Security Principles for Non-Integrated Companies

First publication : September 2022
Current publication : September 2022
Version : V1
Document type : Policy
Scope : Customers and Ecosystem
Confidentiality Status : Public
“As the Schneider Electric extended family of companies grows, so does our exposure to cybersecurity threats, especially for the companies with independently managed IT infrastructures. We work with these non-integrated companies to align our cybersecurity and data protection standards and keep interactions with our customers safe from cybersecurity risk and threats.”

Cybersecurity risks are always evolving, and as Schneider Electric digitizes our core business processes, customer solutions, and supporting technologies, our digital landscape and risk exposure grows and evolves as well. The non-integrated companies in the Schneider Electric family are also digitalizing, leading to an even larger attack surface, and thus, to more cybersecurity threats.

Cybersecurity is an essential business imperative for Schneider Electric. We have developed a strong security posture based on our Trust Charter, which is the driving force behind our interactions with stakeholders and our relationships with customers, shareholders, employees, and the communities we serve. It applies to everyone working at Schneider Electric or any of our subsidiaries, including our non-integrated companies.

We seek to build a trust-based, information-sharing environment within our security ecosystem of non-integrated companies (Security Ecosystem). Security Ecosystem are a valued extension of our company, our brand, and our reputation as they deliver key products and services to our customers. Our collective objective is to reach the highest security standards by deeply understanding risks and determining the solutions to mitigate them.

We work together to develop an understanding of each company’s security posture. Identifying gaps, working collaboratively on solutions, and increasing awareness and communication aids in reducing cybersecurity threats and risks to Schneider Electric and its non-integrated companies. For this, we have built a Trust Standards program upon a set of cybersecurity and data protection trust standards that are aligned with the National Institute of Standards and Technology (NIST) cybersecurity framework. The program is also supported by proactive security actions such as external cybersecurity assessments, vulnerability scanning and remediation. Collectively, our security vision is executed on three consecutive levels, as outlined in Figure 1.

We apply these standards in four key domains:

- **Governance** defines the security framework. It provides the foundation for the cybersecurity and data protection standards that every organization within the Schneider Electric family embraces.
- **People** in the Schneider Electric family embody a cybersecurity culture that is aligned with our governing principles and are critical for managing cyber threats and risks properly.
Technology solutions for information technology (IT) and operational technology (OT) are continually updated and implemented with the latest and most secure versions in order to maintain a strong security posture across our organization.

Process drives the execution and application of our security framework, standards, and technologies used in everyday business interactions to ensure we sustain the highest level of security possible.

Based on these standards and domains, Schneider Electric has developed core principles for our non-integrated companies that guides interactions between us. When appropriate, Schneider Electric works side-by-side with these companies as they implement these principles to improve their security postures. Throughout this journey, each non-integrated entity retains complete ownership and responsibility for executing a security program to improve its security culture and posture.

<table>
<thead>
<tr>
<th>Cybersecurity and Data Protection Trust Standards</th>
<th>Build a Strong Foundation for Cybersecurity and Data Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organization</strong></td>
<td><strong>Security Policies</strong></td>
</tr>
<tr>
<td>Endpoint &amp; Access Management</td>
<td>Network &amp; Cloud Security</td>
</tr>
<tr>
<td>Incident Detection &amp; Response</td>
<td>Data Backup &amp; Restore</td>
</tr>
</tbody>
</table>

Implement Risk Management Protocols

| **Risk Register**                           | **Crown-Jewels Protection**                                    |
| **Application & System Security**           | **Secure Development Cycle**                                    |
| **Digital Asset Inventory**                 | **External Posture Assessment**                                |

Engage and Interact with External Security Experts and Organizations

| **Law Enforcement & Regulation Intelligence** |
| **Third-Party Security Management**          |
| **Threat Intelligence & Detection**          |

Figure 1: Cybersecurity and Data Protection Trust Standards for Non-Integrated Companies

Core Principles for Non-Integrated Companies

1. **Transparency and Visibility**

As we engage with our non-integrated companies, transparency and visibility are key to developing our common goals. With trust and respect for each other, Schneider Electric and the companies jointly examine each organization’s cybersecurity maturity as it aligns with the cybersecurity and data protection standards outlined in Figure 1 above. Through this process, we analyze our organizations’ risk exposure and identify opportunities to enhance security capability and maturity.
2. Continuous Improvement

Managing cybersecurity risk requires ongoing diligence. As a unified team, Schneider Electric and the companies create an action plan to reduce exposures to risk and further mature the security and data protection program. With support from Schneider Electric, the plan is reviewed and updated annually, and is customized to each company’s unique cybersecurity risks and requirements.

3. Ownership

While Schneider Electric extensively supports all of our companies’ continuous improvement action plans, each company retains complete ownership and responsibility for executing the agreed-upon plan. We offer our deep knowledge, expertise, and resources for the companies to leverage within their cybersecurity initiatives and programs.

4. Collaboration

Once a continuous improvement plan is in place, Schneider Electric and each company will continue to collaborate on a regular basis. We collectively monitor and measure the maturity of the program to ensure alignment with stated actions. In addition, we proactively engage in knowledge transfers between our respective security experts to develop best practices for future guidance. We also engage in knowledge sharing within the community of companies so that all can benefit from each other’s experience with ever-evolving cybersecurity intelligence and innovation.

Conclusion

Together with our non-integrated companies, we strive to deliver the highest level of cybersecurity protection for all stakeholders in the Schneider Electric family. We continually collaborate with these companies to improve our cybersecurity posture and respond jointly to any current or future cyber risk.