BUILDING CYBERRESILIENCE IN THE ELECTRICITY ECOSYSTEM

By Walter Bohmayr, Sam Rajachudamani, and Stefan Deutscher

In March 2018, a cyberattack struck the platform of an electronic communications system provider. But the impact went far beyond that one company. Cascading through the ecosystem, the attack disrupted the operations of several natural gas pipeline and utilities customers.

As this example shows, cyberrisk is first and foremost a business and systemic risk, not an IT risk. Cyberthreats affect all industries but are especially challenging for the electricity industry because of the interconnected ecosystem in which electricity organizations operate. In addition, the grid is so vital to our infrastructure that a large-scale blackout would have enormous socioeconomic impact, with damaging consequences for households, businesses, and vital institutions alike.

Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards, a 2019 report developed by the World Economic Forum and Boston Consulting Group, addresses three challenges to cyberresilience in the electricity ecosystem:

- **Interdependent Ecosystem.** The emergence of digital technologies has heightened the level of interconnectivity and has made cyberrisk a much bigger issue than it used to be. That's because the increased connectivity—along with the convergence of information technology (IT) and operational technology (OT), the rising number of Internet of Things (IoT) devices, and the digitization of business models—has expanded the cyberattack surface. Most important, the adoption of these digital technologies has created a "digital transit system" that malicious actors can use to penetrate the ecosystem via a weak link. Once inside, they can jump between organizations' systems to execute their attack. As US Secretary of Homeland Security Kirstjen Nielsen put it: "Hyperconnectivity means that your risk is now my risk and that an attack on the 'weakest link' can have consequences affecting us all." Therefore, organizations in the electricity ecosystem need to work together to develop robust cyberresilience strategies.

- **Siloed Approach to Cyberresilience.** Many organizations don't yet consider the ramifications of a cyberrisk as systematically as they do other kinds of risks, often assigning sole responsibility for cybersecurity to IT. Given the growing number of cyberthreats and the real-time need for energy delivery, cyberrisk must be integrated with business risk and managed across the ecosystem.

- **Culture of Compliance.** Although public sector institutions have introduced various regulations, compliance is only a first step; it's not necessarily enough to ensure cybersecurity. Moreover, as the electricity ecosystem digitizes, regulations may not be able to keep pace with the newest cyberrisks. So it's crucial to adopt a "resilience mindset" and take a strategic approach that goes beyond mere compliance to managing emerging risks.

Understanding the Ecosystem

The first step in addressing cyberresilience challenges is to understand what needs to be protected. In an interconnected universe like the electricity industry, this means answering two questions:

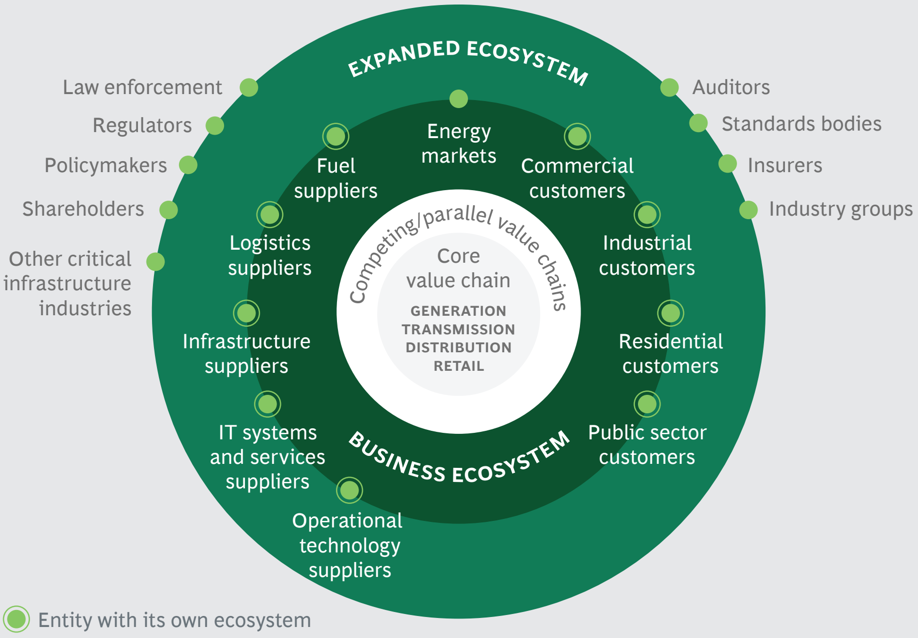
1. Who are the stakeholders in our ecosystem?

2. How are these stakeholders connected to us?

Who. A mapping of the electricity ecosystem includes not only the core industry value chain but also a business ecosystem of suppliers, customers, and peers, and an extended ecosystem that includes policymakers, regulators, and law enforcement. (See Exhibit 1.) It's also important to consider parties that are even more distant from the core, such as suppliers of suppliers and customers of customers.

How. Connections among stakeholders in the electricity industry fall into three categories: physical, network, and strategic. Physical connections enable the flow of electricity from generation to use, while network connections include the system connections that enable data flow. Traditionally, cyberattacks occurred only in the

Exhibit 1 | The Electricity Ecosystem



Source: BCG and World Economic Forum analysis.

network domain. But the IoT enables the connection of physical devices to the internet, meaning that a cyberattack can have physical consequences as well. To identify and manage these potential vulnerabilities, an organization needs to understand which network and physical systems connect to the systems in its value chain and extended ecosystem.

The nature of strategic connections is slightly different. Once the physical and network connections have been identified, leaders need to jointly define strategies for mitigating the cyberrisks that these connections pose. For example, a generation facility and its fuel suppliers should outline ways to manage cyberattacks that could compromise the generation facility's fuel supply. Leaders of electricity organizations also need to develop strategic partnerships with stakeholders in the extended ecosystem. This might include engaging relevant law enforcement agencies to respond to cyberattacks and working with regulators and policymakers to develop regulations with appropriate incentives.

Securing the Ecosystem

Boards of directors need to take responsibility for and oversee cyberrisk management in the organization and across the ecosystem. This is critical for building systemic cyberresilience.

The 2019 report by the World Economic Forum and BCG provides guidance for boards in this undertaking. Augmenting the cyberresilience strategies report that BCG and the World Economic Forum developed in 2017, the new report identifies seven principles and guidelines for boards of directors in the electricity industry. (See Exhibit 2.) To help companies implement these principles, the report offers assessment questionnaires and case studies from leading electricity organizations around the world.

For electricity companies, cyberrisk is an ecosystem-wide challenge. But the electricity industry is not alone. Cyberrisk threatens the aviation, automotive, and healthcare ecosystems as well—and the number of affected industries will continue to grow. As digitization continues, ecosystem stakeholders will increasingly need to come together to manage cyberrisks. Such collaboration will be critical to improving systemic cyberresilience in the long term.

Exhibit 2 | Electricity Board Principles for Cyberresilience

PRINCIPLE 1
Cyberresilience Governance. The board requires management to implement comprehensive cybersecurity governance, which governs information technology (IT), operational technology (OT), physical security, and digital transformation; ensures interoperability within the organization; and drives alignment across the ecosystem.

PRINCIPLE 2
Resilience by Design. The board promotes a security by design/resilience by design culture and requires management to implement such a culture and document progress.

PRINCIPLE 3
Going Beyond Compliance. The board ensures that its cyberresilience posture and efforts extend beyond compliance, toward a holistic risk management approach, and are supported by adequate funding and resourcing.

PRINCIPLE 4
Systemic Risk Assessment and Prioritization. The board holds management accountable for understanding the organization's interdependencies within the ecosystem, reporting on the systemic cyberrisks posed by the ecosystem (especially the supply chain), and planning and prioritizing cyberresilience efforts accordingly.

PRINCIPLE 5
Corporate Responsibility for Cyberresilience. The board encourages management to consider what cyberrisks the organization, its cyberculture, and its practices may pose to the ecosystem, and appropriately explore how such risks can be reduced.

PRINCIPLE 6
Ecosystem-Wide Collaboration. The board empowers management to create a culture of collaboration, set strategic objectives around information sharing, and understand and mitigate cyberrisks in the ecosystem. The board also actively collaborates with industry peers and policymakers.

PRINCIPLE 7
Ecosystem-Wide Cyberresilience Plans. The board encourages management to create, implement, test, and continuously improve collective cyberresilience plans and controls with other members of the ecosystem. These plans should appropriately balance preparedness and protection (e.g., in-depth defense strategies) with response and recovery capabilities.

Source: BCG and World Economic Forum analysis.

About the Authors

Walter Bohmayr is a senior partner and managing director in the Vienna office of Boston Consulting Group and the global leader for cybersecurity. You may contact him by email at bohmayr.walter@bcg.com.

Sam Rajachudamani is a consultant in the firm's New York office. You may contact him by email at rajachudamani.sam@bcg.com.

Stefan Deutscher is an associate director in BCG's Berlin office and the global topic leader for cybersecurity. You may contact him by email at deutscher.stefan@bcg.com.

Boston Consulting Group (BCG) is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients from the private, public, and not-for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with offices in more than 90 cities in 50 countries. For more information, please visit bcg.com.

© Boston Consulting Group 2019. All rights reserved. 2/19

For information or permission to reprint, please contact BCG at permissions@bcg.com. To find the latest BCG content and register to receive e-alerts on this topic or others, please visit bcg.com. Follow Boston Consulting Group on Facebook and Twitter.