WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Centre for Cybersecurity and Electricity Industry Community

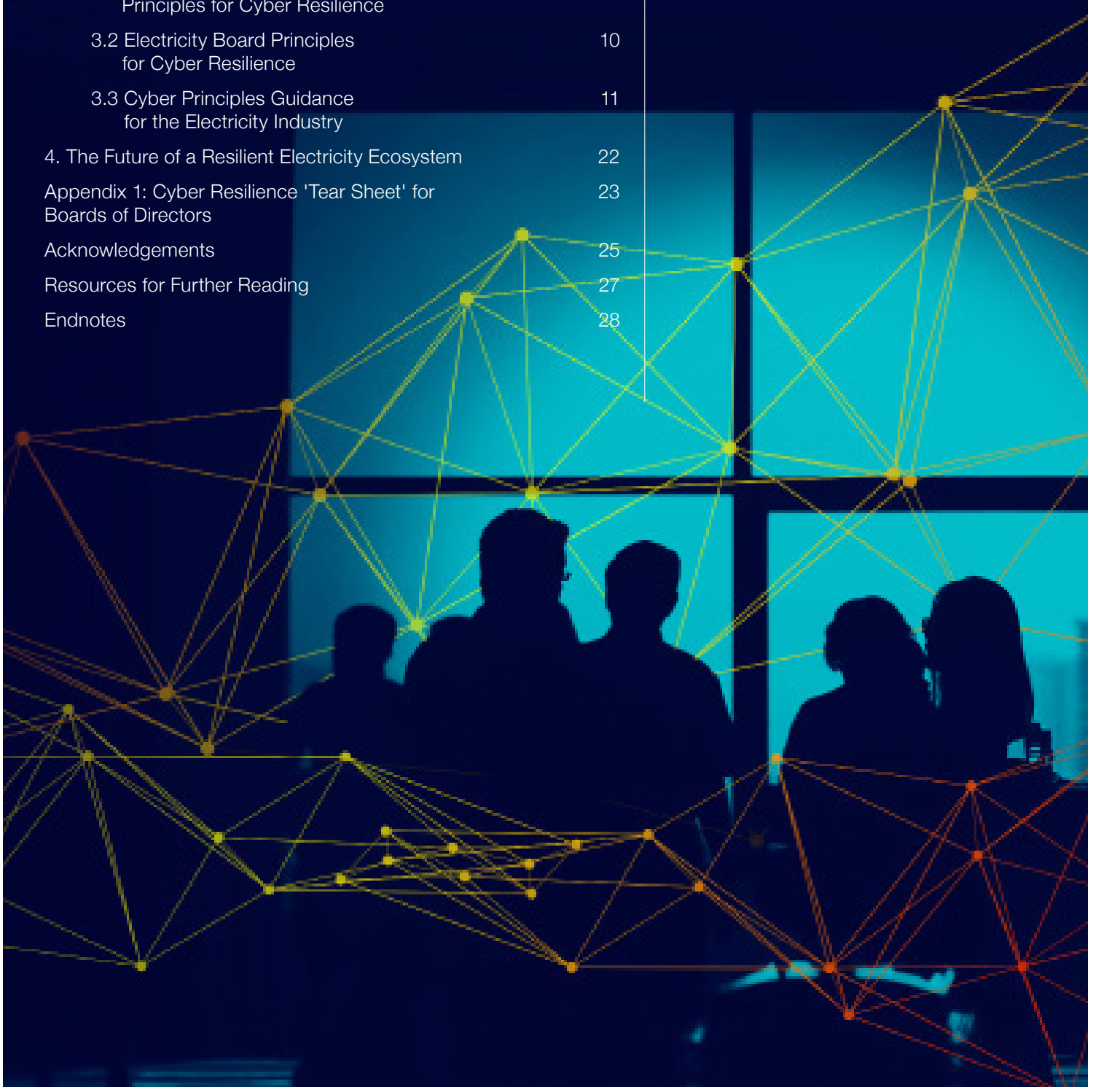
Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards

In collaboration with Boston Consulting Group

January 2019

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

Contents



Preface

Digitalization is driving growth and innovation in the electricity industry and has tremendous potential to deliver shareholder, customer and environmental value. New technologies and business models affecting our operating assets present both opportunities and risk.

As business leaders overseeing the construction, procurement and operations of critical electricity infrastructure, we are well versed in planning for, minimizing and managing risk. This includes cyber risk, which is ubiquitous in our organizations and in the ecosystem in which we operate.

Responsibility for managing this risk starts with the leaders. We, as board members and chief executives, must take it upon ourselves to build a robust and pervasive cyber resilience culture and ensure it is instilled in every person within our organizations, from top to bottom. In addition, cyber risk should be centrally managed similar to other risks; however, it is often delegated to our information technology teams. A key aim of this report is to highlight the need for this to evolve.

While we each have a role and responsibility in managing the cyber risks affecting our organizations, we must realize that individual efforts are not sufficient. In our connected ecosystem, a cyber attack on one can cascade and affect many. As a result, we must collaborate with one another, across the public and private sectors, to develop, adopt and share best practices to ensure collective cyber resilience.

The importance of a cyber resilience culture and of leadership responsibility in managing organizational cyber risk has been well set out in the World Economic Forum's 2017 publication, *Advancing Cyber Resilience: Principles and Tools for Boards*. For the electricity industry, we recognized that more specific guidance is required to help board members meet the unique challenges of managing cyber risk for companies that operate in such an interconnected environment and form such a vital part of critical infrastructure.

Therefore, together we have augmented the original ten principles with seven electricity industry-specific cyber resilience principles. These principles, supported by implementation guidance and case studies from industry leaders, aim to enable boards of directors in advancing ecosystem-wide cyber resilience.

I look forward to implementing these principles and encourage every chief executive and board member to do the same.

Eric Martel

Chief Executive Officer
Hydro-Québec

"Only by joining efforts will we be able to face the cybersecurity challenges introduced by increasing digitization and hyper connectivity. To that end, the World Economic Forum has provided a unique platform and has brought together relevant industry experts who contributed with valuable input to create this guide that will support Boards and senior management in collaboratively approaching cyber resilience in the complex electricity ecosystem."

- Rosa Kariger, Global CISO, Ibderdrola S.A.
Co-chair of the Systems of Cyber Resilience: Electricity working group

"Power systems play a key role in society. Protecting power supply to society against all threats is ensuring a society's prosperity. Joining forces across company borders is an important remedy against fast-evolving cyber threats in the energy sector. It was an honour to co-chair this unique collaboration initiative at the World Economic Forum."

- Pierre-Alain Graf, Senior Vice President, ABB
Co-chair of the Systems of Cyber Resilience: Electricity working group

1. Introduction

Cyber risk is business risk.

In the electricity industry, cyber risk is also an ecosystem-wide risk.

Cyber resilience is a challenge for all organizations, but it is of particular importance for the electricity ecosystem. A large-scale blackout would have socioeconomic ramifications for households, businesses and vital institutions.[1] For example, a six-hour winter black-out in mainland France could result in damages totalling over €1.5 billion ($.1.7 billion).[2] Traditionally, managing this risk has meant dealing with issues such as component failure or inclement weather via robust mitigation and recovery plans. Today, however, existing resilience plans in electricity delivery must integrate a carefully designed cyber resilience strategy.[3]

Three themes have served as the foundation for the World Economic Forum's approach to the topic of cyber resilience in the electricity industry:

Interdependent ecosystem

The electricity ecosystem has always been complex and heavily interconnected. Organizations, large and small, within this environment rely on one another for business-critical components and services and collaborate to manage the risks that this interdependence brings. However, the introduction of digital technologies has amplified the level of interconnectivity and introduced an additional dimension of risk that all organizations within the ecosystem need to manage together – cyber risk. Increased power network connectivity, the convergence of operational technology (OT) and information technology (IT), the proliferation of internet of things (IoT) devices and the digitization of business models are expanding the cyber attack surface for malicious actors to exploit.[4] Simultaneously, legacy infrastructure with a lifespan of over 20 years needs to continue to be managed.

Additionally, with increasingly decentralized grids come more small-scale generators. Cyber attacks on these small-scale generators can affect society just as significantly as compromises to larger entities. Organizations in the electricity ecosystem need to come together to devise effective collective cyber resilience strategies and to integrate these strategies into existing electricity resilience efforts.

Siloed approach to cyber resilience

Because it is a newer fixture on the business landscape and therefore difficult to quantify the risk and return on investment, cybersecurity ramifications are not often considered as systematically as other risks. This mindset induces a culture where responsibility for cyber risk is often solely given to the IT department. In the electricity industry, where there is a real-time requirement for energy delivery, cyber resilience can no longer be managed in isolation and thought of as a "bolt-on" solution. It needs to be integrated with business risk and owned by all parts of the organization and ecosystem.

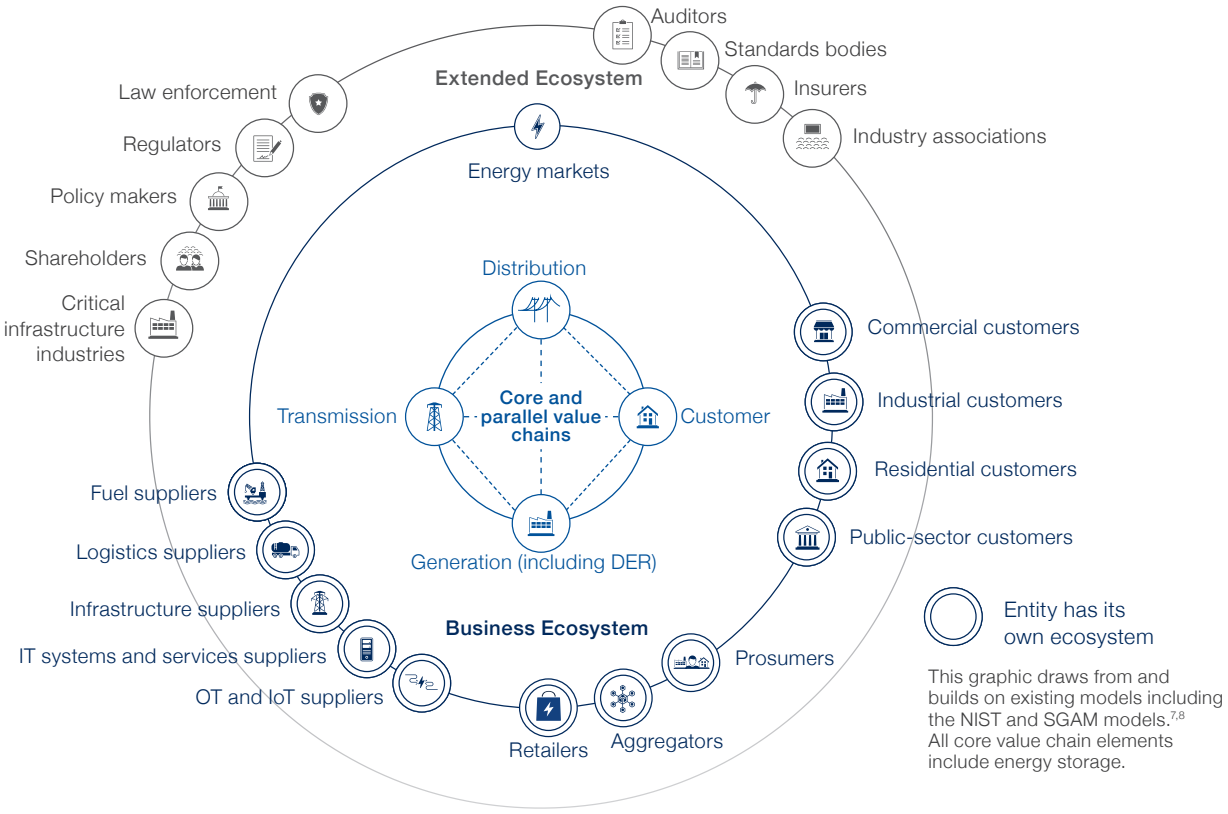
Culture of compliance

Public-sector bodies have attempted to improve the cybersecurity capabilities of all electricity organizations by instituting regulations (e.g. NIS[5],NERC CIP[6]). These regulations have offered requirements for foundational security, but being compliant does not necessarily mean being secure. Moreover, with the rapid digitization of the electricity ecosystem, it may not be reasonable to expect regulation to keep pace with the newest cyber risks. As a result, these organizations need to adopt a "resilience mindset" and take a strategic approach to managing cyber risks.

Based on these themes, this report provides recommendations to electricity industry boards of directors to advance cyber resilience within their organizations and across the broader industry.

Electricity ecosystem

Knowing what needs to be protected is the first step in addressing the cyber resilience challenges of operating in such a complex and interdependent universe.



This graphic draws from and builds on existing models including the NIST and SGAM models.[7,8] All core value chain elements include energy storage.

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).

A mapping of stakeholders starts with the core value chain (i.e. the connected infrastructure) and expands to include the surrounding "business ecosystem" of suppliers, customers and peers. This is then encapsulated by an "extended ecosystem", including policy-makers, regulators, law enforcement, auditors, insurers and standards bodies. In order to ensure that cybersecurity and resilience are effectively included in business strategy, leaders must understand the breadth and nature of these connections. Interactions between stakeholders in this environment are manifested via physical connections, network links and strategic relationships.

The physical layer is often well understood and includes all physical connections between entities, such as the transmission and distribution lines connecting generation to demand.

The network layer includes all computer systems that interact with each other. The complexity of this layer, and its interdependencies, continues to increase with the digitalization of the grid. This layer can be used as a highway to propagate cyber attacks that have cascading effects across the ecosystem.

The strategic layer refers to relationships with entities in the business and "extended ecosystem" (e.g. policy-makers, regulators). These relationships are especially critical as the number of nation state level cyber threats against electricity organizations and the grid grow.[9,10,11] Whether it is working with regulators to develop smart and agile cyber regulation with the appropriate incentives or sharing cyber threat information with law enforcement, every electricity industry organization needs to consider the logic of its cooperation with those in the broader ecosystem.

As a result, when it comes to cyber (and physical) security, it is no longer enough for an electricity organization to secure its own "house". Leaders must realize that their organizations are part of a larger "neighbourhood" where cooperation on cyber resilience is essential between the members of that neighbourhood, ranging from oversight bodies to suppliers, customers and employees.

How do we secure this complex ecosystem?

Advancing systemic cyber resilience in this complex environment requires boards of directors to develop a sense of responsibility for, and maintain oversight of, both organizational and ecosystem-wide cyber risks.

In 2017, to help facilitate board oversight and action in support of organizational cyber resilience, the World Economic Forum, in collaboration with more than 30 leading academics, thinkers and senior executives, developed a set of 10 overarching principles for organizational cyber governance.[12] These principles are meant to enable board action in making cyber resilience a component of overall organizational strategy.

Electricity organizations must go even further. They also need to think about cyber resilience as a component of ecosystem-wide strategy. 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."[13]

The principles and guidance included in this document augment the 2017 general principles by offering additional strategies that go beyond organizational cyber resilience and aid the board in advancing ecosystem-wide cyber resilience. These principles can be prioritized and implemented according to organizational cyber maturity.

Cyber resilient electricity industry

General principles for cyber resilience

- Responsibility for cyber resilience
- Command of the subject
- Accountable officer
- Integration of cyber resilience
- Risk appetite
- Risk assessment and reporting
- Resilience plans
- Community
- Review
- Effectiveness

Industry-specific principles for cyber resilience

- Cyber resilience governance
- Resilience by design
- Going beyond compliance
- Systemic risk assessment and prioritization
- Corporate responsibility for cyber resilience
- Ecosystem-wide collaboration
- Ecosystem-wide cyber resilience plans

2. How this Report is Structured

This report contains three sections to help guide board action with regard to cyber resilience in the electricity industry:

1. Restatement of General Board Principles for Cyber Resilience

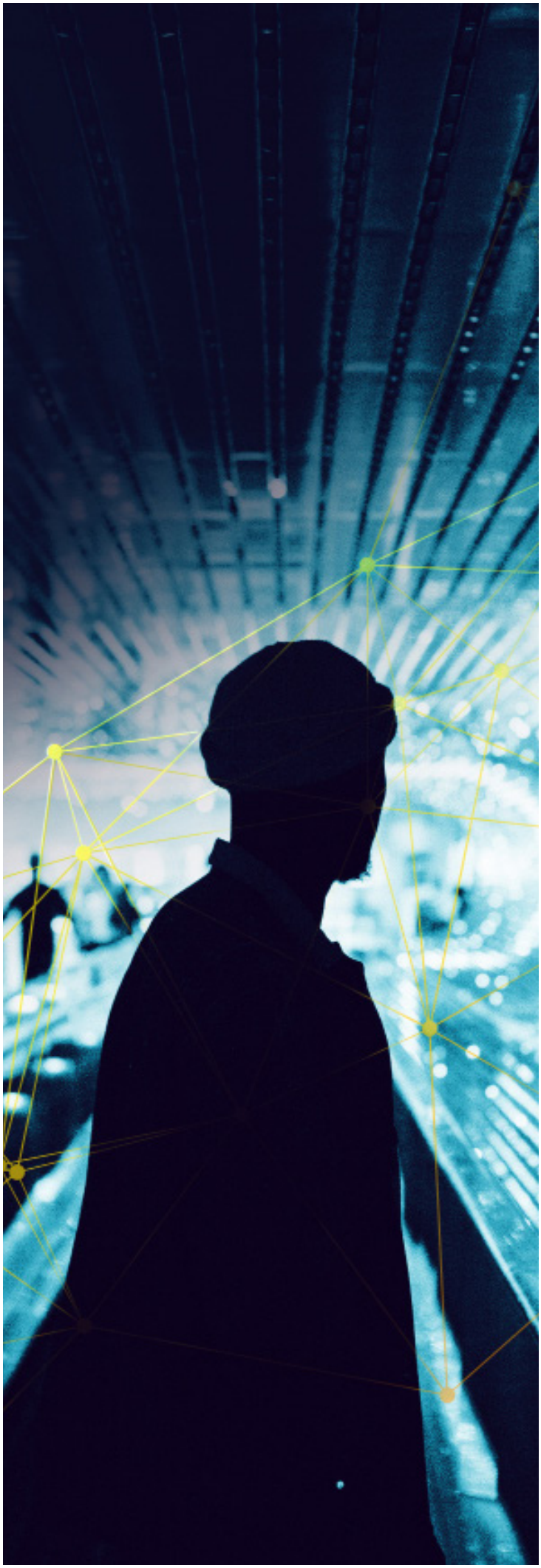
   This section recaps the original 10 general cyber resilience principles published by the Forum. The general principles are relevant and applicable to all electricity organizations.

2. Electricity Board Principles for Cyber Resilience

   Stakeholders have identified a clear need to build upon the original general principles and create electricity industry-specific cyber resilience principles for boards. By evaluating the vital cyber resilience challenges for the electricity industry, seven additional principles are put forth to enable board action in advancing systemic cyber resilience.

3. Cyber Principles Guidance for the Electricity Industry

   Each of the electricity principles is accompanied by guidance to enable board action. For boards, action means first asking the right questions. Therefore, this section provides a questionnaire to facilitate structured dialogue on the industry-specific cyber resilience principles between the board and senior management.



3. Cyber Resilience Principles and Guidance for the Electricity Industry

3.1 Restatement of General Board Principles for Cyber Resilience

We recap the original 10 cyber resilience principles published by the Forum as a precursor to offering principles specific to the electricity industry:

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 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 in the implementation of these principles or seeks independent advice for continuous improvement.

For the detailed guidance associated with these principles, please refer to the Forum's Advancing Cyber Resilience: Principles and Tools for Boards.

3.2 Electricity Board Principles for Cyber Resilience

In addition to the general principles, boards in the electricity industry should adopt seven industry-specific principles to advance systemic 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

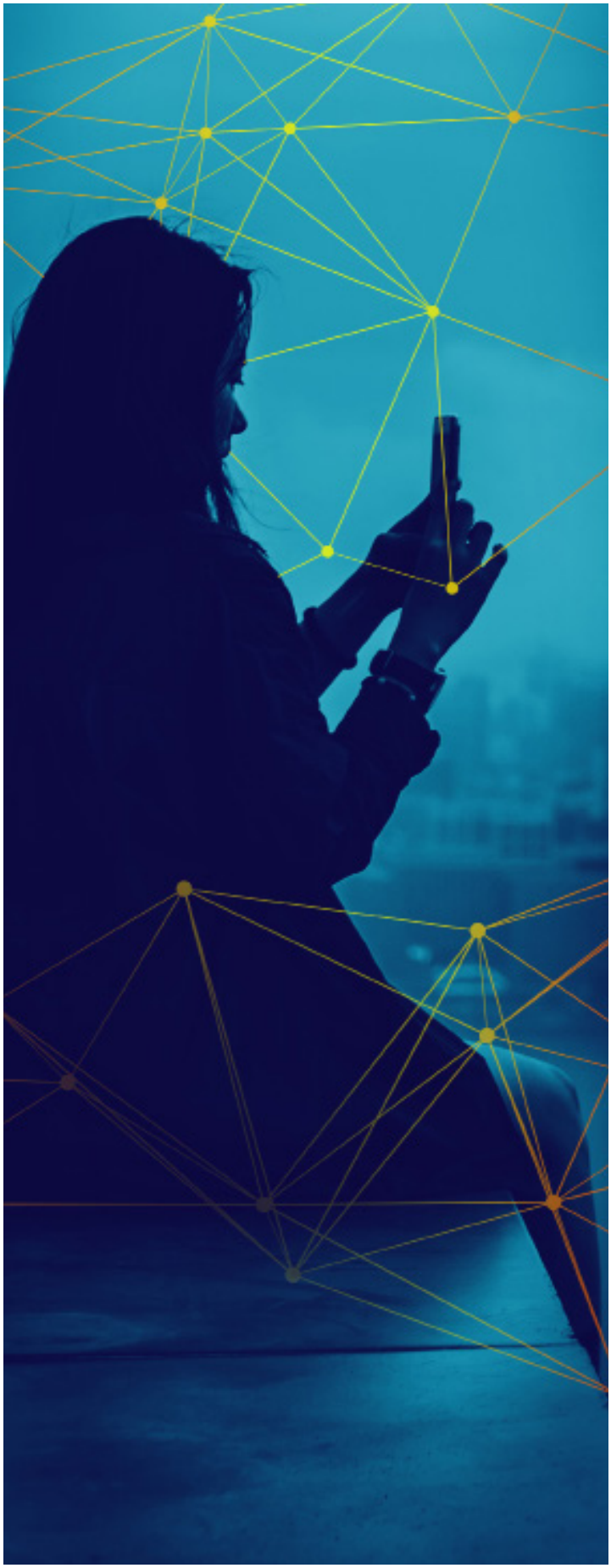
The board empowers management to create a culture of collaboration, set strategic objectives around information sharing and understand and mitigate cyber risks in the ecosystem. The board also actively collaborates with industry peers and policy-makers.

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.

3.3 Cyber Principles Guidance for the Electricity Industry

Each of the board principles is accompanied by a set of questions to enable self-assessment by board members within the electricity industry. The aim of this guidance is to allow board members to better understand how to implement these principles and exercise their oversight responsibilities.



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.

For electricity organizations, cyber resilience is not solely an IT issue. It is a business issue that affects all aspects of the organization and ecosystem. Thus, cyber resilience governance should break down the barriers between IT, OT and physical security groups, facilitate the development of cyber skills and capabilities and institute an appropriate structure to ensure a coordinated cyber resilience strategy and priorities across the organization.

Questions for the board

1. Have clear roles and responsibilities for cyber resilience been established and adhered to across IT, OT and physical security functions?
2. How does the governance model create a collaborative relationship on security between IT, OT and physical security functions? Are effective mechanisms in place for this?
3. How does the governance model enable the development of cyber skills and capabilities for IT and OT personnel? Are effective mechanisms in place for this?
4. To what extent are IT and OT functions structurally integrated? What process led to that level of integration?
5. To what extent are cybersecurity and physical security integrated? What process led to that level of integration?
6. How frequently is the cyber resilience governance model reviewed? How is alignment with the evolving ecosystem and associated cyber risks ensured?

Bridging the gap between IT and OT security

Cyber attacks in the electricity industry are no longer constrained to the digital world. There have been multiple incidents where cyber attacks have crossed the bridge from the digital world to the physical domain. One example is the 2016 BlackEnergy Trojan that disrupted Ukraine's electricity supply.[14] Another example is the Triton malware that aimed to disable the industrial safety systems at a power plant in the Middle East.[15] These events highlight the need for extending robust cyber resilience governance from the IT world into the OT environment. However, instituting effective security governance that integrates IT and OT is easier said than done.[16]

IT and OT environments are foundationally and functionally different: different priorities within a business; different functional requirements; different working cultures; different risk appetites. As a result, they also often have different security requirements. Perhaps the most fundamental difference is that IT security focuses on confidentiality while OT usually prioritizes integrity and availability. The potential societal consequences require a grid asset operator's priority to be ensuring the safe and reliable delivery of electricity. This responsibility leads to other differences across areas, from component lifetimes and patching practices to audit timelines and additional functions.

The security challenges created by differences in priorities are often exacerbated by a communication barrier between IT and OT groups. Additionally, they may have different reporting and governance structures. This lack of coordination and communication is especially risky in times of emergency where the organization needs to respond to, or recover from, a cyber incident.

Information Technology	Characteristic	Operational Technology
Integrity, **Confidentiality**, Availability	Security objective priorities	**Integrity**, **Availability**, Confidentiality
Medium, delays accepted	Availability requirement	Very high
Delays accepted	Real-time requirement	Critical
3–5 years	Component lifetime	Up to and over 20 years
Regular / scheduled	Application of patches	Slow / infrequent
Scheduled and mandated	Security testing/audit	Occasional
High / mature	Security awareness	Increasing

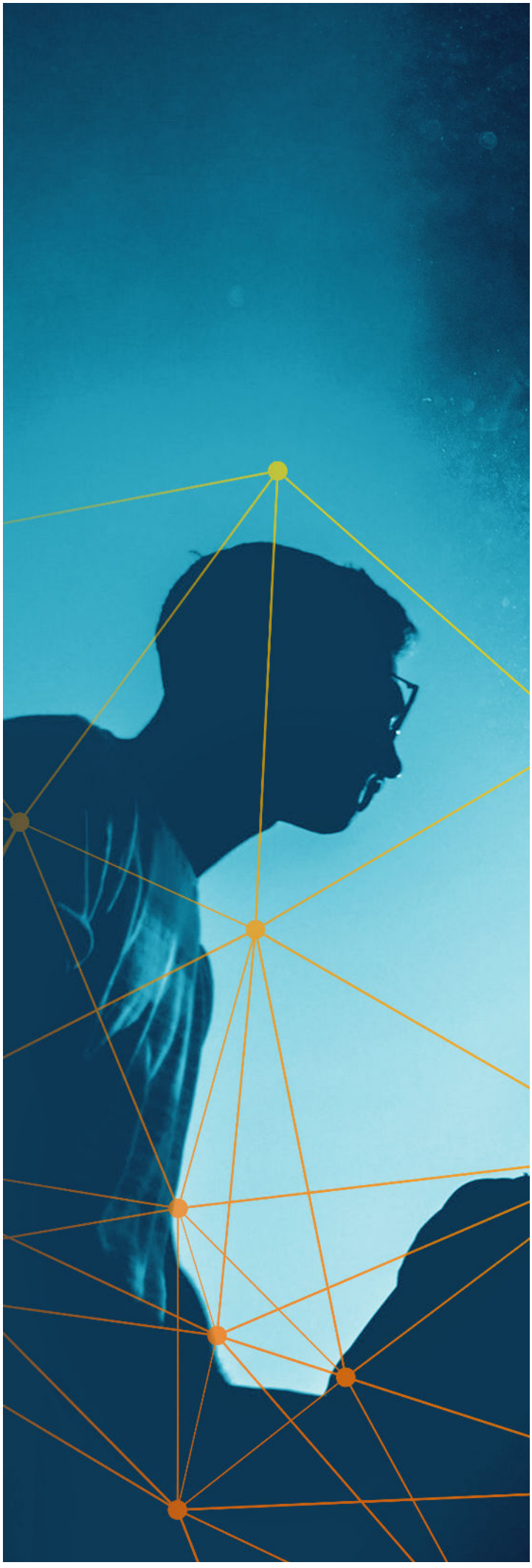
Source: Boston Consulting Group

Case study from ENEL: An example of what can be done

The era of digitization and technological innovation means that organizations are exposed to cyberattacks that are increasingly frequent and sophisticated. The organizational complexity of the Enel Group and the numerous environments it encompasses (data, people and the industrial world) expose the organization's assets to a wide range of cyber- attacks. To address this, the Enel Group has adopted a cyber risk management model based on a "systemic" vision that integrates the traditional information technology sector, the operational technology field most closely linked to the industrial sector and IoT associated with the networking of smart objects.

In particular, Enel has adopted a "Cyber Security Framework," a policy issued by the CEO, defining all processes in order to guide and manage cybersecurity activities. This framework facilitates deep involvement from all business areas, the implementation of regulatory and legal requirements, the use of best-available technologies and an informed workforce. Furthermore, cybersecurity decisions and activities are based on business priorities, and security measures are embedded throughout the design and development lifecycle of applications, processes and services. This model is supported by a global and holistic organizational structure that drives activities and projects based on a risk-based approach in order to balance the benefits of increasingly digital IT/OT/IoT systems with the potential cyber risk and associated business impact.

However, Enel Group has not stopped there. In 2017, Enel Group established a new Cyber Security Risk Management Methodology, applicable to all IT, OT and IoT environments and has created its own active Cyber Emergency Readiness Team (CERT), which is recognized and accredited by national and international communities, in order to direct an industrialized response to cyber threats and incidents.



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.

A security by design/resilience by design culture is one where cybersecurity is embedded in all business processes from the outset and kept top of mind at all times.[17] As numerous electricity organizations begin their digital transformation journeys, it is critical that they also adopt a mindset that puts cyber resilience front and centre. Whether it is designing or integrating a product, instituting a business process or entering into a partnership with another ecosystem organization, cyber risks and implications should be proactively considered, monitored and appropriately managed. This will enable organizations to take advantage of the business efficiencies that digitalization offers while controlling the associated cyber risk.

Questions for the board

1. Are cyber risks and associated implications evaluated, embedded and appropriately managed in all aspects of the business?
2. Are cyber risk and associated risk management activities discussed and planned for when starting a new initiative?
3. Does management ensure that appropriate technical controls (e.g. limited access controls, segmentation and defence in depth) are in place and properly implemented?
4. How does management communicate the cyber risks, the importance of organization and ecosystem-wide cyber resilience, and the relevant cyber risk management policies to all personnel?
5. Are all personnel aware of how cyber resilience impacts their role within the organization? Is there cross-functional and cross-departmental ownership for cyber risk management?
6. What mechanisms are in place to train personnel on cyber resilience and raise awareness about the need to embed cyber resilience in all aspects of the organization?
7. How is the effectiveness of these mechanisms monitored and measured?

Case study from Adani Group: End-to-end approach to cyber resilience

In India, Adani Group faces similar challenges to numerous others in this environment:
- Need for security resources and expertise
- Need to expand investments beyond just prevention
- Need to maintain compliance with cyber laws

To address these challenges, Adani has implemented a cyber strategy consisting of six pillars. This solution delivers a 24/7 and end-to-end focus on cyber resilience. Moreover, it encourages a security-focused culture throughout the organization.

Organization strategy, alignment and governance

- Security blueprint and roadmap (IT/OT)
- Technical advisory board for cybersecurity
- Managed services approach - based on business outcome

Systems and architecture principles designed for safety

- Common design basis for security tech platforms (IT/OT)
- Common security design principles at group level
- Business unit specific framework (IT/OT)

Cybersecurity by design (procedures, policies, tools)

- Design and engineer
- Procure, contract and commission
- Operate and maintain

adani

Threat hunting via big data enabled analytics and KPIs

- Reports, metrics and change management
- Real-time graphical visualization of attacks and blocks
- Behaviour analytics (user, network)

Enterprise risk and cyber compliance management

- Continuous risk posture assessment
- Proactive risk mitigation
- Part of Adani group level risk governance framework

Simulated training and education for response to threats

- Cybersecurity awareness and training across all org levels
- Adversary attack simulation
- Threat response and breach-readiness training

Case study from Schneider Electric: Cybersecurity by design strategy

Leading the digital transformation of energy management and automation, Schneider Electric regards cybersecurity as central to its business strategy – especially at the convergence of OT and IT, where digital threats can affect people, processes and technology across an expanded digital environment. Within its holistic digital risk strategy, Schneider has adopted an end-to-end cybersecurity approach aligned to the National Institute of Standards and Technology (NIST) framework.

In the digital landscape, there is no perimeter. Schneider regards cybersecurity as a continuous, always-on, proactive activity. It therefore advances a cybersecurity by design strategy as both a business process and a technology development principle.

Within the context of this strategy, Schneider:
- Mitigates security gaps by scrutinizing cyber risk using a register that prioritizes high-value assets/crown jewels.
- Integrates security at the beginning of product development within a secure development lifecycle process, implementing cybersecurity by design capabilities and digital locks to mitigate threats at every step.
- Leverages cyber partnerships to secure its factories and global supply chain.
- Secures IT/OT convergence with a 360° and 24/7 monitoring lens supported by a tested fast-response plan.
- Takes advantage of lessons learned from ongoing Reality Checks for faster and better emergency response and improved plans.
- Strengthens its cybersecurity posture by offering cybersecurity services to customers as part of protecting its end-to-end digital environment.

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.

Given the plethora of regulatory and compliance requirements in the electricity industry, cyber resilience efforts often take on a "check-the-box" mindset. However, the electricity ecosystem is a dynamic environment in which cyber threats often evolve faster than regulation. To effectively go beyond compliance, the cyber risk appetite should be aligned with strategic priorities, action plans to manage cyber risks should be aligned with this risk appetite, and initiatives should be appropriately resourced to complete these action plans.

Questions for the board

1. Are cybersecurity requirements assessed based on their bearing on organizational security rather than mere compliance?
2. Is the cyber risk appetite set in alignment with business risk appetite and then reviewed with regards to compliance requirements?
3. What organizational policies and strategies exist to ensure a holistic cyber risk management approach, combining both compliance requirements and strategic needs?
4. Does the board authorize adequate resources (both financial and personnel) to achieve the holistic cybersecurity risk management objectives?
5. Are these resources appropriately distributed across all business functions?

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.

Knowing what needs to be protected is the first step to advancing systemic cyber resilience. In this industry, where every network-connected device represents a potential entry or execution point for a cyber attack, both the organization's asset base and interdependence with ecosystem stakeholders needs to be assessed. However, the ecosystem needs to be mapped by prioritizing dependencies based on the business and cyber risk they pose. Prioritization will focus the discussion and enable best use of organizational resources when managing systemic cyber risk. This is especially critical when it comes to the supply chain. Risk assessments need to explicitly quantify supply chain cyber risk and evaluate whether the processes in place to manage such risks are robust. The Federal Energy Regulatory Commission, in the US, is focused on supply chain cyber risk and recently voted to require all utilities to map their supply chain and assess the associated cyber risk.[18]

Questions for the board

On understanding the ecosystem

1. At a high level, does management understand the links (physical, digital and strategic) with other ecosystem stakeholders?
2. Are changes to the ecosystem landscape monitored and updated at an appropriate frequency?

Case study from Iberdrola: Building a strong organizational cyber culture

In 2015, the Iberdrola S.A. board recognized that being at the forefront of digital transformation required strong cybersecurity and resilience capabilities. In this dynamic, increasingly complex and interconnected environment, ensuring compliance with all IT security, privacy and critical infrastructure protection regulations was not enough.

As a result, the board approved a company-wide cybersecurity risk policy to promote a strong cybersecurity culture and established a Global Cybersecurity Committee with the mandate to lead this cultural change. The goal was to promote cybersecurity and resilience by design and by default throughout the organization. Moreover, it aimed to embed the idea that cybersecurity is everyone's responsibility, and goes beyond individual organizations

How this was accomplished:

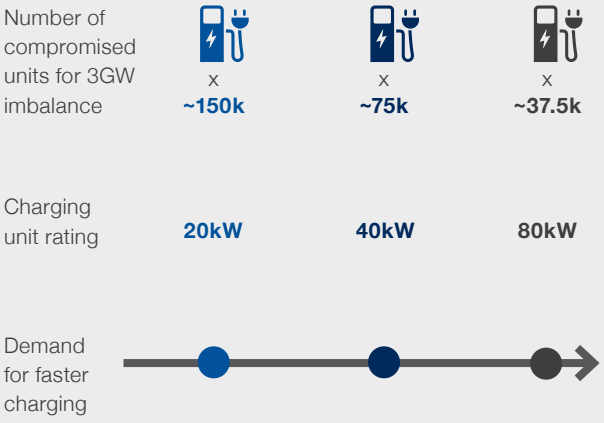
- A new cyber governance framework was approved where IT and Security no longer had sole responsibility for cybersecurity. It is now a responsibility of all businesses and corporate areas.
- The chief information security officers (CISOs) are responsible for ensuring overall coordination, independent oversight and adequate cyber training of their respective boards, senior management and all personnel.
- A common cyber risk methodology and global rules were defined to allow risk-based identification of action plans in all areas. Cybersecurity strategy and action plans for IT, OT and IoT environments are coordinated and supported with investments in technology, processes and people.
- An OT cybersecurity forum brings together Industrial control systems (ICS) and IT security experts across the company to exchange best practices, share results and coordinate initiatives.
- Leadership, including the Global CISO, emphasized collaboration. These collaborative partnerships with technology providers, other companies, industry experts and government agencies now provide threat intelligence for the company and contribute to the resilience of the ecosystem as a whole.

Cyber risks stemming from the demand side

According to the European Network for Transmission System Operators – Electricity (ENTSO-E), the continental European power system synchronized area has been designed to withstand a maximum power imbalance of 3 gigawatts (GW).[19] For other European synchronized areas, this risk threshold or tolerance is significantly less than 3GW. Without adequate countermeasures, the consequences of a 3GW power imbalance could be immense – including total system blackout.

A malicious cyber actor intent on causing maximum damage to the European electricity grid could aim for a cyber attack on critical IT/OT systems and infrastructure causing a greater than 3GW load imbalance. Conventional cyber risks (e.g. advanced persistent threats [APTs], phishing and manipulation of critical data) can be mitigated to some extent by transmission systems operators (TSOs) and distribution system operators (DSOs) deploying effective ISO/IEC 27002:2013-type controls. On the other hand, coordinated and simultaneous attacks against power demand or supply via consumer IoT devices are more difficult to control.

To illustrate, as the rating of electric vehicle charging units grows (many currently greater than 20kW) in line with increasing charging speed requirements, fewer charging units need to be manipulated in order to cause a 3GW imbalance. Thus, when assessing and prioritizing cyber risk in the electricity ecosystem, the potential impact of cyber attacks via consumer-facing and consumer-operated systems also needs to be considered.



On understanding the cyber risk posed by the ecosystem

1. Which ecosystem dependencies present the highest cyber risk to the organization? How is this evaluated?
2. What is the specific risk exposure that comes from these critical dependencies in the ecosystem? Does this include reputational risk?
3. Are changes to critical dependencies (who they are, risk exposure etc.) monitored and updated at an appropriate frequency?

On managing the cyber risk posed by the ecosystem

1. How is cyber risk management integrated into the procurement process?
2. How are the ongoing cybersecurity responsibilities of suppliers, especially critical suppliers, defined and monitored?
3. How prepared is the organization to rapidly replace critical suppliers if one becomes compromised?
4. How does the organization securely integrate significant purchases (e.g. mergers and acquisitions)?
5. How does management prepare for the potential cascading impact that a cyber attack on another ecosystem stakeholder can have on the organization?

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.

As highlighted when describing the ecosystem, organizations in the electricity industry have interdependent relationships. Interdependence means bidirectional relationships. Principle EI4 stressed the need to understand, evaluate and monitor the cyber risk posed by the ecosystem, but, to contribute to systemic cyber resilience (i.e. the resilience of the "neighbourhood"), the cyber risk posed to the ecosystem may need to be considered as well.

Questions for the board

1. Does management consider the cyber related risks that the organization is introducing to the ecosystem?
2. Is the potential impact of these risks to ecosystem stakeholders and the corresponding reputational risk for the organization, understood?
3. Does management consider the potential cascading impact of a cyber attack on the organization to other ecosystem stakeholders?
4. If deemed relevant, how does the organization plan to communicate a potential cyber risk introduced to the ecosystem with relevant parties?
5. What is expected by ecosystem entities in the management of these cyber risks?

Case study from Hydro-Québec: Essential partnerships in critical infrastructure resilience

The global energy transition is in full swing, and Hydro-Québec is a key player in this rapidly changing environment. The vision for Hydro-Québec 4.0 is based on three major priorities: greater customer empowerment, asset digitization and a grid of the future. Achieving this vision also requires a comprehensive cyber resilience strategy, with a particular focus on defence in depth and public-private partnerships.

The government of Canada has developed a National Cyber Security Strategy that empowers both government and private sector partners to meet their goals, even as technologies and cyber threats evolve. The Strategy identifies the leadership role of the government and conveys the importance of strengthening collaboration, particularly through the establishment of services such as the Canadian Centre for Cyber Security (Centre) and the National Cybercrime Coordination Unit within the Royal Canadian Mounted Police.

As an operator of critical infrastructure, Hydro-Québec actively partners with these entities, working specifically with the Centre specifically on a daily basis to improve both organizational cybersecurity and the holistic security of the power grid. For example, there have been several situations where the timely receipt of threat information allowed Hydro-Québec to proactively improve security posture before actual cyberattacks.

Beyond partnership with the government, Hydro-Québec is also an active participant in the Electricity Information Sharing and Analysis Center (E-ISAC).[21] The E-ISAC provides a forum for the organization to share information on cyber issues affecting the industry and best practices for managing these issues with a network of peers.

Partnerships on cyber resilience are essential in protecting Canada's critical infrastructure and provide advantages to all parties.

Participation vs. Subscription

Information sharing in the electricity ecosystem needs to go beyond subscription to information feeds. Leaders, including board members, need to promote collaboration across all levels of the organization and actively participate in information sharing initiatives to ensure that actions are taken to secure the environment against current and future cyber threats.[22]

Principle EI6: Ecosystem-wide collaboration

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

General Principle 8[20] encourages boards to facilitate collaboration in order to achieve systemic resilience. From the electricity industry's perspective, board members should go beyond encouragement and empower management to collaborate with ecosystem stakeholders to facilitate the transparent and agile sharing of information (e.g. threat intelligence, disaster recovery capacities and network monitoring data).

Moreover, board members are uniquely positioned to work with their peers (e.g. board members from other organizations and policy-makers) to set the strategic vision for systemic cyber resilience, and go beyond their oversight responsibilities towards an active role. For example, this could involve working with policy-makers to ensure that regulatory or compliance risk does not prevent voluntary disclosure.

Questions for the board

1. How actively and effectively does the board collaborate with policy-makers in setting the strategic cyber resilience vision and objectives for the electricity ecosystem (e.g. incentives for timely voluntary disclosure)?
2. What formal or informal mechanisms does the board use to share cyber resilience best practices with peers (i.e. other board members)?
3. How does management identify and evaluate the entities (both public and private sector) and information sharing platforms with which the organizations should collaborate?
4. What government resources for cyber risk management, information sharing and collaboration would it be beneficial to participate in?
5. When handling and sharing information with national security implications, how does management ensure that information is shared only via the correct channels and solely with trusted entities?
6. Does the board promote organizational participation in ex-post and proactive information sharing forums?
7. What formal or informal mechanisms does management use to ensure the timely and accurate relay of relevant information across the ecosystem?
8. How does cybersecurity related information received via collaborative initiatives inform corporate strategy?

Information sharing challenges and practical next steps

A survey of over 20 electricity industry leaders from Europe and the United States was conducted to understand their views on the main cultural and structural challenges associated with cyber information sharing. They were also asked for practical next steps to increase the level and usefulness of information sharing in the industry. A selection of their responses is included below.[23]

Survey Results

Cultural norms or biases in organizations that hinder transparent and agile information sharing

It is the fear of media taking attacks out of context which affects the brand value and stock. These are the most important impediments to info sharing.

It is primarily due to the culture within the company. There is no formal process laid out for any information sharing within the company itself.

Opportunities to either save costs or reduce effort encourages information sharing, but effort of sharing reduces willingness.

Partnership is a key part of a cybersecurity strategy. The effort needed to put in place the sharing of information biases the action.

Notion of letting the side down and exposing the fact that the organization did not have sufficient protection in place discourages information sharing.

National security interests, country-specific regulation, competition, trust (or lack of)

Practical steps to increase the level and usefulness of information sharing in the industry

Need to keep the topic active at board level and communicate issues as they happen.

Consolidate forums in order to avoid redundant work and isolated initiatives; align with wider organizations (e.g. ENISA, Interpol etc.)

Promote partnership between government and industry.

Create indicators to show value; promote initiatives to show practical, useful cases of info sharing.

Create a safe zone based on mutual trust; no shame

Create an easy-to-use platform; work on common rules on what and what not to share.

CISO network should be leveraged.

The most common response to improve information sharing was the importance of leader-owned and leader-led collaboration. The following case study provides one such example:

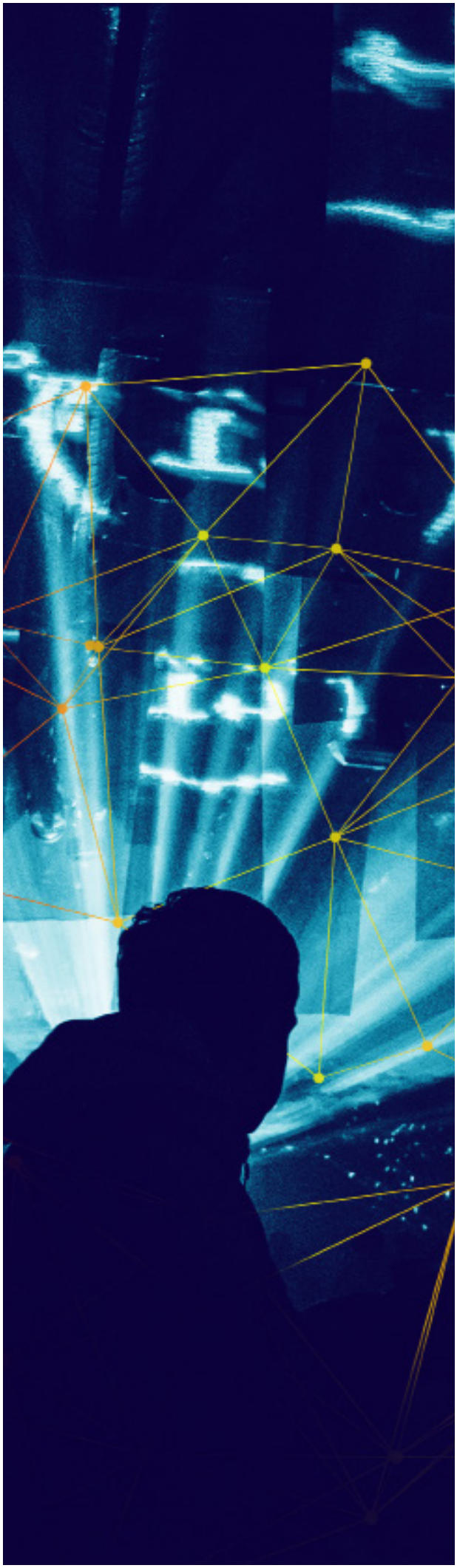
Case study: Siemens' Charter of Trust[24]

The digital world is changing everything. Billions of devices are connected through IoT. This holds great potential for everyone, but also great risk. This is exactly where the Charter of Trust (CoT) comes in. To keep pace with continuous progress in the digital economy and the threats posed by criminal activities, large industrial companies have formed the Charter of Trust to define and implement principles that can make the digital world a safer place.

The power of the CoT stems not only from the fact that it is driven from the very top of the organizations, but also that the implementation is based on the principle of “leading by example”. With cybersecurity having become a top priority among boards of organizations, implementation of the principles, as well as the necessary paradigm shifts are not discussed as merely an option but are instead implemented as an essential ingredient to the future digital business. To underscore this priority, leaders (typically CEOs) from global organizations were not only present at the start of the initiative in February 2018, but are also directly involved in regular CoT board meetings and have since pushed the initiative forward with great success.

By making the Charter of Trust a top priority in their companies, CEOs are driving a culture change, which is critical to the success of the initiative. They are committed to creating baseline requirements for their supply chains and are declaring these standards binding for their companies and its business partners, again following the principle of “leading by example”.

As a credible and reliable voice, the CoT members collaborate with key stakeholders around the world to achieve trust in cybersecurity for global citizens. The Charter of Trust shows that, even in times of imminent trade conflicts and growing mistrust, global collaboration at the highest level is not only possible – it is necessary.



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.

General Principle 7[25] stated that boards need to ensure that organizational cyber resilience plans are created, tested and continually improved. In the electricity ecosystem, boards need to go one step further by promoting the creation, testing and improvement of collective resilience plans. These plans should consider, include and appropriately balance processes to manage the full cyber attack lifecycle. For example, these plans could include defence in depth strategies for cyber preparedness and mutual assistance plans for rapid recovery. Moreover, these plans should augment and be integrated into any existing power resilience plans.

Questions for the board

1. Is there a cyber resilience plan in place covering the organization's ecosystem(s), incorporating incident response, communications, business continuity and disaster recovery?
2. What platforms are employed by the board and management team to advocate for the development of collective resilience plans?
3. Does the board offer appropriate organizational resources (both financial and personnel) for the development of the collective resilience plans?
4. Do the collective resilience plans clearly define the roles and responsibilities of each organization in the ecosystem with respect to cyber resilience?
5. Once developed, are collective resilience plans adequately tested at an appropriate frequency?
6. How do the collective resilience plans evaluate and appropriately balance preparedness with response and recovery across the ecosystem?
7. How are the essential learnings and associated action plans from testing exercises used in updating both organizational and ecosystem-wide cyber resilience plans?

Case Study: The impact of a cyber attack may not equally affect stakeholders within the electricity ecosystem

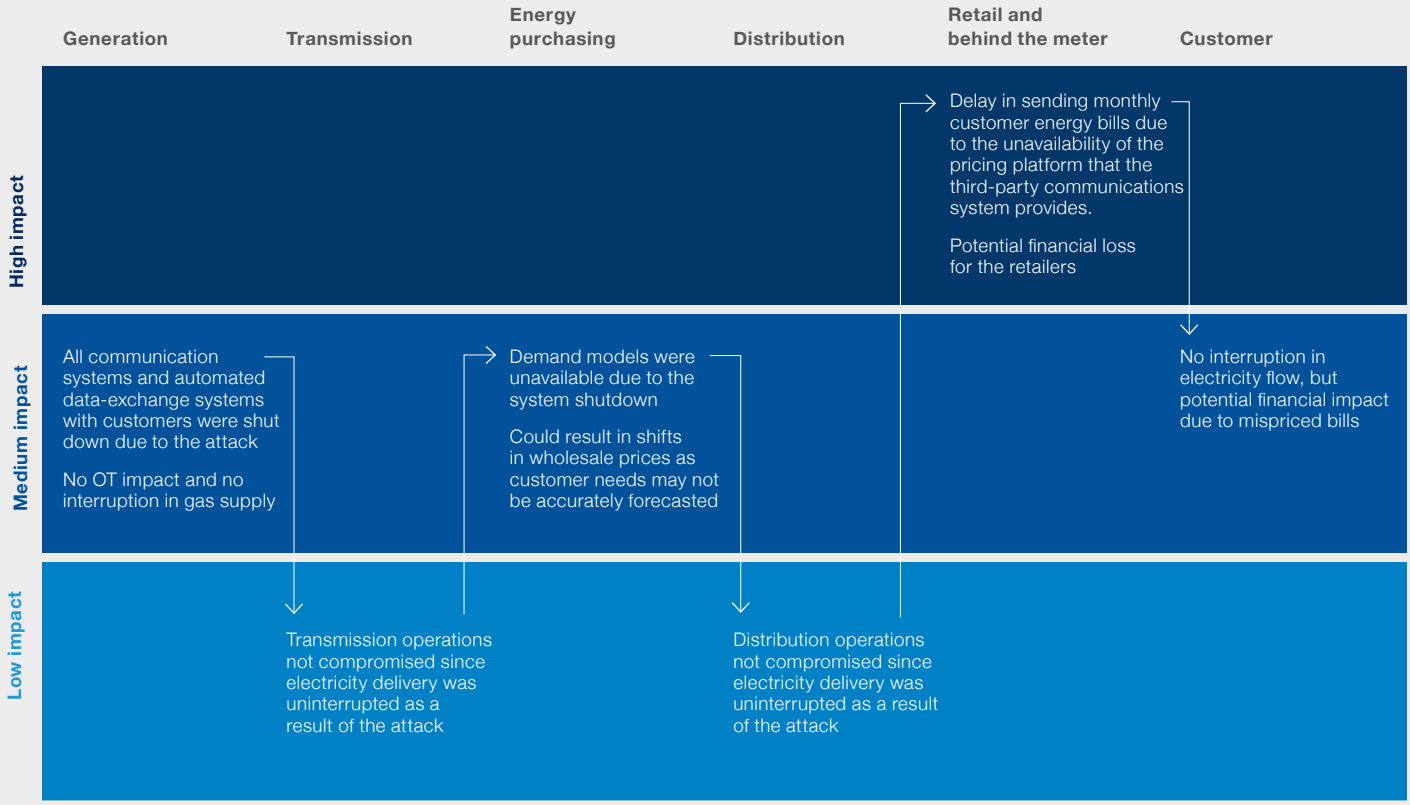
What happened?

In March 2018, a cyber attack compromised an electronic communications system provider's platform in the United States.[26] The effects of this attack were not only felt by the provider, but also by four of its natural gas pipeline customers whose services were disrupted. All of these pipeline companies relied on the platform to help track and schedule gas flows.

However, the disruption did not stop there. The very same platform also supplied electricity prices and demand models to utilities.[27] The utilities lost access to systems they depended on to inform pricing and to determine how much supply to secure from wholesale markets to ensure uninterrupted electricity flow. Their inability to use the platform cascaded the impact even further and, as a result, estimated and partial bills were sent to customers from some of the largest utilities in the US.

Even though this cyber attack did not cause any operational disruption in electricity flow and did not threaten public safety, it illustrates how a cyber attack on a single organization:

1. can have a cascading impact on multiple stakeholders within the ecosystem.
2. is not bound to that organization and can sometimes unevenly affect the financials and even day-to-day operations of other ecosystem stakeholders.



What can be done?

If a single cyber attack can affect multiple stakeholders, then the stakeholders need to work together to manage the risk associated with that single cyber attack.

By being aware of the collective dependency on the communications platform, relevant stakeholders (i.e. communications system providers, pipeline companies and utilities) can proactively collaborate on managing the associated cyber risk. This could result in preventative defence in depth strategies as well as response and recovery strategies (e.g. escalation protocols, manual communication mechanisms and back-up systems) to minimize the cascading impact.

Ultimately, it is critical that the ecosystem stakeholders come together to devise collective strategies for managing cyber risk. Without this collaboration, improving systemic cyber resilience will be difficult.

4. The Future of Resilient Electrical Grids

The principles and guidance in this document will provide the means by which boards and business leaders can ensure cyber resilience strategies are adopted. However, the effort does not stop there. To keep pace with the cybersecurity challenges in the dynamic electricity environment, it is vital that leaders also think about and act on the following:

Navigating the regulatory space

Increasingly decentralized, digitalized and electrified power systems are significantly contributing to both the interconnection and interdependency of global electricity networks. In parallel, cyber attacks have the ability to spread across continents rapidly. Despite this, multinational organizations continue to expend resources navigating cybersecurity regulatory environments in multiple markets, with no guarantee of eventual cyber resilience. To reduce the burden for businesses operating transnationally, many regions are considering harmonization of cybersecurity regulations. A practical first step could be the mapping of regional cybersecurity regulations to a chosen standard framework.

Collective situational awareness

The distributed nature of the electricity industry ecosystem may make it difficult for a single organization to efficiently identify a cyber attack. Overcoming this challenge requires a real-time, transparent sharing of information at machine speed to build collective situational awareness. Moreover, the sharing of real-time information should take into account national security implications as information to manage cyber risks may need to cross national and regional boundaries. An initial approach could be the development of a framework for coordinated real-time, neutral, international electricity-specific information sharing.

Cyber resilience metrics

To effectively integrate cyber risk into business strategy, progress needs to be measured. Monitoring cyber resilience efforts, as well as measuring the effectiveness of cyber resilience investments and capabilities, remains a challenge for electricity ecosystem stakeholders (both public and private sector). Technical cybersecurity metrics are often measured and reported, but these need to be translated into a language that decision-makers (boards and regulators) can act on. Robust cybersecurity metrics in business language are needed to overcome this challenge.

Emerging technologies

The proliferation of IoT and industrial IoT (IIoT) devices raises reasonable concerns regarding the safe and secure use of these technologies. For electricity utilities and other industries, the continuous evolution of technology will present an ongoing challenge to cybersecurity. The implementation of distributed energy and consumer-side devices (e.g. smart-home devices and electric vehicle charging units) will expand the attack surface. The maturity of security analytics, machine learning and artificial intelligence (AI), especially in the OT environment, will provide actionable intelligence to enable proactive and responsive defence measures.[28] In parallel, the sophistication of cyber tools used by malicious actors will continue to grow. For instance, quantum computing may change the encryption landscape as we know it. Leaders in the electricity ecosystem need to be aware of the changes and gaps these cutting-edge technologies bring, and collectively plan to secure them from the start. This approach will allow electricity organizations to reap the benefits while managing the associated risks.

Internet of Things and Power Systems[29]

IoT devices are, and will be, deployed at all levels of electricity systems from grid edge to transmission and generation. This includes private homes (e.g. appliances, lighting, and heating, ventilation and air conditioning [HVAC]) and within transmission and distribution systems to monitor energy flow and aid in predictive maintenance. By enabling the collection of accurate and granular information across the full electricity ecosystem, IoT can improve both operational and cost efficiencies. For example, IoT systems can provide visibility into the performance of legacy systems and offer opportunities for predictive and proactive maintenance. However, it is important to recognize and proactively address the new cybersecurity challenges that will arise with IoT.

As connectivity grows, especially in the control systems environment, so do the number of potential vulnerabilities in the system. “Air gaps” have been thought of as a solution to improve cyber risk, but run counter to one of the main advantages of IoT, which is increased digital connectivity. As a result, managing cyber risks associated with IoT requires a strategic approach that is aligned with the cyber resilience principles outlined in this document. In particular, IoT-related cyber risks need to be integrated into overall business risk and managed systematically.

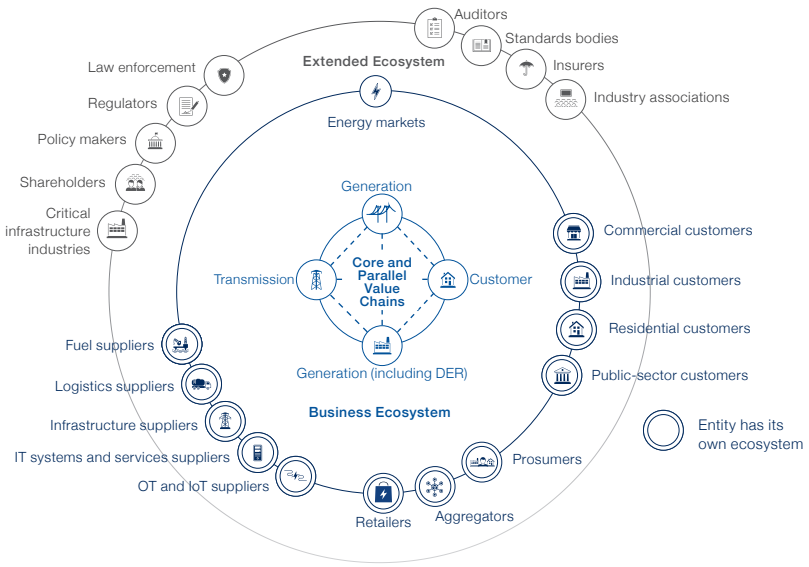
Appendix 1

Cyber Resilience 'Tear sheet' for Boards of Directors

Foundational themes for cyber resilience in the electricity industry

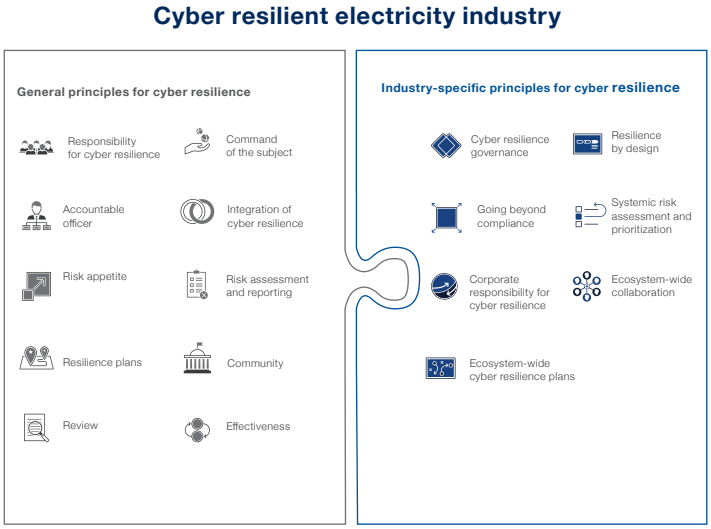
- Interdependent ecosystem
- Siloed approach to cyber resilience
- Culture of compliance

What does this ecosystem look like?



It is no longer enough for an electricity organization to secure its own “house”. Leaders must realize that their organizations are part of a larger “neighbourhood” where cooperation on cyber resilience is essential between the members of that neighbourhood, ranging from oversight bodies to suppliers, customers and employees.

How to secure this complex ecosystem?



Addressing cyber resilience challenges in this ecosystem requires an organizational and systemic view

General principles: Enable board action in making cyber resilience a component of overall organizational strategy.

Electricity principles: Augment the general principles by offering strategies that go beyond organizational cyber resilience and aid the board in advancing ecosystem-wide cyber resilience

Appendix 1

Cyber Resilience 'Tear sheet' for Boards of Directors

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: Integration of cyber resilience

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 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 in 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 empowers management to create a culture of collaboration, set strategic objectives around 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.

Acknowledgements

Lead Authors

Louise Anderson	Electricity Industry Community Lead	World Economic Forum
Daniel Dobrygowski	Head of Governance and Policy	Centre for Cybersecurity, World Economic Forum
Sam Rajachudamani	Project Collaborator	World Economic Forum, Seconded from Boston Consulting Group

Electricity Industry Chair

Eric Martel	CEO	Hydro Québec

World Economic Forum Leadership

Jeremy Jurgens	Head of Centre for Global Industries, Member of the Managing Board	World Economic Forum
Troels Oerting	Head of Centre for Cybersecurity	World Economic Forum

Working Group Co-Chairs

Pierre-Alain Graf	Senior Vice President	ABB
Rosa Kariger	Global CISO	Iberdrola S.A.

Advisory Team

Roberto Bocca	Head of Energy and Basic Industries	Member of the Executive Committee, World Economic Forum
Kristen Panerali	Head of Electricity Industry	World Economic Forum
Walter Bohmayr	Senior Partner and Managing Director	Boston Consulting Group
Stefan Deutscher	Associate Director	Boston Consulting Group

Working Group

Ashtad Engineer	Vice President of Technology and Digitization	Adani Group
Stefano Bracco	Knowledge Manager	Agency for the Cooperation of Energy Regulators
Scott Pinkerton	Cyber Security Programme Manager	Argonne National Laboratory
Reena Pathak	Director - IT Risk and Assurance	Centrica Plc
Chris Lanigan	Centrica Director of Security Architecture and Consulting/BISO UK Business	Centrica Plc
Dexter Casey	Chief Security Officer (CSO)	Centrica Plc
Nynke Stegink	International Public Private Participation Lead	Dutch National Cyber Security Centre
Paulo Moniz	Director Information Security and IT Risk	Energias de Portugal SA
Markus Wolf	Regional Manager for International Stakeholders	Electric Power Research Institute
Matt Wakefield	Director of Information, Communication and Cyber Security	Electric Power Research Institute
Candace Suh-Lee	Principle Technical Leader – Cyber Security	Electric Power Research Institute
Yuri G. Rassega	Chief Information Security Officer (CISO)	Enel Group
Aniello Gentile	Director Cybersecurity	Enel Group
Matthieu Pestel	Deputy Chief Information Officer (CIO)	ENGIE Group
Olivier Vandelaer	Director Cybersecurity	ENGIE Laborelec
Michaela Kollau	Policy Officer	European Commission

Luigi Rebuffi	Secretary General	European Cyber Security Organisation
Nina Olesen	Senior Policy Manager	European Cyber Security Organisation
Nicolas Richet	Chief Information Officer (CIO)	European Network of Transmission System Operators for Electricity
Keith Buzzard	Chief Information Security Officer (CISO)	European Network of Transmission System Operators for Electricity
Pekka Eira	CIO and Head of Fortum Business Services IT	Fortum Corporation
Patric McElroy	VP, Chief Software Engineer	GE
Daniel Alvarez	Director, Cyber Security	Hydro Québec
Agustin Valencia Gil-Ortega	Head of OT Cybersecurity	Iberdrola S.A.
Florian Haacke	SVP, CSO/Head of Group Security	innogy SE
Boris Beuster	Head of Information Security	innogy SE
Guido Gluschke	Director	Institute for Security and Safety (ISS)
Kristina Sander	Research Fellow	Institute for Security and Safety (ISS)
Brecht Wyseur	Product Manager, Internet of Things (IoT) Security	Kudelski Group / EE-ISAC
Maximilian Urban	Information Security Officer and Innovation Manager	Netz Niederösterreich GmbH / EurElectric
Gerda Retbøll-Bauer	Chief Information Security Officer (CISO)	Ørsted
Eric Singer	Chief Information Security Officer (CISO) EMEA	Schneider Electric
Christophe Blassiau	Senior Vice President, Digital Security and Global CISO	Schneider-Electric
Ingo Susemihl	Partner Management, Charter of Trust	Siemens AG
Leo Simonovich	Vice President and Global Head, Industrial Cyber and Digital Security	Siemens Corporation
Vlada Spasic	Senior Advisor, Energy and Utilities	SV Energy Sàrl
Anne-Marie Zielstra	Director, Cyber Security and Resilience	TNO

Numerous other contributors supported this work by providing input, expertise and thoughtful commentary during the project development including Remi Mayet (European Commission), Tim Conway (SANS Institute), Max Everett (US Department of Energy), Margaret Hayden (EirGrid), Tim Daly (AEMO - Australia), Stuart Johnston and Heath Frewin (Energy Networks - Australia), Carrie Shirtz (US Embassy in Switzerland), Hala Furst (US Department of Homeland Security), Florian Pennings (ENISA), Professor John Villasenor (UCLA), Alex Asen (BCG), Nadya Bartol (BCG), and Troy Thomas (BCG).

Resources for Further Reading

- Australian Government Security and Critical Infrastructure Division. 2008. Cyber Storm II National Cyber Security Exercise. Australian Government Attorney General's Department, pp. 12–18. https://www.tisn.gov.au/Documents/Cyber+Storm+II+Final+Reports.pdf (link as of 26/11/18).
- Bartol, Nadya. 2015. Cyber Supply Chain Risk Management for Utilities: Roadmap for Implementation. Utilities Technology Council, pp. 5–13. https://utc.org/wp-content/uploads/2018/02/SupplyChain2015-2.pdf (link as of 26/11/18).
- Boison, Gregory, WalterBohmayr, Stefan Deutscher and Michael Bechauf. 2017. It Takes a Coalition to Protect the Internet of Things. Boston Consulting Group. https://www.bcg.com/publications/2017/technology-digital-engineered-products-infrastructure-coalition-protect-internet-things.aspx (link as of 26/11/18).
- Cyber Security Council (CSR). 2018. Cybersecurity Guide for Boardroom Members. Cyber Security Council Netherlands, p. 6. https://www.cybersecurityraad.nl/binaries/Handreiking_Bestuurders_ENG_DEF_tcm107-323477.pdf (link as of 26/11/18).
- Energy Expert Cyber Security Platform. 2017. Cyber Security in the Energy Sector – Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector. EECSP, pp. 17–25, 64–71. https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf (link as of 26/11/18).
- Energy Sector Control Systems Working Group. 2014. Cybersecurity Procurement Language for Energy Delivery Systems, pp. 1–10. https://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf (link as of 26/11/18).
- Geiger, Rick. 2014. Benefits of Combining Utility IT and OT. Electric Light & Power. https://www.elp.com/articles/powergrid_international/print/volume-19/issue-4/features/benefits-of-combining-utility-it-and-ot.html (link as of 26/11/18).
- Internet Security Alliance. 2018. Managing Cyber Risk: A Handbook for UK Boards of Directors, pp. 12–26. https://isalliance.org/wp-content/uploads/2018/04/CyberRisk-DSHandbook_UK_Final.pdf (link as of 26/11/18).
- IT Security Expert Advisory Group. 2008. Defence in Depth. Australia Trusted Information Sharing Network for Critical Infrastructure Protection, pp. 6–23, 44–78. https://www.tisn.gov.au/Documents/SIFTD-I-D+-+Full+-++15+Oct+2008+-+1.pdf (link as of 26/11/18).
- National Institute of Standards and Technology. 2015. Best Practices in Cyber Supply Chain Risk Management – Exelon Corporation. US Department of Commerce, pp. 3–10. https://www.nist.gov/sites/default/files/documents/itl/csd/NIST_USRP-Exelon-Case-Study.pdf (link as of 26/11/18).
- National Institute of Standards and Technology. 2015. Best Practices in Cyber Supply Chain Risk Management – Utility Sector. US Department of Commerce, pp. 2–11. https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Utility_093015.pdf (link as of 26/11/18).
- National Observatory for Cyber Security, Resilience and Business Continuity of Electrical Grids, The. 2018. Principles, Guidelines and Good Practices for Management of Cyber Security, Resilience and Business Continuity of Electric Operators, pp. 7–10, 14–18. https://circie.unige.it/Guidelines_CYBER_Electrical_System.pdf (link as of 26/11/18).
- North American Electric Reliability Corporation. 2018. Grid Security Exercise GridEx IV. NERC, pp. 13–18. https://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20IV%20Public%20Lessons%20Learned%20Report.pdf (link as of 26/11/18).
- Paulsen, Celia, Jon Boyens, Nadya Bartol and Kris Winkler. 2018. Criticality Analysis Process Model Prioritizing Systems and Components. US Department of Commerce, pp. 1–8. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8179.pdf (link as of 26/11/18).
- Ponemon Institute. 2017. Data Risk in the Third-Party Ecosystem. Ponemon Institute, pp. 3–17. https://cdn2.hubspot.net/hubfs/2575983/Ponemon_report_Final%20(1).pdf (link as of 26/11/18).
- Schneider Electric. 2018. Addressing IT/OT Convergence in a Versatile Cyber Ecosystem. https://www.schneider-electric.com/en/download/document/998-20244304/ (link as of 26/11/18).
- Schneider Electric. 2018. Cybersecurity by Design: Building a Company Culture to Strengthen a Digital Business. https://www.schneider-electric.com/en/download/document/998-2095-12-06-18AR0_EN/ (link as of 19/12/18).
- United States of America. 2018. National Cyber Strategy of the United States of America, pp. 8–11, 15, 24–26. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (link as of 26/11/18).

Endnotes

1. Dobrygowski, Daniel. 2018. Critical Infrastructure Cybersecurity and Resilience, a Shared Responsibility. CIOReview. https://critical-infrastructure-protection.cioreview.com/cxoinsight/critical-infrastructure-cybersecurity-and-resilience-a-shared-responsibility-nid-27380-cid-201.html (link as of 26/11/18).
2. Energie Institute an der Johannes Kepler Universitat Linz. Black Simulator. Simulation parameters – 6 hour blackout starting at 17:00 on December 20 in mainland France. http://www.blackout-simulator.com/ (link as of 26/11/18).
3. Hawk, Carol, and Akhlesh Kaushiva. 2014. Cybersecurity and the Smarter Grid. The Electricity Journal, p. 1. https://www.energy.gov/sites/prod/files/2014/10/f19/Cybersecurity_SmarterGrid_2014.pdf (link as of 26/11/18).
4. Bartol, Nadya and Michael Coden. 2017. Our Critical Infrastructure Is More Vulnerable than Ever – It Doesn't Have to Be that Way. https://www.bcg.com/en-us/publications/2017/engineered-products-critical-infrastructure-vulnerable-doesnt-have-to-be-that-way.aspx (link as of 26/11/18).
5. European Union. 2016. EU Network and Information Security Directive. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (link as of 19/12/18).
6. North American Electric Reliability Corporation. 2016. Critical Infrastructure Protection Standards. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (link as of 19/12/18).
7. National Institute of Standards and Technology. 2014. Guidelines for Smart Grid Cybersecurity – Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements. US Department of Commerce, pp. 15–17. https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf (link as of 26/11/18).
8. CEN-CENELEC-ETSI Smart Grid Coordination Group. 2012. Smart Grid Reference Architecture. CEN-CENELEC-ETSI Smart Grid Coordination Group, pp. 20–21, 30. https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf (link as of 26/11/18).
9. Greenberg, Andy. 2017. How an Entire Nation Became a Test Lab for Cyberwar. Wired. https://www.wired.com/story/russian-hackers-attack-ukraine/ (link as of 26/11/18).
10. Knake, Robert K. 2017. Cyberattack on the U.S. Power Grid. Contingency Planning Memorandum No. 31. Council on Foreign Relations Center for Preventative Action.
11. O'Flaherty, Kate. 2018. Cyber Warfare: The Threat from Nation States. Forbes. https://www.forbes.com/sites/kateoflahertyuk/2018/05/03/cyber-warfare-the-threat-from-nation-states/ (link as of 26/11/18).
12. World Economic Forum. 2017. Advancing Cyber Resilience: Principles and Tools for Boards. World Economic Forum, p. 8. http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf (link as of 26/11/18).
13. US Department of Homeland Security. 2018. Secretary Kirstjen M. Nielsen Remarks at the RSA Conference. 17 April. https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nielsen-remarks-rsa-conference (link as of 26/11/18).
14. ICS-CERT. 2016. Alert Cyber-Attack Against Ukrainian Critical Infrastructure. 25 February. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (link as of 26/11/18).
15. Johnson, Blake, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker and Christopher Glyer. 2014. Attackers Deploy New ICS Attack Framework "Triton" and Cause Operational Disruption to Critical Infrastructure. FireEye, 14 December. https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html (link as of 26/11/18).
16. Voster, Wam. 2018. Establish Successful Executive Security Steering in an Integrated IT/OT Environment. Gartner.
17. International Energy Agency. 2017. Digitalization and Energy. IEA, p. 128. https://www.iea.org/publications/freepublications/publication/DigitalizationandEnergy3.pdf (link as of 26/11/18).
18. Sobczak, Blake. 2018. FERC Signs off on Cyber Rules for "Highest-Risk" Grid Systems. EnergyWire. 18 October.
19. European Network of Transmission System Operators for Electricity. 2016. Frequency Stability Evaluation Criteria for the Synchronous Zone of Continental Europe. pp. 6-7. https://docstore.entsoe.eu/Documents/SOC%20documents/RGCE_SPD_frequency_stability_criteria_v10.pdf (link as of 19/12/18).
20. World Economic Forum. 2017. Advancing Cyber Resilience: Principles and Tools for Boards. World Economic Forum, p. 8. http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf (link as of 26/11/18).
21. EE-ISAC. 2018. The European EE-ISAC announced a Memorandum of Understanding with the US E-ISAC and Japanese ISAC in October 2018. This partnership will include exchange on regulations and good practices in cybersecurity provision to build trust. http://www.ee-isac.eu/node/71 (link as of 19/12/18).
22. Pinkerton, Scott. 2018. What Does Coordinated Information Sharing Look Like for the Energy Industry? Argonne National Laboratory, 25 October.
23. World Economic Forum. 2018. Working Group Meeting. 25 October.
24. Siemens. 2018. Time for Action: Building a Consensus for Cybersecurity. 17 May. https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/cybersecurity-charter-of-trust.html (link as of 26/11/18).
25. World Economic Forum. 2017. Advancing Cyber Resilience: Principles and Tools for Boards. World Economic Forum, p. 8. http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf (link as of 26/11/18).
26. Malik, Naureen S, Ryan Collins and Meenal Vamburkar. 2018. Cyberattack Pings Data Systems of at Least Four Gas Networks. April 03. https://www.bloomberg.com/news/articles/2018-04-03/day-after-cyber-attack-a-third-gas-pipeline-data-system-shuts (link as of 26/11/18).
27. Malik, Naureen S. and Ryan Collins. 2018. The Cyberattack that Crippled Gas Pipelines Is Now Hitting Another Industry. April 04. https://www.bloomberg.com/news/articles/2018-04-04/cyberattack-bleeds-into-utility-space-as-duke-sees-billing-delay (link as of 26/11/18).
28. Simonovich, Leo. 2018. Using the Power of Analytics to Address Cyber Security. November 05. https://www.linkedin.com/pulse/using-power-analytics-address-cyber-security-leo-simonovich/ (link as of 26/11/18).
29. Villasenor, John, 2018. Working Group Interview. 31 August.

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

World Economic Forum LLC
350 Madison Ave, 11th Floor,
New York, NY 10017, USA
Tel.: +1 212 703-2300
Fax: +1 212 703-2399
forumusa@weforum.org
www.weforum.org