Cybersecurity at Schneider Electric: Addressing IT/OT convergence in a versatile Cyber ecosystem

by Schneider Electric

Executive summary

Cybersecurity and data privacy are integral to Schneider Electric's business strategy. Overall, Schneider aims to protect itself in order to protect its customers, following a multifaceted Cybersecurity posture that includes several aspects:

- Securing internal activities (e.g., secure collaboration, applications, etc.)
- Protecting strategic IT systems and assets
- Leading the digital transformation of energy management and automation within a Cybersecure framework
- Designing and developing new products and solutions with end-to-end Cybersecure measures and protection
  (i.e., from ideation to implementation)

This white paper covers the ways in which Schneider Electric mitigates Cyber risk from the top, led by Schneider Digital, to ensure that Schneider Electric and its customers and partners can thrive securely in today's digital economy.

Introduction

What keeps many executives up at night in the face of their company's digital transformation? *Cybersecurity*. A 2017 PwC study of global CEOs revealed that nearly two-thirds (62%) indicated that Cyber threats are a concern for their company's growth prospects. In fact, suffering a Cyberattack was the top 2018 concern of U.S. CEOs surveyed about "threats in a faster-growth world."[i]

It comes as no surprise, then, that IDC recently projected that by 2020, potential Cybersecurity and IoT-related physical safety concerns "will pressure CIOs at G2000 companies to increase IoT security spending by up to 25%, temporarily neutralizing business productivity gains."[ii]

Some of the swirling risks include the following:[iii]

- Threats to revenue and reputation due to data breaches
- System risk due to bogus system access and control
- Inherent system vulnerabilities from cloud data storage and computing
- Physical damage to machines and factories from malicious attacks

A recent report released by McKinsey[iv] shows some impressive figures: More than 100 billion lines of code are created annually, and, every year, hackers produce some 120 million new variants of malware.

Cybersecurity and data privacy therefore are integral to Schneider Electric's business strategy. Overall, Schneider aims to protect itself in order to protect its customers, following a multifaceted Cybersecurity posture that includes several aspects:

- Securing internal activities (e.g., secure collaboration, applications, etc.)
- Providing elevated levels of protection of strategic IT systems and assets
- Leading the digital transformation of energy management and automation within a Cybersecure framework
- Designing and developing new products and solutions with end-to-end Cybersecure measures and protection (i.e., from ideation to implementation)

In addition, Schneider Electric develops and proposes Cybersecurity services to support its customers in their own Cybersecurity posture. These services consider the full lifecycle of Cybersecurity in the context of people, processes, and technology in the OT space for the customer environment.

As Gartner analysts note, "Cybersecurity is the foundation of digital business and innovation."[v] Schneider Electric views Cybersecurity accordingly. Indeed, it is *a business priority* — not just an IT issue. In recent years, Schneider elevated its Cybersecurity strategy to top leadership and governance, with oversight and initiatives throughout the Company.

Mitigating risk from the top

As a transversal division of Schneider Electric with a worldwide presence, Schneider Digital governs and coordinates Cybersecurity initiatives, projects, and actions companywide. Schneider Digital leverages a network of Cyber Experts and Digital Risk Leaders distributed across many businesses and territories.

For example, Schneider Digital oversees the continual implementation of Cybersecurity and data privacy layers holistically throughout Schneider Electric and its Extended Enterprise. In particular, this includes protection across:

1. The enterprise level, including Endpoints Protection, Identity and Access Management, and Security Operations Center
2. Assets and systems in customer sites that Schneider Electric remotely manages (with our IoT & Digital Offers)
3. Products and systems sold to customers (with our Product Security Office)

$3.62 million

Average total cost of a data breach in 2017

Schneider Electric, like other organizations with a similar global footprint and presence, is exposed to the risk of Cyberattacks and data privacy breaches. By 2020, 60% of digital businesses will have suffered a major service failure.[vi] The setback is costly: average total cost of a data breach in 2017 was $3.62 million;[vii] a major incident will cost a multiple of this. As breaches cannot be realistically avoided entirely, the objective of Schneider Electric, therefore, is to be both breach-resistant and breach-ready.

Digital Security Approach

Figure 1

NIST Framework

In line with the NIST framework[viii] with its five concurrent and continuous functions — *Identify, Protect, Detect, Respond, and Recover* — Schneider Electric has identified Cyber risks and vulnerabilities with its **Risk Register** (*Identify*), including key **High-Value Assets** (i.e., "Crown Jewels"). Threats are mitigated by initiatives implementing **Capabilities & Digital Locks** (*Protect*) — i.e., enforcing mechanisms. Events and incidents are monitored through a Security Operations Center driven jointly with IBM (*Detect & Respond*). Schneider Electric posture is continuously revisited and adapted through **Reality Check** (*Recover*), including emergency and improvement plans across the Company.

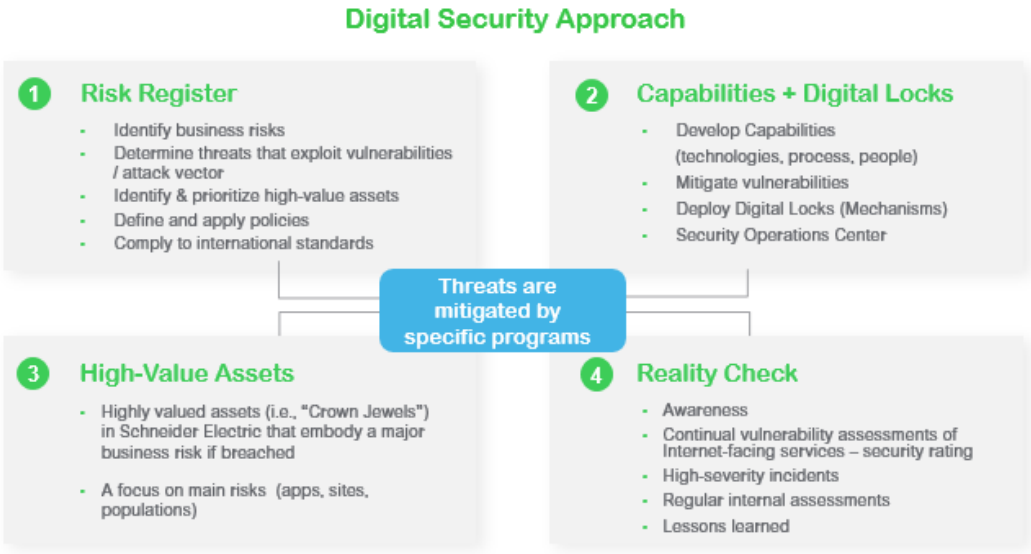


Figure 2

Schneider Electric Digital Security Approach

(1) Risk Register

Identification of the Cybersecurity-related business risks based on a potential impact assessment. This includes an assessment of potential vulnerabilities and attack vectors and definition of a remediation approach (that may encompass technologies, processes, and people), for the critical business risks identified.

(2) Identification and Prioritization of High-Value Assets

Specific and differentiated protection for the most sensitive corporate assets by ensuring that the right organization, technology, people, and governance are in place to prevent any durable impact on business continuity or quality of service provided to customers.

(3) Capabilities + Digital Locks

Implementation of 12 internal Cybersecurity capabilities (outlined below) that best mitigate identified vulnerabilities: (i) **technologies** such as Endpoint protection or Endpoint Detection and Response (ii) **processes** such as Security Operations Center to monitor incidents;(iii) **people** such as Awareness and Training programs on specific populations exposed to Cyber risks.

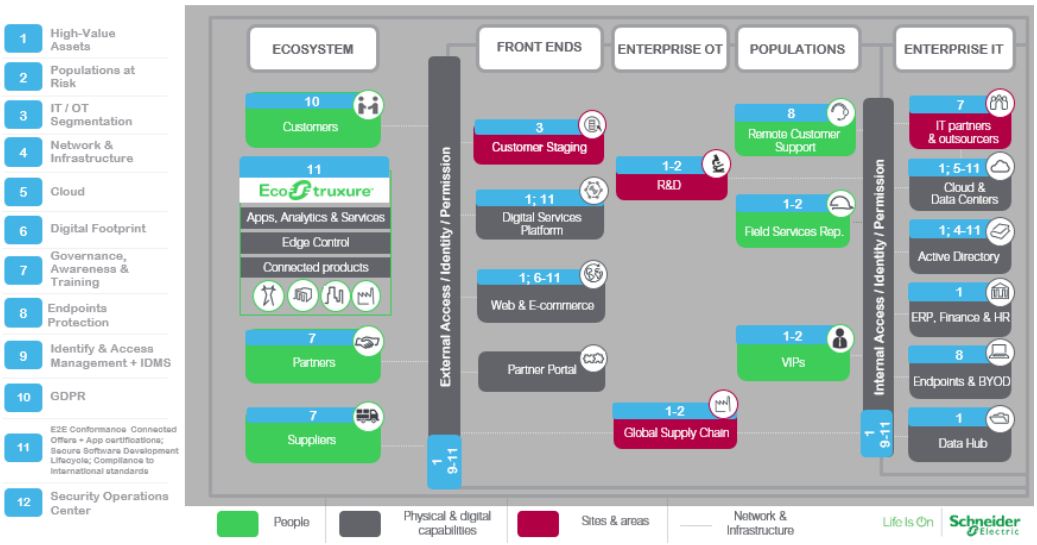
(4) Reality Check

Implementation of frequent third-party security ratings and assessment to further secure Schneider Electric's infrastructure and, in turn, the operations it supports. Additional regular internal vulnerability assessments and drills also are conducted, especially for Schneider's most critical sites (i.e., Global Supply Chain and R&D).

Risk Register: 12 Cyber Capabilities

Figure 3

A closer look at the 12 Schneider Electric Cyber Capabilities



IDENTIFY

Tailor protection in specific areas

(1) High-Value Assets ("Crown Jewels"), (2) Populations at risk, (3) IT / OT segmentation

For specific needs and sensitive areas such as Research and Development (R&D) labs, Schneider Electric protects its network with segmentation capabilities.

Relying on its *Crown Jewel initiative*, Schneider Electric has identified sensitive corporate assets, in turn deploying a series of specific control measures to enhance the level of protection against threats and vulnerabilities. Schneider Digital Security teams provide dedicated training and additional support to specific populations with high exposure to risk among these corporate assets. For instance, Field Services Representatives have been defined as a population at risk. Dedicated processes and tools have been put in place to meet their specific needs (e.g. working in remote locations and being connected to customers assets while ensuring maximum level of security).

Schneider Electric follows local regulations and uses additional industry established frameworks where needed to conform to Cybersecurity standards, such as IEC62443 and the ISO2700x suite, for its products, solutions, and services. The Company is in the process of applying these frameworks to its Supply Chain, through independent audits, certification requirements, and vulnerability management programs. For specific needs and sensitive areas such as Research and Development (R&D) labs, Schneider Electric is increasingly protecting its network with segmentation capabilities.

Schneider Electric also takes an active part in the evolution of today's industrial Cybersecurity standards, contributing to the standards and frameworks that will secure our products and services now and in the future.

PROTECT & DETECT

Secure our digital infrastructure

(4) Network and Infrastructure, (5) Cloud, (6) Digital Footprint

Schneider Electric relies on its own internal Public Key Infrastructure, enabling the organization to deliver digital certificates to secure applications and corporate data flows, and to control access to sensitive assets through mass device recognition and fleet management.

In addition, Schneider Electric engaged in a multiyear initiative to revamp its corporate Active Directory system, including the introduction of a dedicated operations and management organization for this key infrastructure component.

Schneider Electric also operates a high number of websites, portals, and partner tools, supported by mutualized or dedicated hosting facilities and service providers. Given that these front-end platforms could represent a major risk for most companies, the Company conducts regular penetration testing and vulnerabilities scanning on these infrastructures.

Secure our digital workplace

(7) Governance, Awareness & Training, (8) Endpoints protection

Through its global digital transformation program, Schneider Electric is applying Cybersecurity requirements to its continuously evolving digital workplace. With dedicated initiatives such as Endpoints protection, Schneider Electric ensured that the adoption and deployment of Windows 10 work-stations for its employees was complemented with the systematic introduction of Cybersecurity best practices in endpoint management. These relate to considerations such as use cases for granting and revoking administrative privileges, baseline BIOS configuration for laptops, automatic data sharing with Microsoft, and the installation of third-party applications on Schneider Electric assets.

23%

open phishing emails

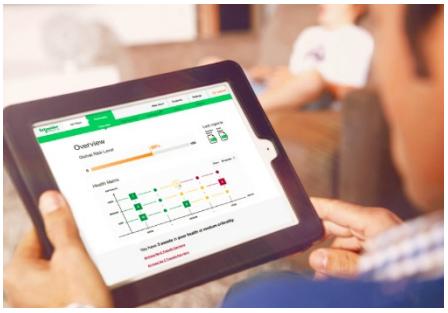
"Building a Security Practice with Microsoft" presentation by Anne Johnson, Microsoft VP, Strategic, Enterprise & Cybersecurity

In addition, a global learning and training initiative increases awareness and discipline about Cybersecurity for its employees, partners, and customers through regular trainings and phishing awareness exercises. Each employee plays a critical role here by participating in the annual mandatory Cybersecurity training campaign. Microsoft® has cited that 23% of recipients open phishing emails, and it takes only 24 hours to escalate from "click to compromise."[ix] To tackle this issue, white phishing campaigns (aiming at maintaining awareness of our employees in relation to phishing risks) and debriefs are organized globally in Schneider Electric.

The Company doesn't stop at its internal measures. As explained by McKinsey & Company, "[Companies] might have well-tuned security operations and incident-response processes. But what about third-party suppliers, which might be the weakest link of a company's value chain?"[x] To ensure maximum security along the entire Schneider Electric value chain, vendor risk and Cyber assessments are regularly conducted for key partners and third parties.

Protect identity and privacy

(9) Identity & Access Management + IDMS, (10) General Data Protection Regulation (GDPR)



Schneider Electric leads the digital transformation of energy management, automation, and industrial software and hardware for customers worldwide. The Company provides its customers with the Cybersecurity expertise needed to help them secure their installations, bridge the gap between IT and OT security, and better integrate Schneider Electric products and solutions within their industrial ecosystems in a secure fashion.

For example, Schneider Electric offers analytics services to clients that need to continuously monitor their mission-critical environments, facilities, buildings, or plants. Schneider Electric focuses on securing data flows coming from connected products and solutions (whether they connect to non-Schneider hosts or platforms managed by Schneider Electric), and on aligning to the latest data integrity and privacy regulatory requirements such as the European General Data Protection Regulation (GDPR). Schneider Electric runs dedicated compliance control and implementation programs to align to these regulations, under the leadership of the Company's Data Protection Officer (DPO).

In 2015, Schneider Electric decided to transform internal collaboration by bridging the gap between identity, access, and Cybersecurity. Through a multiyear effort and a dedicated program, Schneider Electric replaced its legacy Identity and Access Management (IAM) platform with a new one, allowing for a Single Sign On service associated with a multifactor authentication service for increased security of sensitive assets.

This approach has had a direct impact on improving the digital experience of Schneider Electric employees, partners, and contractors. Indeed, today, the Schneider Electric IAM platform addresses this entire population and protects more than 150 applications and portals. It also has improved the digital customer experience by protecting specific applications and portals.

Power innovation

(11) End-to-end Conformance Connected Offers + Secure Products (PSO) + App certifications

Research and Development is a key function at Schneider Electric, as it delivers innovation to customers and enhances the performance and efficiency of their operations. Cybersecurity priorities and measures enable Schneider to accelerate innovation and embrace IoT advancements such as analytics.

Schneider Electric integrates Cybersecurity in its products and solutions development lifecycle (“Cybersecurity by design”).

Schneider Electric therefore has integrated Cybersecurity in its products and solutions development lifecycle (*“Cybersecurity by design”)* to address relevant threats and attack vectors, establishing an innovation foundation wherein:

- The products, solutions, and secure software development lifecycle conforms to Cybersecurity standards, such as IEC62443 and the ISO2700x suite, followed and across Schneider Electric products and solutions portfolio, where appropriate.

- Schneider Electric connects its existing installed base with IoT solutions to augment proactive services and its Cybersecurity posture on existing installations. The Company runs a separate Public Key Infrastructure for its R&D division (*R&D PKIs*) to enable secure product development and customer deployment.

- Schneider Electric relies on and supports a wide range of partnerships with universities, private institutions, think-tanks, and government agencies to further strengthen its efforts on innovation and to improve the way security is built into Schneider Electric products and solutions. Schneider Electric, for example, is a member in MIT IC^3 (Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity).

- R&D teams, in collaboration with Strategic Digital Alliance partners such as Microsoft and Intel are advancing innovation where IoT and the Edge converge, thereby adding another layer of Cybersecurity protection. Such “Edge intelligence” can flag anomalies while ruling out false positives so operators can respond immediately to secure assets and operations.

- To secure identity management, authentication, and authorization across offers and integrated systems, a common capability has been put in place to speed up our go-to-market without duplicating effort.

RESPOND & RECOVER

Be resilient on incident response

(12) Security Operations Center and Incident Response

99 days

on average to detect a covert attack

McKinsey & Company, "A new posture for cybersecurity in a networked world," March 2018

In today's digital world, the prevention of Cyber-attacks is no longer sufficient. Ramping up a detection and response strategy, in addition to preventive measures, is fundamental to being able to counterattack breaches and threats immediately. In fact, by 2020, 60% of enterprise information security budgets will be slated for rapid detection and response approaches (vs. just 20% in 2015).[xi] According to McKinsey & Company, "companies still need about 99 days on average to detect a covert attack."[xii]

Schneider Electric uses a standards-based approach 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 website.

Schneider Electric helps its customers manage the risks associated with networked assets and greater use of connected systems, with a range of Cybersecurity services (to reduce the potential risk and associated damage from attacks, taking into consideration the unpredictability of hacker attack patterns and the impossibility of eliminating risks entirely).

Schneider Electric continues to invest in strengthening its resilience and responsiveness capabilities, in particular with its Security Operations Center (SOC) and Incident Response team, run in partnership with IBM Security.

Partnering with Strategic Partners

Schneider Electric works with strategic partners for its global Cybersecurity strategy and initiatives:

- Deloitte, for professional services and implementation of corporate Cybersecurity programs
- IBM, for the monitoring of key Schneider Electric assets and Security Operations Center (SOC)
- Microsoft, for corporate IT technology, collaboration enablers, and digital services
- McAfee, for Endpoint protection
- ZScaler, for cloud security gateway
- Illumio, for computer-based micro segmentation
- Cisco, for routers and network
- Amazon Web Services, for Schneider Electric web and internal cloud infrastructure
- Intel and US Department of Energy, for securing FPGA (for example, microgrid)

- BitSight on Cybersecurity rating
- Lookout, for mobile Endpoint protection
- An ecosystem of emerging Cybersecurity partners and startups

In addition to global partnerships, Schneider Electric is partnering with a regional ecosystem of stakeholders:

- Cooperation with local authorities and governments
- Network of national or regional partners, where relevant

Schneider Electric also leverages partnerships with best-in-class technology providers in its offers, in order to advance Cybersecurity and data privacy innovation within the EcoStruxure™ architecture, digital solutions, and services portfolio.

Indeed, as it embraces IT and OT convergence, Schneider Electric understands that many of its customers have third-party solutions integrated with Schneider solutions. This environment raises the risk for open gates to our systems. The Company's approach to mitigate this risk is to integrate its IT and OT partners and third-parties in a collaborative approach to address people, processes, and technology in the customer environment.

Conclusion

Thriving in the digital economy

At Schneider Electric, Cybersecurity is not an afterthought. Its companywide Cybersecurity posture, led by Schneider Digital, aims at securing the digital journey of Schneider, its partners, and its customers through:

- Strong and comprehensive digital governance and risk management
- A set of risk prevention, detection, and response capabilities and operational plan
- Specific attention to High-Value Assets
- A set of Reality Check metrics

This Cybersecurity posture fuels Schneider Electric innovation in IoT and enables the Company to advance IT/OT convergence and to ensure that Schneider, its partners, and customers can thrive in today's digital economy.

EcoStruxure™
Innovation At Every Level

EcoStruxure™ is our open, interoperable, IoT-enabled system architecture and platform. EcoStruxure delivers enhanced value around safety, reliability, efficiency, sustainability, and connectivity for our customers. EcoStruxure leverages advancements in IoT, mobility, sensing, cloud, analytics, and cybersecurity to deliver Innovation at Every Level. This includes Connected Products; Edge Control; and Apps; Analytics & Services. EcoStruxure has been deployed in 480,000+ installations, with the support of more than 20,000 system integrators and partners, connecting over 1 billion devices.

Find out more about EcoStruxure Click here.

References

[i]"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. http://pwc.blogs.com/resilience/2017/03/for-ceos-Cybersecurity-is-both-rising-concern-and-significant-opportunity.html; *PwC's 20th Global CEO Survey*, full report available at https://www.pwc.com/us/en/library/ceo-agenda/ceo-survey.html; "U.S. business leadership in the world in 2018." US supplement to the *21st Annual Global CEO Survey*, January 2018. https://www.pwc.com/us/en/library/ceo-agenda/pdf/21st-annual-global-ceo-survey-us-supplement.pdf

[ii]*IDC FutureScape: Worldwide IoT 2018 Predictions*, by Vernon Turner, SVP & IoT Research Fellow and Carrie MacGillivray, VP, IoT & Mobility, November 2, 2017.

[iii]For more on cloud risks for 2018, see "The dirty dozen: 12 top cloud security threats for 2018," by Bob Violino, CSO Online, January 5, 2018. Available at https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html

[iv]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

[v]Gartner Special Report. *Cybersecurity at the Speed of Digital Business*, Refreshed: 7 December 2017 | Published: 30 August 2016 ID: G00315580.

[vi]Gartner Special Report. See footnote v. Statistic cited at https://www.gartner.com/newsroom/id/3337617.

[vii]Ponemon Institute, *2017 Cost of Data Breach Study: Global Overview*, June 2017. Sponsored by IBM Security, independently conducted by Ponemon https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&. Survey profile: 419 companies in 13 country or regional samples.

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

[ix]Building a Security Practice with Microsoft" presentation by Anne Johnson, Microsoft VP, Strategic, Enterprise & Cybersecurity.

[x]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

[xi]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.

[xii]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

