# Cybersecurity, Product Security, and Data Protection at Schneider Electric

## Securing critical infrastructure through Zones of Influence: People, Company, Supplier/Partners, and Customers

Posture Paper


## Executive summary

This document details Schneider Electric's holistic approach to cybersecurity risk management along the value chain. The company's dedication to safeguarding critical infrastructure is articulated through its Zones of Influence via four key dimensions: people, company, suppliers and partners, and customers and authorities.

# Introduction

Critical infrastructure forms the backbone of society around the globe, and it is pivotal for maintaining economic stability, public safety, and overall well-being. This infrastructure spans vital sectors, such as energy, water, transportation, telecommunications, manufacturing, and healthcare, which are all integral to everyday life. The digital era has brought about a heightened level of connectivity in the critical systems and products that support the infrastructure in each of these sectors. This is a trend that has been accelerated by significant global events like the Covid-19 Pandemic and the advent of generative artificial intelligence (AI) capabilities. This has enabled advancements like increased innovation, remote operations, and enhanced efficiency and productivity.

The connectivity available today presents new risks and accelerates existing ones, particularly the exposure to sophisticated cyber physical threats that can severely impact critical infrastructure through disruptions such as plant shutdowns or interrupted service delivery.

The reality of this increased risk highlights the need to safeguard critical infrastructure. Schneider Electric's approach to cybersecurity aims to support the continuity of critical infrastructure essential services and strives to maintain the trust our customers place in us, as well as our broader value chain of suppliers, asset owners, asset operators, and system integrators.

# Building trust and resilience into everything we do

## Creating a strong cybersecurity risk management approach

Cybersecurity risk management is integral to Schneider Electric's flagship initiatives, from our offer lifecycle management framework to digital solutions powered by EcoStruxure©. As an open, interoperable IoT-enabled system architecture and platform, EcoStruxure is designed to enhance safety, reliability, efficiency, sustainability, and connectivity in critical infrastructure environments. It leverages advancements in IoT, mobility, sensing, cloud, analytics, AI, and cybersecurity to support various digital solutions across multiple sectors, including buildings, data centers, industry, and infrastructure.

Trust in EcoStruxure is paramount and built on the assurance that security measures are implemented throughout the lifecycle of our offers. As a global organization operating and delivering critical infrastructure and digital solutions in over 100 countries, Schneider Electric manages cybersecurity risks by building trust based on three principles as core in our Trust Charter: security, survivability, and transparency.

**Security** encompasses the comprehensive measures implemented to shield our company, operations, people, and assets. It includes securing our offers.

**Survivability,** also known as resilience, focuses on maintaining a holistic continuity of operations for essential systems and services, even in the face of challenges such as cyberattacks or natural disasters.

**Transparency** is about offering clear and consistent information about our security posture and actions as well as the origins, integrity, and performance of our products and services, including the data and processes underpinning them.

This trust is further enhanced by a holistic approach to resilience throughout the value chain that fosters stakeholder engagement and embraces a clear responsibility framework.

# Protecting critical infrastructure through Zones of Influence

## Recognizing different level of influence through the value chain

Schneider Electric addresses critical infrastructure cybersecurity risk through “Zones of Influence,” which encompass four key areas — people, company, suppliers and partners, and customers and authorities (Figure 1).

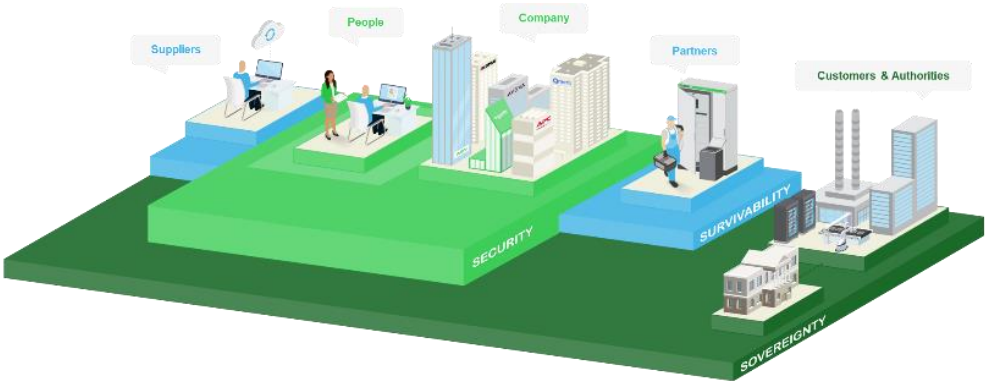



**Figure 1**

*Schneider Electric’s Zones of Influence*

These zones provide a structured approach which aims to shape a horizontal and collaborative security culture, provides accountability for risk mitigation, drives the designing and manufacturing of secure products, and safeguards the integrity of critical systems and services. They are also intended to support the sovereignty and compliance agenda of our customers and their countries, as every country has the duty to protect its citizens by securing critical infrastructure.

The Zones of Influence answer four questions that are key to building trust and resilience:

- People – How do we minimize human risk?
- Company – How do we secure the company?
- Suppliers & Partners – How do we stay resilient with suppliers and partners?
- Customers & Authorities – How do we protect customers via transparency?

# People: How do we minimize human risk?

## Focusing on people to reduce cyber risk

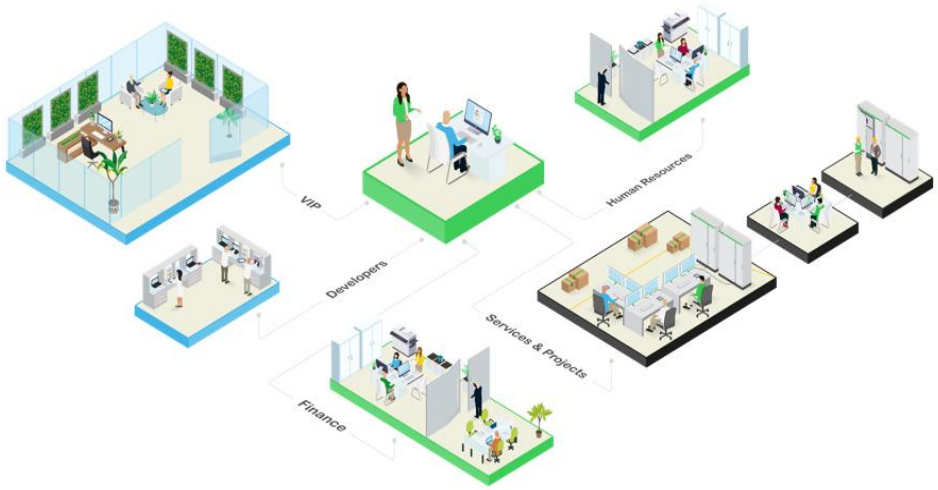
Humans, or the people within an organization, significantly influence our cybersecurity posture. They can be perceived as potential targets for malicious actors and threats to the company. However, when they are adequately trained and educated in cybersecurity, they can serve as a robust human firewall and a first line of defense.

Human error is a prevalent and significant source of cyber incidents and even the most diligent individuals can make mistakes. These errors can range from downloading malicious attachments to using weak passwords or misplacing storage devices, all of which can compromise system or data security. Human mistakes are amplified by AI-driven threats that leverage misinformation to deceive individuals for financial or other malicious motives. Additionally, employees can unintentionally become vectors for cyber threats due to the increasingly indistinct boundaries between their personal and professional lives.

Schneider Electric's companywide approach to cybersecurity culture, education, and training integrates elements of people, processes, and technology controls. We customize our training and awareness programs to suit diverse employee groups, including high-risk populations such as VIPs, human resources, services and projects, finance and treasury, and developers (Figure 2). This empowers each employee group to practice secure behaviors adapted to the risks associated with their roles.

**Figure 2**

*Schneider Electric's diverse employee groups and high-risk populations*




## Driving companywide training and awareness initiatives

As part of Schneider Electric's comprehensive training and awareness program, employees must complete the mandatory annual cybersecurity training refresher course each year to keep up to date on secure practices and the evolving cybersecurity threat landscape. We created a tailored version for shopfloor employees, highlighting specific risks they may face in an OT environment and associated good practices.

To reinforce security awareness and behavior, the company conducts regular phishing campaigns to identify and address any knowledge gaps based on the latest threat landscape and advanced tactics of malicious actors. In the event of a failed phishing test, immediate guidance is provided to highlight the red flags.

We run awareness campaigns to educate and engage our workforce on various cybersecurity risks. We cover both general and specific aspects of the threat landscape, including the types, sources, and impacts of cyberattacks, the methods and techniques used by cybercriminals, and the current and emerging trends and challenges in cybersecurity.

Employees have access to a cybersecurity page on the company's intranet that offers key insights into Schneider Electric's cybersecurity posture and includes guidelines, policies, and good practices materials.

## Tailoring training and awareness for specific populations

Schneider Electric identifies key personnel — such as VIPs, customer-facing employees, developers, and employees in human resources — who have access to sensitive or critical data and systems and often are a prime target for cyber criminals. We provide them with tailored security training, policies, and tools to protect their devices, networks, and accounts, and to prevent data leakage, phishing, malware, or unauthorized access. An example of this is targeted training for our customer-facing population through Schneider Electric's Cyber Badge Certification, which attests that these people have the knowledge and tools to interact securely with our customers.

## Mitigating human risk with process and technology controls

Schneider Electric is committed to empowering our workforce by fostering a culture where cybersecurity is recognized as part of everyone's role. We actively encourage employees to "see something, say something," drawing on their understanding of cyber risks to maintain secure practices and encourage reporting when applicable.

We've set up cyber risk leaders and professionals by domains of expertise or in risk areas such as finance, human resources, and manufacturing plants. Their role is to monitor the threat landscape, potential exposure, implement cybersecurity initiatives, and respond to incidents.

We use automation and technology to minimize human error, enhancing the security and efficiency of processes and tasks vital to critical infrastructure. This includes implementing encryption, authentication, the principle of least privilege, role-based access control, authorization, backup, and recovery. Email security controls such as secure gateways, email filtering, and real-time scanning are employed to monitor potential threats.

Additionally, exposure monitoring for our IT and OT operations is conducted through Schneider Electric's 24/7 Security Operations Center (SOC), which monitors social media and the dark web, and leverages threat intelligence feeds.

# Company: How do we secure the company?

## Aligning to regulatory requirements, maturing our cyber posture

In today's rapidly evolving digital landscape, the enforcement of cyber controls is no longer optional but a regulatory imperative. Governments and regulatory bodies worldwide are increasingly emphasizing the need for strong risk ownership and accountability in cybersecurity. Schneider Electric embraces regulations with transparency and alignment, underscoring that compliance results from a maturing cybersecurity posture rather than a compliance-specific approach. Furthermore, as numerous regulations emerge, we advocate for interoperability and mutual recognition.

For example, in 2023, the U.S. Securities and Exchange Commission introduced cyber incident reporting rules, requiring public companies to disclose material cyber risks and incidents in a timely manner. Similarly, the Network and Information Security 2 Directive (NIS2) is a significant development in the cybersecurity landscape of the European Union (EU). As the successor to the original NIS Directive, NIS2 aims to establish a higher common level of cybersecurity across the EU and requires businesses to adopt a proactive approach to cybersecurity, demonstrating both policy compliance and operational resilience. In China, there is a similar policy that was first introduced in 2017, the Multi-Level Protection Scheme 2.0 (MLPS 2.0), which provides a framework for cybersecurity requirements and data

processing oversight. Recently, the Chinese government signed a decree that announced new regulations for regulating network data processing activities, protecting the legitimate rights and interests of individuals and organizations, and safeguarding national security and public interests.

Schneider Electric's cybersecurity risk management approach relies on formal mechanisms with explicit risk ownership and end-to-end accountability at our leadership level to make regulatory compliance a result of a robust cybersecurity posture. These mechanisms align with the National Institute of Standards and Technology (NIST) risk management framework and are continuously challenged by reality checks (Figure 3).

**Figure 3**

*Application of the NIST Cybersecurity Framework at Schneider Electric*


## Meeting expectations through policies and standards

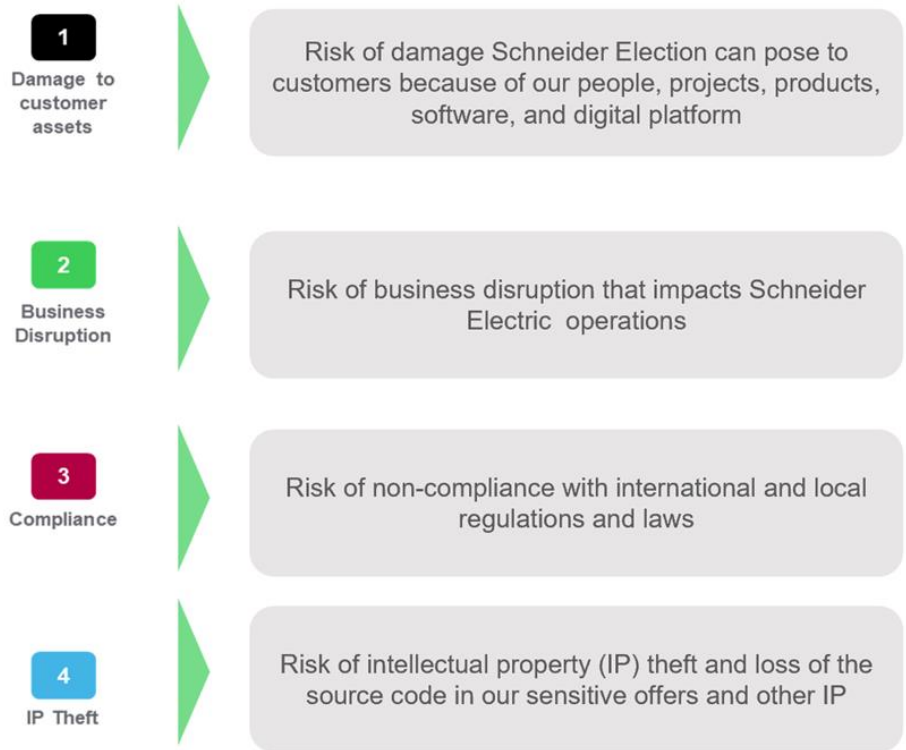
Schneider Electric has approximately 40 compulsory cybersecurity policies for all employees and contractors that are designed to help them understand how to implement critical tasks securely and meet behavioral and management's expectations. These policies are updated every year and reviewed independently by an external party every three years. The policies, which are foundational to our security posture, align with industry and regulatory standards such as ISO/IEC 27001 (for IT systems), ISA/IEC 62443 (for industrial automation and control systems), and the NIST framework mentioned above.

## Managing risks by enforcing clear roles and responsibilities

Schneider Electric analyzes risk across our extended digital, product, and operational landscape using a companywide Cyber Risk Register that segments cyber risks into four categories (Figure 4).

**Figure 4**

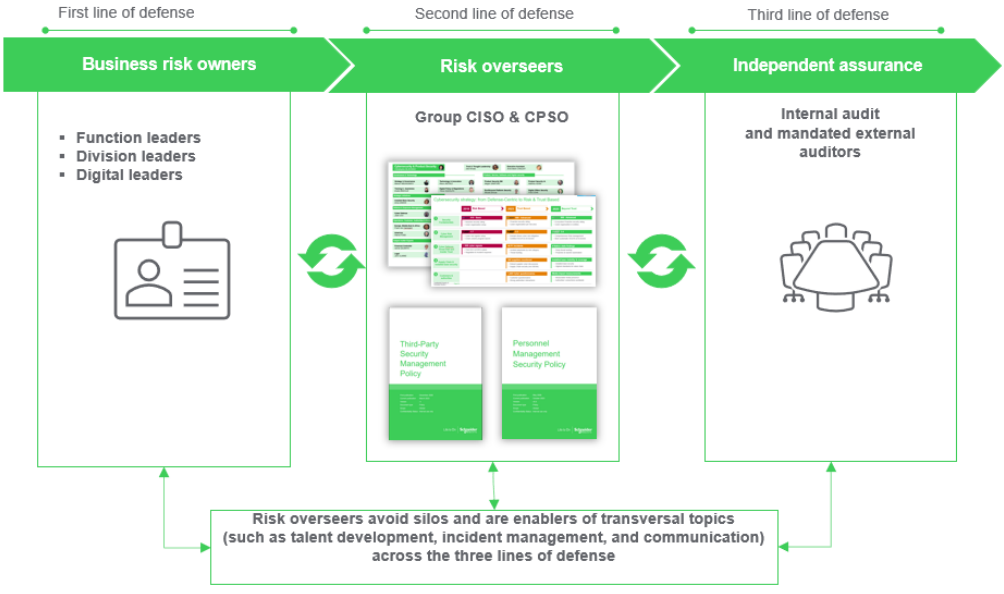
*Schneider Electric's major cyber risk categories*




Our Cyber Risk Register identifies relevant cyber risks across the company and associates them with business, functional, and operational owners through our three lines of defense framework (Figure 5). Their role is to mitigate risks where they are generated through appropriate controls that are embedded in the frameworks, processes, and daily activities of the risk areas they oversee.

**Figure 5**

*The application of the Three Lines of Defense Model*



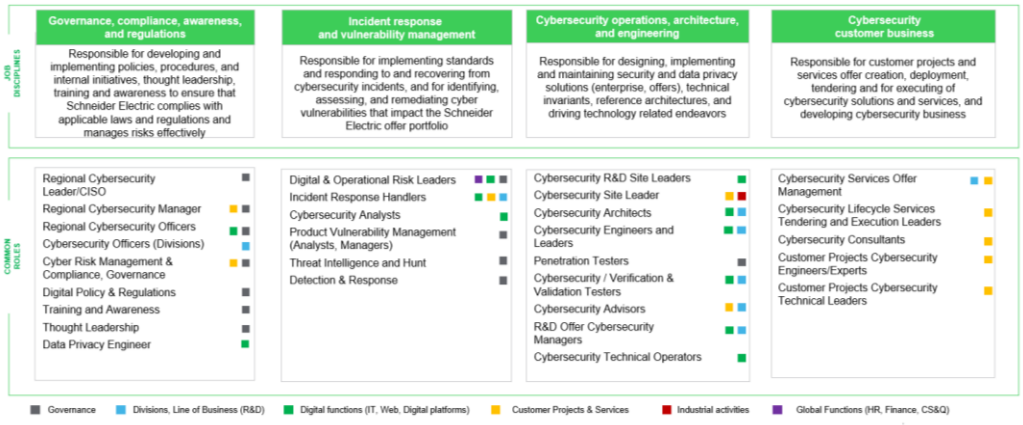

The risk owners in our first line of defense understand and explicitly acknowledge their risk accountability and prioritize attention and resources to risk mitigation.

They are supported by security leaders such as business division cyber officers and digital and operational risk leaders.

The second line of defense includes cyber and product risk oversight groups who are led by the company's group Chief Information Security Officer (CISO) and Chief Product Security Officer (CPSO) (Figure 6). This line of defense sets the guardrails and rules to empower the first line of defense by instilling a culture of risk awareness and promoting proactive risk management and resilience. They influence the risk threshold of the first line by clearly articulating the cyber, product, regulatory, and reputational risk implications of business decision being taken. We have approximately 800 cybersecurity professionals who benefit from a structured skills architecture and framework that offer formalized structured talent development, and growth opportunities within the company and our ecosystem companies.

**Figure 6**

*Cyber and product security role framework*




The third line provides assurance, typically through an internal auditing team and other external independent reviewers. The auditors and reviewers provide guidance that includes reality checks like assurance reviews, assessments, and audits for the first and second lines of risk mitigation. The external reviewers provide an independent measurement of Schneider Electric's posture against the NIST levels of defense for every risk area.

## Enforcing a compliant environment with key internal controls

In environments where compliance cannot be digitally enforced due to discretion or process-driven factors, Schneider Electric employs key internal controls, managed by the three lines of defense mentioned above. Each risk in our Cyber Risk Register is mapped to specific policies and associated controls, which require formal assertions, evidence of compliance levels, and action plans signed off by first line of defense risk owners. Their rigorous self-assessments not only confirm the effectiveness of risk reduction but are also suitable for diligently responding to customer and authority requests.

## Identifying and protecting Crown Jewels

To ensure the resilience of our operations, Schneider Electric has differentiated protection to some systems including but not limited to our Active Directory, e-commerce platform, certain partner portals, CRM, ERP and data platforms. Compromise of these "Crown Jewels" could hamper our operations and impact our customers. Each asset must be breach-resistant to detect and respond to an attack. This means that these assets are subject to administrative and technical controls, regular auditing, quarterly vulnerability scans, and periodic penetration testing. They must be breach-ready, and therefore, disaster and recovery plans are reviewed, approved, and tested every year

as a mandatory, recurrent control. Our Crown Jewels have strict data protection requirements, with appropriate controls in place for:

- Access: The principle of "least privilege" and securing admin workstations
- Storage: Encrypting at rest and systematic backups, tested restore
- Protection: Application patching, OS, and database hardening
- Data flow and consumption: Monitoring data interaction, inventory of connectors & API

## Mitigating risk with zero trust

Schneider Electric approaches zero trust from two angles. First, zero trust is applied to risk areas in our Cyber Risk Register through our Cyber Assurance Principles for our IT and OT infrastructures. These principles are core to our cybersecurity posture, and they align with a broad and non-technical definition of zero trust provided by the World Economic Forum.

Our zero trust principles, which are vital to managing our cyber risks and ensuring resilience, are:

- Continuous verification: Leverage data to verify systems, devices, and users
- Least-privilege access: Provide secure access to only what is necessary
- Logical segmentation: Isolate and limit the impact of security threats
- Supply-chain risk awareness: Collaborate with suppliers and customers
- Scaling with automation: Automate defenses to reduce manual tasks
- Proactive detection: Adopt a breach mindset to proactively detect threats
- Business resilience: Learn from incidents to improve contingency strategies

We have woven these principles into our digital and operational domains as a foundational element that embodies a risk-centric approach which continues to evolve as we mature our zero trust controls and capabilities.

Secondly, zero trust is applied to Schneider Electric's digital foundation, making it an essential requirement and enforcing compliance digitally. Zero trust in the digital core includes three ongoing initiatives:

- Secure remote access: This initiative continually improves the process for securing third-party remote access, which encompasses hundreds of entities and engagements globally.
- Secure WAN: We are working to ensure that our software-defined wide area network (SD-WAN) devices comply with regulations, and that they have secure configurations and are managed using a privilege access management (PAM) platform. The network-level kill switch capability is available at Schneider Electric sites, with plans for a hard kill switch.
- Secure application access. This initiative requires a continual transformation of how applications are accessed from the internet. It provides a higher level of security and assurance by managing controls, in-app permissions, access limitations, behavior monitoring, and control of user actions.

As a result of these efforts, we are reducing the discrepancy between cyber risk perception and reality as we follow the zero trust philosophy of "never trust, always verify."

## Developing offers with a product security discipline

Schneider Electric's commitment to product security starts with a secure development lifecycle (SDL) process and includes steps like threat modeling, secure

design, security testing, and privacy reviews. Before any product is released, it undergoes rigorous security checks such as software composition verifications, static and dynamic code analysis, and independent testing by in-house CREST-certified security labs.

For our sensitive offers, we built a comprehensive source code governance program to mandate critical controls for protecting source code which meets or exceeds the requirements of customers and regulations. This multi-layered approach ensures the security of both the products and the underlying code that drives them. Our SDL process is IEC 62443-4-1 and ISASecure SDLA certified, demonstrating adherence to industry recognized secure-by-design concepts. Following a product's release, we maintain security throughout its service period by adhering to the ISO3011 standards for vulnerability management. This demonstrates a continuing commitment to identifying and addressing potential threats throughout the product lifecycle.

Schneider Electric regularly monitors emerging requirements for adherence to the minimum software development standards for software and firmware. These software attestation requirements are expected to extend on a global scale as part of upcoming regulatory frameworks, such as the EU's Cyber Resilience Act (CRA) and its Radio Equipment Directive (RED). These frameworks recommend product transparency as a business necessity and act as a license to sell products in some critical markets. We embrace these movements and have already implemented dedicated compliance initiatives to address them.

Further, Schneider Electric has a defined list of essential product security requirements that help us comply with regulatory guidance and drive a robust cybersecurity posture. These are foundational security measures designed to ensure we have comprehensive product and system security. They are mapped to align with standards and CRA regulations, promoting secure development and lifecycle management. These measures include:

- Basic product authenticity: Ensuring secure boot and hardware-based root of trust.
- Secure storage for sensitive security parameters and personally identifiable information (PII): Utilizing secure hardware elements for key storage and best practice cryptography.
- Signed firmware and software: Requiring digital signatures for firmware and software to validate authenticity.
- Secure update capability: Providing mechanisms for secure software updates.
- Cryptographic agility: Implementing flexible and robust cryptographic solutions.
- Authentication and authorization management: Enforcing password policies and preventing hardcoded accounts.
- Security monitoring: Logging security events and sending logs to centralized systems.
- Secure communications: Employing certificate-based mutual authentication and best-practice cryptography for communications.
- Security by default: Enabling security settings out-of-the-box and ensuring robustness against denial of service (DoS) attacks.
- Configuration trust: Validating configuration integrity and alerting unusual changes.

In this context, we aim for our products to be:

- Future-ready by creating product security essentials that align to requirements to future enforceable standards such as the EU's CRA.

- Secure-by-design by making investments in new installations of products systematically and implementing security controls in brownfield products for those staying on the market.

Schneider Electric highlights the importance of managing cybersecurity risk across all our affiliated entities — including our core, standalone, and minority interest companies. All entities are managed and aligned according to our Trust Charter.

## Suppliers / Partners: How do we stay resilient with suppliers and partners?

### Managing the extended enterprise of suppliers and partners

As value chains become increasingly complex and interconnected, suppliers and partners represent a significant risk vector. A threat actor can bypass an organization by compromising a smaller, more vulnerable target such as a component used in a manufacturing machine, through its provider, law firm, or distributor.

Beyond engaging with over 50,000 suppliers, Schneider Electric fosters business-to-business relationships and interacts with the market through channel partners such as electricians, system distributors, systems integrators, and large general infrastructure contractors (Figure 7).

**Figure 7**

*Supplier and partner landscape for Schneider Electric*


These channel partners can be a vector of attack on our company. For instance, systems integrators could be manipulated to infiltrate a customer's systems, while ransomware attacks on distributors could cause significant business disruption for us and our customers. We consider our suppliers and partners to be an extension of our company, and they align with our third-party security principles. Maintaining a resilient value chain requires a comprehensive approach across key areas such as secure sourcing and market resilience through channel partner cybersecurity.

### Securing our sourcing and supplier operations

Schneider Electric's supplier footprint is vast and spans over three major categories:

- Direct procurement for soft and fabricated components and services used directly in our digital or non-digital products destined for our customers.
- Indirect procurement for products or services used to support business operations such as cloud services, information technology, HR, marketing, and others.

- Solutions partnerships which deliver end-to-end solutions at a customer site with Schneider Electric offers and other third-party products.

As part of our third-party security principles, we have a tiered system for categorizing our suppliers (Figure 8) that is grounded in a comprehensive risk-based framework with mitigating controls based on several critical factors:

- Risk related to third-party components: Risks due to compromised components, software tampering, risk of known or zero-day vulnerabilities, or lack of transparency and control.
- Business continuity impact: The extent to which failure or a breach by suppliers, such as large components or third-party logistics suppliers, could disrupt operations.
- Data access levels: The type and sensitivity of data that suppliers, such as consulting companies or statutory auditors, can access and manipulate.
- Level of access to customer-facing or internal systems: The degree of access for suppliers, such as technology operators or business outsourcing partners, can have to the systems and networks of Schneider Electric or our customers.
- Potential impact on operations or intellectual property: How the cyber posture of suppliers, such as R&D engineering augmentation and support, connected service, or digital offers contractors, could affect our intellectual property and operational capabilities.

**Figure 8**

*Supplier tiering by criticality and impact*


Schneider Electric's supplier cybersecurity is co-managed by our cybersecurity and procurement teams and is integrated into our supplier lifecycle process (Figure 9). When we award business to a supplier, its cybersecurity and data privacy posture is a key selection criterion. We evaluate the risk profile of the supplier, which includes cyber maturity scores from external cyber scoring platforms, and risk indicators like the Ransomware Susceptibility Index.

**Figure 9**

*Cybersecurity and data privacy controls embedded into the supplier lifecycle process*


Upon identifying potential suppliers, we conduct an in-depth evaluation based on the supplier responses, with justifying evidence, to a questionnaire tailored to the specific product or service under consideration. For direct suppliers, we seek details on the specific component and product security practices. This process uses a customized in-house capability for direct procurement suppliers and an external standard capability for suppliers of indirect products and services. Our approach to indirect procurement includes continuous posture monitoring with external validation. All supplier contracts, depending on the procured goods or services and the supplier's risk profile, are subject to cyber and privacy contractual terms and conditions.

After a supplier is onboarded, we proactively collaborate with C-Level connections at critical suppliers on a joint cybersecurity posture and assist where needed on incident responses. We continuously monitor our suppliers' postures via threat intelligence platforms and external scoring agencies throughout the entire engagement lifecycle to identify any emerging weaknesses for corrective action. When a third-party technology company needs to be onboarded for internal usage, we have a dedicated security and privacy validation process with a set of policy-driven controls that must be verified and deployed before implementation. The controls include single sign on and multi-factor authentication, a data privacy review, and others.

## Securing our channel partner operations

In a business model that relies heavily on an indirect approach of leveraging channel partners, Schneider Electric takes into consideration more than our core operations in both our upstream and downstream relationships in the extended supply chain. With downstream distributors, we foster a collaborative cybersecurity engagement with security C-level executives where best practices and strategies are shared.

We require comprehensive cybersecurity training for project and services partners, emphasizing appropriate behavior, security hygiene, and discipline. This training ensures that our partners are well-versed in the latest security requirements, reducing the risk of vulnerabilities introduced through human error or misconfigured or infected devices. In addition, EcoXpert™ and Alliance partners are required to align with formal cybersecurity requirements that parallel our safety expectations. By implementing these stringent measures, we not only protect our operations but also reinforce the security of our entire ecosystem, improving survivability for all stakeholders.

Customers: How do we secure customers through transparency and engagement?

## Serving critical infrastructure customers

Critical infrastructure is a prime target for threat actors because of its potential for widespread disruption and devastation. The connectivity of assets, systems, and environments in critical infrastructure segments expands the attack surface. On top of this, ransomware attacks on critical infrastructure can be highly lucrative for cybercriminals, as the resulting disruptions can pressure organizations to pay hefty ransoms to quickly restore operations.

Energy segments are often targeted by sophisticated and well-funded malicious groups, typically nation-state actors, aiming for disruption or intellectual property theft to gain an unfair competitive advantage. Their methods can vary, from direct ransomware attacks to targeting vendor components in customer environments to cause harm.

An attack on one part of critical infrastructure, such as a power grid, can trigger a cascading effect, impacting other interconnected companies. A power grid outage can cripple communication networks and disrupt emergency services.

## Driving transparency through collaborative engagement

Transparency is a core value at Schneider Electric, driving us to exceed regulatory requirements and customer expectations. Our commitment to transparency is evident in our routine disclosure of relevant data and documentation to both government

authorities, and customers. This practice not only informs but builds trust through sustained, mutual communication channels.

We have several initiatives that are aimed at increasing transparency and trust, such as our Cybersecurity Transparency Report, software attestations, product validations, crisis simulations, and secure by operations.

As an example, our Transparency Report is a high-level document that shares key metrics, data, and information about our company's digital and security governance, released twice a year. The report focuses on our cybersecurity commitments and enforcement measures with data points such as completion rates of general and tailored trainings, volume of customer requests received and responded, product vulnerability challenges managed, and relevant certifications. Our Transparency Report is unique in that it specifically addresses the critical infrastructure audience.

## Engaging to validate and test products with authorities

In specific circumstances, we conduct highly detailed product assessments including supply chain illuminations, analytical assessments, and supply chain audits for key customers. These illuminations are performed to uncover and assess risks deep within the supply chain, providing a comprehensive view of potential vulnerabilities. This process helps Schneider Electric make informed decisions, guide R&D teams, and ensure the security and integrity of product.

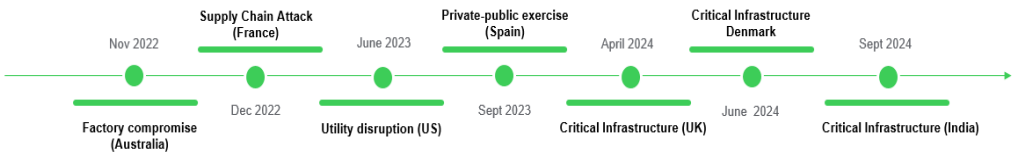
Since 2020, Schneider Electric has actively participated in the U.S. Department of Energy's Cyber Testing for Resilient Industrial Control Systems (CyTRICS) Program. This initiative aims to identify high-priority operational technology (OT) components within the US energy infrastructure for component-level evaluation. As part of the program, we conduct testing to identify supply chain vulnerabilities and provide remediation recommendations. Schneider Electric has tested several of its products, including the Power Monitoring Expert (PME) and the Foxboro DCS.

## Practicing with critical infrastructure and authorities

Crisis simulations are training activities that Schneider Electric conducts as meticulously organized, detailed, and targeted exercises with customers and authorities (Figure 10). These events are an intense and deliberative collaboration through a true multi-stakeholder approach that replicates real-life crisis scenarios as closely as possible and aims to evaluate and enhance the collaborative response and recovery efforts of all participants.

**Figure 10**

*Timeline of joint cyber crisis simulations*




On a routine basis, we develop realistic simulations for two types of incidents: business crises (broad scope) and high-priority cyber incidents (reduced scope). Preparation for these simulations necessitates transparency about current processes and procedures from Schneider Electric, our customers, and government authorities. We all share comprehensive information about our organizational structure and priorities.

This level of transparency establishes a foundation of trust based on shared information, missions, and outcomes. Each simulation features up to 50 participants,

each of whom is empowered through well-defined roles and responsibilities to provide a unique voice and enable organizational growth.

The simulations have resulted in the following benefits for all the involved parties:

- Cyber and non-cyber senior executive training in a realistic environment
- Strengthened relationships with external parties, including customers, national authorities, CISOs, and other key personnel
- Increased internal awareness and communication
- Calibrated incident response and crisis processes
- Identification of how to behave individually and collectively in times of crisis

## Building secure by operations on top of secure by design

Schneider Electric recognizes the importance of securing the value chain in a comprehensive and systematic manner. As mentioned earlier, we have adopted a secure-by-design approach that focuses on building systems with security integrated from the outset, ensuring that products like industry control systems or other critical infrastructure are inherently robust against threats.

However, this proactive approach is only part of the security lifecycle, especially when products are built to operate on a 20–30-year lifecycle or more. Once our systems are deployed at our customer sites, new risks emerge due to evolving threat landscapes, exposure to local network environments, and system misconfigurations. That's why, as a value chain, we need to move beyond secure-by-design to a comprehensive secure-by-operations approach.

Secure by operations involves maintaining and protecting systems over time through activities such as regular patching, continuous monitoring, network segmentation, and hardening of the surrounding infrastructure. Unlike secure by design, which is static and applied during development, secure by operations is a dynamic and require continuous adaptation to the threat landscape. Without ongoing security measures, even well-designed systems can become vulnerable to cyberattacks, particularly as attackers develop new methods to exploit weaknesses.

To tackle this known industry challenge, Schneider Electric has partnered with BitSight to create a program called the Installed Base Security initiative, which is an OT threat intelligence effort. The objective of the program is to identify industrial and critical assets associated with our customers that are exposed to the internet and thus potentially vulnerable. In response to the initiative, BitSight released research which found that 100,000 industrial control systems (ICSs) owned by global organizations were exposed to the public internet.

Beyond identification, we perform a crucial step of contextualization based on our knowledge of these kinds of assets and associated risks for customers. This capability provides actionable information to customers for remediation actions and assists in decreasing the risk that comes with asset exposure.

From an authority engagement standpoint, Schneider Electric has contributed to and endorsed secure by operations initiatives championed by authorities such as the U.S. Department of Energy's Supply Chain Cybersecurity Principles. Developed in collaboration with several vendors, these principles specifically define the responsibilities and behaviors required by suppliers and asset owners to maintain a strong security posture. Secure operations are essential for ensuring the long-term resilience of critical systems, complementing the foundational work done by manufacturers during the design phase.

# Conclusion

Schneider Electric's cyber risk management strategy for securing critical infrastructure is based on three foundational principles — security, survivability, and transparency. These pillars, combined with Schneider Electric's regional structure, contribute to the goal of collective national sovereignty. While the concepts of security and survivability are widely recognized and form the basis of the secure by design principle across various industries, it is Schneider Electric's distinctive focus on transparency and engagement that establishes its leadership in digital transformation and sustainability. Embracing transparency, we promote a collective responsibility culture and advocate for clearly defined roles and responsibilities among ecosystem stakeholders.

Schneider Electric works toward this goal through implementing the initiatives and programs within its Zones of Influence — people, company, suppliers and partners, and customers and authorities. These include key security programs and initiatives such as secure development lifecycles, threat detection and response, and stringent supply chain security measures. The Zones of Influence require that we go beyond our scope of accountability by guiding customers on how to secure their environments. At the same time, by working with and influencing authorities, we drive the right regulation and transparency initiatives to build resilience into critical infrastructure. By fostering a culture of trust and confidence through these efforts, we can better protect our critical infrastructure from an ever-evolving landscape of cyber threats.