

Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain

WHITE PAPER
DECEMBER 2020



Contents

3	Executive summary
5	Introduction
7	1 Redefining roles and responsibilities across the value chain
14	2 Key reflections when securing the product lifecycle
16	3 Appendices
17	Appendix A: Taxonomy
18	Appendix B: Electricity board principles for cyber resilience
19	Appendix C: Roles and responsibilities cheat sheet
21	Appendix D: Cybersecurity programmes
23	Acknowledgements
25	Endnotes

Inside: Getty images/ipopba; Getty images/frk; Getty images/LeoPatrizi; Getty images/onlyyouqj; Getty images/metamorworks; Getty images/deepblue4you; Getty images/sesame; Unsplash/Lukas Bato

© 2020 World Economic Forum. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.

Executive summary

The electricity industry has evolved rapidly from majority large generation assets, top-down energy distribution and one-way digital communication, to a type of customer-centric energy consisting of decentralized, agile, resilient and secure collections of real-time, networked assets.

As a result, effective and sustainable measures for protecting the electricity industry supply and value chains now go beyond securing individual products or systems, driving the need for an adaptation of roles and responsibilities, from procurement and design through to retirement. An isolated approach will no longer suffice to secure and achieve a resilient ecosystem. Industry stakeholders must address their individual as well as their shared responsibilities.

The World Economic Forum's Systems of Cyber Resilience: Electricity community, comprised of senior cybersecurity executives from the electricity industry ecosystem, created this report to redefine the cybersecurity-related roles and responsibilities

across the industry's value chain. The effort was initiated by the manufacturing company members and then refined through consultation with the broader community.

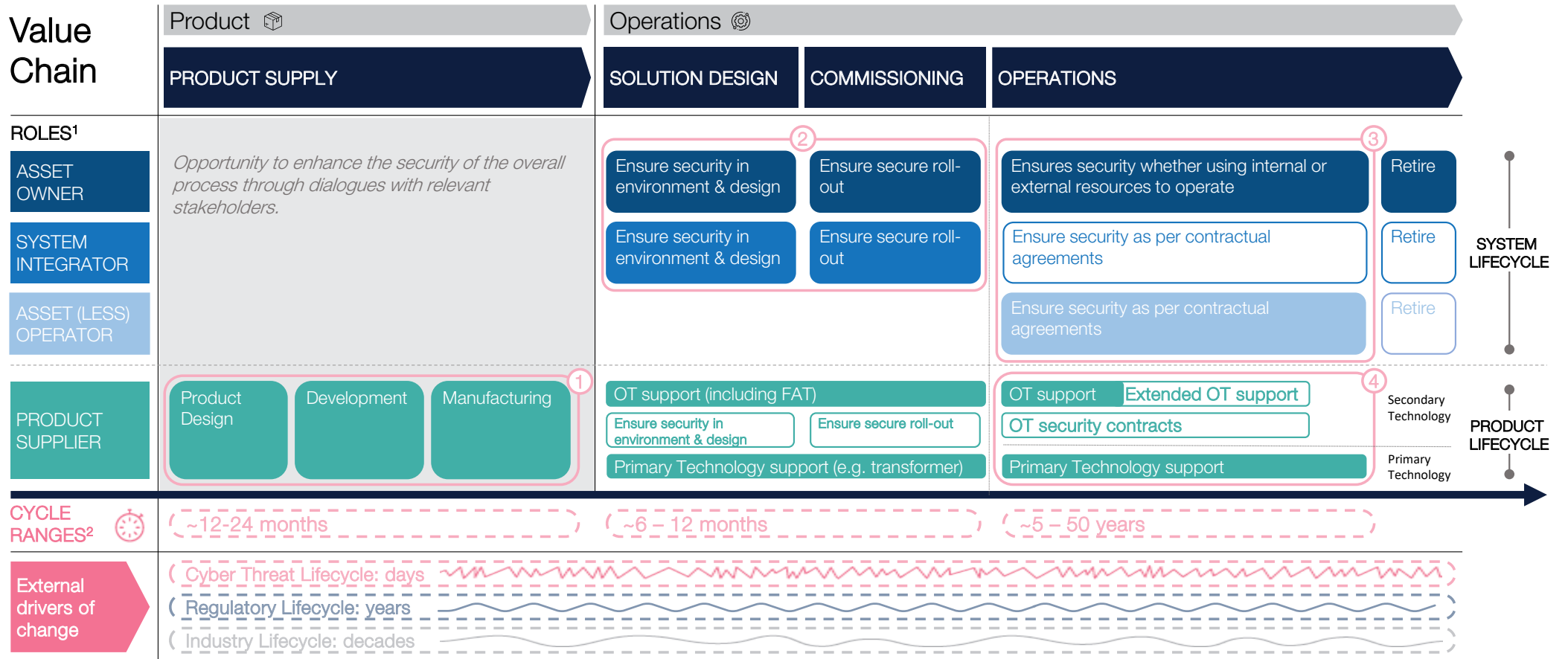
This report aims to share the newly proposed electricity industry value chain responsibility model (Figure 1) and provoke further dialogue and action on this topic.

The report contains three sections:

- The first section introduces the drivers of change responsible for the evolution of roles and responsibility across the electricity industry value chain.
- The second section redefines roles and responsibilities across the value chain.
- The third section provides key reflections on securing the value chain.



FIGURE 1 | Electricity industry value chain security responsibility model



LEGEND: 1—4 Focus areas Responsibility by default Extended Activities by Contract

1. Each entity can play different roles during the product or system lifecycle

2. The cycle ranges are indicative and approximative depending on the type of products and systems, as well as contractual agreements

Introduction

“ Primary technology and OT Technology are two indivisible components. The difference of their lifespans requires an active management, throughout the time, with clear responsibilities among the roles involved in the value chain

Yuri G. Rassega,
Chief Information
Security Officer,
Enel Group

“ Cybersecurity should be included by default in new business initiatives and must not be undercut by pricing negotiations.

Rosa Kariger,
Global Chief
Information Security
Officer, Iberdrola

With the growing number of novel interactions between people, machines, services and various feedback processes, the complexity of the networked society is increasing rapidly and continually. In the electrical industry ecosystem, information technology (IT) and operational technology (OT) systems are becoming more interdependent. This can increase the efficiency as well as the consequences of cyberattacks.

Effective and sustainable cybersecurity measures need to consider the different dynamics of the key

drivers of change in the industry, global environment and threat landscape. As supply and value chains become more complex, measures must also evolve and go beyond the securing of individual systems. A static approach will not suffice¹ – industry players need to address their individual as well as shared responsibilities to secure the ecosystem.

In response, World Economic Forum's Systems of Cyber Resilience: Electricity community members have developed this report, which proposes a new value chain responsibility model.

Key drivers of change

Three key drivers of change are responsible for the evolution of the value chain as illustrated in Figure 1.

- **Evolving electricity industry:** Up to 15 years ago, electricity networks were considered slow moving bulk systems. Today, they are in the middle of a global evolution of energy systems, with energy generated, stored and distributed closer to the final customers through the acceleration of distributed renewables and energy storage technologies. Digitalization allows customers and electricity system operators to control where, when and how electricity is being used. New and more energy uses are being electrified (e.g. transport, heating of buildings). Nonetheless, real transformational change of such critical infrastructure takes decades (e.g. construction of large-scale grid infrastructure still takes at least 10 years in many countries).
- **Global regulatory environment:** Regulators are challenged to keep regulations current given the rapid and evolving threat landscape. The importance of a stable environment for

stakeholders means that regulators are faced with the competing challenges of providing medium-term clarity in a fast-changing context where 100% security is never guaranteed. The incorporation of standards into legislation or regulation offers some flexibility on this topic, but changes occur in terms of years.²

- **Rapid change of cyberthreat landscape:** In this interconnected and new cyber-social world, digital information drives real events and components increasingly make autonomous decisions. This nonstop innovation and improvement of existing technologies, coupled with the velocity by which criminals and intelligence agencies can acquire and exploit these opportunities, allow for a continuous stream of new types of previously unconceivable attacks.^{3,4} Predictability and controllability are a matter of proper systems design and operation, including increased cooperation across the ecosystem. Without adaptation, previously secure systems and environments become insecure.

Securing the value chain

As digital products become more widespread, the growing complexity of the supply and value chains poses a significant threat to the electricity ecosystem. The traditional approach to securing the supply chain works on the assumption that the threat is greatest at the manufacturing stage. However this approach needs to be broadened to include the value chain:

- Threats are shifting towards the design of chips, components, software and their respective development environments and tooling.

- Digital products, more so than non-networked products, require security updates due to their connection to the ever-changing network landscape and due to continuous new vulnerabilities discovered.
- Digital products can change long after commissioning, e.g. through faulty software updates, misconfigurations, or backdoors.

Securing the value chain must address the end-to-end product lifecycle, including design, commission

and operations until retirement. The different entities in the value chain collaborate on business-critical activities for products and systems, and hence an isolated approach will not suffice. A resilient ecosystem requires individual as well as shared responsibilities.

This shift of approach follows the principles of resilience by design, systemic risk assessment and prioritization, as well as ecosystem-wide collaboration and cyber resilience plans from the report [Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards](#).⁵

What is the value chain?

The end-to-end lifecycle for hardware, product, system or services that delivers value to an entity. The end-to-end lifecycle goes through different phases, from the design, commission and operation until the end-of-life stage.

What is the supply chain?

The end-to-end processes and network of entities required for transforming raw materials into final products.



1

Redefining roles and responsibilities across the value chain



The value chain represents the end-to-end lifecycle for hardware, product, system or services that delivers value to an entity. The end-to-end lifecycle goes through different phases, from the design, commission, operation until the end-of-life stage.

Figure 1 depicts the value chain phases for typical electricity industry products. It also defines cybersecurity roles and responsibilities and focus

areas for relevant stakeholders across the value chain. Roles and responsibilities broadly follow the IEC 62443⁶ definitions. With the rapid adoption of emerging technologies, the responsibility model outlined in Figure 1 should be re-evaluated in the future to ensure it continues to reflect the responsibility of different stakeholders for these new services.

Value chain phases

From the cybersecurity perspective, the value chain can be divided into product and operation phases.



Product phase

This phase includes the *product supply activities*, with a cycle ranging between 12 to 24 months.

- *Product supply* includes product-centric design, development of products and manufacturing of products brought into the market.



Operations phase

This phase is composed of three main activities:

- *Solution design* refers to activities required to integrate the product into the broader system following a site-specific design.
- *Commissioning* is the systematic process by which a product is tested to verify that it functions in accordance with the design intent and operational and security requirements. This activity together with the solution design can take between 6 to 12 months.
- *Operations* refer to ensuring the security of the product as part of the broader system during its operational life until retirement – 5 to 50 years depending on the technology.

Roles

A common understanding of the different roles is important to ensure cybersecurity across the value chain. Each entity can play single or multiple roles throughout the value chain. Taking as reference

roles identified in the relevant standards, and in particular IEC 62443,⁷ this model considers the following roles:



Product supplier

Entity that designs and produces a final product or sub-system to be sold to asset owners. The product is built from components of various suppliers and in-house developed components and software originating from different supply chains.



System integrator

Entity that engineers and integrates components and sub-systems from multiple product suppliers into a site-specific system.



Asset owner

Entity that owns and often operates site-specific systems, over decades, and ultimately retires components (e.g. utilities and prosumers).



Asset (less) operator

Entity that operates assets or performs processes within the electricity ecosystem (e.g. aggregators).

The electricity ecosystem entities can play different roles throughout the *product or system lifecycle*.

Responsibility model

The proposed responsibility model outlined in Figure 1 aims to clarify the shared responsibilities of each role throughout each phase of the product lifecycle. Each role should adhere to general ecosystem and phase-specific responsibilities. A set of associated

cybersecurity programmes (see Appendix D) are recommended to drive accountability and ownership in the different phases of the value chain: product security programme, supplier management programme, industrial security programme.

“ Every part of the value chain has a clear play to protect, detect and respond in our digital ecosystem.

Christophe Blassiau,
Senior Vice-
President, Digital
Security and Global
CISO, Schneider-
Electric

All stakeholders in the value chain should ensure cybersecurity foundations and best practices⁸ are enforced on products in the different phases of the value chain. The responsibilities below are applicable and recommended to all stakeholders and roles to ensure cybersecurity maturity across the ecosystem.

Ensure security by design: Each entity is responsible to:

- Secure the infrastructure, services and environments to ensure the integrity and availability of digital assets (on which businesses may critically rely on).
- Ensure products or services are adequately specified, designed, developed and manufactured, including the required cybersecurity protections (to be maintained, updated or upgraded along their service life) to prevent becoming a vector of compromise to customers or downstream peers.
- Develop defenses-in-depth based on the assumption that systems will be breached, and ensure timely detection and response on suspicious events, as well as communication to relevant entities across the ecosystem.

Embed cybersecurity into the supplier management process. The procurement process needs to start considering security from vendor selection to the terms and conditions in contracts by:

- Developing sourcing decisions through multistakeholder input (e.g. include sourcing, legal, engineering, operations, product security and risk management).
- Defining standard security terms and conditions to be included in all requests for proposals.

- Evaluating suppliers based on defined criteria and security requirements linked to the criticality of the products and services provided, and their respective lifecycles impact across all phases.
- Establishing cybersecurity requirements for all proposed solutions as part of the procurement process. Vendors which do not or cannot meet these standards should be excluded from consideration.
- Including buyer audit rights to assess vendor adherence to contractual commitments and requirements.




Implement security policies consistent with industry best practices, such as ISO 27001,⁹ ISO 20243,¹⁰ IEC 62443,¹¹ NIST CSF,¹² NIST Secure Software Development Framework (SSDF),¹³ Business Software Alliance Framework for Secure Software¹⁴ and set up business continuity and disaster recovery procedures.

Provide training and support knowledge sharing and awareness activities across the value chain.

- Provide and support internal as well as ecosystem wide training opportunities.
- Create mutual trust in the ecosystem, and secure economies of scale, through collaboration and knowledge sharing opportunities.
- Support training offered to the involved players to develop the required knowledge and skills in security throughout the value chain, including security operations and configurations.

Responsibilities per phases and focus areas

Responsibilities shift throughout the product lifecycle phases. One or more focus areas correspond to each phase as per Figure 1.

Phases	Focus areas
 Product supply	1. Ensure security during the product supply phase
 Solution design and Commissioning	2. Secure the solution design and commissioning phases
 Operations	3. Manage and operate system security 4. Ensure product security support

Product supply phase

“ Cybersecurity has to be built in by design at every stage and component of the electricity value chain, rather than a bolt on approach to power systems.

Ashtad Engineer,
Head of Technology,
Adani Energy
Business, Adani

The product phase includes product supply activities such as product design, development and manufacturing (Focus Area 1). The product supplier is solely responsible to ensure the cybersecurity requirements of the products and services provided. It is good practice for the product supplier to seek feedback by engaging in dialogues with relevant stakeholders from the inception of the product development phase.

In addition, product suppliers should implement a product security programme (Appendix D) which integrates security into product development processes from the outset and manages the cyber and business risks from the design phase. The product security programme ensures that security is considered in the product development process to prevent delays in the delivery to the market and customers.

Responsible roles: Product supplier

Associated cybersecurity programme: Product security programme

Product supplier

- Execute the implementation of a comprehensive product security programme.
- Establish cybersecurity requirements, secure design reviews and threat modelling analysis.
- Ensure secure development and manufacturing by building products with security and integrity from the outset. This would include secure development practices, such as secure coding guidelines, and static and dynamic code analysis.
- Perform security testing to validate requirements in the product development process.

See Appendix D for further details.

Product security programme

The product security programme is a process of managing cybersecurity throughout the product development process of bringing products to market.



Solution design and commissioning phase

“ In today’s interconnected world, it is crucial to look beyond one’s own risk, and manage third-party risk. Only through value chain collaboration may resilience be achieved.

Kai Hermsen,
Global Coordinator
for the Charter
of Trust, Siemens

The second focus area is the solution design and commissioning phase (Focus Area 2). This phase is where part of the cybersecurity responsibility transition begins, from the product supplier to those integrating and operating the systems. Upon handover of the product, the relevant product supplier is responsible for both primary and secondary technology support throughout the respective stated product life.

For this phase to be adequately managed, asset owners should have established a supplier management programme during the procurement process. Beyond evaluating the vendors, this programme should also define the requirements to securely integrate the product into the broader system.

Product suppliers, system integrators, asset owners and asset (less) operators must collaborate to

ensure that the future security state of the product and system is taken into consideration at the outset of the design process. This responsibility starts with the definition of the cybersecurity requirements for the future system being defined by the asset owner and/or system integrator, often in collaboration with the product supplier.

Once these requirements are defined, the system integrators can drive component selection within the design process. During this phase, product suppliers should provide support and training to ensure the effective configuration of the system and that asset owners are able to operate independently the security configurations. This shared responsibility continues through final commissioning, with a ramp-up security responsibility adopted by the asset owners.

Responsible roles: Asset owners, system integrators

Associated cybersecurity programme: Supplier management programme, industrial security programme

Asset owners

- Ensure that a supplier management programme is in place to assess cybersecurity posture of vendors, ensure cybersecurity requirements are included into any request for tenders and are addressed in the vendor selection stage of the procurement phase.
- Ensure cybersecurity requirements agreed during the procurement phase are realized in the system integration and commissioning.
- Define the cybersecurity requirements for the system’s future state, enabling the system integrators to drive the components’ selection within the design process.
- Ensure a secure operation and design of systems by initiating the execution of a comprehensive industrial security programme to manage the cybersecurity risks.

System integrators

- Ensure cybersecurity requirements agreed during the procurement phase are realized in the system integration and commissioning.
- Enforce a secure and agile solution design of systems by setting the foundations for the execution a comprehensive industrial security programme.
- Perform the commissioning and delivery of the system to the asset owners, with a gradual transition of security responsibilities shifting from the system integrator to the asset owner when the system is commissioned.

Product supplier

- Support asset owners and system integrators with the effective configuration of security capabilities offered in the target system’s environment.
- Provide the OT product support, including vulnerability management, quality fixes and security patches from the solution design phase through commissioning and throughout stated product life, following the product security programme.

See Appendix D for further details.

Supplier management program

The Supplier management program defines the process to evaluate and continuously monitor the cybersecurity posture of vendors.

Industrial security programme

The industrial security programme aims to include and manage cyber risks from the design phase throughout the process of operating an industrial environment, following the “*resilience-by-design*” principle.¹⁵ The industrial cybersecurity programme should manage cybersecurity controls in industrial environments in adherence with the enterprise’s risk tolerance.



Operations phase

The operations phase aims to ensure security in two focus areas:

- **System operational security.** The asset owner is responsible for the operational security aspects by providing a failsafe and secure environment to operate products (Focus Area 3). This is typically accomplished via an industrial security programme (Appendix D),
- **Product operational security.** The product supplier should provide cybersecurity support and remediate vulnerabilities for the product throughout the stated product life (Focus Area 4).

“ It is critical that we continually assess and strengthen the cybersecurity safeguards we entrust to our supply chain partners to ensure alignment with our evolving operations and data-protection imperatives.

Eric Trapp,
Vice-President,
Security and
Technology,
Sempra Energy

Responsible roles: Asset owners, product suppliers

Associated cybersecurity programme: Product security programme, supplier management programme, industrial security programme

Asset owners

- Ensure management and monitoring of the supplier management programme and industrial security programme.
- Operate the asset while ensuring infrastructure capabilities beyond “patching” industrial components and to support automated testing and deployment of critical updates.
- Keep an accurate and complete inventory of all assets with plans to test and deploy updates timely and at scale.

Product supplier

- Provide the OT product support, including vulnerability management, quality fixes and security patches from handover and throughout stated product life, following the product security programme.
- Ensure continuous OT product support by building the capability to perform timely security incident response for product and services during security incidents.
- Ensure timely production and deployment of security patches for products.
- Where requested, make available additional security services. This allows for new value generating models between asset owners and product suppliers.
 - Extended OT support – such contracts serve to extend the operations and continued need for security patches and adaptations to go beyond the stated product life.
 - OT security contracts – additional security services can be provided if asset owners want to ensure security of wider system containing multiple connected products from different OEMs.

See Appendix D for further details.

Guiding principles for the focus areas

The following guiding principles are recommended to cover four focus areas highlighted in Figure 1, while addressing the challenges associated with the diversity of roles and competing interests:



*Relevant product supplier is responsible for both primary and secondary technology support throughout the respective stated product lives. Primary technology support (e.g. transformer) is not described in detail in this report as the cybersecurity-related implications are focused on the secondary technology (or OT) support.

- 1 Embedding security in the product supply phase requires a comprehensive product security programme established and maintained by the product supplier.
- 2 Incorporating security in the design phase of systems in an electricity network requires a comprehensive industrial security programme from the asset owners, in conjunction with operators and system integrators, to manage the cybersecurity risks.
- 3 Securing the operations phase is a shared responsibility that requires (A) secure products (product supplier) to be integrated (B) into a secure system and operated (C) in a secure context – asset owner and asset (less) operator.
- 4 Ensuring product security support from handover of the product throughout the stated product life.

2

Key reflections when securing the product lifecycle



“ This report shows clearly the challenges in safeguarding older OT environments - I hope we can continue to address these legacy issues in future discussions...”

Guido Gluschke,
Director, Institute for
Security and Safety
(ISS)

This section lists reflections from the Systems of Cyber Resilience: Electricity community on securing the electricity industry value chain. These reflections aim to support stakeholders across the electricity ecosystem when considering cybersecurity during the product lifecycle.

Increase ecosystem resiliency.

All security measures need to consider the different types, origins and dynamics of change of cyberthreats as well as the evolution of the industry, global environment, and, of course, increasingly sophisticated cyberattacker capabilities.

Embrace a collaborative approach to security.

A structured and collaborative approach needs to be adopted by the different entities to address cybersecurity-related challenges. Building effective collaboration and integration between the entities along the value chain requires clarity on roles and responsibilities. Asset owners, system integrators, product suppliers and asset (less) operators each have distinct and complementary responsibilities (and sometimes even competing interests which must be considered) when approaching security problems and ensuring the security of the overall system. Building trust and improving transparency are key considerations.

Prioritize the security of the supply chain and the value chain.

To be effective in securing the value chains, approaches much include both defense in depth (which covers the entire product lifecycle starting with design) and defense in breadth (which spans from the organization's suppliers to asset owner and eventually to system integrators and operators) strategies.

Balance product and systems level security requirements.

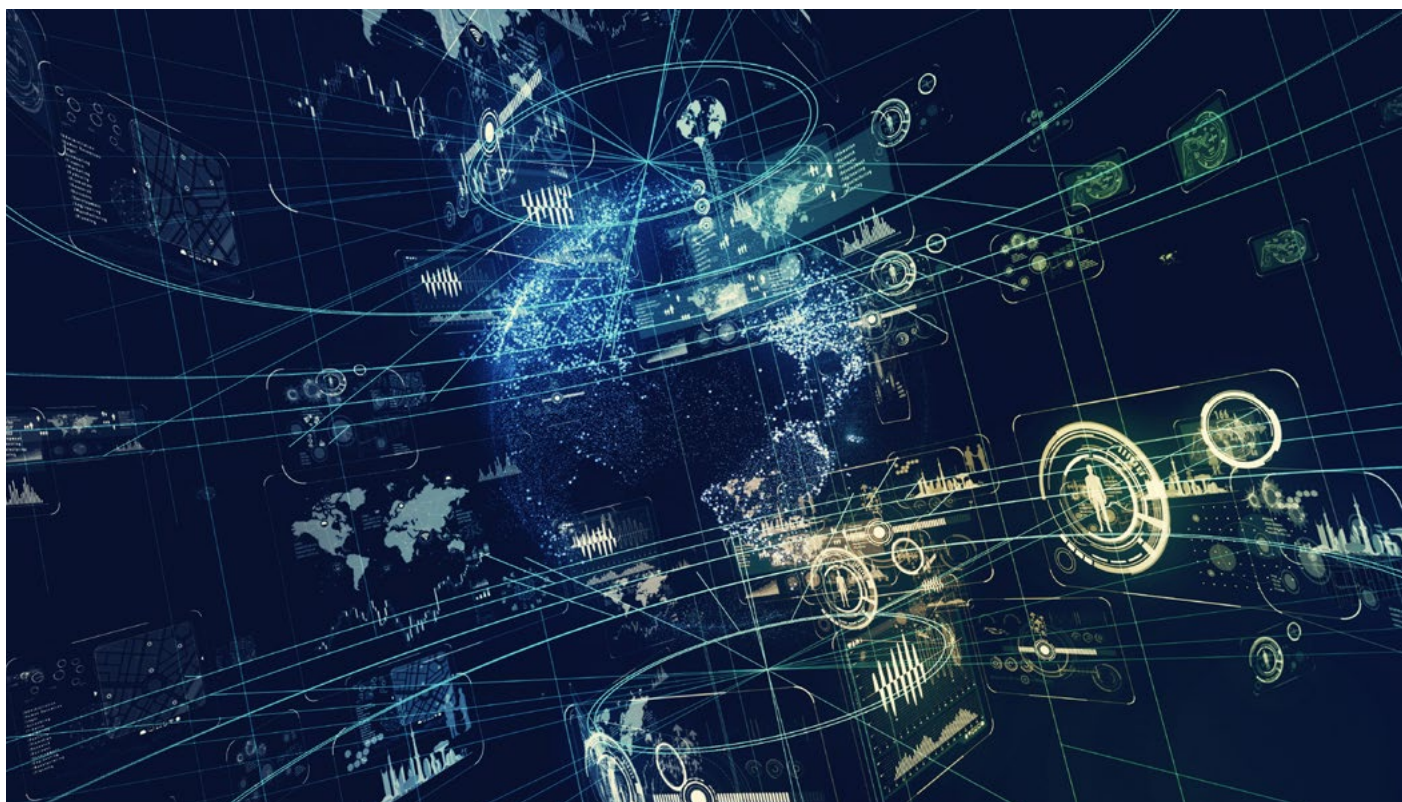
Organizations within the electricity industry cannot operate in silos. Effective and sustainable measures for protection go beyond the securing of individual products and systems. Product and systems-centric programmes must be established. These programmes require a common understanding and acceptance of the different stakeholders' responsibilities.

Adapt approaches for security and resilience.

Continuous evolution must be an integral part for any measures or programmes across the value chain. Such evolutions will need a commitment from asset owners to adapt updates to actual systems during their lifespan, and in such manner that resilience is guaranteed.

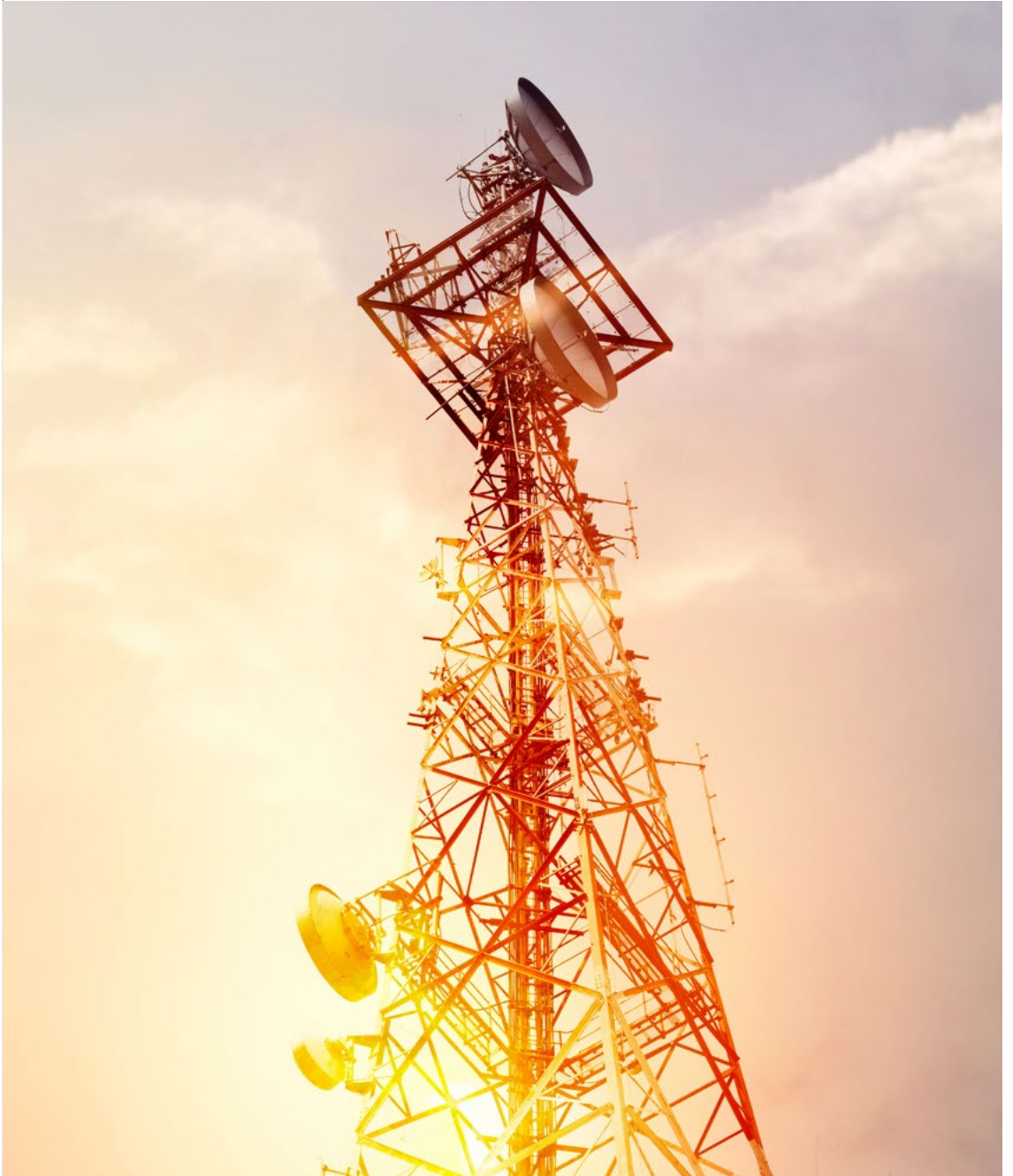
Understand and adjust the way complex technologies are acquired, integrated and operated.

Ensure a close dialogue between asset owner, product supplier and, where relevant, asset (less) operator and system integrator, on security during the procurement process. This is to ensure that the best possible security outcomes can be reflected during the tender processes and may sometimes require invoking dispensations in tenders. The need to adapt to how systems are operated will also need a trusted relationship among asset owners, operators and suppliers to find the optimum ways to address cybersecurity practice according to operation regimes. This trust is being built through transparency, sharing of insights, best practices, incidents and threat intelligence.



3

Appendices





Taxonomy

The definitions below establish a common ground and taxonomy with respect to language supporting this report.

Term	Description
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)
Value chain	The end-to-end lifecycle for hardware, product, system or services that delivers value to an entity. The end-to-end lifecycle goes through different phases, from the design, commission, operation until the end-of-life stage.
Supply chain	The supply chain represents the end-to-end processes and network of required entities for transforming raw materials into final products.
Product	A product, system, sub-system or component that is manufactured, developed or refined for use by other products.
System	An integration or combination of products and component subsystems into a whole in accordance with project specification.
Primary technology	Primary technology refers to assets such as transformers, circuit breakers and other products with expected life cycles of approximately 50 years. Note that the cybersecurity implications in this report are focused on the secondary technology (or operational technology).
Secondary technology: Operational technology (OT)	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems and physical access control mechanisms. ¹⁶ OT has an expected life cycle of between 5-10 years, much shorter than the primary technology which it monitors and manages. OT lifecycles tend to decrease when integrated with IT components.
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.



Electricity board principles for cyber resilience

The table below describes the board principles for cyber resilience for the electricity industry.¹⁴

Principle	Description
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. defense in depth strategies) with response and recovery capabilities.



Roles and responsibilities cheat sheet

The table lists the joint responsibilities and principles valid and applicable for all ecosystem stakeholders. Responsibility shifts after delivery from manufacturer to operator, from functional to operational security.

Responsibility	Description
<p>ALL Secure by design</p>	<ul style="list-style-type: none">- Secure your own infrastructure, services and environment to ensure the integrity and availability of business operations (on which others may critically rely).- Ensure your product or service output is secure in order not to become an infection point or attack vector to customers or downstream peers.- Develop your defenses based on the principle that your systems will be breached, ensure a breach can be timely detected and remediated, including proper communication to support trust in the ecosystem.
<p>ALL Supplier management</p>	<p>Procurement needs to build in security considerations from vendor selection through the terms and conditions in the contracts:</p> <ul style="list-style-type: none">- Develop sourcing decisions developed with multistakeholder input, e.g. include sourcing, legal, engineering, operations, product security and risk management.- Evaluate suppliers based on defined criteria and security requirements- Have inventory of components from upstream third-party suppliers.- Standard security terms and conditions are included in all requests for proposals (RFPs).- The security requirements for any and all proposed solutions should be clearly defined as part of the procurement process. Vendors which do not or cannot meet these standards should be excluded from consideration.- Buyer should have audit rights to assess vendor adherence to contractual commitments and requirements.
<p>ALL Adherence to best practices</p>	<ul style="list-style-type: none">- Implement security policies consistent with industry best practices, such as ISO 27001, ISO 20243, IEC 62443, NIST CSF, NIST Secure Software Development Framework (SSDF), Business Software Alliance Framework for Secure Software and set up business continuity and disaster recovery procedures.- Jointly push the development of standards and security requirements

Responsibility	Description
<p>ALL Training</p>	<ul style="list-style-type: none"> - Provide and support internal as well as ecosystem wide training opportunities. - Create mutual trust in the ecosystem, and secure economics of scale, through joint training, collaboration and knowledge sharing opportunities. - Support training offered to the involved players to develop and develop the required skills throughout the value chain.
<p>PRODUCT SUPPLIER Integrity and authenticity of parts</p>	<ul style="list-style-type: none"> - Ensure integrity and authenticity and security of components of the built products (see product security programme) - Offers ways to differentiate genuine from counterfeit products to support downstream peers securing their supply chain.
<p>PRODUCT SUPPLIER Product lifecycle support</p>	<ul style="list-style-type: none"> - Provide support to both primary and secondary technology from handover to stated end of product life.
<p>PRODUCT SUPPLIER Vulnerability and patch management</p>	<ul style="list-style-type: none"> - Provide vulnerability and patch management support (see product security programme) throughout the stated product life. - Respond to product vulnerability discoveries and notifications, including appropriately handling vulnerabilities in supplied third-party components. - Establish a coordinated disclosure and vulnerability handling processes. - Ensure production and deployment of security patches for products and/or mitigation.
<p>PRODUCT SUPPLIER Continued support</p>	<ul style="list-style-type: none"> - Capability to perform timely security incident response for products and services for confirmed security incidents.
<p>ASSET OWNER Agility and control</p>	<ul style="list-style-type: none"> - The infrastructure should be designed and set up to support automated testing and deployment of critical updates. - Keep accurate and complete inventory of all assets with plans to test and deploy updates at scale.



Cybersecurity programmes

With the challenges identified in the ecosystem, there is a tremendous opportunity to provide value to the existing model and roles by introducing programmes that drive accountability and ownership within the different phases of the value

chain. Each is centred around the perspectives of both suppliers (via the product security programme) and asset owners (via the supplier management programme and industrial security programme).

Product security programme

The product security programme is a process of managing cybersecurity risk to the vendor organization throughout the process of bringing products to market. The cost of bringing a product or solution to market is the driving factor. The result is that product companies have traditionally ignored the longer-term maintenance of the installed base of product from the standpoint of cybersecurity.

The challenge of product security is further exacerbated in the critical infrastructure space for three reasons: criticality of impact, operational lifecycle duration and limited possibility of delivering security updates. These challenges pose unique issues for both product supplier and asset owner as neither of them can be entirely successful in the cybersecurity space in a vacuum.

To address the challenge, product suppliers must adopt a product security programme to govern product development from the standpoint of security, as well as to manage the cyber and business risks from the design phase. From the standpoint of product development, there are a number of stage gates that are introduced to ensure cybersecurity quality and cybersecurity values are included:

- **Security requirements:** No backdoors, signed and validated code/firmware, all security compiler options enabled (DEP, ASLR, etc.), least privilege.
- **Lifetime security management:** Plan and design for the provision of security support throughout the stated product life.
- **Supplier management programme:** Product suppliers should maintain a supplier management programme for their upstream

supply chain to ensure a secure supply of parts and services used for product development and manufacturing (as described under supplier management programme below).

- **Design reviews:** Review and validate developer direction in architecture (all) for security quality. Feedback to net new requirements.
- **Threat modelling:** Evaluate and report theoretical attack vectors for exploiting the product/point system, system or system of system. Feedback to net new requirements.
- **Secure coding:** Ensure modern security coding practices are followed. Training may be required.
- **Static/dynamic code analysis:** Tools used to ensure that secure coding guidelines and practices are followed.
- **Testing:** Validates everything to this point (i.e. requirements, design, coding, etc.).
- **Secure manufacturing:** Building the product with security and integrity at the forefront.
- **Product security incident response team (PSIRT):** This is the function where the organization has the ability to ingest third-party information regarding product security integrity. A PSIRT capability represents a large mitigating risk factor for vendors and is often the first interaction between a vendor and third parties when considering the disclosure and vulnerability management processes.

The IEC 62443 standard clarifies further the responsibilities of all involved parties and should be applied across the industry.

Supplier management programme

While product suppliers are responsible for bringing products to the market which adhere to adequate cybersecurity standards, they also need to remain profitable. Cybersecurity is a necessary cost avoidance requirement that requires adequate funding. The market has to recognize its value and be willing to incorporate it in the overall process in the same manner as other compulsory requirements related to safety or sustainability for instance. In the absence of a regulatory mandate (even if this is changing in many countries), products with poor cybersecurity features may likely enter the market, due to price pressures, increasing ecosystem-wide exposure to cyberattacks. Compensating measures may be deployed afterwards by asset owners and/or system integrators, with increased complexity, less effectiveness and at a higher cost.

When buying products or services, asset owners and product suppliers (for their upstream supply chain) need to perform a risk-based approach, by including standard cybersecurity requirements in the tender process and ensure that they are met by all potential bidders before their offers are evaluated by their procurement team, weighing in the risk score along with other criteria. Moreover, considering the cascading effects cyber risks might have on the entire value chain, vendor evaluation processes across the entire ecosystem shall take into consideration the management of cyber risks coming from the supply chain by prioritizing products (including raw components) and suppliers that have internally adopted holistic and robust practices to cybersecurity, and by ensuring that residual risks are identified and communicated to the executive committee and board.

Industrial security programme

The industrial security programme is a concept of managing cybersecurity risk to the asset owner organization starting from the design phase as per the E2: Resilience by design principle,¹⁷ throughout the process of operating an industrial environment. For many organizations, such practice may well be included in the overall cybersecurity programme. The purpose of creating an industrial cybersecurity programme is to right size the investments in governance and cybersecurity controls and adhere to the defined enterprise's risk tolerance.

Balanced security

For industrial environments, there is a core concept of a balanced security programme. This is a concept that closely mirrors technical controls (i.e. firewall rules, file permissions, etc.) to non-technical controls (i.e. policy, procedure, guidelines, etc. general governance). This concept reinforces human behaviour to align with technical direction, serving to shift the overall maturity and culture of the environment. Security programmes that are not balanced often lead to a false sense of security. For example, an attack vector exists where technical

controls can be bypassed by exploiting human beings who are not properly trained and controlled by governance mechanisms. The inverse can also prove true.

Secure product in secure environment

It is often reported that cybersecurity is a "team sport" and nowhere is that truer than in critical infrastructure sectors. Context is needed to ensure the end-to-end security of systems is designed into the design phase and maintained throughout their lifecycles. This disparity in available features and capabilities inherent in products versus their implementation drives a divergence between the vendors and asset owners. Additionally, even if the vendor cybersecurity value has been provided and implemented by the asset owner, it does not equate to a secure system. The completion of a defense in depth strategy is a prerequisite to ensure a secure power system. This further underscores the need for balanced security programmes, as well as the transparency and collaboration of vendors, system integrators, asset owners and asset (less) operators.

Acknowledgements

The World Economic Forum thanks the following individuals for contributions that led to the development of this report.

System of Cyber Resilience: Electricity Co-Chairs

Pierre-Alain Graf – Senior Vice-President, Global Security, Hitachi ABB Power Grids, Switzerland

Rosa Kariger – Global Chief Information Security Officer, Iberdrola, Spain

System of Cyber Resilience: Electricity Community

Adani Group, India - Ashtad Engineer

Argonne National Laboratory, USA – Scott Pinkerton

Avangrid, USA – Felicia Brown

Australian Energy Market Operator, Australia – Tim Daly

Centrica, United Kingdom – Dexter Casey

Consolidated Edison, USA – Mikhail Falkovich

Cybersecurity and Infrastructure Security Agency, USA – Robert Watson

Edison Electric Institute (EEI), USA – David Batz

EDP – Energias de Portugal, Portugal - Paulo Moniz

Eletrobras, Brazil – Alexandre Albuquerque Faustino

Electric Power Research Institute, USA – Candace Suh-Lee, Matt Wakefield

Enel, Italy – Mario Bocchiola, Francesco Ciancarelli, Aniello Gentile, Yuri G. Rassega

ENGIE Laborelec, Belgium – Olivier Vandelaer

European Cyber Security Organisation, Belgium – Nina Olesen, Luigi Rebuffi

European Network of Transmission System Operators for Electricity (ENTSO-E), Belgium – Keith Buzzard

European Union Agency for the Cooperation of Energy Regulators, Sloveni – Stefano Bracco

Fortinet, USA – Phil Quade

Fortum, Finland – Juha Harkonen

GE Renewable Energy, France – Cole Sinkford

Hydro Québec, Canada – Alain Vallières

Iberdrola, Spain – Agustin Valencia Gil-Ortega

IBM Corporation, USA – Priscilla Koepke

Institute for Security and Safety (ISS), Germany – Guido Gluschke, Swantje Westpfahl

Kudelski Group, Switzerland – Brecht Wyseur

Landis+Gyr, Switzerland – Bodo Zeug

MIT - Sloan School of Management, USA – Stuart Madnick

National Grid Group, United Kingdom – Philip Tonkin

National Association of Regulatory Utility Commissioners (NARUC), USA – Lynn Costantini

Naturgy, Spain – Jesús Sánchez

Netz Niederösterreich, Austria – Maximilian Urban

North American Electric Reliability Corporation (NERC), USA – Manny Cancel

Norwegian Energy Regulatory Authority, Norway – Øyvind A. Arntzen Toftegaard

Office of Gas and Electricity Markets (Ofgem), United Kingdom – Mohammed Zumla

Ørsted, Denmark – Martin Knudsen

Power Authority of the State of New York, USA – Kenneth Carnes

Saxion University of Applied Sciences, Netherlands – Johan Rambli

Schneider-Electric, France – Christophe Blassiau

Sempra Energy, USA – Eric Trapp

Siemens, Germany – Michael Deckert, Kai Hermsen, Leo Simonovich

Singapore Power Group (SP Group), Singapore – Shih Hsien Lim

Southern Company, USA – Tom Wilson

SV Energy, Switzerland – Vlada Spasic

Tech Mahindra Limited, India – Dhaval Bhatt

Tennessee Valley Authority, USA – Andrea Brackett, Jeremy Fisher

The Chertoff Group, USA – Michael Chertoff, David London

Viccon Consulting, Germany – Julia Fuller

The World Economic Forum also wishes to acknowledge the contributions of Stefan Frei and Bradford Hegrat from Accenture and Roman Hagen from Pobos Consulting, as well as thank Stephan Lechner, Director of Euratom Safeguards and Cybersecurity Coordinator with the Directorate-General for Energy at the European Commission, for his feedback.

World Economic Forum team

Louise Anderson – Community Lead, Electricity Industry

Filipe Beato – Project Lead of Cybersecurity Industry Solutions, Centre for Cybersecurity

Georges De Moura – Head of Industry Solutions, Centre for Cybersecurity

Kristen Panerali – Head of Electricity Industry

Endnotes

1. World Economic Forum, *Ecosystem-wide collaboration principle in Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards*, January 2019, http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf.
2. World Economic Forum, *Cyber Resilience in the Electricity Industry: Analysis and Recommendations on Regulatory Practices for the Public and Private Sectors*, July 2020, http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem_Policy_makers_2020.pdf.
3. Helbing, Dirk, "Globally networked risks and how to respond", *Nature*, vol. 497, 2 May 2013.
4. "Significant cyber Incidents", Center for Strategic & International Studies (CSIS), 2020, <https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents>.
5. World Economic Forum, *Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards*, January 2019, http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf.
6. "Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models", International Electrotechnical Commission (IEC), July 2009, https://webstore.iec.ch/preview/info_iec62443-1-1%7Bed1.0%7Den.pdf.
7. International Electrotechnical Commission (IEC), 62443 series, <https://webstore.iec.ch/searchform&q=62443>.
8. World Economic Forum, *Cyber Resilience in the Electricity Ecosystem: Playbook for Boards and Cybersecurity Officers*, June 2020, http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem_Playbook_for_Boards_and_Cybersecurity_Officers_2020.pdf.
9. "ISO/IEC 27001: Information Security Management", ISO, 22 June 2020, <https://www.iso.org/isoiec-27001-information-security.html>.
10. "ISO/IEC 20243-1:2018 Information technology – Mitigating maliciously tainted and counterfeit products – Part 1", ISO, <https://www.iso.org/standard/74399.html>.
11. International Electrotechnical Commission (IEC), 62443 series, <https://webstore.iec.ch/searchform&q=62443>.
12. National Institute of Standards and Technology - Cybersecurity Framework v1.1, April 2018. <https://www.nist.gov/cyberframework>.
13. Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF), 23 April 2020. <https://csrc.nist.gov/publications/detail/white-paper/2020/04/23/mitigating-risk-of-software-vulnerabilities-with-ssdf/final>.
14. Business Software Alliance Framework for Secure Software, 1 May 2019, <https://www.bsa.org/news-events/media/bsa-releases-framework-for-secure-software>.
15. World Economic Forum, *Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards*, January 2019, http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf.
16. National Institute of Standards and Technology, US Department of Commerce, <https://csrc.nist.gov/glossary/term/operational-technology>.
17. World Economic Forum, *Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards*, January 2019, http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf.
18. Ibid.



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