WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Shaping the Future of Cybersecurity and Digital Trust

Cyber Resilience in the Electricity Ecosystem: Playbook for Boards and Cybersecurity Officers

In collaboration with Accenture and the Electricity Industry Community

June 2020

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

Contents

Foreword

Rosa Kariger, Global Chief Information Security Officer, Iberdrola

Co-chair of the Systems of Cyber Resilience: Electricity Working Group

From its inception, the electricity industry has been thorough in addressing security risks in order to protect critical infrastructure and ensure continuity and quality of power supply. Companies have invested in resilient grid design and implemented incident and crisis management procedures and business continuity plans to face physical attacks and weather events, such as large storms. But with increased automation and digitization, electricity companies are exposed to new cybersecurity risks that are testing the resilience of the power infrastructure. In this new context, business leaders and regulators struggle to identify the best countermeasures to mitigate these risks and must embrace a collaborative and risk-informed approach to adapt and ensure a resilient ecosystem.

To reflect on the unique challenges that the electricity industry is facing in properly understanding and addressing cybersecurity risks, spanning both the information technology (IT) and operational technology (OT) environments, the World Economic Forum has brought together a group of more than 50 senior executives from utilities, technology manufacturers, government entities and academic institutions with the goal of enhancing cyber resilience across the electricity ecosystem.

It has been a privilege to work with this very engaged community of purpose. I hope other companies in the industry will find value in the insights shared and tools developed and will be compelled to actively collaborate with other ecosystem agents to enhance cyber resilience not only within their companies, but across the electricity ecosystem as a whole.

Georges DeMoura, Head of Industry Solutions, World Economic Forum

Platform for Shaping the Future of Cybersecurity and Digital Trust

Kristen Panerali, Head of Electricity Industry, World Economic Forum

Platform for Shaping the Future of Energy and Materials

Maintaining cyber resilience across the ecosystem is a challenge for all organizations and a significant priority for critical infrastructure sectors such as electricity. Furthermore, the COVID-19 crisis is having a dramatic impact on our society and has forced everyone to become heavily reliant on the internet and its digital economy.

Systems of Cyber Resilience: Electricity is a public-private collaboration initiative with the objective of enhancing cyber resilience across the electricity ecosystem. It is the one place in the world where chief information security officers (CISOs), experts and policy-makers can convene in a trusted, neutral environment, and focus on advancing global cyber resilience in the electricity ecosystem.

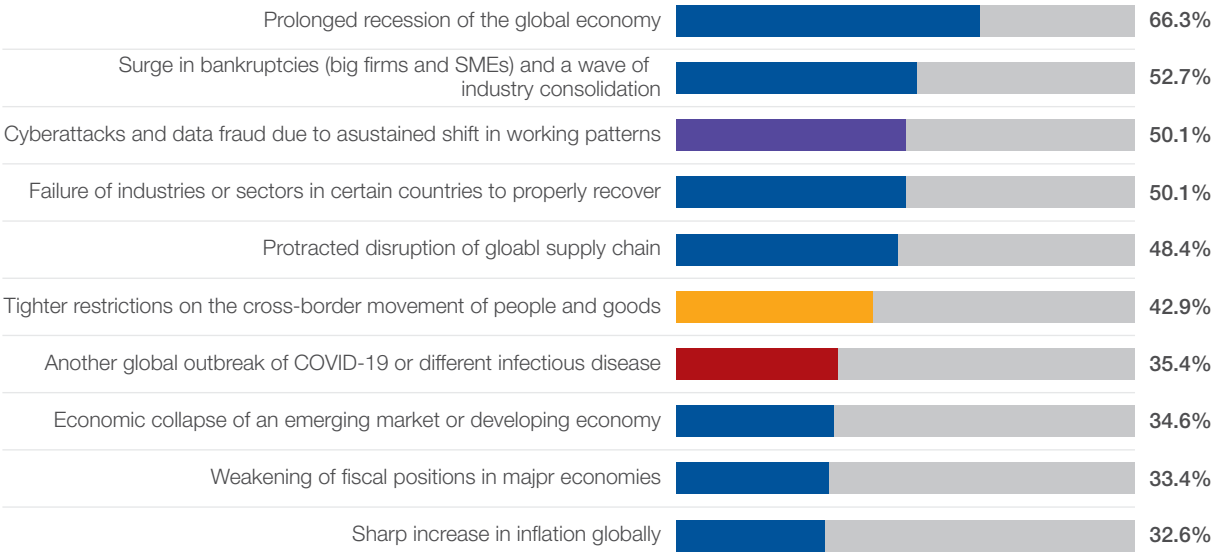
We hope that this paper, the result of a collaborative effort, helps leaders to strategically manage information risks, work towards a culture of shared cyber-risk ownership across the organization and take a more strategic approach to cyber resilience. Effective cyber resilience requires a combined, aligned multidisciplinary effort to move beyond compliance to cohesive business and digital enablement.

The COVID-19 crisis and cybersecurity

The World Economic Forum's *COVID-19 Risks Outlook* survey of companies found that the third greatest concern for companies is that new working patterns may increase cyberattacks: "as the COVID-19 crisis accelerates dependency on technologically enabled economic processes, it is also exacerbating […] cyber risks".[1]

Top ten most worrisome risks for your company

Economic Societal Tech Geopolitical Environmental



Executive summary

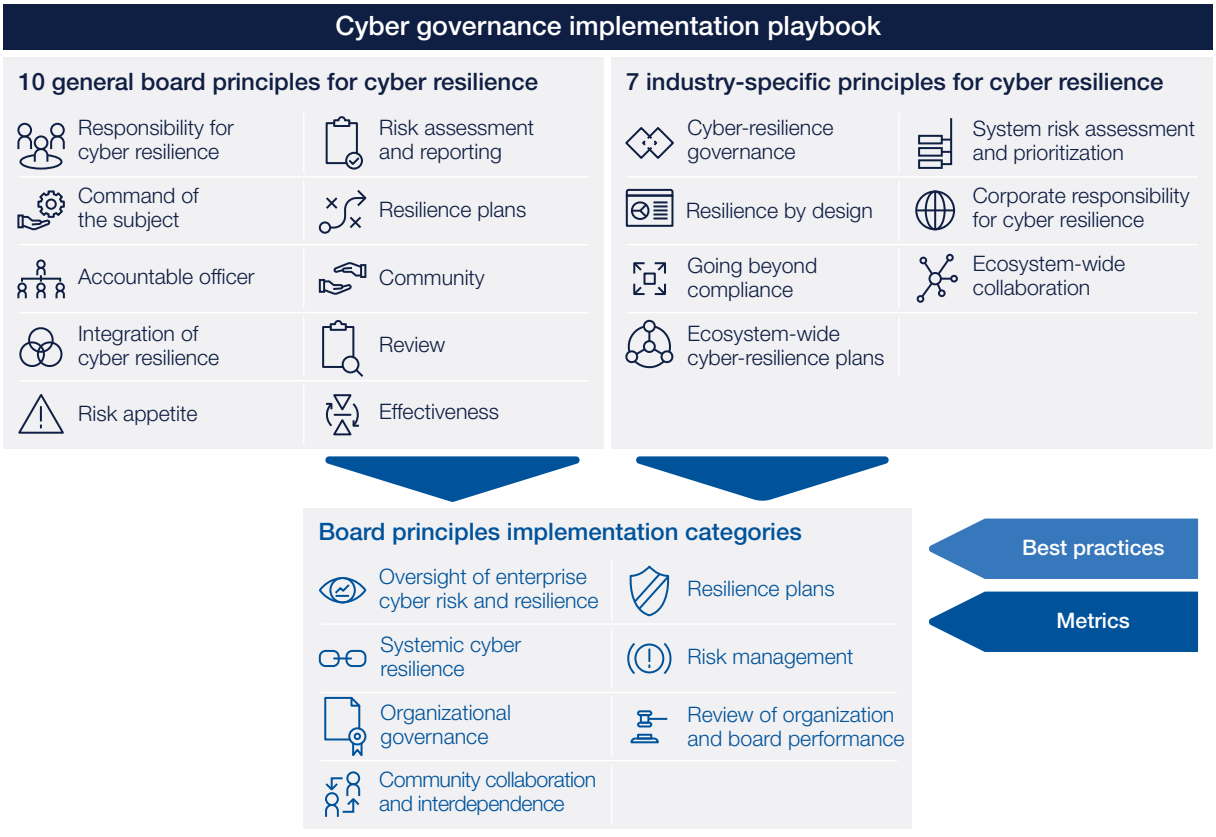
Businesses need to consider cyber resilience from a business perspective, looking at the cyber element of operational risks to their business as they become increasingly dependent on the internet and digital channels but also adopting a resilience mindset governing how they would respond to and recover from any major cyber event.

Part of the World Economic Forum's Systems of Cyber Resilience: Electricity project, a community comprised of senior cybersecurity executives from the electricity industry ecosystem defined an effective approach to support strategic leaders in the implementation of best practices for cyber-risk governance.

The result of the group's efforts is this report, *Cyber Resilience in the Electricity Ecosystem: Boards and Cybersecurity Officers*. Serving as a companion to the World Economic Forum's guidance on cyber resilience for corporate boards released in 2017 and its electricity industry-specific guidance released in 2019, this report presents up-to-date and achievable advice for cyber-aware electricity industry companies' boards of directors to begin taking action immediately on this important and growing business risk. This initiative identified seven implementation categories that require pressing action at the highest strategic level:

1. Oversight of enterprise cyber risk and resilience
2. Organizational governance
3. Risk management
4. Systemic cyber resilience
5. Resilience plans
6. Review of organization and board performance
7. Community collaboration and interdependence

It is important for leaders to note that these implementation categories are not listed in order of importance; rather, they each support cyber resilience within electricity companies. In fact, the category "community collaboration and interdependence" is especially vital because shared risk demands shared efforts to ensure cyber resilience.



This report addresses two distinct audiences (board directors and corporate officers accountable for cyber resilience) and offers a method for finding a common language to encourage collaboration. Moreover, it presents three areas for consideration:

The journey to cyber resilience

The bridge between board directors and corporate officers accountable for cyber resilience focuses on translating and communicating cyber risks, incorporating them in the enterprise risk register and aligning those risks with business strategic objectives – with maintaining operational resilience as the end goal. First, this report frames the journey towards a company's cyber resilience. Seven categories, which go from oversight of cyber risk through to organizational performance reviews, define the ability of a company to move from a reactive to a proactive cyber-resilience posture.

Recommendations for the directors of the board

Only the board of directors can instil the cultural shifts and motivate the organizational shifts that must take place to ensure cyber resilience. The section on actions for the board offers clear and achievable steps that directors should take immediately in order to improve the cyber resilience of their company. This section also recognizes the important role that the board plays in embedding cyber resilience in the broader industry's ecosystem.

Recommendations for corporate officers accountable for cyber resilience

This report provides corporate officers (and other senior cybersecurity executives) accountable for cyber resilience with the tools to communicate the most relevant and salient information in an effective way to support and guide the board of directors to make better risk-informed decisions related to cyber resilience. It also highlights opportunities for the strategic-technical collaboration necessary to ensure cyber resilience.

Corporate officers and managers responsible for cyber resilience

Most medium and large organizations identified the need to establish a role the main responsibility of which is to ensure the overall cyber resilience of the enterprise. The Forum's 2017 and 2019 guidance to boards recommends the identification of "one corporate officer accountable for reporting on the organization's capability to manage cyber resilience and progress in implementing cyber-resilience goals".[2] The chief information security officer (CISO) is often the individual within the organization who is responsible for overseeing the organization's cyber-resilience programme aimed at protecting digital infrastructure and assets against cyber threats and ensuring the continuity of business operations. (However, this title does not always bear ultimate accountability to the board for cyber resilience; therefore, this report uses a more generic reference to officers with accountability for cyber resilience.) This officer is often a senior executive essential in leading and overseeing the overall cyber-resilience strategy of the company and reporting to and advising the board of directors regarding cyber risks.

The cooperative approach between technical and strategic functions outlined here will encourage company cyber resilience and, in so doing, support the resilience of the electricity ecosystem as a whole.

The journey to cyber resilience

Cyber resilience is a dimension of cyber-risk management that describes the capacity of systems and organizations to develop and execute long-term strategies to withstand and recover from cyber events.[3] Being resilient requires those at the highest leadership levels to acknowledge the importance of proactive risk management and focus more on the ability of the organization to absorb and recover from a cyberattack that would disrupt essential services.

Many organizations have already begun this journey in piecemeal fashion as a matter of necessity, given the pervasive and fast-changing nature of cyber threats. The electricity industry, after all, is no stranger to resilience planning with regard to physical security and the threat of natural events. Fewer companies, however, have engaged in a holistic approach to moving towards cyber resilience, which requires leadership at the highest levels to ensure it remains a focus of every business unit. Fewer companies still have taken the vital steps necessary to ensure cyber resilience of the electricity ecosystem as a whole, understanding the broader interdependencies and risks posed by and to the ecosystem and addressing them in a coordinated way with other actors in the ecosystem.

Implementation of cyber-resilience techniques requires a continuous process across the seven defined categories, with an acknowledgement that ecosystem-wide collaboration is essential to the success of such a journey. The journey towards cyber resilience is illustrated opposite.

The journey to cyber resilience is a continuous process across the implementation categories, with collaboration across the internal and external ecosystem.

Recommendations for directors of the board

The board of directors can inspire the cultural shifts and motivate the organizational shifts that must take place to ensure cyber resilience. The Systems of Cyber Resilience: Electricity community, through consultation with their respective company leaders, has curated the following suggestions for clear, achievable steps that the board should take immediately in order to improve its governance of the cyber-resilience programme of its organization.

CATEGORY 1 – Exercise effective oversight of enterprise cyber risk and resilience

The board is ultimately responsible for the oversight of cyber risk and enterprise cyber resilience. Boards should implement the following actions in order to effectively exercise this responsibility:

- Assign primary oversight activity to a permanent committee of the board (e.g. the risk committee or a newly created committee).
- Establish a programme of continuing education on cybersecurity risk issues and cyber resilience for the entire board, along with a cyber-resilience orientation programme for new directors, which is regularly updated with information from internal and external resources.
- Establish a regular cadence of cyber-resilience reporting by the officer accountable for cyber risk and resilience and define metrics included in periodic reports from the heads of all business units to ensure business ownership and alignment with business objectives.

> *Boards need CISOs to translate complex technical and engineering concepts into relatively simple language, just as is needed for other specialized areas of risk.*

UC Berkeley Center for Long-Term Cybersecurity[4]

CATEGORY 2 – Create the right organizational governance

In an effective corporate structure, the board requires management to implement comprehensive cybersecurity governance, which governs IT and OT – as well as their convergence in the internet of things (IoT) – along with physical security and digital transformation, ensuring interoperability within the organization and driving alignment across the ecosystem. The board should implement the following actions to ensure an effective governance model:

- Assign accountability for cyber resilience to a senior corporate officer who will report on the organization's capacity to manage cyber resilience and progress in implementing cyber-resilience goals, and who is charged with responsibility for governance and oversight of cybersecurity strategy across the IT and OT environments.
- Ensure that this officer has the proper level of authority, access to the board, command of the subject matter, experience and resources to fulfil these duties.
- Create a regular board agenda item for cyber-resilience reports.
- Ensure that all businesses designate an empowered individual with the responsibility to integrate cyber resilience into asset and process design.
- Establish a clear preference for, and encourage, cyber resilience by design throughout the organization's processes and systems and require management to document progress.

> *Board members should set clear expectations with management about the format, frequency, and level of detail of the cybersecurity-related information they wish to receive … This should begin with using the cybersecurity expertise within the company…*

National Association of Corporate Directors (USA)[5]

CATEGORY 3 – Assess and prioritize cyber-risk management

The board ensures that its cyber-resilience posture and efforts extend beyond compliance towards a holistic risk-management approach and are supported by adequate funding and resourcing. The board includes cyber risk in its enterprise risk-management approach. Moreover, it holds management accountable for understanding the organization's interdependencies within the ecosystem, reporting on the systemic cyber risks posed by digitalization, emerging technologies and by the broader ecosystem (especially the supply chain), and planning and prioritizing cyber-resilience efforts accordingly.

In order to appropriately assess and prioritize cyber risk, the board should implement the following actions:

- Define and seek quantification of enterprise and business risk tolerance relative to cyber resilience.[6]
- Review budgeting and resource allocation to ensure that cyber risk and the company's appetite for cyber risk is fully integrated into enterprise-wide governance and risk-management frameworks activities.
- Require identification of company "crown jewels" (the most vital assets and processes)[7] beyond those designated by existing critical infrastructure protection regulations and ensure/demand strong cyber-resilience assessment and oversight of supporting systems and vendors.

> *[Cybersecurity] should also be integrated into a wide range of issues to be presented to the board including discussions on new business plans and product offerings, mergers and acquisitions, new market entry, deployment of new technologies, major capital investment decisions such as facility expansions or IT system upgrades and the like. As corporate assets have increasingly become digital assets, virtually all major business decisions before the board will have cybersecurity components to them. In many ways, cybersecurity is now a cross-cutting issue similar to legal and finance. Effective boards approach cybersecurity as an enterprise-wide risk-management issue.*
>
> **National Association of Corporate Directors (USA)[8]**

- Ensure that management integrates assessment of cyber resilience and cyber risk into the overall business and digital transformation strategy and into enterprise-wide risk management, as well as budgeting and resource allocation.

CATEGORY 4 – Build and support systemic cyber resilience

The board recognizes that electricity organizations operate in an interconnected and interdependent environment where the consequences of a cyberattack on one can cascade to numerous others.

> *[D]irectors should ensure that management is assessing cybersecurity not only as it relates to the organization's own networks, but also with regard to the larger business ecosystem in which it operates.*
>
> **National Association of Corporate Directors (USA)[9]**

The board should implement the following actions to build systemic cyber resilience:

- Adopt a holistic risk-management vision that ensures systemic risk affecting the ecosystem as a whole is considered when making strategic decisions.
- Require regular cyber-resilience reporting by the officer accountable for cyber risk and resilience of the cyber risks posed to the company by ecosystem dependencies (especially the supply chain) and by the company to the wider ecosystem.[10]
- Hold management accountable for understanding these interdependencies and planning and prioritizing cyber-resilience efforts in accordance with the company's risk profile.
- Ensure that risk assessments quantify supply-chain cyber risk and evaluate whether the processes in place to manage such risks are robust.

CATEGORY 5 – Implement and test cyber-resilience plans

The board understands that basic resilience planning, including business continuity, communications, disaster recovery and incident response, is crucial to cyber resilience. To achieve an adequate level of resilience across the ecosystem, businesses should embed cyber resilience within their business-resilience planning. The board should implement the following actions to strengthen the company's cyber-resilience planning:

– Identify the creation of a robust, formal joint cyber-resilience plan and related procedures

  (which cover response through recovery, as well as crisis-management processes), with explicit incorporation of the board's role, as one of the organization's strategic priorities.

– Set a regular cadence of reporting on cyber-resilience plans, to include developing regular end-to-end testing and updating the organization's resilience plan in the board's assessment of upper management performance.

– Begin conducting regular cybersecurity preparedness exercises at the board level, in conjunction with providers and vendors where relevant, that include systemic failure and recovery as a component or focus of the exercise.

– Ensure that management supports the officer accountable for cyber resilience through the creation, implementation, testing and ongoing improvement of cyber-resilience plans, which are appropriately harmonized across the business.

CATEGORY 6 – Continuously assess and review organizational and board performance

To confirm that the company is achieving the appropriate level of cybersecurity and resilience maturity, the board ensures that its performance and that of the entire organization is reviewed. In assessing its ability to provide effective oversight of cybersecurity, the board should ask the following question, taken from the USA's National Association of Corporate Directors' 2020 Cybersecurity Guidance: "Can all directors effectively contribute to a robust conversation with management about the current state of the company's cybersecurity? In which areas does our lack of knowledge/understanding of cyber matters prevent effective oversight?"[11]

The board should implement the following actions to ensure that performance is continuously assessed and reviewed:

– Schedule regular internal or external reviews of the organization's cyber preparedness and maturity for reporting to and interactive discussions with the board.

– Review board composition and either include directors with the experience and ability to understand cyber risk or ensure such experience is accessible to the board.

– Ensure that the organization's cyber-resiliency mechanisms are subject to independent third-party review on a regular basis, and that the results of and recommendations from these reviews are incorporated into the board's strategic and tactical cyber-resilience planning and roadmaps.

CATEGORY 7 – Identify interdependencies and the need for collaboration

In a highly interconnected and interdependent ecosystem, cyber risks are shared across all ecosystem partners. Therefore, directors enable management to create a culture of collaboration. The board should implement the following actions to identify interdependencies and strengthen collaboration:

- Set an example by actively collaborating with industry peers and other stakeholders and take an active role in setting the strategic vision for systemic cyber resilience.
- Enable management to collaborate with ecosystem stakeholders and system-wide cybersecurity bodies to facilitate the transparent and agile sharing of information and creation of cyber intelligence (e.g. achievable threat intelligence, incident reporting and effective techniques for mitigating the main threats).
- Enable management to set strategic objectives in terms of information sharing and understand and mitigate cyber risks in the ecosystem.
- Request cyber-risk assessment of key agents and dependencies across the supply chain and promote collaboration with important vendors and partners to raise systemic cyber resilience.
- Promote collaboration with main suppliers and business partners to improve the cybersecurity of products and services.

Recommendations for corporate officers accountable for cyber resilience

This playbook for corporate officers accountable for cyber resilience provides pragmatic and achievable recommendations when communicating and engaging with their board about cyber resilience.

Corporate officers accountable for cyber resilience should build situational awareness and answer the following questions before using this playbook:

- What are the main cyber-related risks and threats to the organization?
- What is the organization's cybersecurity posture?
- What is the cybersecurity strategy, including roadmap, prioritization and investments required to protect the crown jewels and maintain business continuity?
- What are the main actions and decisions required from senior management and the board, respectively?

To ensure efficient communication in the electricity industry, organizations should begin by prioritizing the implementation of effective cybersecurity best practices based on the categories identified in this document in alignment with business strategy.

This playbook suggests a set of metrics to help monitor the efficacy and maturity of the implementation based on defined outcomes. A board-level dashboard can be an effective communication tool to convey vital information about organizational cyber posture and high-risk areas as well as to help make better-informed decisions on risk-mitigation measures and associated investments. See the Appendix for an example dashboard that could be used to present key points to the board.

CATEGORY 1 – Exercise effective oversight of enterprise cyber risk and resilience

Corporate officers accountable for cyber resilience must provide empirical data on key cyber risks for the board to exercise its responsibility for oversight of enterprise cyber risk and resilience. To support effective oversight, corporate officers accountable for cyber resilience should rely on a set of meaningful metrics to demonstrate the state of implementation, maturity and performance to the board.

The cyber-resilience officer should implement the following actions to ensure effective oversight of cyber risks and resilience by the board:

- Schedule regular reports on the state of the organization's cyber risk and resilience, ideally every quarter.
- Work with the heads of other business units to facilitate the reporting and mitigation of cyber risks and metrics within their respective areas.
- Provide visibility of the cyber risks related to the company's critical assets by highlighting the potential consequences and mitigation actions.

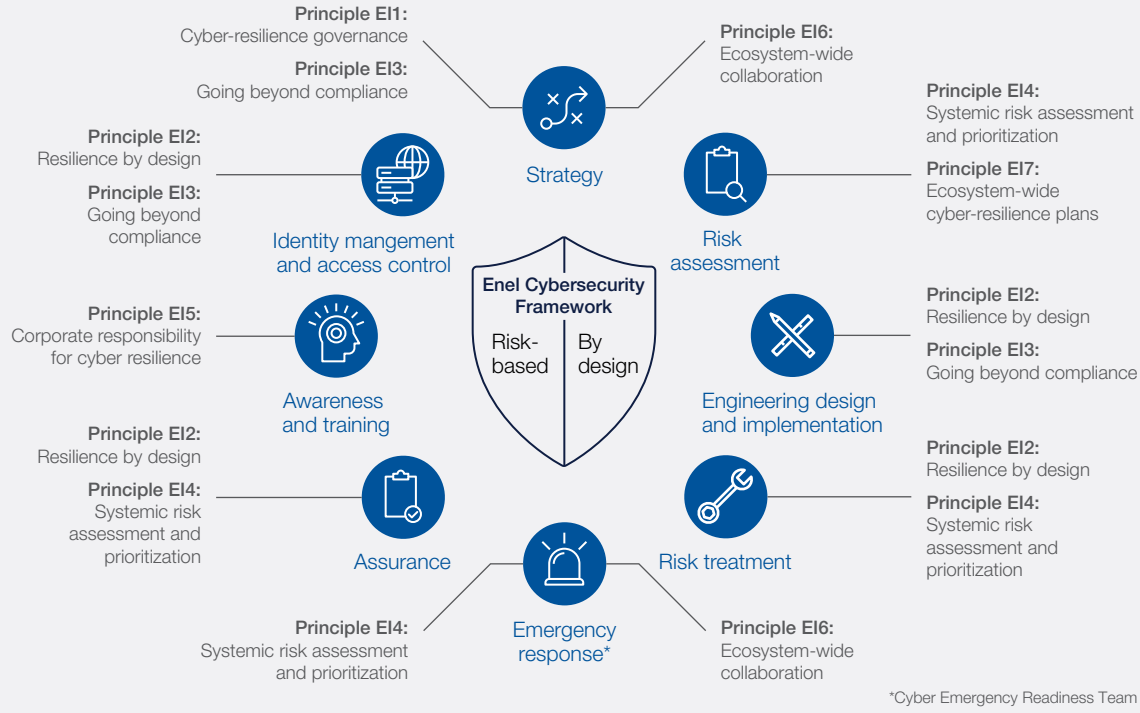
Suggested metrics can include:

- Frequency of cyber-risk and cyber-resilience reporting to the board.
- Number of open vs. closed actions arising from cyber-risk and resilience reviews with the board.
- Number of major cybersecurity incidents within the industry, affecting the company, with quantified impact, e.g. financial, operational, reputational, compliance.
- Status of business units' strategic cyber-risk reporting (number of risks accepted, denied, mitigated).
- Percentage of business units that report cyber risk.
- External cyber-risk ratings compared to industry average and competitors.

USE CASE: **Enel**
A journey to improve the oversight of cyber resilience

The continuous increase of digital connectivity in the electricity sector increases exposure to potential cyber risks, in particular for global industrial companies operating in complex environments such as the Enel Group. To keep pace and better monitor cyber risks, the Enel Group embedded cybersecurity strategy into its corporate group strategy, developing a cybersecurity framework that encompasses eight processes (as depicted in the figure below). It is easy to observe the full match with the World Economic Forum's *Advancing Cyber Resilience: Principles and Tools for Boards*.

World Economic Forum's cybersecurity electricity industry principles and Enel's cybersecurity framework processes



*Cyber Emergency Readiness Team

In its journey to cyber resilience, and in order to improve its oversight of enterprise cyber risk, Enel established its Cyber Security Risk Committee. Enel's chief executive officer acts as chairperson, with the aim of addressing and approving the organization's cybersecurity strategy as well as checking periodically on the progress of its implementation. This committee comprises key executive directors overseeing Enel's critical businesses and services from different geographies along with the group Chief Information Officer and Chief Information Security Officer.

In addition, Enel, within its cybersecurity cross-organization, defined the new "cyber-risk manager" organizational role – for each area of business – reporting to the Chief Information Security Officer and representing business priorities related to cyber-risk management.

This governance allowed the extension and adoption of a group-wide, risk-based cybersecurity framework to all business areas and geographical locations, improving the control of the Enel Group's cyber resilience. The expansion of a holistic cyber-risk management approach represents an ongoing priority at Enel to encourage ecosystem cyber maturity by employing and collaborating with external parties.

Currently Enel is strongly engaged in the community working group developing a cyber security Network Code for the electricity ecosystem in Europe.

This case illustrates the implementation of Categories 1, 2 and 3.

CATEGORY 2 – Create the right organizational governance

Corporate officers accountable for cyber resilience should implement the following actions to ensure an effective governance model by the board:

- Present the cyber-resilience organizational structure to the board, covering corporate IT, OT and IoT environments as well as integration with each business unit.
- Provide regular quarterly updates on the cyber-resilience strategy implementation and budget in close collaboration with different business functions and unit leaders.
- Ensure communication with experts and contact points from different business areas.
- Promote a cyber-hygiene culture by communicating best practices regularly through training, communication awareness and tests across the organization and, in particular, targeting high-risk groups, e.g. board, C-suite, IT, engineering, HR and finance.
- Integrate or launch collaboration meetings and working groups with different stakeholders in the ecosystem to align and share experiences in order to report trends to the board.

Suggested metrics can include:

- Percentage of employees who have completed cybersecurity awareness education programmes on cyber-hygiene practices, with a focus on high-risk groups, e.g. board, C-suite, IT, engineering, HR and finance.
- Number of full-time equivalents (FTEs) responsible for cybersecurity/cyber experts in the different business areas.
- Number of cyber meetings/committees with involvement in the businesses.
- Number of outstanding and closed critical actions resulting from reviews of the cybersecurity framework relating to executive management accountability and responsibility.

USE CASE: **Iberdrola**
Setting a baseline to improve global cyber resilience

Iberdrola Group's cybersecurity transformation started in 2015 when the board of directors approved a cybersecurity risk policy recognizing the significance of cyber risk for the group. This policy expressed the company's commitment to promoting adequate cybersecurity and resilience mechanisms across the IT and OT environments and to strengthening capabilities to detect, prevent, defend and respond to cyberattacks and incidents.

The approach established by Iberdrola focuses on embedding cyber resilience into business strategies, operational decisions and daily activities and improving implementation of the World Economic Forum's 2017 and 2019 board principles to improve governance and oversight of cyber risk at a global level and promote collaboration across the group (IT, OT, physical and digital) and with the relevant ecosystem agents.

To set the baseline for a culture change and ensure cyber-risk awareness in risk owners, the board defined an organizational strategy that would ensure strong leadership and oversight plus the effective integration of cybersecurity and resilience into all businesses and corporate areas.

The group board's Audit and Risk Supervision Committee was designated responsible for overseeing the group's cyber-risk and resilience capabilities and a global chief information security officer was appointed to lead its cyber-resilience strategy, governance and oversight across the group's IT and OT environments. The global chief information security officer provides the board with specific cyber training, including best practices and an introduction to board principles, with quarterly updates about the cybersecurity risks specific to the company and the evolution and effectiveness of the programmes defined to address them.

Local chief information security officers were appointed in all countries and cybersecurity experts were assigned by all businesses and corporate areas (including but not limited to IT) responsible for ensuring implementation of cybersecurity programmes and operations in alignment with the global cybersecurity strategy. A Global Cybersecurity Committee was constituted to ensure proper coordination across the group, encourage collaboration and information exchanges and ensure a coordinated incident response.

The cybersecurity committee defined a global cybersecurity strategy and framework, including roles and responsibilities and global rules and procedures, to ensure a common language and a coordinated approach to cyber resilience across the group. Additional key metrics and dashboards have been established to facilitate risk-management decision-making and communication of cyber risk between business leadership, chief information security officer and board members and to prioritize resource allocation by focusing on protecting critical business processes and infrastructures beyond the ones designated by existing regulations.

With the increasing maturity of the implementation categories, Iberdrola aims to improve not only its own cyber-resilience posture and cyber-risk oversight capabilities, but also to enhance ecosystem-wide resilience through active collaboration with important public and private stakeholders.

This case illustrates the implementation of Categories 1, 2 and 7.

CATEGORY 3 – Assess and prioritize cyber-risk management

Corporate officers accountable for cyber resilience should implement the following actions to ensure cyber risks are appropriately assessed and prioritized by the board:

- Define and quantify the business risk tolerance relative to cyber resilience in collaboration with other business units.
- Provide, in an objective manner, the list of critical/high strategic cyber risks and financial risk exposure related to corporate IT, OT and IoT environments and supplier/business partners with cyber loss reduction measures and investments.
- Review investment and resource allocation per business function and unit with respect to mitigation of critical and high cyber risks.
- Share objectively the effectiveness of the investment made against the company's cyber-risk appetite.

Suggested metrics to follow include:

- Frequency of budgeting and resource allocation reviews to ensure that cyber risk and the company's appetite for cyber risk is adequately reflected.
- Number of critical systemic risks (affecting the industry as a whole) covered by risk analysis.
- Frequency of risk assessments conducted for critical business assets, functions and suppliers/business partners, e.g. based on the business impact analysis (BIA) information.
- Number of critical/high cyber risks for these critical assets, functions and suppliers.
- Percentage of critical non-compliances/ exceptions closed at the agreed time.
- Evolution (tendency) of key threats and potential financial impacts.
- Number of critical/high risks related to cyber resilience that are above the defined tolerance on the quantified financial impact, with investments required to mitigate them to an acceptable level.

USE CASE: **New York Power Authority**
Implementing the principles to improve the active management of cybersecurity and resilience

The New York Power Authority (NYPA) focuses on security and resilience, implementing board principles through monitoring and implementing the toolkit for cyber resilience in the electricity sector. The NYPA has strong board engagement on the critical role the organization plays in New York State and an understanding of how security and resilience of the services provided need clear emphasis.

In working towards improved oversight of cyber resilience, the NYPA has implemented a board-level security committee focused on cyber and physical security, including overall resilience. The committee is augmented at the business level by the NYPA Secure Committee, which includes top-level business leaders who intersect or partner with security teams. As part of this institutional structure, NYPA's three-year cybersecurity roadmap and integrated resilience roadmap undergo regular updates and reviews, including annual reviews and status updates to the board.

This process also ensures that cyber risk is aligned with, and managed in concert with, enterprise risk-management processes to ensure mitigation, response and monitoring. Risk owners are identified and assigned, with cyber resilience being mostly coordinated by the executive business lead (e.g. chief information security officer) as the assigned risk owner. Integration with enterprise risk management was achieved by aligning the Secure Committee with the Enterprise Risk Management Committee for clearly defined risk appetite and effectiveness metrics and escalation. Systemic risks are raised through the various channels, ultimately making their way to the board in quarterly updates. Resilience is reviewed and improved by business and industry exercises that move beyond the tabletop to action. These assessments and the corresponding after-action reports drive decision-making and prioritization to continually reduce cyber risk and increase business resilience. The NYPA confirms these actions and mitigations with intensive internal audit functions and through the use of external assessments. The NYPA continues to implement the cyber-resilience principles to ensure the right services and focus takes overall resilience into account.

The implementation of the principles clarified a top-down understanding of NYPA's cyber risk in comparison to all enterprise risk, allowing a clear and decisive management of security risks across all business and critical functions. Risks in terms of supply chain, compliance and the new normal (e.g. post-COVID) will continue to drive cooperative measures, services and initiatives. By using the implementation of these categories to achieve the board's principles, the NYPA aims to continuously improve the active management of cybersecurity and resilience while coping and adapting to any future changes and challenges.

This case illustrates the implementation of Categories 1, 2 and 3.

CATEGORY 4 – Build and support systemic cyber resilience

Corporate officers accountable for cyber resilience should implement the following actions to build systemic cyber-resilience oversight by the board:

- Ensure identification and mitigation of cyber risks posed by own or external businesses to the wider ecosystem.
- Establish clear and comprehensive cyber-resilience policies, standards and guidelines throughout the organizations, including IT, OT and IoT environments and third-party business suppliers and partners.
- Create baseline requirements on cyber resilience when working with third-party partners and vendors and include standard contractual service-level agreements and key performance indicators (KPIs).
- Collaborate with other business unit designees and individuals who have the responsibility to integrate cyber resilience into asset and process design.

Suggested metrics to follow include:

- Percentage of strategic/critical suppliers/partners assessed (cyber-resilience due diligence) and with security clauses embedded in their contract.
- Number of critical/high cyber risks related to suppliers/business partners by status (open, mitigated, avoided).
- Number of cyber incidents detected/shared within the ecosystem and actions in place to remediate reported vulnerabilities per quarter.

USE CASE: **ENTSO-E**
Enforcing cybersecurity in the European energy market through the electricity network codes

Recent cyberattacks on European electricity companies have reinforced the need for a common and collaborative effort to enhance ecosystem-wide cyber resilience, e.g. ENTSO-E,[12] EDP[13] and ELEXON.[14] The European Commission Regulation on the Internal Market for Electricity (COM/2016/0861) provides for the adoption of technical rules (e.g. a network code) across the electricity ecosystem.

In April 2019, an EU Commission recommendation on cybersecurity in the energy sector highlighted that "smart grid" digitalization increasingly exposes the energy system to cyberattacks and incidents that may jeopardize the security of energy supplies.[15] Already, the European transmission system operator (TSO; ENTSO-E) and distribution system operator (DSO; E-DSO, EURELECTRIC, GEODE and CEDEC) communities are working together to develop recommendations and drive a consultation process on initial proposals for a cybersecurity network code. The initial proposals include recommendations on:

- Inclusion of ISO 27001 certification using a common scope.
- Identification of critical IT and OT systems and components through a common cyber-risk assessment process.
- Inclusion of a common set of functional security requirements for systems and components.
- Inclusion of a product assurance scheme whereby functional security requirements can be independently tested and results shared.
- Introduction of an information-sharing process for the distribution of technical cyber-incident information.

The selected recommendations will undergo a formal consultation process with other energy-sector stakeholders in 2021 supported by ENTSO-E. Once finalized, the cybersecurity network code recommendations will affect the European energy sector by enforcing energy stakeholders to comply and implement cybersecurity actions.

This case illustrates the implementation of Categories 4 and 7.

CATEGORY 5 – Implement and test cyber-resilience plans

Corporate officers accountable for cyber resilience should implement the following actions to strengthen cyber-resilience planning oversight by the board:

- Develop a cyber-resilience plan in close collaboration with all business function and unit leaders and explicitly incorporate the board's role as one of the organization's strategic priorities.
- Set a regular cadence of reporting on cyber-resilience plans, to include vital updates, testing frequency and results.
- Conduct regular cybersecurity exercises and tests on cyber resilience that include systemic failure and subsequent recovery as a component or focus of the exercise. Examples of useful exercises are those that demonstrate the maturity improvements of cyber-resilience-related controls on human capital, processes and digital landscapes within the company, such as business-continuity and disaster-recovery simulations based on various cyberattack scenarios.
- Ensure that the cybersecurity strategy and programme include the detection of anomalies linked with internal and external sources, management of incidents, response and recovery capabilities (from a people, process and technology perspective).
- Include cybersecurity-related events and resilience by design in existing business continuity plans with offline recovery measures, out-of-band communication methods and independent recovery sites.

Suggested metrics include:

- Number of hours of interruption/ disruption of essential business services (with financial impact).
- Percentage of critical open actions and closed actions resulting from cybersecurity preparedness exercises (with systemic failure testing as a component or focus of the exercise).
- Percentage of critical systems for which contingency planning/disaster recovery has been implemented and tested successfully this quarter.
- Percentage of critical services/processes for which there is a failover system with restore time within the BIA recovery time objectives.

USE CASE: **Adani Group**
Resilience plans – IT/OT transformation programme

Adani Group began its IT and OT cybersecurity transformation programme in relation to more than 2,000 assets in approximately 80 locations and on 170 networks; these include areas such as power, renewables and transmission.

The full programme aims to ensure business continuity by protecting critical infrastructure assets from attack, damage, unauthorized access and rejection of service. The programme has a centralized strategy, roadmap and planning governance that integrates business, IT and OT teams supported by original equipment manufacturers (OEMs) plus technology and process partners. The programme is overseen by management, and includes monthly reports and steering committee reviews.

The integration of holistic cybersecurity management detection and response (MDR) capabilities among different parties represents one of the programme's priorities, focusing on technology and process areas for global risk mitigation. In addition to the creation of common IT/OT policies, procedures and guidelines and clear IT/OT-integrated detection and responses, the programme includes the deployment of detection and monitoring technology and network segmentation for OT infrastructure, such as intrusion detection systems and OT firewall monitoring. With these, Adani aims to mitigate the risks and create proactive threat detection and response capabilities to better manage any possible future cyber incidents.

This case illustrates the implementation of Categories 1, 3 and 5.

CATEGORY 6 – Continuously assess and review organizational and board performance

Corporate officers accountable for cyber resilience should implement the following actions to ensure that the board's performance is continuously assessed and reviewed:

– Validate with internal audits that independent assessments are conducted on the performance of the board as it relates to the oversight of the cyber-resilience strategy and plan.

Suggested metrics include:

Note that the board's internal audit is generally beyond the scope, responsibility and authority of the corporate officers accountable for cyber resilience. However, they may provide useful information to the board regarding the frequency of such audits as well as how findings are communicated and implemented through the organization.

– Frequency of internal audits of the organization's cyber-preparedness and -maturity for reporting to the board of directors.

– Number of critical actions outstanding from regular internal or external reviews focusing on the organization's cyber-preparedness and -maturity, and year-on-year trends with respect to cybersecurity maturity scores.

– Number of critical actions and recommendations from internal or external cybersecurity reviews that have been incorporated into the board's strategic and tactical cyber-resilience planning and roadmaps, and those for which no action has been planned or implemented.

CATEGORY 7 – Identify interdependencies and the need for collaboration

Corporate officers accountable for cyber resilience should implement the following actions to identify interdependencies and strengthen collaborations with the broader ecosystem:

– Perform an end-to-end review of the supply- and value-chain dependencies and highlight blind spots and high risks related to cyber resilience.

– Lead or engage in cyber-resilience communities and initiatives (under the stewardship of industry, national or international organizations) that encourage information-sharing, strengthen collaboration across the ecosystem and drive collective action.

– Collaborate with ecosystem stakeholders and actively participate in system-wide cybersecurity information-sharing bodies.

– Establish tracking measures for evolving regulatory frameworks and related compliance actions on cybersecurity-relevant issues, in all of the countries where the company is active and recognized as an operator of essential services.

Suggested metrics:

– Frequency of events with ecosystem and industry peers.

– Frequency of meetings with regional security officials and with cyber-response experts (national security and intelligence officials or private-sector cyber-response and legal experts) and critical incidents being tracked/closed.

– Number of critical incidents reported to law enforcement agencies, regulatory bodies or organizations (industry, national or international).

– Number of threat intelligence reports/ briefings exchanged with peers across the ecosystem.

USE CASE: **Siemens**

Collaborating to build a secure and trusted energy community

The spate of attacks against the world's critical infrastructure put into focus the urgent need to address industrial cybersecurity. Siemens is taking a leading role by ensuring secure design processes and certification on its products and solutions. As the electricity industry becomes increasingly interconnected, no company can address this complex challenge alone.

Recognizing that resilience requires strengthening and building trust with customers, suppliers and the electricity community as a whole, Siemens has worked closely with the World Economic Forum to develop board principles as part of a joint mission to build trust for a secure digital world. To that end, Siemens established the Charter of Trust, bringing together leading energy companies, technology providers, insurers and manufacturers committed to advancing cybersecurity and digitalization.

Highlights from this work include:

- Initiating change from the top by hiring a chief security officer to report directly to the deputy chief executive officer and the Siemens board.
- Implementing security processes and certifications on Siemens technologies and establishing voluntary, third-party certifications throughout its supply chains.
- Supporting the growth of a technology ecosystem of leading security companies to build novel industrial cyber technologies in the areas of monitoring and vulnerability management.
- Collaborating with global standards and industry bodies to set global and national guidelines for securing critical assets.
- Developing national workforce programmes to overcome the acute talent shortage of industrial cyber professionals in the electricity sector.
- Quickly responding alongside Charter of Trust members to respond to COVID-19, ensuring safe and secure remote telework, all while maintaining critical operations for Siemens and its customers.

This case illustrates the implementation of Category 7

Conclusion

In an ecosystem such as the electricity industry, cyber resilience can, ultimately, result only through large-scale and continual collaboration and partnership. This means that a variety of stakeholders must work together, inside the enterprise, between companies and between the companies and the public sector. Without a common understanding and systemic approach to cyber risks, public- and private-sector leaders will struggle and even fail in implementing appropriate countermeasures to mitigate them. It is crucial for all stakeholders in the value chain to embrace a collaborative and risk-informed cybersecurity approach to adapt and ensure a secure ecosystem.

In this report, the World Economic Forum and its working group have presented a model for collaboration within a company, specifically between the board with responsibility for overall corporate strategy and the cyber resilience accountable officer with responsibility for cybersecurity and resilience. The report is another step towards developing the habits of collaboration necessary to meet the current cybersecurity challenges. By fostering a culture of collaboration within organizations, it is hoped that individual companies in the electricity ecosystem can become more secure, adaptable and effective partners and thus ensure the resilience of this vital industry as a whole.

Appendices

This section presents appendices supporting the report results.

Taxonomy

The table below provides definitions of the most-used terms throughout the document for reference.

TERM	DEFINITION
Board and board of directors	Corporate fiduciaries responsible for overseeing management strategy, as well as the identification and planned response to enterprise-wide risks affecting a company and its value to stakeholders and shareholders[16]
Cyber-resilience	A dimension of cyber-risk management, representing the ability of systems and organizations to develop and execute long-term strategy to withstand cyber events
Cyber-resilience officer	A senior executive within the organization who is responsible for developing and implementing the organization's cyber-risk and resilience programme
Electricity ecosystem	Electricity organizations have interdependent relationships with numerous stakeholders that can span multiple degrees of separation from the organization. They rely on these relationships to provide business-critical components and services (everything from core operational assets and smart devices to on-site servicing)[17]
Information technology (IT)	Information technology (IT) covers any form of technology – that is, any equipment or technique used by a company, institution or any other organization that handles information
Operational technology (OT)	Operational technology (OT) monitors and manages industrial process assets and manufacturing/industrial equipment. OT has existed for much longer than IT or information technology – ever since people started to use machinery and equipment powered by electricity in factories, buildings, transportation systems, the utility industry etc.
Legacy systems	A legacy system refers to outdated IT or OT systems, programming languages or application software that are used instead of an available upgraded version

Cyber-resilience board principles ‘tear sheet’

The tables below recap the general and electricity-specific board principles.

General board principles for cyber resilience

Principle 1: Responsibility for cyber resilience

The board as a whole takes ultimate responsibility for oversight of cyber risk and resilience. The board may delegate primary oversight activity to an existing committee (e.g. risk committee) or new committee (e.g. cyber-resilience committee)

Principle 2: Command of the subject

Board members receive cyber-resilience orientation upon joining the board and are regularly updated on recent threats and trends – with advice and assistance from independent external experts being available as requested

Principle 3: Accountable officer

The board ensures that one corporate officer is accountable for reporting on the organization’s capability to manage cyber resilience and progress in implementing cyber-resilience goals. The board ensures that this officer has regular board access, sufficient authority, command of the subject matter, experience and resources to fulfil these duties

Principle 4: Integration of cyber resilience

The board ensures that management integrates cyber resilience and cyber-risk assessment into overall business strategy and into enterprise-wide risk management, as well as budgeting and resource allocation

Principle 5: Risk appetite

The board annually defines and quantifies business risk tolerance relative to cyber resilience and ensures that this is consistent with corporate strategy and risk appetite. The board is advised on both current and future risk exposure as well as regulatory requirements and industry/societal benchmarks for risk appetite

Principle 6: Risk assessment and reporting

The board holds management accountable for reporting a quantified and understandable assessment of cyber risks, threats and events as a standing agenda item during board meetings. It validates these assessments with its own strategic risk assessment using the board’s cyber-risk framework

Principle 7: Resilience plans

The board ensures that management supports the officer accountable for cyber resilience by the creation, implementation, testing and ongoing improvement of cyber-resilience plans, which are appropriately harmonized across the business. It requires the officer in charge to monitor performance and to regularly report to the board

Principle 8: Community

The board encourages management to collaborate with other stakeholders, as relevant and appropriate, in order to ensure systemic cyber resilience

Principle 9: Review

The board ensures that a formal, independent cyber-resilience review of the organization is carried out annually

Principle 10: Effectiveness

The board periodically reviews its own performance on the implementation of these principles or seeks independent advice for continuous improvement

Electricity board principles for cyber resilience

Principle EI1: Cyber-resilience 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 EI2: 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 EI3: Going beyond compliance

The board ensures that its cyber-resilience posture and efforts extend beyond compliance, towards a holistic risk-management approach, and are supported by adequate funding and resourcing

Principle EI4: Systemic risk assessment and prioritization

The board holds management accountable for understanding the organization’s interdependencies within the ecosystem, reporting on the systemic cyber risks posed by the ecosystem (especially the supply chain), and planning and prioritizing cyber-resilience efforts accordingly

Principle EI5: Corporate responsibility for cyber resilience

The board encourages management to consider what cyber risks the organization, its cyber culture and practices may pose to the ecosystem, and appropriately explore how such risks can be reduced

Principle EI6: Ecosystem-wide collaboration

The board enables management to create a culture of collaboration, set strategic objectives in terms of information-sharing and understand and mitigate cyber risks in the ecosystem. The board also actively collaborates with industry peers and policy-makers

Principle EI7: Ecosystem-wide cyber-resilience plans

The board encourages management to create, implement, test and continuously improve collective cyber-resilience plans and controls together with other members of the ecosystem. These plans should appropriately balance preparedness and protection (e.g. defence-in-depth strategies) with response and recovery capabilities

Mapping of the implementation categories to the board principles

The table below illustrates the mapping of the implementation categories to the Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards.

#	Implementation category	Associated board principles for cyber resilience
1	**Oversight of enterprise cyber risk and resilience**	P1 – Responsibility for cyber resilience P2 – Command of the subject
2	**Organizational governance**	P3 – Accountable officer EL1 – Cyber-resilience governance EL2 – Resilience by design
3	**Risk management**	P4 – Integration of cyber resilience P5 – Risk appetite P6 – Risk assessment and reporting EL3 – Going beyond compliance EL4 – Systemic risk assessment and prioritization
4	**Systemic cyber resilience**	P1 – Responsibility for cyber resilience P2 – Command of the subject EL5 – Corporate responsibility for cyber resilience
5	**Resilience plans**	P7 – Resilience plans EL7 – Ecosystem-wide cyber-resilience plans
6	**Review of organizational and board performance**	P9 – Review P10 – Effectiveness
7	**Community collaboration and interdependence**	P8 – Community EL6 – Ecosystem-wide collaboration

Cyber-resilience dashboard

The following image depicts an illustrative example of how a high-level dashboard can be created by a cyber-resilience officer to present and communicate cyber-resilience key messages and actions to the board of directors.

The board of directors must support systemic cyber resilience by establishing a secure business foundation enabled by the latest technology advancements, skilled people and efficient processes. Hence, the illustrative dashboard in this example contains three simple indicators to show the state of cyber-resilience security across those three domains (people, process and technology) aligned with the seven implementation categories:

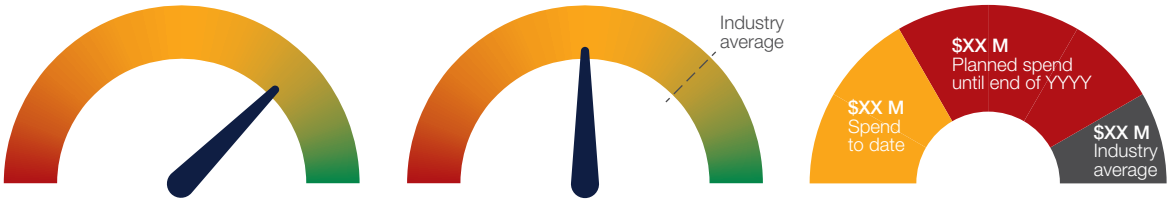
- The “security culture” indicator represents the status of cyber resilience in terms of people, i.e. the organization’s employees’ cybersecurity awareness and skills.
- The “critical asset security” indicator shows the cyber-resilience status of the technology landscape across the company and its overarching ecosystem.
- The “security roadmap spend” indicator illustrates the cyber-resilience “processes” status, in terms of progress on overall strategic and tactical cyber-resilience roadmap spend, plans and objectives/ milestones met accordingly. (The “industry target” is calculated based on the organization’s revenue, using the following baseline: IT Investment = x% of revenue, security investment = x% of IT investment.)

Sample cyber-resilience officer executive dashboard
High level state of cyber resilience

Indicators show the state of cyber-resilience security across people, process and technology domains within the company

Indicators show the cyber state of key asses and industry comparison

Indicators show how cybersecurity roadmap and objectives are being executed



SECURITY CULTURE
80% of employees pass on phishing test

CRITICAL ASSET SECURITY
External audit reports that 45% of critical assets have critical or high vulnerabilities

SECURITY ROADMAP SPEND
Review of budget allocation for security roadmap execution urgently required

The list under each indicator shows key actions and related latest progress/results

Security culture ▲	Critical asset security ▶	Security roadmap ▼
Employee security awareness training completed – 65% pass (down 5%) 🟡	Average response time for critical incidents improved by 10% this quarter 🟢	Only 60% of planned resources available to execute cyber-resilience roadmap (actual vs. plan) 🔴
80% phishing tests correctly detected – improvement of 20% 🟢	Two critical systems fail over mechanisms that did not function within failover time limit during testing 🔴	Network segregation implementation and testing two months behind target 🔴
Security design review process has led to 20% improvement in penetration testing results 🟢	No critical asset visibility from Shodan scan 🟢	Disaster Recovery Plan Phase 2 completed 🟢
Weekly security briefings started for all IT/OT security personnel 🟢	90% penetration test coverage – shows 10 critical vulnerabilities (reduction of 15%) 🟡	Risk analysis completed on 75% of critical assets (on target to complete next quarter) 🟢

Implementation categories covered:

2. Organizational governance
4. Systemic cyber resilience
5. Resilience plans
6. Review of organization and board performance
7. Community collaboration and interdependence

Implementation categories covered:

3. Risk management
4. Systemic cyber resilience
5. Resilience plans

Implementation categories covered:

1. Oversight of enterprise cyber risk and resilience
2. Organizational governance
3. Risk management
4. Systemic cyber resilience
5. Resilience plans
6. Review of organization and board performance
7. Community collaboration and interdependence

Contributors

Lead authors

Filipe Beato	Project Lead of Cybersecurity Industry Solutions, Centre for Cybersecurity, World Economic Forum
Daniel Dobrygowski	Head of Corporate Governance and Trust, Centre for Cybersecurity, World Economic Forum
Allan Haughton	Associate Director, Accenture
Pablo Andres Vaquero	Senior Manager, Accenture

Working group co-chairs

Pierre-Alain Graf	Senior Vice-President, Global Security, ABB
Rosa Kariger	Global Chief Information Security Officer, Iberdrola

Advisory team

Louise Anderson	Community Lead, Electricity Industry, World Economic Forum
Georges De Moura	Head of Industry Solutions, Centre for Cybersecurity, World Economic Forum
Samuel Linares	Managing Director, Accenture
Kristen Panerali	Head of Electricity Industry, World Economic Forum
Floris van den Dool	Managing Director, Accenture

Working group

David Batz	Senior Director, Cyber and Infrastructure Security, Edison Electric Institute (EEI)
Christophe Blassiau	Senior Vice-President, Digital Security & Global Chief Information Security Officer, Schneider Electrics
Mario Bocchiola	Head of Operation Technology Cyber Security Engineering, Enel
Stefano Bracco	Knowledge Manager, Agency for the Cooperation of Energy Regulators
Andrea Brackett	Vice-President and Chief Information Security Officer, Tennessee Valley Authority
Felicia Brown	Chief Security Officer, Vice-President Physical and Cyber Security, Avangrid (Iberdrola)
Manny Cancel	Senior Vice-President and Chief Executive Officer of E-ISAC, North American Electric Reliability Corp
Kenneth Carnes	Vice-President and Chief Information Security Officer, New York Power Authority
Dexter Casey	Chief Information Security Officer, Centrica
Francesco Ciancarelli	Head of Cyber Security Standards and External Stakeholders, Enel
Tim Conway	Director of SCADA and ICS, Sans Institute
Lynn Costantini	Deputy Director Center for Partnerships and Innovation, National Association of Regulatory Utility Commissioners
Ivan Dragnev	Cyber Security Principal Technical Lead Europe, Electric Power Research Institute
Ashtad Engineer	Vice-President of Technology and Digitization, Adani Group
Hala Furst	Director of Cybersecurity and Innovation, US Department of Homeland Security, USA
Aniello Gentile	Cyber Security Manager, Enel
Agustin Valencia Gil-Ortega	Head of OT Cybersecurity, Iberdrola
Guido Gluschke	Director, Institute for Security and Safety (ISS)
Juha Harkonen	Vice-President Security, Fortum Corporation, Finland, Fortum Corporation
Harshul Joshi	Cybersecurity Partner, PwC
Kai Hermsen	Global Coordinator for the Charter of Trust, Siemens

Michaela Kollau	Policy Officer, DG Energy, European Commission
Martin Knudsen	Lead Information Security Officer, Ørsted
Paulo Moniz	Director, Information Security and IT Risk, EDP
Scott Pinkerton	Cyber Security Programme Manager, Argonne National Laboratory
Philip Quade	Chief Information Security Officer, Fortinet
Johan Rambi	Faculty Instructor, Saxion University of Applied Sciences
Yuri Rassega	Chief Information Security Officer, Enel
Jesus Sanchez	Head of Global Cybersecurity, Naturgy
Eric Singer	Chief Information Security Officer, EMEA, Schneider Electrics
Leo Simonovich	Vice-President and Global Head, Industrial Cyber and Digital Security, Siemens
Cole Sinkford	Chief Information Security Officer, GE Renewable Energy
Vlada Spasic	Senior Advisor, SV Energy
Candace Suh-Lee	Principal Technical Leader – Cyber Security, EPRI (Electric Power Research Institute)
Eric Trapp	Chief Security Officer, Sempra Energy
Maximilian Urban	Information Security Officer and Innovation Manager, Netz Niederösterreich
Alain Vallieres	Cyber Security Manager, Hydro Quebec
Olivier Vandelaer	Director Industrial Cybersecurity, ENGIE Laborelec
Matt Wakefield	Director of Information, Communication and Cyber Security, Electric Power Research Institute
Swantje Westpfahl	Institute for Security and Safety (ISS), Co-Director
Thomas Wilson	Senior Vice-President and Chief Information Security Officer, Southern Company
Brecht Wyseur	Product Manager, IoT Security, Kudelski Group
Mohammed Zumla	Head of Cyber Security and Resilience, NIS Competent Authority, Office of Gas and Electricity Markets (Ofgem)

The Forum also wishes to acknowledge contributions from Rebekah Lewis (Project Lead, Centre for Cybersecurity, World Economic Forum) and Sergio Platon Martinez (Project Collaborator, World Economic Forum, seconded from Iberdrola), plus Marco Molinaro, Gib Sorebo, Bart de Jong and Anshu Sharma from Accenture.

Endnotes

1. World Economic Forum, *COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications*, 2020, p. 43.
2. World Economic Forum, *Advancing Cyber Resilience Principles and Tools for Boards*, 2017; World Economic Forum, *Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards*, 2019.
3. World Economic Forum, *Advancing Cyber Resilience Principles and Tools for Boards*.
4. UC Berkeley Center for Long-Term Cybersecurity, *Resilient Governance for Boards of Directors: Considerations for Effective Oversight of Cyber Risk*, 2020, p. 5: https://cltc.berkeley.edu/wp-content/uploads/2020/01/Resilient-Governance-for-Boards-of-Directors-Report.pdf (link as of 26 May 2020).
5. National Association of Corporate Directors and Internet Security Alliance, *Cyber-Risk Oversight 2020: Key Principles and Practical Guidance for Corporate Boards*, 2020, p. 20.
6. For more guidance on risk appetite, there are several sources available for boards, e.g. PwC Governance Insight Center, *Board Oversight of Risk: Defining Risk Appetite in Plain English,* 2014: https://www.pwc.com/us/en/governance-insights-center/publications/assets/pwc-risk-appetite-management.pdf (link as of 26 May 2020).
7. For more detail on the board's relation to the most important corporate assets, see National Association of Corporate Directors and Internet Security Alliance, *Cyber-Risk Oversight 2020*, "Identifying the Company's 'Crown Jewels'", p. 13.
8. National Association of Corporate Directors and Internet Security Alliance, Cyber-Risk Oversight 2020, p. 22
9. Ibid., p 14.
10. World Economic Forum, *Cyber Resilience in the Electricity Ecosystem*, p. 6.
11. National Association of Corporate Directors and Internet Security Alliance, *Cyber-Risk Oversight 2020*, p. 41.
12. Owaida, Amer, *European Power Grid Organization Hit by Cyberattack,* WeLiveSecurity, 12 March 2020: https://www.welivesecurity.com/2020/03/12/european-power-grid-organization-entsoe-cyberattack/ (link as of 26 May 2020).
13. Gatlan, Sergiu, *RagnarLocker Ransomware Hits EDP Energy Giant, Asks for €10m*, Bleepingcomputer, 14 April 2020: https://www.bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m/ (link as of 26 May 2020).
14. Coyne, Brendan, *Elexon Hit By Cyber Attack*, The Energyst, 14 May 2020: https://theenergyst.com/elexon-hit-by-cyber-attack/ (link as of 26 May 2020).
15. European Commission, *Commission Recommendation of 3.4.2019 on Cybersecurity in the Energy Sector*, 2019: https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf (link as of 26 May 2020).
16. National Association of Corporate Directors and Internet Security Alliance, Cyber-Risk Oversight 2020, p. 6.
17. World Economic Forum, *Cyber Resilience in the Electricity Ecosystem*, p. 6.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744

contact@weforum.org
www.weforum.org