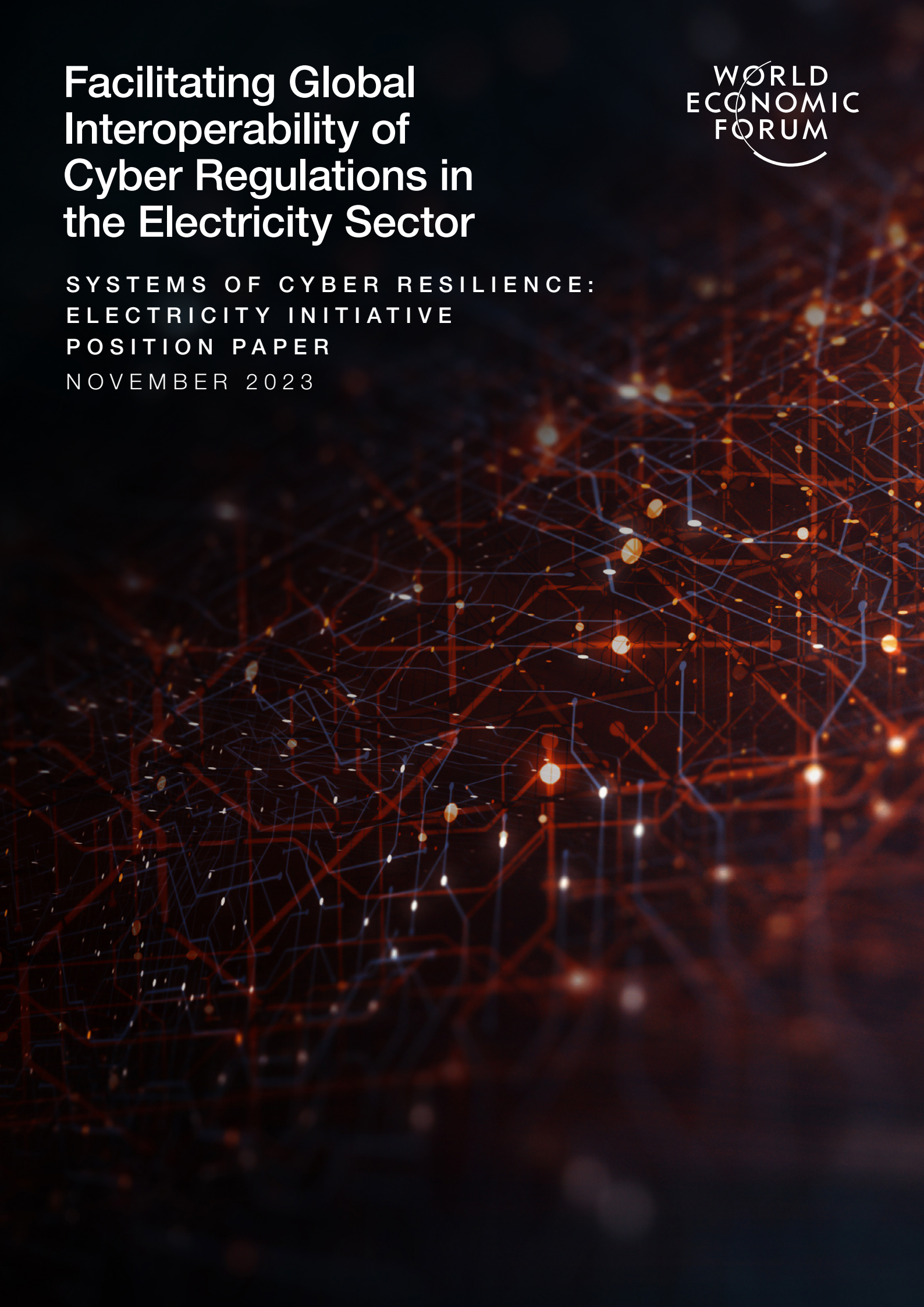
Facilitating Global Interoperability of Cyber Regulations in the Electricity Sector

WORLD ECONOMIC FORUM

SYSTEMS OF CYBER RESILIENCE: ELECTRICITY INITIATIVE
POSITION PAPER

NOVEMBER 2023



Images: Getty Images

Contents

Introduction

In today's interconnected world, the electricity sector stands as a cornerstone of societal functioning, powering industries, homes and critical infrastructure. As power systems go through rapid digital transformation, the critical link between cybersecurity and the energy landscape becomes increasingly evident. The need for global interoperability in cyber regulations in the electricity sector has become paramount.

The evolution of technology has significantly reshaped the electricity industry, ushering in smarter grids, integration of renewable energy and improved operational efficiencies. However, this evolution presents a new set of challenges, particularly in safeguarding these intricate systems from cyber threats. The increasing interdependencies among power systems across borders and the growing sophistication of cyberattacks underscore the importance of a harmonized, global approach to cybersecurity regulations in the electricity sector.

This position paper from the Systems of Cyber Resilience: Electricity (SCRE) initiative aims to consolidate a cohesive stance from the electricity sector on cybersecurity. It advocates for interoperability among nations to cultivate a cybersecure, resilient and standardized approach around the world. By scrutinizing the current landscape of cyber regulations, the paper endeavours to tackle existing gaps and complexities while proposing collective positions to standardize cybersecurity practices across diverse regulatory environments. Its objective is to champion international cooperation, mutual understanding and the adoption of common standards to fortify the electricity sector against emerging cyber threats while encouraging innovation and growth.

Ultimately, this position paper strives to contribute to the ongoing discourse on harmonization of regulations to nurture a secure, interoperable and resilient global electricity ecosystem, ensuring a reliable and safe energy supply for the world's population in an increasingly digitalized world.

The Systems of Cyber Resilience: Electricity Initiative

Since 2018, the World Economic Forum's Systems of Cyber Resilience: Electricity (SCRE) initiative has brought together representatives of over 60 electricity utilities, energy service providers, regulatory bodies and other pertinent organizations worldwide. Their efforts aim to achieve cooperation and fortify a cyber resilient electricity ecosystem. The SCRE stands out as the only global public-private partnership tailored for the electricity industry, where cybersecurity experts collaborate to enhance resilience across the electricity ecosystem.

> **It is a great opportunity to create a collaborative environment, focused on increasing global cyber resilience, based on the sharing of information, on the development of common initiatives, on the definition of principles and the alignment around them by the main actors of our industry.**
>
> Jesús Sánchez, Head of Global Cybersecurity, Naturgy

The Global Regulations Working Group

In September 2022, the SCRE community had identified global regulatory interoperability in the electricity sector as one of its key focus areas, and had set up the Global Regulations working group towards this end.

The working group addresses the intricate global regulatory challenges prevalent throughout the electricity sector, marked by fragmentation, inconsistency and sporadic conflicts. These regulatory barriers impede the attainment of global interoperability, resulting in increased costs, inefficiencies and missed opportunities. Resources are diverted to resolve regulatory issues rather than improving cybersecurity postures specific to the sector and its various organizations.

1 Current state of affairs

Regulators and government agencies responsible for establishing cybersecurity requirements in various industries worldwide often adopt different approaches to tackle similar cybersecurity challenges due to the lack of a global consensus. This results in complex, industry-agnostic, fragmented, inconsistent and occasionally conflicting sets of regulations. These regulations not only lack mutual interoperability but actively hinder it. The dynamic nature of cybersecurity threats further compounds the problem as regulators frequently tighten regulations in response. This forces organizations to allocate their limited resources towards compliance rather than concentrating on bolstering their cybersecurity defences.

Achieving regulatory interoperability may present challenges. Differences in cybersecurity standards, legal systems and national priorities among various jurisdictions can lead to conflicts and inconsistencies, making it difficult to establish and maintain interoperability over time. One notable challenge is the issue of data privacy laws, as different countries have unique data protection regulations tailored to their cultural, economic and political landscapes.

A similar challenge arises in incident reporting laws. For instance, some countries mandate the reporting of all data breaches, regardless of their severity, while others have thresholds for reporting based on the number of affected individuals or the level of harm. These differences can create difficulties in incident response and information sharing, particularly in cases where a breach spans multiple jurisdictions. Creating synergy among these diverse regulations is a complex and intricate process, especially given the rapid pace of digital innovation. This dynamic environment necessitates constant updates and revisions to ensure the regulations remain relevant and effective.

Moreover, there is a pressing concern to ensure that regulatory interoperability does not compromise national security. Nations must strike a balance between the need for a collective cybersecurity front and the need to protect their individual interests and security.

Despite the obstacles, solutions can be found. Initiatives such as working groups, international forums and collaborative agreements can play a pivotal role in promoting dialogue and establishing robust systems to monitor, evaluate and update regulatory frameworks. These mechanisms not only contribute to a more secure and resilient digital landscape but also foster innovation and growth.

Many regulators and government agencies have begun to recognize the need for regulatory harmonization and multiple efforts have been put into practice, such as the European Commission's Cyber Resilience Act (CRA) and the White House Office of the National Cyber Director (ONCD)'s request for information (RFI) on cybersecurity regulatory harmonization.

Simultaneously, several international dialogues are going on between states, such as the EU-US Cyber Dialogue, US-Japan Cyber Dialogue and France-United Kingdom Cyber Dialogue, in addition to regulatory reciprocity schemes such as the EU-US Data Privacy Framework, Singapore Cybersecurity Labelling Scheme and APEC Cross-Border Privacy Rules (CBPR) system.

While these efforts are in the right direction, they are far from achieving global interoperability and much work remains to be done by both the public and private sectors to build a more cyber resilient electricity ecosystem.

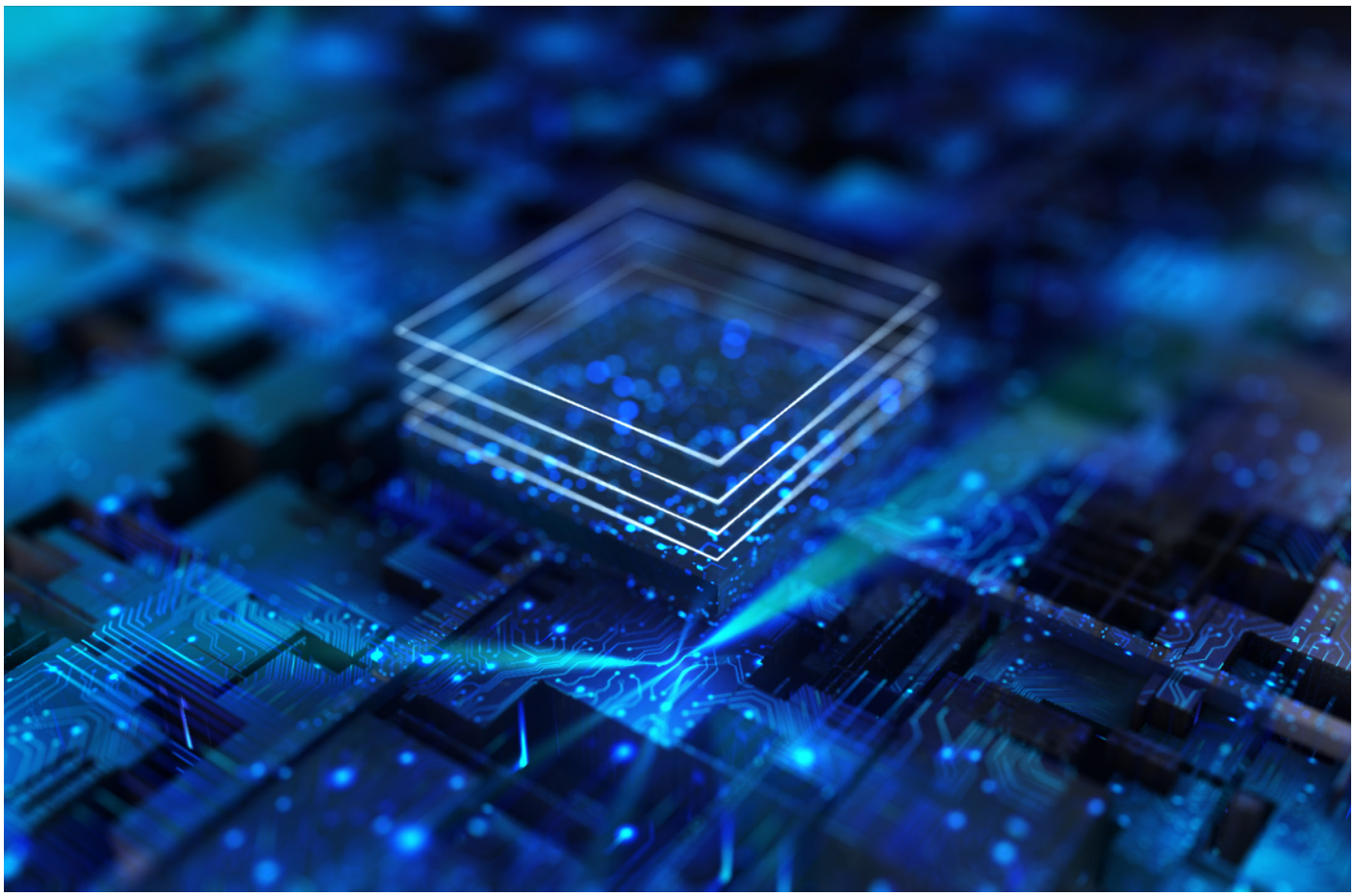
2 Importance of global regulatory interoperability

Aligning cybersecurity regulations globally ensures uniform cybersecurity practices, enabling companies operating across multiple regions to adhere to consistent standards. Harmonization reduces complexity and confusion, simplifying compliance efforts. Moreover, interoperability fosters enhanced collaboration and information sharing among various entities globally, facilitating joint efforts to combat cyber threats and exchange best practices.

A unified approach to cybersecurity regulations allows for a comprehensive understanding and management of risks, transcending different regions in the electricity industry. Standardizing regulations minimizes the complexity and costs of compliance for global corporations, eliminating the need to navigate a multitude of divergent regulations.

Global interoperability also leads to more robust defence mechanisms against cyber threats by enabling standardized cybersecurity practices, bolstering overall cyber resilience. A harmonized regulatory landscape fosters a fair playing field, encouraging innovation and the development of new cybersecurity technologies, free from varying compliance requirements.

In a cyber incident with global implications, uniform regulations enable a coordinated and efficient response across multiple jurisdictions, significantly mitigating the impact of such incidents. Given the global spread of supply chains, being able to rely on shared prevention, mitigation, information sharing and incident response practices will lead to a more sustainable, cyber resilient ecosystem worldwide. Ultimately, regulatory interoperability for cybersecurity around the world is imperative to foster a more secure digital and physical environment. It can align standards, promote collaboration, reduce costs and effectively manage and respond to cyber threats worldwide.



3 10 key themes for global regulatory interoperability

After analysing multiple regulations, the community has identified 10 key global regulatory themes for regulators to consider.

FIGURE 1 **Key themes for facilitating global interoperability of cyber regulations**

Source: SCRE Global Regulations working group.

4 Community position on the key themes

The SCRE Global Regulations working group has adopted the following positions on the 10 key global regulatory themes:

1. **Compliance and enforcement**: Global commitment to prioritize cybersecurity best practices over compliance. This implies a shift in mindset. Instead of merely meeting regulatory requirements, the focus is on prioritizing cybersecurity measures and protocols, sometimes beyond what is mandated. This approach emphasizes a proactive stance in ensuring a high level of cybersecurity rather than just checking the boxes to comply with regulations.

2. **Data protection and privacy**: Global commitment to support data protection and privacy regulations such as the General Data Protection Regulation (GDPR) of the European Union (EU). This commitment indicates a recognition of the importance of safeguarding sensitive information. Its ambit includes data privacy, ensuring the confidentiality, integrity and availability of data while aligning with the principles of privacy by design and default.

3. **Information sharing**: Global commitment to create and use a common information-sharing protocol and taxonomy worldwide, and to support the respective electricity information sharing and analysis centres (ISACs). Establishing a common information-sharing protocol and taxonomy globally is vital. It allows for consistent communication and collaboration among various stakeholders in the electricity sector, enhancing the ability to promptly identify and respond to threats. This commitment extends to supporting ISACs.

4. **Incident response and reporting**: Global commitment to adopt a common and efficient international incident reporting taxonomy and requirements. This commitment would ensure a standardized approach to reporting cybersecurity incidents. Such a taxonomy facilitates a better and shared understanding of the nature and impact of incidents, enabling a coordinated and timely response both within and across borders.

5. **Cybersecurity hygiene internal policies and procedures**: Global commitment to establish basic cyber hygiene principles specific to the electricity sector. This commitment would provide for a foundational level of security across all operations, reducing vulnerabilities, enhancing overall resilience and promoting a cybersecurity culture.

6. **Penetration testing**: Global commitment to regular internal penetration testing, which includes operational technology (OT) penetration testing. This allows for identifying and addressing potential weaknesses in systems and infrastructure, fortifying defences against cyber threats.

7. **Vulnerability disclosure and management**: Global commitment to sectorial vulnerability disclosure among closed groups of sector-specific, pre-authorized entities. This would foster a secure environment for information sharing within closed groups, allowing for proactive resolution of vulnerabilities without risking widespread exposure.

8. **Risk assessment and management**: Global commitment to applying risk assessment methodology consistently across information technology and operational technology environments. Applying consistent risk assessment methodology across IT and OT environments ensures a comprehensive understanding of potential risks, allowing for better-informed and timely decision-making regarding cybersecurity matters.

9. **Third-party risk management**: Global commitment that every organization in the supply chain must consider and be responsible for the cybersecurity of its scope of work. This would ensure a comprehensive approach to managing and mitigating risks associated with third-party involvement, securing and embracing ecosystem-wide resilience in the electricity sector.

10. **Adoption of existing international standards versus creation of unique, national (or regional) standards**: Global commitment to adoption of mature existing international standards such as ISO 27001 and the ISA/IEC 62443 series. Adopting existing international standards rather than creating unique regional standards would ensure a more universally accepted and harmonized approach to cybersecurity practices, leveraging established best practices. These standards should be updated when needed to allow for a harmonized approach to global regulations instead of frequent changes trying to account for evolving technologies and threats.

Conclusion

These collective commitments help regulators and other stakeholders in the electricity sector to share a common vision and understand what the electricity sector deems as important to be cyber resilient. Together, they embody the direction that the global community is heading towards.

Achieving global interoperability of cybersecurity regulations in the electricity sector demands a significant shift in approach. This transformation involves prioritizing security measures over mere regulatory compliance, taking a proactive stance to bolster cybersecurity standards and ensuring a higher level of protection. It requires the establishment of consistent risk evaluations, uniform standards and shared responsibility throughout the supply chain to strengthen the cybersecurity structure of the sector.

Additionally, the adoption of international standards and the promotion of secure information-sharing environments play a critical role. These actions encourage collaboration, innovation and effective strategies for responding to incidents worldwide. Support for standardized data protection laws, such as GDPR, highlights the commitment to safeguarding sensitive information and ensuring its integrity and confidentiality.

Ultimately, the journey towards a more secure and robust electricity sector involves aligning regulations, fostering collaboration and streamlining endeavours across diverse jurisdictions. This collective endeavour not only mitigates cyber threats but also promotes innovation and coordinated response mechanisms, thus establishing a resilient and unified global cybersecurity approach within the electricity industry.

Contributors

Lead author

Kesang Tashi Ukyab
Lead, Cyber Resilience, Electricity
World Economic Forum

World Economic Forum

Filipe Beato
Lead, Centre for Cybersecurity
World Economic Forum

SCRE Global Regulations Working Group leads

Christophe Blassiau
Senior Vice-President, Cybersecurity and Product Security; Global Chief Information Security Officer and Chief Product Security Officer, Schneider-Electric, France

Yuri G. Rassega
Chief Information Security Officer (CISO), Head, Cyber Security, Enel, Italy

SCRE community

Jose Manuel Alonso Barril
CISO, Iberdrola, Spain

Stefano Bracco
Knowledge Manager, ACER, Slovenia

Manny Cancel
SVP and CEO of E-ISAC, NERC, USA

Tim Conway
Director of SCADA and ICS, SANS Institute, USA

Sebastijan Cutura
Policy Manager, European Cyber Security Organisation, Belgium

Todd Davis
Head of Cyber Risk & Strategy Trends, Vestas, Denmark

Mark Antony D'Ambrogio
Regional Information Security Officer, Orsted, United Kingdom

Gabriele De Luca
Cybersecurity Expert, Enel, Italy

Joe Doetzl
CISO, Hitachi Energy, Switzerland

Morten Duus
Chief Information Security Officer, Vestas, Denmark

Mikhail Falkovich
Chief Information Security Officer, Consolidated Edison, USA

Peter Frøkjær
Senior Security Architect, Vestas, Denmark

Loris Gasparrini
Head of Cyber Security Standards and External Stakeholders, Enel, Italy

Agustín Valencia Gil-Ortega
OT Security Business Development, Fortinet, Spain

David Andres Hurtado
Head of OT Cybersecurity & Resilience, Naturgy, Spain

Frederik Lilleøre Jæger
Chief Information Security Officer, Orsted, Denmark

Rosa Kariger
Global Security Governance & Intelligence, Iberdrola, Spain

Jesus Sanchez Lopez
Head of Global Cybersecurity, Naturgy, Spain

Stuart Madnick
John Norris Maguire Professor of Information Technologies and Professor of Engineering Systems, MIT – Sloan School of Management, USA

Angelica Marotta
Affiliated Researcher, Cybersecurity, Massachusetts Institute of Technology, USA

Paulo Moniz
Director - Information Security and IT Risk, EDP - Energias de Portugal, Portugal

Charmaine Ng
Director, Digital Policy, Asia-Pacific, Schneider Electric, Singapore

Goran Novkovic
Head of Critical Infrastructure Protection, NEOM, Saudi Arabia

Ranjan Pal
Research Scientist, Cybersecurity, Massachusetts Institute of Technology (MIT), USA

Trevor Rudolph
Vice President, Global Digital Public Policy, Schneider Electric, USA

Gabriella Serino
Cyber Expert, Enel, Italy

Leo Simonovich
Vice President; Global Head, Industrial Cyber and Digital Security, Siemens Energy, USA

Henrik Loth Thiesen
Global Director of Information Security & Risk Management, Vestas, Denmark

Philip Tonkin
Chief of Staff, Dragos, United Kingdom

Maximilian Urban
Information Security Officer and Innovation Manager, Netz Niederösterreich, Austria

Swantje Westpfahl
CEO, Institute for Security and Safety (ISS), Germany

Tom Wilson
SVP & CISO, Southern Company, USA

Sander Zeijlemaker
Research Affiliate, Cybersecurity, Massachusetts Institute of Technology (MIT), USA

Annex 1: Related publications

1. Cyber Resilience in the Electricity Ecosystems: Principles and Guidance for Boards
https://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf

2. Cyber Resilience in the Electricity Industry: Analysis and Recommendations on Regulatory Practices for the Public and Private Sectors
https://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem_Policy_makers_2020.pdf

3. Cyber Resilience in the Electricity Ecosystems: Playbook for Boards and Cybersecurity Officers
https://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem_Playbook_for_Boards_and_Cybersecurity_Officers_2020.pdf

4. Cyber Resilience in the Electricity Ecosystems: Securing the Value Chain
https://www3.weforum.org/docs/WEF_Securing_the_Electricity_Value_Chain_2020.pdf

5. European Commission's Cybersecurity Package: Commentary in light of recent sophisticated supply chain attacks
https://www3.weforum.org/docs/WEF_Commentary_in_light_of_recent_sophisticated_supply_chain_attacks_2021.pdf

6. Response to the White House's Request on Harmonizing Cybersecurity Regulations https://www3.weforum.org/docs/WEF_Response_to_the_White_House%E2%80%99s_Request_on_Harmonizing_Cybersecurity_Regulations_2023.pdf

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