable is the first step to protecting them. Schneider’s comprehensive cybersecurity assessment and analysis can reveal the gaps between where you are now and worry-free protection.

Start here with Schneider Electric’s cybersecurity assessment service. Discover more

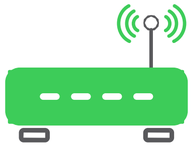
People

Strong cyber protection requires an educated and aware workforce. In many cases, your people are your first and last lines of defense. A crucial element of this area is creating and communicating a company-wide security culture, advanced by ongoing training on standards, such as ISA / IEC 62443, and recognized good practices to reduce the chance of human error.



Process

SA recommended way to identify and eliminate cyber risks is to establish and adhere to good processes, practices, and policies. Companies should begin to perform consistent, regular risk and threat assessments and gap analyses. For example, what is your clear plan for incident response? What steps are you taking to secure your R&D, your supply chain, and your deployment channels?



Technology

Your cyber defense is only as strong as the technology that manages and controls your operations. This, too, requires a collaborative approach. This facet is all about protecting what your company develops and deploys, as well as ensuring that the technology coming from your supply chain vendors is secure. Attention is required both at a product level and at a system level.

What does your risk landscape look like?

Any company mapping out a cybersecurity strategy starts with the same challenge: identifying risk across the extended enterprise. The biggest mistake you can make is not taking the time to scrutinize where your potential risks are and, just as important, how unaddressed vulnerabilities will affect your business. In addition to securing your enterprise, you must determine your gaps and areas of weakness, at the points of IT / OT convergence.

What are the key parts of this digital landscape?

Enterprise IT
Enterprise resource planning, cloud, data center, finance, human resources, endpoints and bring your own device, data hub

Product lifecycle
R&D and product development, IoT architecture and integration, product upgrades

Manufacturing sites
Factories, field service representatives, distribution centers, suppliers

Customers
Remote customer support, digital services tools and platforms, Web, e-commerce

Ecosystem
Cloud business platforms, digital solution offers, partners / providers

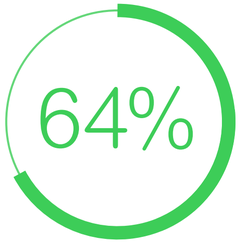
Communicating to stakeholders

Once you have created a strong cybersecurity approach to securing your digital ecosystem, the next step is to make sure your providers and / or suppliers understand and comply with your security policy. If you're considering new collaborations such as Joint Ventures or mergers and acquisitions, carefully evaluate the cyber-risk. Develop a cyber due diligence process alongside other areas of due diligence during a transaction to avoid unanticipated risk exposure.

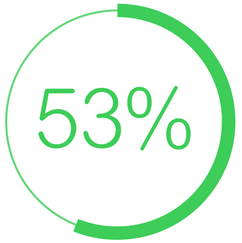
50%

Increase in cyberattacks on the biotech and pharma industry between 2019 and 2020

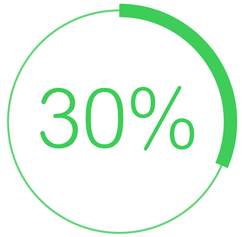
Common causes of OT / industrial control / industrial network incidents[6]:



conventional malware / virus outbreaks



Breaches in pharma and biotech industries as a result of malicious activity



ransomware attacks

Protect the end-to-end ecosystem

Safeguarding efficiency, safety, reliability, and uptime at the onvergence of IT/OT

120M
new malware variants every year

More than 100 billion lines of code are created annually, and hackers produce some 120 million new variants of malware every year.[7] A defense-in-depth approach is essential to protect your full digital ecosystem.

Protecting people, process, and technology

Adopting a defense-in-depth approach is a good way to bolster your company's cybersecurity strategy. Here are three considerations to help you solidify your stance:

1. View cybersecurity as a business enabler

The first step here is lining up the right stakeholders to connect the dots across your company. Right now, only 30% of CIOs work in conjunction with CISOs to take steps, together, to ensure a business-led approach to digital risk across the organisation.[8] In addition to addressing safety at all times, it's important to frame security in the context of a business conversation: "What is the bottom-line impact of cyber threats to cost, continuity and collaboration. What is the risk to research and innovation?" "What is the risk to brand and reputation?"

2. Widen the risk aperture beyond the perimeter

Remember that there is no perimeter for any digital enterprise. View risk beyond your own companies boundaries; Life Science organisations are reliant on a large number of third parties, including IT providers, data collection, external advisors and analytic firms as well as contract manufacturing organisations (CMOs) and clinical research organisations (CROs). The use of third parties means that businesses rely on systems and data over which they don't have complete control, making them even more susceptible to a cyber event. Working alongside these third parties to develop security and resilience reduces the risk across the entire supply chain.

3. Adopt a "secure-by-design" approach

Cybersecurity must be a continuous activity, summed up as an always-on "secure-by-design" business process and mindset. This means addressing security at every step as a proactive business imperative and enabler of successful digital transformation instead of as a reactive, costly afterthought.

“Your cybersecurity strategy cannot be reactive. Your digital transformation is a business opportunity, but it requires a proactive, end-to-end approach to identify, mitigate and reduce cyber risks. It is a business conversation that spans the entire organization and supply chain, including your digital ecosystem of partners.”

Christophe Blassiau, Chief Information Security Officer, Schneider Electric

Gaining confidence from a “secure-by-design” approach

As a digitally transforming enterprise, you must strike a balance between investment, threat mitigation, and the integration of IoT-enabled technology innovations that deliver business value. Standards provide good indicators and assurances that the products and systems you integrate from vendors arrive inherently secure, thereby allowing you to protect uptime and lower cyber risk.

Products guided by the ISA / IEC 62443-4-1 standard Secure Development Lifecycle process, for example, address security from the very beginning of product development through the lifecycle. This standard is the internationally recognised standard for the development of industrial automation and control system environments. Schneider Electric delivers secure systems and solutions following this “secure-by-design” lifecycle development process, which is based on three driving principles:

1. Alignment to the IEC 62443-4-1 standard for the Secure Development Lifecycle Process.

2. Increased rigor and consistency to ensure a common approach to building security into our products for all of Schneider Electric based on IEC 62443-4-2.

3. Support of Schneider’s own end-to-end initiative across all software and system development lifecycles using IEC 62443-3-3.

“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, Chief Product Security Officer, Schneider Electric

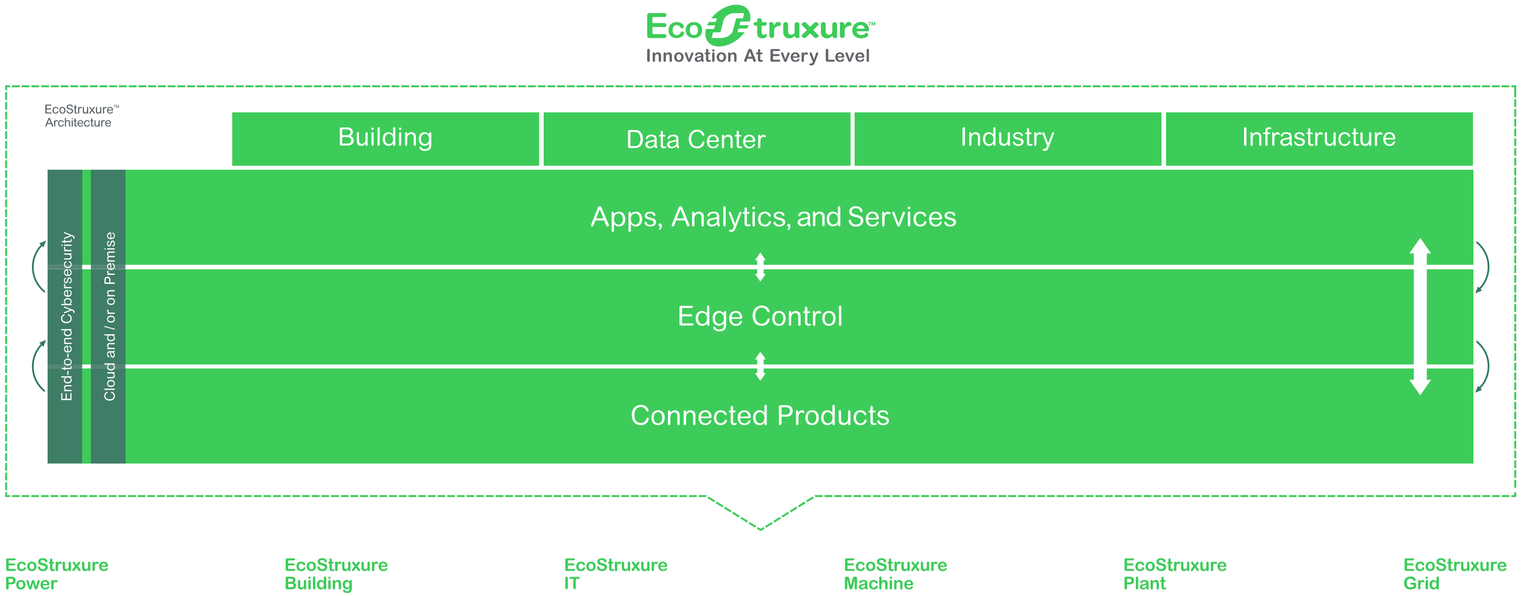
A continuous cycle

The Schneider Electric approach to SDL process adopts a user-centric strategy where all project members (roles) have responsibilities. secure-by-design principles for products support the defense-in-depth strategy as a key element for success.

A secure IoT-enabled architecture

As a manufacturer itself, Schneider Electric embeds security throughout its 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, embedded across these layers, which converge IT and OT equipment and solutions, software, and services within six domains of expertise.

Discover more

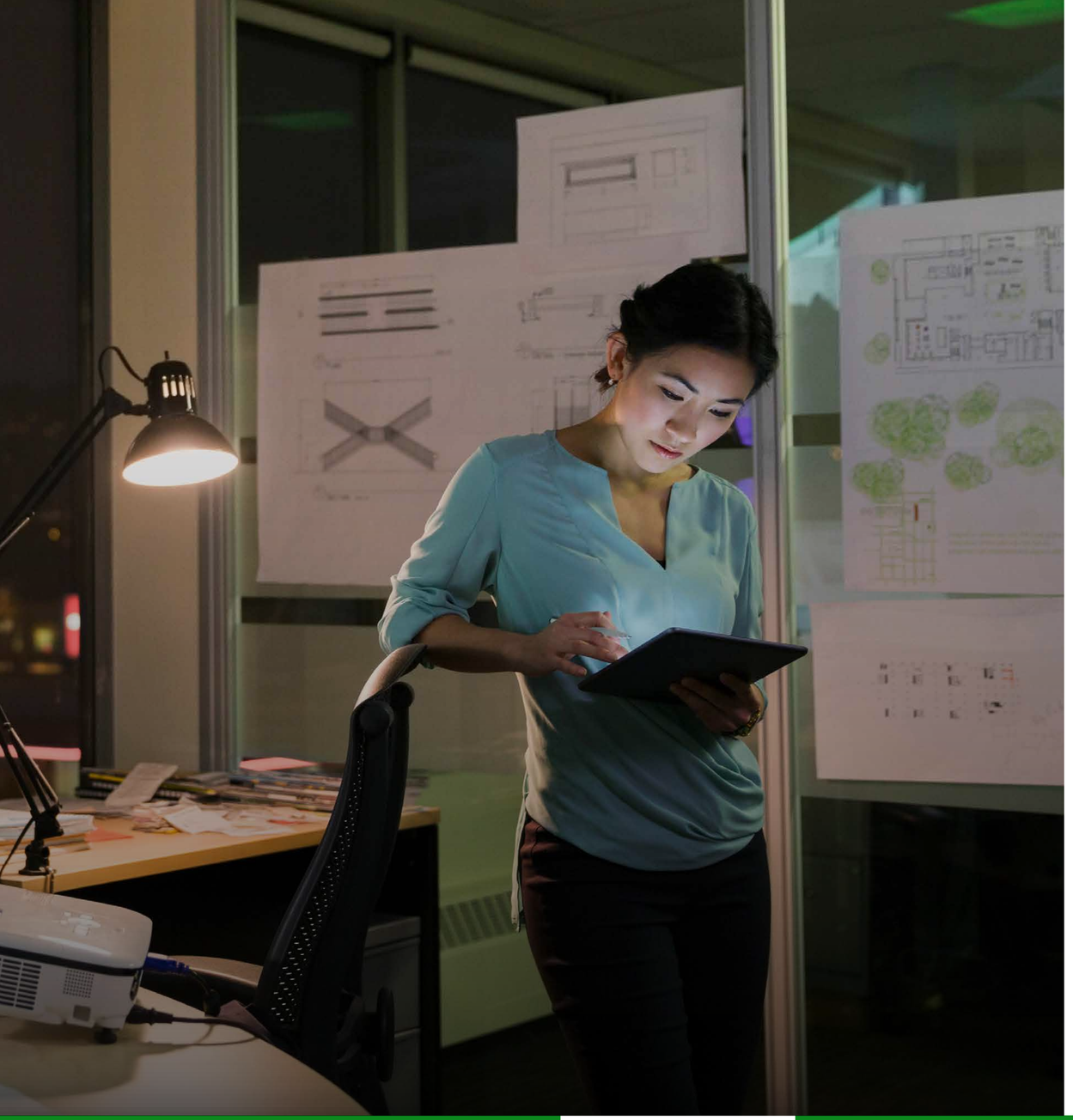


Partnering with cybersecurity experts

Every digital company today must leverage an extended enterprise approach to address, reduce, and eliminate vulnerabilities, working with an open ecosystem. Working together toward the greater good of our digital economy is essential. This practice includes engaging in public and private partnerships. For instance, Schneider is an active member of Cybersecurity at MIT Sloan (CAMS), 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. Schneider is also a founding member of the ISA Global Cybersecurity Alliance.

Strengthening digital trust:
As a member of the Cybersecurity Coalition, Schneider Electric affirms openness and advocacy for securing the digital economy and strengthening cybersecurity policies and laws to benefit customers, partners, and its extended ecosystem.

ISA GLOBAL CYBERSECURITY ALLIANCE
Founding Member



Protecting legacy systems

One of the major challenges for securing both IT and OT equipment, however, is how to address the cybersecurity hurdles of pre-digital legacy systems. 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.

Patching whenever possible

Continually securing your legacy operations and systems is a challenge, but it’s not impossible. In much the same way software updates are regularly provided to computer users, your mission-critical operating assets can sometimes be updated too. Make sure you subscribe to providers’ updates and notifications regarding end-of-life support or newly discovered vulnerabilities. In many cases, your providers will provide an immediate fix via download, recommend workarounds, or other mitigations, and put you on a path to risk mediation.

Protecting legacy systems

Of course, it's also critical to always adhere to industry recognised practices to further reduce threats to your legacy installations. Taking these precautions and speaking with certified cyber service consultants and providers can significantly increase your layers of protection:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Implement physical controls so that no unauthorized person has access to the ICS and safety controllers, peripheral equipment, or the ICS and safety networks.
- Lock all controllers in cabinets and never leave them in the "program" mode.
- Keep all programming software locked in cabinets and never connect them to any network other than the network for the devices that it's intended.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before using in the terminals or any node connected to these networks.
- Ban laptops that have connected to any other network besides the intended network from connecting to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and / or systems, and ensure that they are not accessible from the Internet.
- Use secure methods, such as Virtual Private Networks (VPNs), when remote access is required, recognizing that VPNs may have vulnerabilities and should be updated to the most current version available.
- Recognize that VPN are only as secure as the connected devices.

Detect and respond quickly

Monitoring threats 24 / 7 to anticipate and reduce their impact

$1M

recovered companies that contained data breaches within 30 days of detection[9]

Acting quickly to lower the impact of data breaches is imperative. The Ponemon Institute reports significant recovery cost savings if breaches are contained quickly vs. 30+ days to resolve.

Monitoring incidents 24 / 7 with a 360° lens

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 detectand-respond strategy, in addition to preventive measures, is critical for being able to counterattack breaches and threats immediately.

By 2020, 60% of enterprise information security budgets will be slated for rapid detection and response approaches (vs. just 20% in 2015).[10] According to McKinsey & Company, "companies still need about 99 days on average to detect a covert attack."[11]

Strengthening the ability to monitor threats

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 also can furnish regular reports regarding the nature and volume of threats and the actions that have been taken to neutralize those threats. 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.

Leveraging artificial intelligence

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. It is important to note that AI is the next frontier for hackers, too. Malicious actors are already using AI to make themselves harder to detect and stop. That's why it has become even more critical to stay one step ahead.

99 days on average to detect a covert attack.[11]

No in-house expertise?
24 / 7 managed services are available.

Discover more

Developing incident response plans

The response to an incident — regardless of whether it's an enterprise IT issue or threat or attack on your operational infrastructure — must be based on a proactive, tested plan to minimise risk, protect customer trust, and strengthen customer assurance. In addition to lowering business impact and cost, a rapid response can protect the safety of factory and industrial site workers, and / or the public at large.

In some cases, 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. But this approach, which gives industrial players a transparent response that doesn't inconvenience the user, doesn't eliminate the need to keep up with available patches and other good practices (as discussed on pages 19 and 20) to provide maximum security along the entire value chain.

Don't forget third-parties

As always, look across your digital ecosystem. As explained by McKinsey & Company, "[Companies] might have welltuned security operations and incidentresponse processes. But what about thirdparty suppliers, which might be the weakest link of a company's value chain?"[12] Be sure to assess vendor risk regularly for key partners and third parties.

Discover more

Recover and share lessons learned

Learning from each and every incident to strengthen resilience

2/3
of global CEOs concerned about cyber and growth

A 2017 PwC study of global CEOs revealed that nearly 62% indicated that cyber threats are a concern for their company's growth prospects.[13] Indeed, cybersecurity is a business strategy.

Learning from every incident

Should an incident occur, take every step to learn as much from the incident as possible, and to revisit and adapt your 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.

The goal of recovery is to eliminate the cause of the breach and its impacts in order to get back up and running as safely, securely, and quickly as possible.

To learn as much as possible through root cause analysis:

1. Uncover key learnings related to people, process, and technology

2. Map the issues that may be roadblocking prevention

Open knowledge sharing To move the needle forward across industry, collaborative knowledge sharing is essential. For example, the ISA Global Cybersecurity Alliance fosters open sharing of ongoing lessons learned, encouraging vendors to step forward to share incident information for the betterment of all while reducing the risk of such collective intelligence.

Because taking on newer, more innovative and increasingly dangerous threats can't be limited to a single company, industry or region, Schneider Electric commits to being open, transparent, and collaborative to help global industry prevent and respond to cyber-attacks.

Need help creating a recovery roadmap?
Connect with our cybersecurity consultants.
Discover more

Building a cyber-resilient culture

Security is everyone's problem. It must be something that everyone at your digital company inherently thinks about every day, everywhere. About 90% of malware is still delivered by email.[14] It takes just one bad click to open the gates to the nefarious cyber underworld. Cybersecurity therefore must become ingrained in each of your employee's daily actions.

Learning and enablement

In most companies today, lack of cybersecurity training represents a big gap in terms of overall readiness and digital security. A comprehensive program must account for the human element in a digital ecosystem. More than just hardware and software resilience, security rigor includes a process and plan that define the roles and responsibilities of employees and workers. It defines the types of actions and activities that are allowed to be performed, and includes clearly communicated consequences for noncompliance.

Ongoing learning and enablement about cybersecurity is essential. When developing your training programs, think about creating basic level awareness sessions to expert-level courses, depending on the roles of your individual employees. Training should include online options, classroom training, hands-on configuration awareness training for your first line of defense, and table top sessions with your cybersecurity organization to simulate and address "What if?" scenarios.

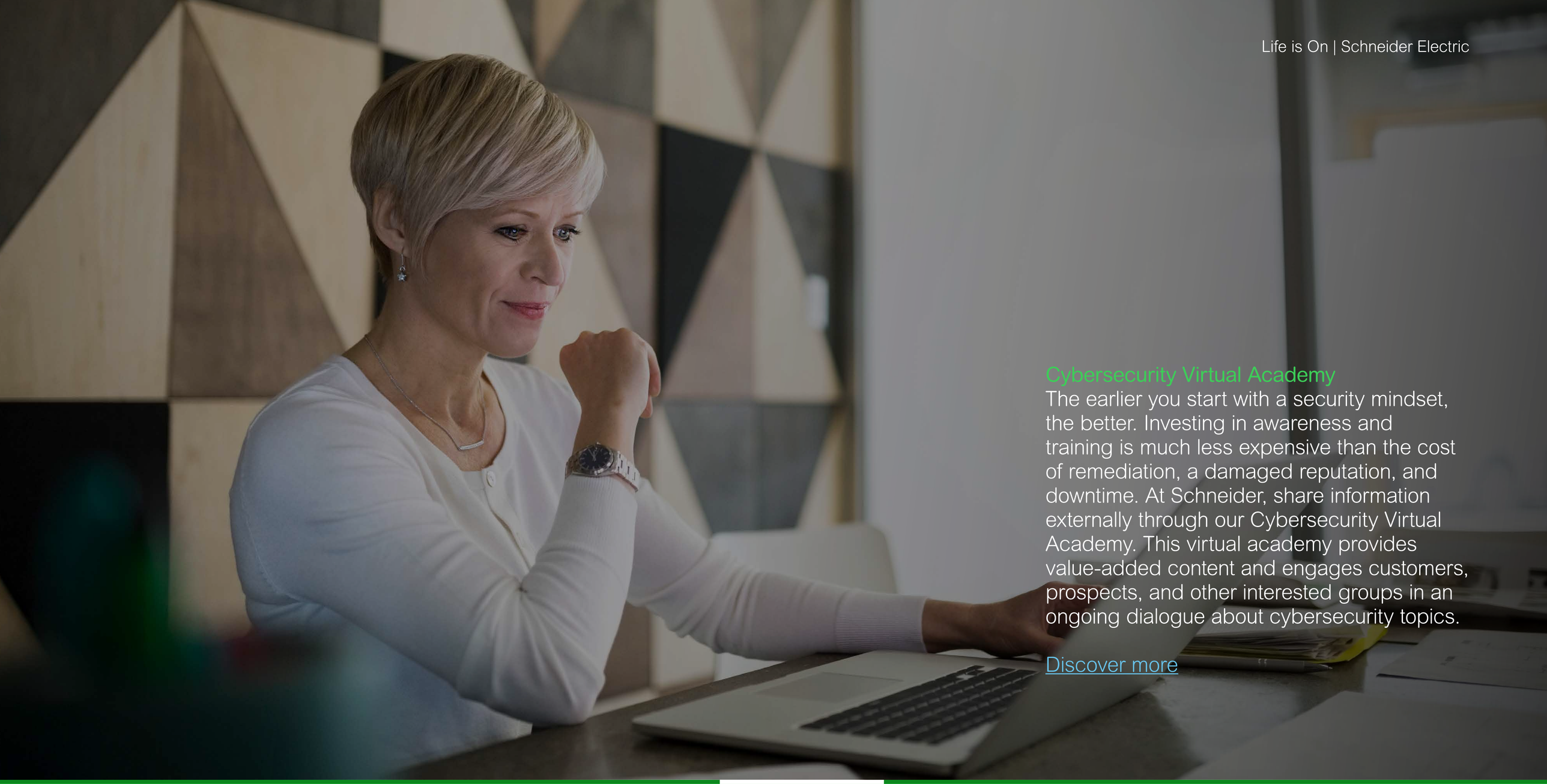
It's important, too, to integrate both an understanding of the ISA / IEC 62443 standard and, more important, learning how to apply it across the business, operation, or function. Trainers and training can be certified as well.

Empower your staff

Schneider's extensive education modules teach security controls and methods, as well as cybersecure behavior. Discover more

“For any employee to be a good cyber citizen, they need a solid understanding of what digital trust means to the company and to our shared global digital economy. Depending on their role, some employees may need a deeper understanding than others. But all should be thinking, ‘Am I doing the basics to get my job done today while keeping cybersecurity and data privacy top-of-mind?’”

Elizabeth Hackenson, Chief Information Officer, Schneider Electric



Cybersecurity Virtual Academy

The earlier you start with a security mindset, the better. Investing in awareness and training is much less expensive than the cost of remediation, a damaged reputation, and downtime. At Schneider, share information externally through our Cybersecurity Virtual Academy. This virtual academy provides value-added content and engages customers, prospects, and other interested groups in an ongoing dialogue about cybersecurity topics.

Discover more

Improve security at IT / OT convergence

Seizing the benefits of IT / OT convergence across the digital ecosystem

98% of industrial companies expect to increase efficiency by 2020 with digital technologies, including predictive maintenance and augmented reality.[15]

Rethinking security for today's digital landscape

The IT / OT convergence can enable you to make better, real-time business and operating decisions so you can react far more quickly to changingmarket dynamics and the competitive landscape. But to take advantage of it, you need to think differently about cybersecurity. Leveraging realtime operating data to inform better supply chain decisions or to improve customer relationship management requires new tactical approaches and a different mindset.

You no longer can expect your OT and production systems to be obscured by proprietary standards and hard-wired connectivity. So how will you protect an attack surface that has been widened by the prevalence of sensors, intelligent devices, and other at-risk digital endpoints? Without a strong, resilient, standards-based strategy and approach, each of these endpoints is a possible entry point for would-be attackers. Fortunately, there are ways for you to reduce these risks:

1. Re-think your strategy for OT

Hackers understand OT's traditional "set it and forget it" mindset. It's time to re-think your patching strategy for the OT world to enable fast patching where applicable, combined with a defense-in-depth strategy. Making sure connected systems are patched whenever possible to close any known vulnerabilities is a dose of cyber risk prevention that goes a very long way.

2. Secure your supply chain by mapping out OT indicators

Map out what constitutes normal behavior across your industrial infrastructure. This exercise is very different for OT, as risk indicators can be unique across systems. A meshing of IT skills with specialized domain expertise is essential for knowing which signals demand immediate attention.

3. Adopt a defense-indepth approach

Defend your enterprise's perimeter and then add layered protection and practices across your digital ecosystem. In our hyper-connected world, the mindset should be one of "zero-trust," meaning that you assume that no environment is completely trustworthy. For product cybersecurity, design your component expecting the outer layer to fail with inherent safeguards for protection.

Security takes an extended enterprise.

Discover how Schneider Electric cybersecurity Services can accelerate your own digital transformation in a safe, secure way. Discover more

Sources

01. Gartner Annual Security and Risk Survey, February - March 2017, cited in Rob McMillan and Paul E. Proctor, Gartner, “Cybersecurity and Digital Risk Management: CIOs Must Engage and Prepare.” Published 17 January 2018 - ID G00349114
02. IDC FutureScape: Worldwide IoT 2018 Predictions, November 2, 2017. Doc # US43161517
03. Gartner Annual Security and Risk Survey, February – March 2017, cited in Rob McMillan and Paul E. Proctor, Gartner, “Cybersecurity and Digital Risk Management: CIOs Must Engage and Prepare.” Published 17 January 2018 - ID G00349114
04. 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
05. The Symantec 2018 Internet Security Threat Report.
06. Wolfgang Schwab and Mathieu Poujol, “The State of Industrial Cybersecurity 2018 White Paper,” commissioned by Kaspersky Lab, June 2018.
07. McKinsey Cybersecurity and Cyberrisk Service Line, cited in “Digital and Risk A new posture for cyber risk in a networked world,” March 2018.
08. Gartner Security and Risk (2017) above. A total of 297 respondents answered the question (A03), “Does your organization have a Risk Steering Committee or Advisory Board?” Cited in Rob McMillan and Paul E. Proctor, Gartner, “Cybersecurity and Digital Risk Management: CIOs Must Engage and Prepare.” Published 17 January 2018 - ID G00349114
09. Ponemon Institute, “The 2018 Cost of a Data Breach Study,” July 2018
10. Ayal Tirosh and Paul E. Proctor, Gartner, “Shift Cybersecurity Investment to Detection and Response,” Refreshed: 3 May 2017’ Published: 7 January 2016 ID: G00292536.
11. Thomas Poppensieker and Rolf Riemenschnitter, McKinsey & Company, “A new posture for cybersecurity in a networked world,” March 2018.
12. McKinsey Cybersecurity and Cyberrisk Service Line, cited in “Digital and Risk A new posture for cybersecurity in a networked world,” March 2018.
13. For CEOs, Cybersecurity is both rising concern and significant opportunity,” by Dave Burg, US and Global Cybersecurity & Privacy Co-Leader, PwC; Grant Waterfall, US & Global Cybersecurity& Privacy Co-Leader, PwC; and Christopher Castelli, Director, PwC, 23 March 2017.
14. Verizon’s 2019 Breach Investigations Report.
15. PwC, “Digital Factories 2020; Shaping the future of manufacturing,” April 2017.

Life Is On | Schneider Electric

To learn more about **EcoStruxure**, visit
Schneider Electric Internet of Things

se.com

Schneider Electric
Stafford Park 5,
Telford TF3 3BL,
United Kingdom

Schneider Electric
Maynooth Business Campus,
Maynooth, Co. Kildare, W23 Y7XO
Ireland

998-xxxx