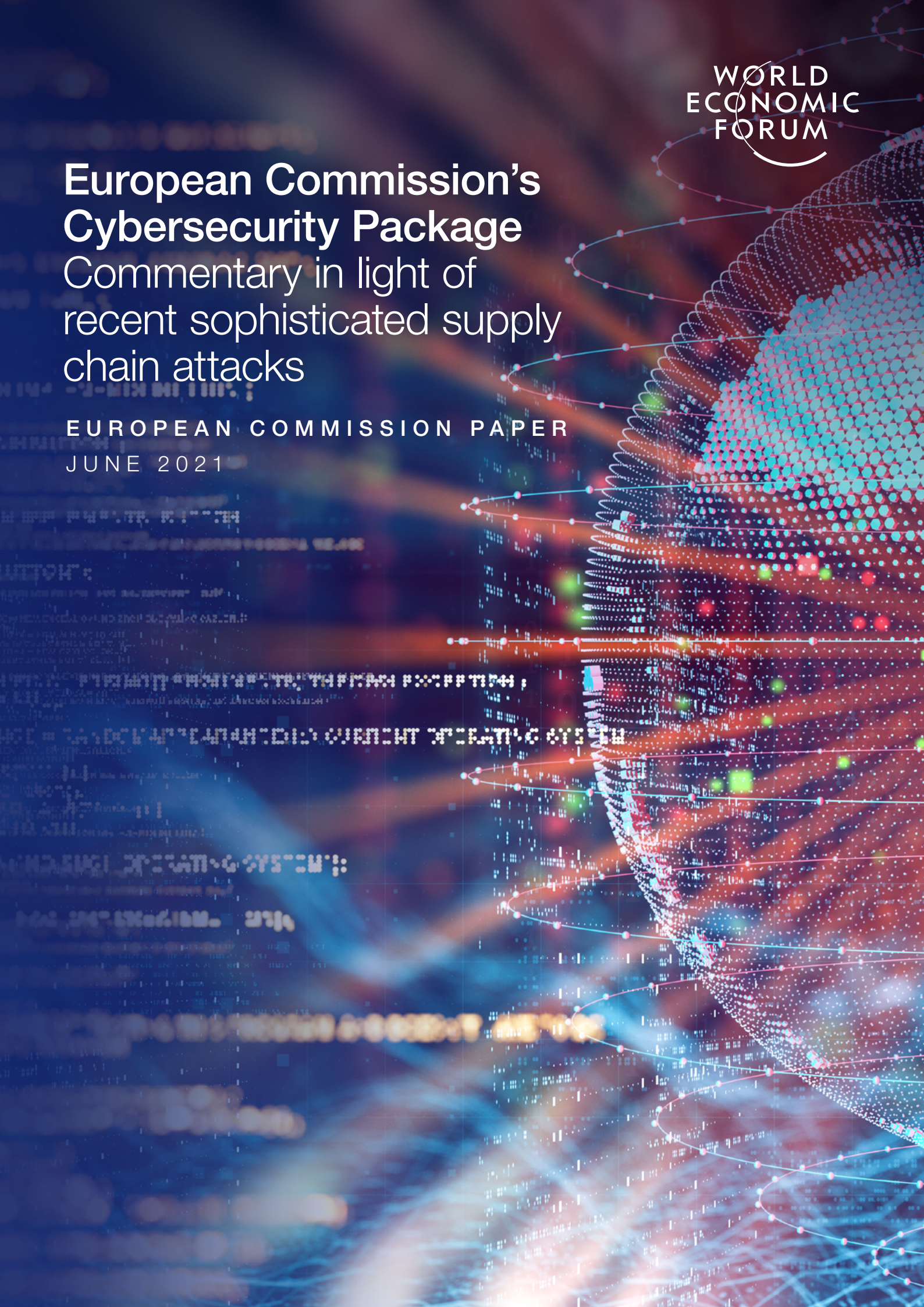


WORLD ECONOMIC FORUM

European Commission's Cybersecurity Package

Commentary in light of recent sophisticated supply chain attacks

EUROPEAN COMMISSION PAPER

JUNE 2021

Cover: GETTY/MF3d
Inside: all GETTY/Vasyl Dolmatov, Chainarong Prasertthai, Piranka, Gremlin, ArtistGNDphotography, Studio-fi

Contents

© 2021 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

On 16 December 2020, the European Commission (EC) adopted a cybersecurity and critical infrastructure package. The package contains a European Union (EU) Cybersecurity Strategy and two proposals for Directives on Security of Network and Information Security (NIS 2.0) and on the Resilience of Critical Entities (CER). These proposals have been sent for discussion, negotiation and approval by the European Council and European Parliament. Once the proposed directives have been agreed, they will need to be transposed into national law by the EU member states.

Meanwhile on the other side of the Atlantic, during December 2020, FireEye, a leading cybersecurity provider, uncovered a global cyber intrusion campaign that compromised software updates to the widely deployed SolarWinds IT management software product. This software update was downloaded by as many as 18,000 SolarWinds customers, spanning government agencies, critical infrastructure entities and private sector organizations. This campaign, which began as early as October 2019, has demonstrated patience, persistence, and complex tradecraft.[1]

While the EC Cybersecurity Package is welcomed and timely, the SolarWinds supply chain attack raises some important questions on the preparedness and systemic resilience of the energy sector. Are the proposed directives adequate to support critical energy infrastructure companies in mitigating the impact of systemic supply chain cyber attacks? Are there opportunities for further improvements to the draft directives based on the lessons learned from cyber attacks such as SolarWinds?

As well-documented by the World Economic Forum[2], critical energy infrastructure organizations must adapt quickly to the pace of change in the digital threat landscape, to improve detection, prevention, response and recovery from increasingly frequent, larger-scale and more sophisticated cyber attacks. Moreover, the digital nature of emerging technologies makes them intrinsically vulnerable to cyber attacks that can take a multitude of forms – from data theft and ransomware to the overtaking of systems with potentially large-scale harmful consequences.

The EC Cybersecurity Package is welcomed by the World Economic Forum's energy community and is seen as a positive step forward.

This paper focuses on opportunities for further improvements (both at the European and the global level), considering the strategic implications of sophisticated supply chain attacks such as SolarWinds. The recommendations are as follows:

1. **Establish a consistent approach across the EU member states through a NIS 2.0 regulation**. Promote a framework to support this regulation ensuring a common language and a consistent approach, in the context of a global network and a global supply chain.

2. **Apply a minimum baseline of cybersecurity to all small/micro enterprises (SMEs)** and, where needed, relevant EU member states could provide resources to support roll-out of these basic cybersecurity requirements.

3. **Increase the focus on incentivizing and rewarding good cybersecurity practices and behaviours** across all actors of the energy supply and value chain, as a complement to administrative sanctions.

4. **Ensure a consistent and harmonized approach across the EU through a CER regulation**. Align implementation roadmaps and enforcement of both NIS 2.0 and CER across member states.

5. **Include provisions for improving cross-border resilience**, e.g., threats and risks from/to non-EU member states, particularly with the neighbouring countries already involved in aggregated regional initiatives such as electricity market coupling projects.

6. **Improve management of concentration risk**. The interconnection of hardware, software and services (including cloud, internet service providers and the equipment supply chain) means that a highly prevalent service offering with a high degree of privilege can result in a potentially concentrated source of risk (e.g., SolarWinds), combined with the potential for compromise to have severe and systemic impacts. These risks cannot be addressed by organizations acting alone. Harmonized policy interventions are required across the EU that ensure critical shared resources (both sector-specific and cross-sectoral) and their key dependencies are identified, communicated, monitored and their risks appropriately managed.[3, 4]

7. **Promote use of common international information-sharing frameworks and best practices**. Common information-sharing frameworks can be developed globally to deliver situational awareness and facilitate real-time and automated defence in the face of increasingly complex technology environments, but also covering systemic component defects, severe climate events and terrorist threats to the energy system. These need to be effective across national boundaries as well as throughout value chains, recognizing divergent national security and regulatory regimes, and must be respectful of personal privacy.[5] The newly proposed EU-wide Cyber Shield and a Joint Cyber Unit should expand to cover broader resilience.

8. **Clarify the responsibility model for a resilient critical energy infrastructure value chain**. Policy-makers must shift focus beyond the supply chain to include the creation of a resilient value chain. Roles and responsibilities must be described and applied to enhance the resilience of this ecosystem (including regulators, procurement teams, manufacturers, system integrators, system operators, hardware and software suppliers, cloud providers).

9. **Foster cross-sector collaboration**. Policy-makers can play a key role in enhancing resilience across the energy ecosystem by facilitating cross-sector collaboration through regular dialogues and partnerships on enhancing the resilience of physical and virtual infrastructures, as well as IT and OT networks. By sharing successes and failures, as well as finding areas where cooperation is possible, a broader systemic resilience can be accelerated.

10. **Create an Energy Sector Cyber-Resilience Profile**. The EC could support a public-private collaboration led by the private sector to develop an Energy Sector Cyber-Resilience Profile, which aggregates cybersecurity regulatory requirements from several global regions, identifies where requirements are shared and describes how a firm can achieve compliance across multiple regions. Like the financial services sector, this profile should then be mapped to cybersecurity frameworks, thus reducing the burden of compliance for companies operating in multiple jurisdictions.

11 **Agree a common, minimum global baseline standard (or set of globally accepted principles) on cybersecurity for the energy sector**. Policy-makers and the global energy ecosystem should collaborate to agree a common, minimum global baseline standard or set of principles on the basic requirements to ensure cybersecurity within the energy sector. This work should reference and draw from existing widely used standards possible. This will be particularly useful for new entrants with low cyber maturity and low resources (e.g., community wind farm connections). For regulators, better alignment would also promote the adoption of best practices from one region to another.

12 **Shift the design and operation of a future integrated energy system, including its global network and value chain, and go beyond security to systemic resilience.** Policy-makers and regulators will play a key role in ensuring the resilience-based design and operation of a future integrated energy system. Global governance can evolve to ensure that systemic resilience is not compromised because of incompatible or diverging policy and regulatory requirements across interdependent sectors or borders. Cyber resilience shall be an integral element of a systemic resilience approach.

13 **Establish collective assistance capabilities**. Policy-makers and business leaders can prioritize interventions to improve the response from the ecosystem following a disruption to critical infrastructure. A long-standing tradition in the electricity sector is the practice of providing mutual aid in the event of a large-scale emergency. This aid can be extended to incorporate cyber mutual assistance.

14 **Build trust through ecosystem-wide cooperation**. Policy-makers and regulatory bodies can facilitate global conversations among regulators of critical infrastructure to share learnings from successes and failures. Build stronger cooperation between government agencies (including regulators) and energy companies by establishing and carefully curating regular cross-border dialogues on priority cyber resilience related topics. Regulators should be able to leverage industry and academic knowledge on cybersecurity challenges and solutions.

15 **Level up on cybersecurity understanding across the energy industry**. Policy-makers can encourage regulators, industry stakeholders and academics to take joint training courses designed to “level up” cybersecurity understanding across the industry. In addition, comprehensive regional cyber resilience exercises (expanding on Cyber Europe and GridEx) should be designed and executed in collaboration with regulators, industry stakeholders and academics representing multiple interconnected industries to build practical know-how on system restoration following a cybersecurity-related disruption.

1 A Resilient Future Energy System

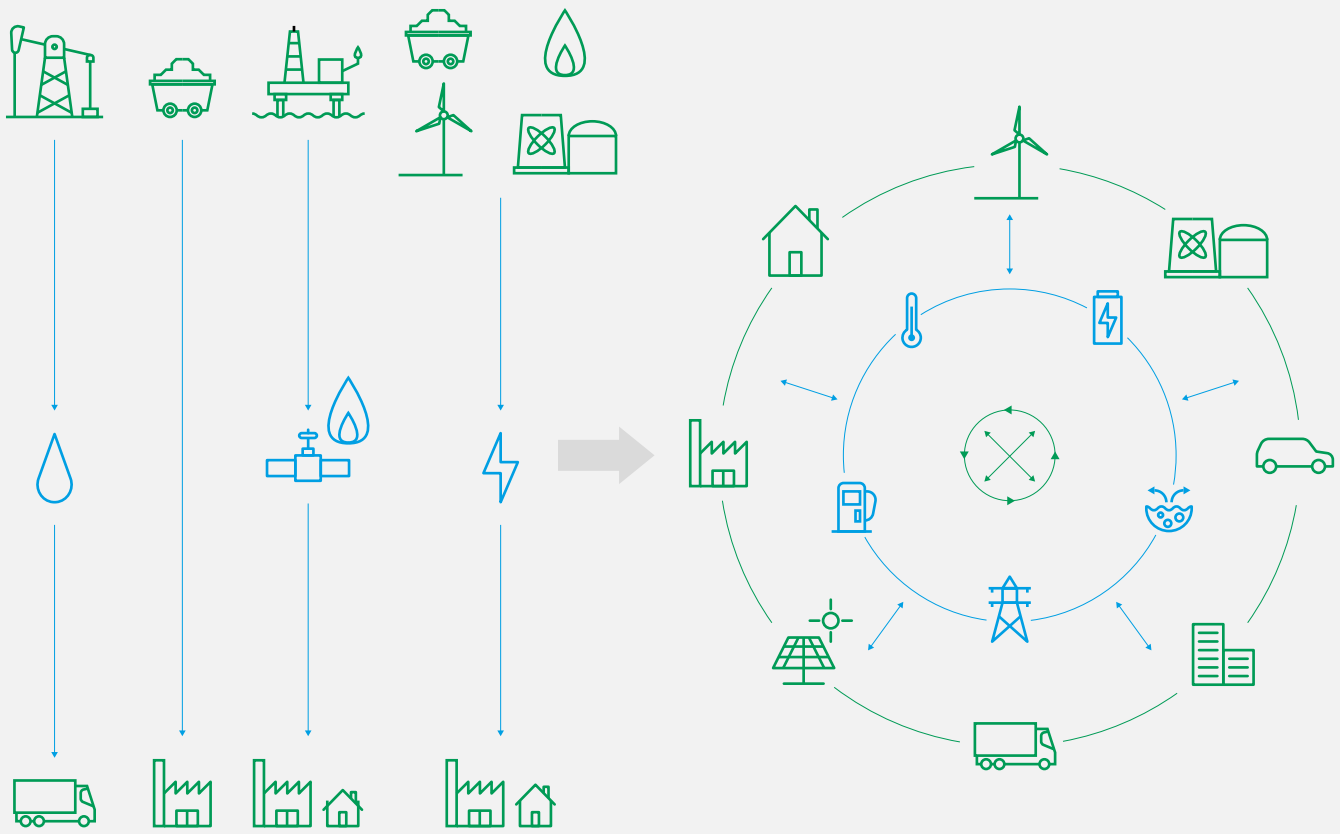
A future climate neutral integrated energy system will link energy sources, infrastructure and geographies to support the objectives of the European Green Deal.[6]

Driven by political, economic and environmental objectives, a climate-neutral integrated energy system will enable the coordination of energy systems operations and planning across multiple technology pathways and/or geographical scales. The European Single Market will be one of the foundations to reach that goal. The result will be reliable, resilient, sustainable and affordable energy services.

FIGURE 1 **European Commission's EU Energy System Integration Strategy**

The energy system today: linear and wasteful flows of energy, in one direction only

Future EU integrated energy system: energy flows between users and producers, reducing wasted resources and money



Adapted graphic from: European Commission

More than 60% of final energy demand in the EU will need to be electrified by 2050 but many scenarios have the share of electricity in the energy mix even higher.[7] Wind and solar will likely be the dominant form of generation – connected both at the transmission and, increasingly so, at the distribution level. Grids, networks and markets will need to adapt to the increasing number of power suppliers and the variability of the power supply.

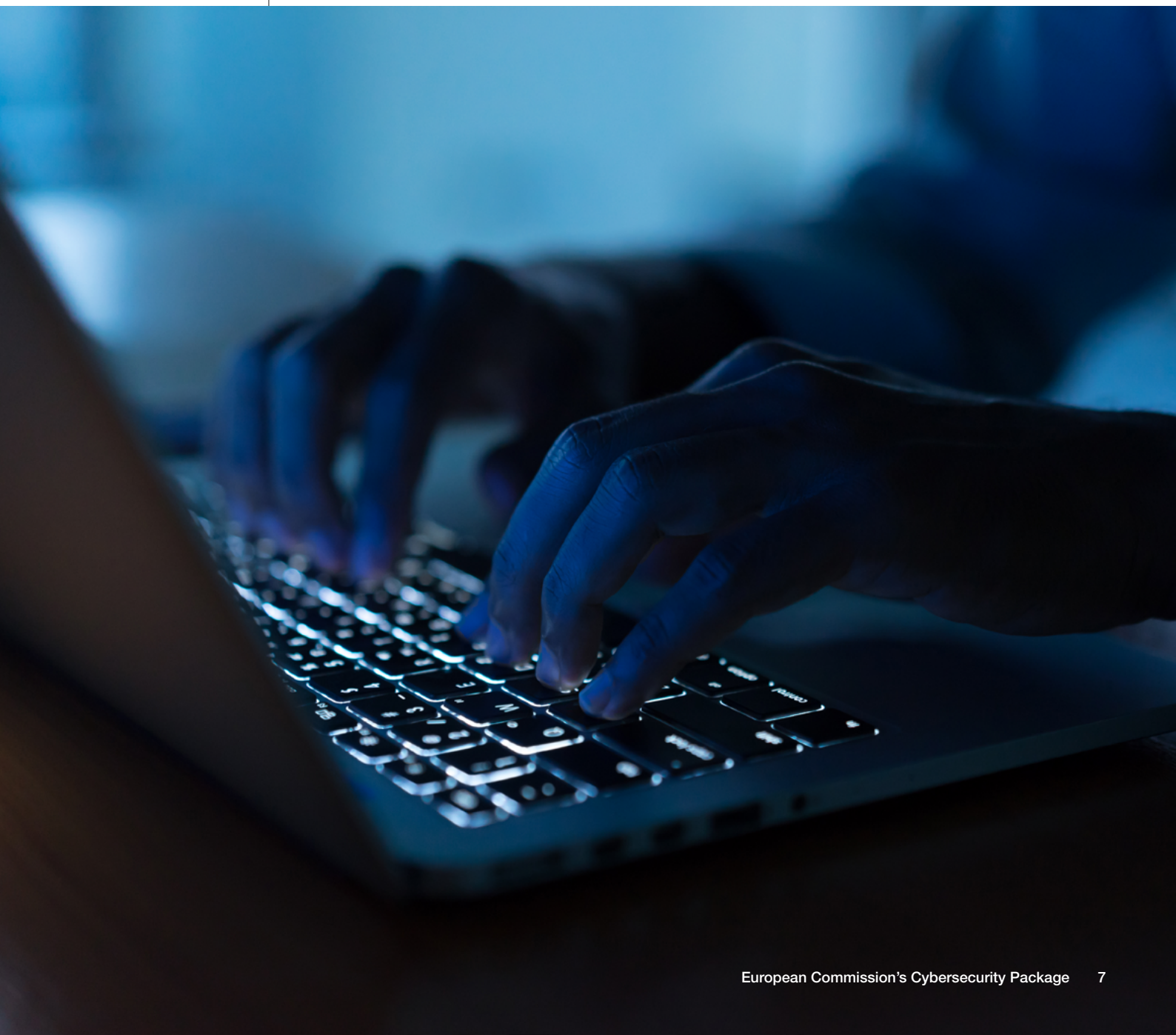
On the demand side, the electrification of transport, buildings and industry will introduce a myriad of grid-connected devices, counting on increased digitalization to optimize two-way flow of energy, data and money as consumers evolve into prosumers. Enhanced systemic efficiency and circularity across the energy system will also rely on improved sensing capabilities and communications. Different forms of energy storage will play an

important role, as will low carbon and renewable gases, including hydrogen, for the “hard-to-abate” sectors. At different times, supply will follow demand and demand will follow supply.

Infrastructure such as smart metering, electric vehicle (EV) charging stations will be ubiquitous, relying on digital technologies and telecommunications to optimize their interactions with each other and with power markets. The integrated energy system will interconnect and interact in real-time with other large-scale infrastructures including water, gas, transport and data and communications networks. A multitude of digital technologies will enhance real-time visibility of the energy system, as well as the ability to respond to disruptions.

This future integrated energy system must be designed and operated around resilience. Every interconnected entity and device will contribute to the resilience of the whole. Such a complex interdependent system must be able both to withstand and quickly bounce back from a variety of disruptions – from extreme weather events and component failure, to physical, cyber and hybrid attacks. IT and OT cyber resilience will not be a stand-alone topic but designed in as an important pillar of a broader systemic resilience. The ability to utilize multiple tools and tactics to respond to disruptions will be complemented by technologies such as artificial intelligence, predictive data analytics and quantum computing. As breakthrough technologies become faster, smarter and more widely applied, the pace of transformation will only accelerate. New commitments and partnerships will be necessary to move beyond technological optimism.[8]

A carbon-neutral integrated energy system will be transformational for society, improving the air quality of cities, safeguarding the environment and creating skilled jobs for the economy, while guaranteeing a reliable, affordable and sustainable supply of energy. Taking a strategic and systematic approach to the resilience of this system from today will give businesses and citizens confidence in the energy system of tomorrow.



2 EU Cybersecurity Package

The EU Cybersecurity Package consists of three elements: EU Cybersecurity Strategy, and two proposals for Directives on Network and Information Security and on the Resilience of Critical Entities. Comments are provided on the two proposed directives, considering the SolarWinds supply chain attack.

Proposal for a Network and Information Security Directive: NIS 2.0

The NIS Directive was the first EU-wide law on cybersecurity and came into force in 2016 aiming to increase and level up the security of network and information systems across the EU. In view of the unprecedented digitalization in recent years, the feedback from member states and society, and the need for a more harmonized implementation across member states, the time has come to refresh it.

The following recommendations address potential improvements to the proposed NIS 2.0 directive, considering the SolarWinds attack.

Recommendation 1: **Establish a consistent approach across the EU member states through a NIS 2.0 regulation. Promote a framework to support this regulation ensuring a common language and a consistent approach, in the context of a global network and a global supply chain.**
One purpose of the NIS 2.0 proposed directive is to overcome the divergences in implementation of the original NIS 1.0 directive between the member states.[9] The fragmented implementation of NIS 1.0 affected the cross-border provision of services and the overall level of cyber resilience due to the application of different requirements, as well as differing approaches to the identification of operators of essential services (OES), of which energy companies are one sector.

The community believes that while the proposed NIS 2.0 is a positive evolution of NIS 1.0, it does not go far enough. A consistent approach to cybersecurity across the European (and indeed global) energy ecosystem will support improved prevention, detection, response and recovery capabilities. Additionally, a consistent EU-wide approach to the identification of critical national infrastructure components is required to ensure that cross-border risk aggregation is not hidden; to avoid concentrated risk associated with dependence on a small number of major IT/OT ecosystem providers and to reduce cascade risks associated with increased interdependence of IT-enabled business processes. The implementation of a regulation, instead of a directive, will ensure consistent application across the EU. This regulation should be supported by a high-level framework based on a risk management approach.

The supply chain of any essential or important entity operating in a member state may easily include products or services provided across borders. An effective NIS 2.0 approach to managing cybersecurity risks in the energy sector should be promoted to non-EU member states, and particularly the Energy Community and Transport Community Contracting Parties, for consideration and adoption.

Recommendation 2: **Apply a minimum baseline of cybersecurity to all small/micro enterprises (SMEs) and, where needed, relevant EU member states could provide resources to support roll-out of these basic cybersecurity requirements.**
Among the most important updates to NIS 2.0 is the scope inclusion of all medium-sized entities (more than 50 employees and annual turnover and/or annual balance sheet total is higher than €10 million), which were excluded from the previous version. It also provides a set of criteria for exceptional qualification regardless of the size, which allows some SMEs to be qualified in specific circumstances. The identification of small and

micro entities to be included in the scope of NIS 2.0 is complicated. A central body is necessary to identify this (e.g., the Commission and the Cooperation Group, should issue guidelines on the implementation of the criteria applicable to micro and small enterprises).[10]

The exclusion of small and micro entities, except for those who qualify exceptionally, may become a source of increased risk. In a future energy system, we can expect to see a myriad of SMEs connecting to grids and networks. These include renewable energy producers, aggregators, closed networks (micro-grids) and consumers (as prosumers through roof-top solar, storage capacity or electric vehicle chargers).[11] If an SME is digitally connected to an essential or important entity, it could become the source of a cyber attack which proliferates across the network, particularly in the case of a supply chain attack.

Applying a minimum baseline of cybersecurity to SMEs will result in a levelling up of security across the region. Where SMEs struggle with the implementation of these requirements, EU member states could make resources available to support. As an example, InvestEU is one of the programmes of the next EU budget (2021-2027), with pillars focused on small and medium businesses, as well as sustainable infrastructure and digitalization. A portion of this fund could be dedicated to promoting security and resilience.[12]

Recommendation 3: **Increase the focus on incentivizing and rewarding good cybersecurity practices and behaviours across all actors of the energy supply and value chain, as a complement to administrative sanctions.**
NIS 2.0 sees the introduction of more stringent supervision measures and enforcement. For example, a list of administrative sanctions, including fines for breach of the cybersecurity risk management and reporting obligations is established (up to €10,000,000 or up to 2% of the total world revenues of the affected organization).[13]

However, moving towards a complementary incentive-based system could result in a more resilient ecosystem, particularly for critical energy infrastructure. One option could be that the fines imposed for failing to meet the proposed NIS 2.0 requirements could be invested into specific resilience improvement measures for the ecosystem (without creating conflicting incentives – such as investment in compliance or other – and with regard to any insurance compensation). Alternatively, those fines could be used for financing – e.g., a national cybersecurity authority – ensuring that the beneficiary is not the entity responsible for applying the sanction. Beyond the sanctions, additional government and market incentives could help reward good behaviour and practices.

Critical Entities Resilience Directive

The EC proposed a new directive replacing Council Directive 2008/114/EC on the protection of European critical infrastructure applying to energy and transport. The new proposed directive is designed as a horizontal framework covering 10 sectors from energy to water, cross-sectorial interdependencies and improving resilience to not only man-made risks (attacks) but also natural disasters.

Recommendation 4: **Ensure a consistent and harmonized approach across the EU through a CER regulation. Align implementation roadmaps and enforcement of both NIS 2.0 and CER across member states.**
The CER is a cross-sectoral, cross-border horizontal resilience framework for critical entities, a necessary step in developing a resilient carbon-neutral integrated energy system. While a shift from ensuring resilience of critical infrastructure to critical entities is welcomed, the evolution requires a broader framework ensuring the resilience of an integrated energy system.

The CER aims to ensure closer alignment with the NIS 2.0 Directive. However, while both CER and NIS 2.0 are being proposed as directives, it will be up to the member states how they choose to interpret each directive and who they choose at the national level to ensure compliance. This approach increases the risk of uncoordinated implementation across member states, diminishing the desired outcomes.

In addition, the introduction of two new directives impacting on energy companies (both as essential entities and critical entities) increases the complexity of compliance, particularly those operating in more than one EU member state. As is well documented, compliance does not guarantee either security or resilience.[14] A lack of interoperability at an EU governance level could lead to a web of resilience-security-compliance requirements; and suboptimal resource usage as companies try to comply, while struggling with the shortage of cybersecurity specialists.

Recommendation 5: **Include provisions for improving cross-border resilience, e.g., threats and risks from/to non-EU member states, particularly with the neighbouring countries already involved in aggregated regional initiatives such as electricity market coupling projects.**
The CER does not provide detail on cross-border aspects with neighbouring non-EU member states. When it comes to system disruptions for critical entities utilizing interconnected infrastructure (e.g., energy, transport, communications, information systems or other networks), disruptions may cross “third-country borders” in the same way they cross member state borders. The COVID-19 pandemic was an example of this, as was the separation of continental Europe’s electricity system earlier in 2021. By including a provision for these non-member states, the directive will contribute to enhancing the resilience of the broader ecosystem.

3 A New Cybersecurity Landscape for Critical Infrastructure

The increasing digitalization of critical infrastructure sectors and associated industrial systems is changing the nature of cyber risks. The convergence of information technology (IT) and operational technology (OT) is adding increased connectivity to industrial control systems (ICSs) for critical infrastructure. This, compounded with the growth of the industrial internet of things (IIoT) and accompanying risks, is exposing organizations to a new and increasingly aggressive threat landscape, the impact of which has been demonstrated by recent sophisticated attacks:

SolarWinds supply chain attack

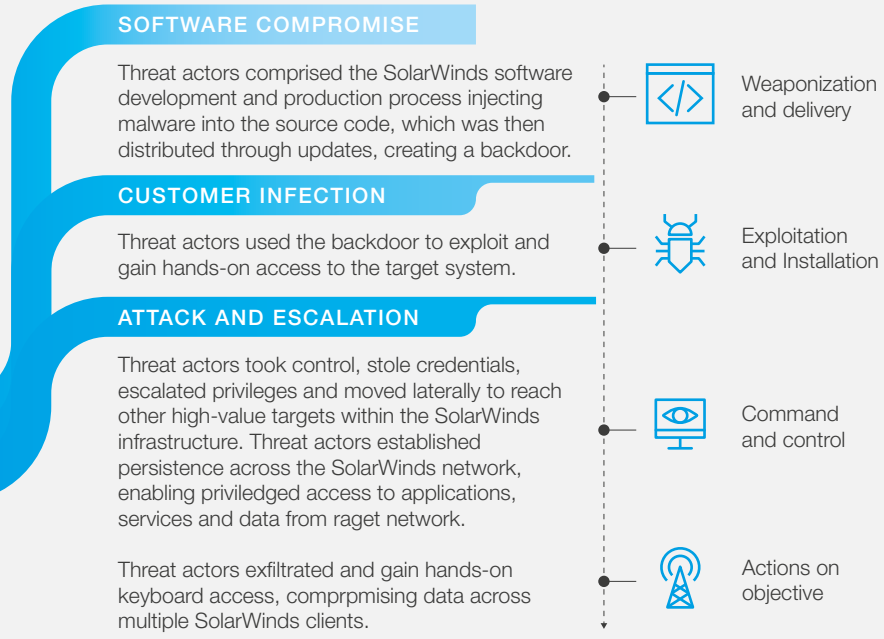
The cyber attack on SolarWinds Corp., a producer of network-management software, was unique in its complexity, breadth and success. During the development and production phase of the ICT Supply Chain Life Cycle[15], hackers planted malware in source code which translated into an infected software update that SolarWinds sent out to its customers, affecting as many as 18,000 organizations, including the United States Departments of Homeland Security, Commerce and Treasury. The threat actor remained in the network for months, leaving only after it had compromised the company's build servers and used its update process to infiltrate customer networks.

The technique of attacking an organization through a trusted vendor is not new. It happened in 2013 when hackers used the stolen credentials of a contractor working with Target Corp. to breach the retailer's computer network, and again in 2017, when hackers planted malicious code in the updates to a tax program sent out by a small Ukrainian company, Intellect Service (now Linkos Group), leading to the NotPetya cyber attack that crippled the computer networks of multinational companies worldwide.

FIGURE 2 **SolarWinds supply chain attack**

In December 2020, US-based security form **FireEye** announced **it had suffered a cybersecurity breach**. The initial point of compromise is now known to be the **breach of SolarWinds**, a supply-chain contact for FireEye and other organizations worldwide, including government agencies, universities and software and telecommunications companies.

The attack can be described by three phases



Source: Accenture and World Economic Forum

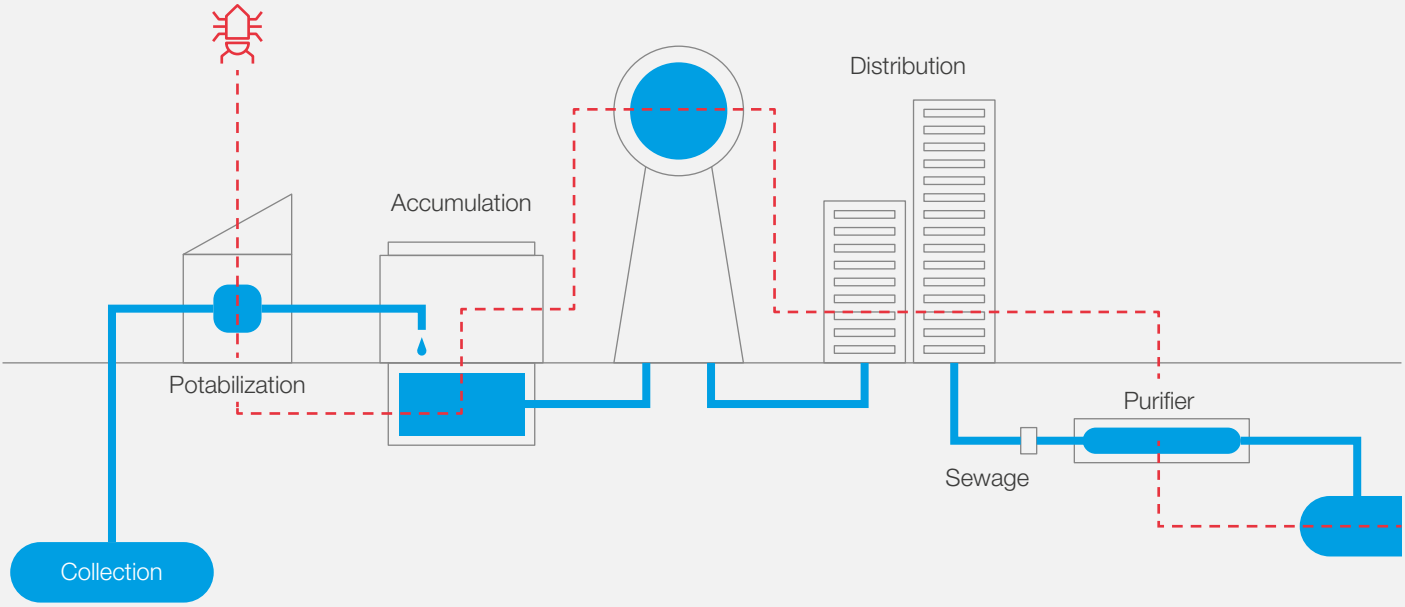
Florida water treatment plant attack

In February 2021, malicious actors tampered with a water treatment facility in Florida, in the US (see Figure 3). They accessed the Supervisory Control and Data Acquisition (SCADA) system, which enables the monitoring and control of all peripherals (e.g., actuators and sensors) managed by it. The attackers exploited this access to change the chemical levels of the water supply.

A supervisor observed the attack in real time (by watching the cursor moving on the screen) and corrected the changes.

A similar attack in 2020 was attempted on the command-and-control systems of Israel's wastewater treatment plants, pumping stations and sewage treatment facilities[16].

FIGURE 3 **Florida water treatment plant attack**



Adapted graphic from: Accenture

4 Learnings from Recent Sophisticated Attacks

The attacks described above represent the evolution of the type of threats that organizations deal with. The success of such events depends on shortcomings within the measures/controls in place to mitigate the threats. In the specific case of the attacks described above, there are three macro-areas for improvement:

Supply and value chain security
It is imperative to better understand the nature and extent of third-party cyber risks. SolarWinds was relatively unknown to most energy sector leaders before December 2020 yet 80% of the Fortune 500 companies were using its products.

The use of privileged management interfaces like SolarWinds requires a vendor-customer relationship that inherently enables a high degree of administrative control on the host network. However, with this degree of control comes the need for the following issues to be addressed:

- Critical infrastructure companies lack visibility of supplier's risk posture and practices
- Cyber hygiene practices are not enforced consistently across organizations
- Ensuring adequate risk assurance of all hardware, software and services is challenging given the complexity of different suppliers, system integrators, operators and their interconnectivity
- Complex, misaligned regulatory landscape prevents establishing a common baseline of cybersecurity practices across jurisdictions
- Organizations often lack effective capabilities to detect and prevent abnormal activities during the early stages of an attack

Enhanced visibility
Lessons learned from the above attacks highlight the lack of timely cyber situational awareness across the sectors. This creates opportunities for adversaries, including greater return on investment from their operations.

It is critical that organizations have the ability to continuously discover, inventory, manage and monitor all internet-facing assets, both on premises and in the cloud, to understand their overall organizational risk to newly discovered supply chain compromises or critical vulnerabilities.

Assuming compromise across our networks increases the importance of visibility and detection capabilities. Without appropriate insights into IT and OT networks and infrastructure, it is difficult to detect and respond to a compromise successfully, consequently also reducing the resilience of the organization.

Product assurance and development lifecycle practices
Enhanced hardware and software assurance and development lifecycle practices must be

developed across the entire ecosystem. For the SolarWinds attack, the company's code was compromised in the development and production process and the company was used as a host while the attacker used its update processes to infiltrate customer networks. While more stringent source-code policies and resilient-by-design product development is required, it will not solve the problem.

Whether deliberate or not, software flaws on the supply chain represent an attack vector that can create a type of "digital pandemic" – where the impact of one line of code can be felt across the entire economy. Another example would be the 2021 Microsoft Exchange Server data breach, which allowed attackers access to 7,000-8,000 servers in the UK, 30,000 US organizations, and many others.

Beyond this, the supply chain focus should extend to the value chain. Creating a resilient value chain for critical infrastructure requires setting the appropriate responsibilities across the end-to-end product lifecycle, including design, integration, commissioning, operation and retirement. As laid out by the World Economic Forum, roles and responsibilities across the value chain must be described and enforced to ensure the resilience of this ecosystem (including regulators, procurement teams, manufacturers, system integrators, system operators, hardware and software suppliers, and cloud providers).

Recommendations

6. **Improve management of concentration risk:**
The interconnection of hardware, software and services (including cloud, internet service providers and the equipment supply chain) means that a highly prevalent service offering with a high degree of privilege can result in a potentially concentrated source of risk (e.g., SolarWinds), combined with the potential for compromise to have severe and systemic impacts. These risks cannot be addressed by organizations acting alone. Harmonized policy interventions are required across the EU that ensure critical shared resources (both sector-specific and cross-sectoral) and their key dependencies are identified, communicated and monitored, and their risks appropriately managed.[17] [18]

7. **Promote use of common international information-sharing frameworks and best practices:**
Common information-sharing frameworks can be developed globally to deliver situational awareness and facilitate real-time and automated defence in the face of increasingly complex technology environments, but also covering systemic component defects, severe climate events and terrorist threats to the energy system. These must be effective across national boundaries as well as throughout value chains, recognizing divergent national security and regulatory regimes, and must be respectful of personal privacy.[19] The newly proposed EU-wide Cyber Shield and a Joint Cyber Unit should expand to cover broader resilience.

8. **Clarify the responsibility model for a resilient-critical energy infrastructure value chain:**
Policy-makers must shift focus beyond the supply chain to include the creation of a resilient value chain. Roles and responsibilities must be described and applied to enhance the resilience of this ecosystem (including regulators, procurement teams, manufacturers, system integrators, system operators, hardware and software suppliers, and cloud providers).

5 Learnings from Other Sectors on Energy-Related Policy

Numerous approaches implemented in different sectors have proven effective and could provide learning for the critical energy infrastructure sector.

Financial services sector

The development of cybersecurity rules and regulations across borders is not yet coordinated and harmonized in the financial services sector, even though the cyber threat is an international one. The sector developed the Financial Services Cybersecurity Profile, which aggregates cybersecurity regulatory requirements from several regions, identifies where requirements are shared and describes how a firm can achieve compliance across multiple regions. This profile can then be mapped to cybersecurity frameworks such as the National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO) to simplify the process for organizations trying to implement the controls. A similar initiative is needed for energy companies operating in multiple jurisdictions.

In the same way that the energy system is seeing an influx of new (and often small-scale) ecosystem stakeholders, financial technology (fintech) companies are a vital source of accelerated innovation-driven improvements for the financial services industry. The fragmentation of cybersecurity frameworks is a barrier for fintech companies to create trusted commercial partnerships with established firms. In addition to the limited resources of fintech companies, there is a lack of coherence across the sector as to which standard fintechs should implement.

The World Economic Forum's Fintech Cybersecurity Consortium was established in 2018 and aims to accelerate the adoption of a single, global, industry-wide baseline standard on cybersecurity for the financial services sector, providing much needed clarity for low-maturity, low-resource fintech firms."

Aviation sector

The International Civil Aviation Organization (ICAO) Assembly has recognized the need to boost resilience to cyber threats on a global scale and has identified actions to be taken by states and other stakeholders. The ICAO's efforts include calls to action to national governments through Assembly Resolutions (A39-19 in 2016[20] and A40-10 in 2019[21]), and an Aviation Cybersecurity Strategy[22] (2019), among others.

Simultaneously, with the establishment of a multidisciplinary Trust Framework Study Group (TFSG), the ICAO is developing a trust framework to support information exchange in a global, digitally connected environment. The ICAO Cybersecurity Action Plan has identified priorities, including working towards a common baseline for cybersecurity standards and recommended practices, and developing information-sharing platforms and mechanisms.

Cross-sector collaboration with at least the above sectors could accelerate the development of a common, minimum international baseline on cybersecurity for the critical energy infrastructure sectors, as well as enhance information-sharing.

Agriculture sector

Interestingly, cyber-resilience principles from the electricity sector[23] are being consulted by the European agriculture sector. The sector is exploring how to increase overall cyber resilience.

As an initial step, a voluntary agreement is in place between the main industry players to ensure a quicker adoption of the existing security requirements.

Recommendations from other sectors in energy policy

9. Foster cross-sector collaboration:
Policy-makers can play a key role in enhancing resilience across the energy ecosystem by facilitating cross-industry collaboration through regular dialogues and partnerships on enhancing the resilience of physical and virtual infrastructures, as well as IT and OT networks. By sharing successes and failures, as well as finding areas where cooperation is possible, a broader systemic resilience can be accelerated.

10. Create an Energy Sector Cyber-Resilience Profile:
The European Commission could support a public-private collaboration led by the private sector to develop an Energy Sector Cyber-Resilience Profile, which aggregates cybersecurity regulatory requirements from several global regions, identifies where requirements are shared and describes how a firm can achieve compliance in multiple regions. Like the financial services sector, this profile should then be mapped to cybersecurity frameworks, thus reducing the burden of compliance for companies operating in multiple jurisdictions.

11. Agree a common, minimum global baseline standard (or set of globally accepted principles) on cybersecurity for the energy sector:
Policy-makers and the global energy ecosystem should collaborate to agree a common, minimum global baseline standard or set of principles on the basic requirements to ensure cybersecurity within the energy sector. This work should reference and draw from existing widely used standards possible. This will be particularly useful for new entrants with low cyber maturity and low resources (e.g., community wind farm connections). For regulators, better alignment would also promote the adoption of best practices from one region to another.

6 Learnings from Physical Events that Can Increase Systemic Resilience

Traditionally, managing the risk of a major outage in the energy sector meant dealing with issues such as component failure, terrorism or inclement weather via robust mitigation and recovery plans. Tomorrow's integrated energy system will need to be able both to withstand and quickly bounce back from a variety of disruptions – including extreme weather events; component failures; physical, cyber and hybrid attacks; and supply chain disruptions.

Some recent events illustrate this point:

- While the world focused on the systemic threat posed by COVID-19, cybercriminals were ready to use the implications to their advantage. A significant increase in phishing emails (and other attack vectors) tried to capitalize on the increased attack surface due to the new volumes of remote connections, particularly within the energy sector.

- The European market integration project is the most ambitious multi-country power integration project in the world. However, during January 2021, the Continental Europe Synchronous Area was separated into two areas (the North-West area and the South-East area) due to cascaded trips of several transmission network elements. The European Transmission System Operators resolved the issue and resynchronized the continental Europe power system after about one hour. Due to the fast and coordinated approach, no major loss of load or damages were observed in the power system. Nonetheless, the incident was described as a "Scale 2" or "Extensive Incident".

- In the US, exceptionally cold weather in Texas in February 2021 resulted in extensive power outages affecting over 4 million customers. The weather conditions increased electricity demand, while a drop in natural gas production due to frozen wells resulted in generation outages. The impact in terms of outage duration and customers affected was greater than that of the rolling outages in California in 2020 due to wildfires.

- In March 2021, the Suez Canal was blocked for six days after a container ship became wedged across the waterway. This incident had a significant negative impact on trade (to the value of almost $10 billion) between Europe, Asia and the Middle East. Such disruptions have the potential to negatively impact the global supply chain (e.g., the timely availability of critical replacement assets or energy sources).

A coordinated approach to the resilient design and operation of the future integrated energy system is needed, including its global network and supply chain. Cybersecurity requirements must be incorporated into a broader systemic resilience approach for this integrated energy system, reflecting cross-sector and cross-border interdependencies.

When disruptions happen, as described above, stakeholders across the energy ecosystem should be ready and able to support each other as needed, including in the case of cyber attacks. Electricity companies have often assisted neighbouring countries physically after large-scale emergencies. A similar approach is required to assist recovery after a cyber attack. The US Electricity Subsector Coordinating Council's Cyber Mutual Assistance Program[24], which was developed to provide emergency cyber assistance within the electric power and natural gas industries, is a good example to build on.

Recommendations

12. **Shift the design and operation of a future integrated energy system, including its global network and value chain, and go beyond security to systemic resilience:**
Policy-makers and regulators will play a key role in ensuring the resilience-based design and operation of a future integrated energy system. Global governance can evolve to ensure that systemic resilience is not compromised because of incompatible or diverging policy and regulatory requirements in interdependent sectors or borders. Cyber resilience shall be an integral element of a systemic resilience approach.

13. **Establish collective assistance capabilities:**
Policy-makers and business leaders can prioritize interventions to improve the response from the ecosystem following a disruption to critical infrastructure. A long-standing tradition in the electricity sector is the practice of providing mutual aid in the event of a large-scale emergency. This aid can be extended to incorporate cyber-mutual assistance.

7 New Forms of Public-Private Interactions to Improve Systemic Resilience

Around the world, there are different models and approaches for governing cybersecurity of critical infrastructure. Very few attempt to deliver systemic resilience of critical energy infrastructure, and OT cybersecurity is not given adequate consideration.

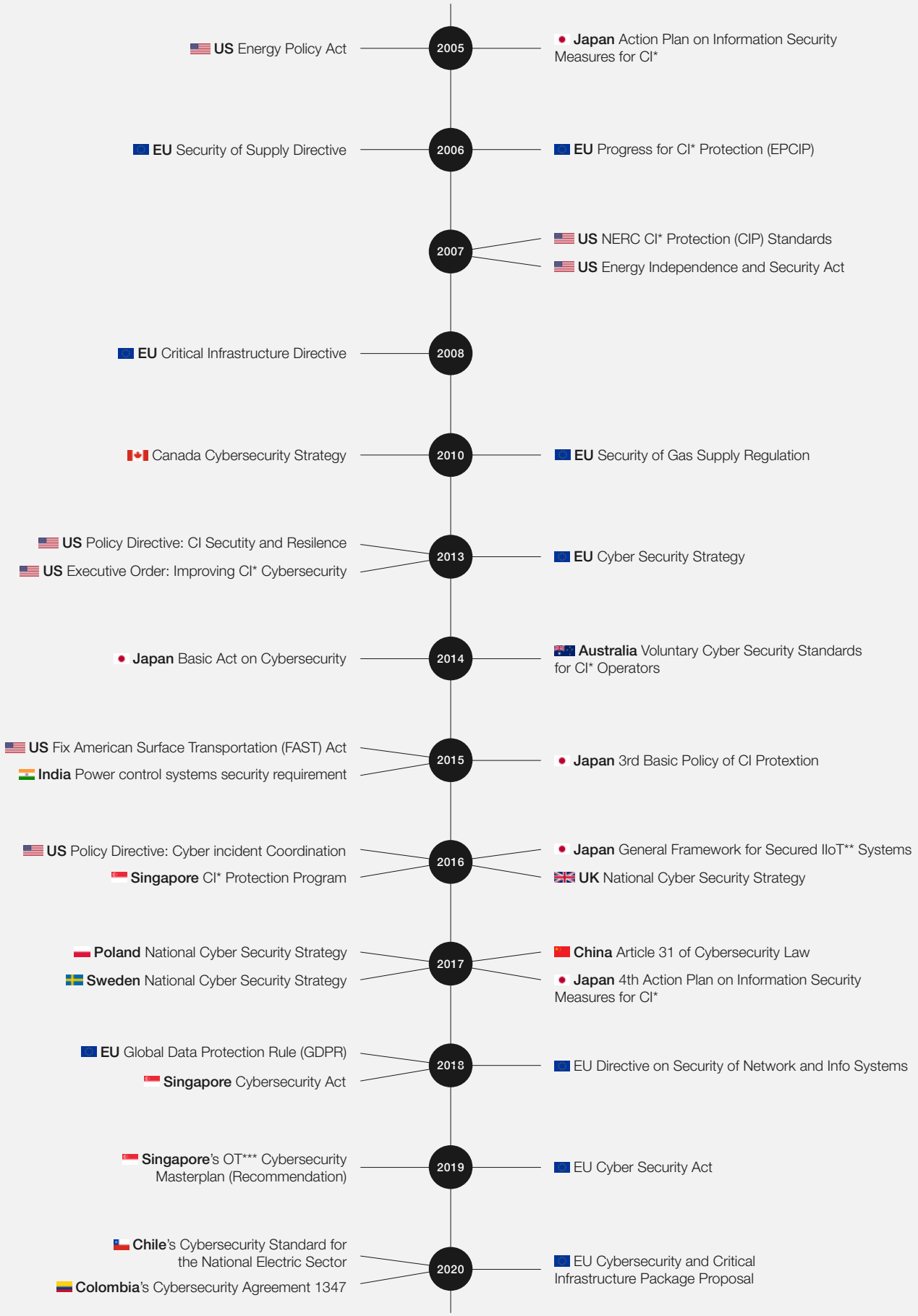
China is midway through building an extensive governance regime for cyberspace and ICT, a matrix of interlocking strategies, laws, regulations and standards covering rules from data protection to critical infrastructure[25].

In Singapore, the relationship between regulators and the critical infrastructure organizations is an excellent example of strong collaboration in the sector. Cybersecurity is a central tenet of the Smart Nation initiative,[26] with the governance model relying on trust-based cooperation between ecosystem stakeholders, and collaboration with other countries in the ASEAN region and more globally. A particular focus is placed on uplifting the cybersecurity posture across critical infrastructure operators through to SMEs. Interestingly, Singapore released an OT Cybersecurity Masterplan in 2019. [27]

In the UK, Ofgem, the regulatory authority, tries to strike a balance between the rigid requirements of NERC CIP and somewhat more high-level criteria applied in the EU. It leverages an outcomes-based framework and combines it with a risk-based approach. The outcomes-based framework developed by the National Cyber Security Centre is based on principles, objectives, and outcomes. Ofgem request those Operators of essential services, to use expert judgement whilst assessing against the outcomes, and where outcomes are not being fully achieved, to assess risks against these. Where risks are above tolerance, operators are encouraged to leverage from industry accepted practices where possible. Hence network and system cyber risks can be managed in an appropriate and proportionate manner. Additionally, Ofgem's "economic" regulations include a framework allowing for cyber-resilience investment during the current price control period.[28]

In 2020, a detailed comparison[29] was carried out on the regulatory approaches in the US and EU, detailing the highly prescriptive reliability standards from NERC CIP[30] in the US and the high-level frameworks common in the EU.

FIGURE 4 | **Global policy and regulatory landscape evolution**



*CI: Critical Infrastructure, **IIoT: Industrial Internet of Things, ***OT: Operational Technology

Source: Press releases, BCG and Accenture analysis

When it comes to interactions with regulators, energy companies struggle with a lack of coherence between directives and regulations in different jurisdictions; a focus on resource-intensive compliance; laws and penalties that disincentivize information-sharing; skills shortage; as well as not enough focus on OT cybersecurity. On the other hand, for some companies, cybersecurity budgets are dependent on compliance requirements.

Meanwhile, regulators are restricted in scope to their own geographies. The energy ecosystem is complicated and becoming more interconnected; conversations with industry are complex; finding a balance between legislation, regulation and standards or frameworks is challenging combined with differentiating between small and large companies while driving competition. Setting appropriate levels of cybersecurity investment for the industry is further complicated by understanding how to benchmark the benefits of those investments. Depending on the size of the country, cybersecurity may be one of many priorities and regulators may be operating without specialist knowledge.

Energy companies and regulators share several challenges, including how to fill the knowledge gap; how to find resources with knowledge of critical infrastructure and cybersecurity; and how to build greater trust and collaboration. Regional cyber-resilience exercises, involving multiple interdependent sectors from energy to water to telecommunications, focusing on how to efficiently recover after a cyber attack, are useful for this type of collaborative learning. Expanding the existing Cyber Europe programme from ENISA[31], and incorporating learnings from the US GridEx,[32] which simulates a cyber and physical attack on the grid, would be a good starting point.

Recommendations

14. Build trust through ecosystem-wide cooperation:
Policy-makers and regulatory bodies can facilitate global conversations among regulators of critical infrastructure to share learnings from successes and failures. Build stronger cooperation between government agencies (including regulators) and energy companies by establishing and carefully curating regular cross-border dialogues on priority cyber resilience related topics. Regulators should be able to leverage industry and academic knowledge on cybersecurity challenges and solutions.

15. Level up on cybersecurity understanding across the energy industry:
Policy-makers can encourage regulators, industry stakeholders and academics to take joint training courses designed to “level up” cybersecurity understanding across the industry. In addition, comprehensive regional cyber-resilience exercises (expanding on Cyber Europe and GridEx) should be designed and executed in collaboration with regulators, industry stakeholders and academics representing multiple interconnected industries to build practical know-how on system restoration after a cybersecurity-related disruption.

Annex

Regulatory element	Definition
Regulation	A regulation is a **binding legislative act**. It must be applied in **its entirety across the EU**.
Directive	A directive is a legislative act that sets out a **goal** that all EU countries must achieve. However, it is up to the **individual countries** to devise their own laws on how to reach these goals.
Policy	A policy is any **statement** of **general applicability** that aims to bring benefits to citizens, businesses and other stakeholders
Standard	Standards are technical specifications defining requirements for products, production processes, services or test methods. These specifications are **voluntary**.
Recommendation	A “recommendation” is **not binding** and does not have any legal consequences. A recommendation allows the institutions to make their views known and to suggest a line of action without imposing any legal obligation on those to whom it is addressed**.**

Acknowledgements

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

Leaders of the initiative
Michael Chertoff, Co-Founder and Chairman, The Chertoff Group

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

Rosa Kariger, Global Chief Information Security Officer, Iberdrola

Contributors

Adam Isles	Principal	The Chertoff Group
Agustin Valencia Gil-Ortega	Head of OT Cybersecurity	Iberdrola
Alexandre Albuquerque Faustino	Chief Information Officer	Centrais Elétricas Brasileiras SA - Eletrobras
Andrea Brackett	Vice-President and CISO	Tennessee Valley Authority
Aniello Gentile	Cybersecurity Manager	Enel
Ashtad Engineer	Head of Technology	Adani Group
Brecht Wyseur	Product Strategy, Internet of Things (IoT) Security	Kudelski Group
Brian Harrell	Vice-President and Chief Security Officer	Avangrid
Bruce Byrd	Executive Vice President, General Counsel	Palo Alto Networks
Candace Suh-Lee	Researcher	University of Nevada, Las Vegas
Christophe Blassiau	Senior Vice-President, Digital Security and Global CISO	Schneider-Electric
Cole Sinkford	CISO	GE Renewable Energy
Danielle Kriz	Senior Director, Global Policy Palo Alto Networks, USA	Palo Alto Networks
Dhaval Bhatt	Global Business Development Cybersecurity	Tech Mahindra Limited
Eric Trapp	Vice-President, Security and Technology	Sempra Energy
Guido Gluschke	Director	Institute for Security and Safety (ISS)
Ivan Dragnev	Cybersecurity Principal Technical Lead Europe	Electric Power Research Institute

Jeremy Fisher	Vice-President and Chief Information Officer	Tennessee Valley Authority
Jesús Sánchez	Chief Information Officer	Naturgy
Joanna Syrda	Assistant Professor of Economics	University of Bath
Johan Rambi	Faculty Instructor	Saxion University of Applied Sciences
Jordan Rahlwes	Head of Cybersecurity (DACH-Region)	ENGIE Laborelec
Julia Fuller	Chief Operating Officer	Viccon Consulting
Kai Hermsen	Global Coordinator for the Charter of Trust	Siemens AG
Keith Buzzard	CISO	European Network of Transmission System Operators for Electricity (ENTSO-E)
Kenneth Carnes	Cybersecurity Director	Tennessee Valley Authority
Leo Simonovich	Vice-President and Global Head, Industrial Cyber and Digital Security	Siemens Corporation
Loris Gasparrini	Head of Cybersecurity Standards and External Stakeholders	Enel
Lynn Costantini	Deputy Director, Center for Partnerships & Innovation	National Association of Regulatory Utility Commissioners
Maninder Singh Narang	Corporate Vice-President, Cybersecurity and Governance, Risk and Compliance Services	HCL Technologies Ltd
Manny Cancel	SVP and CEO of E-ISAC	North American Electric Reliability Corp
Mansur Abilkasimov	Director, Cybersecurity Governance	Schneider Electric
Mario Bocchiola	Head of Operation Technology Cyber Security Engineering	Enel
Markus Wolf	Regional Manager for International Stakeholders	Electric Power Research Institute
Martin Knudsen	Lead Information Security Officer	Ørsted
Matt Wakefield	Director of Information, Communication and Cybersecurity	Electric Power Research Institute
Maximilian Urban	Information Security Officer and Innovation Manager	Netz Niederösterreich GmbH
Mikhail Falkovich	Chief Information Security Officer	Consolidated Edison Inc.
Neelakarun Asari	Associate Director	HCL Technologies Ltd
Nina Olesen	Senior Policy Manager	European Cyber Security Organisation
Olivier Vandelaer	Director Industrial Cybersecurity	ENGIE Laborelec
Paulo Moniz	Director - Information Security and IT Risk	EDP - Energias de Portugal SA
Mohammed Zumla	Head of Cyber Security and Resilience at NIS Competent Authority	OFGEM

Philip Tonkin	Global Head of Cyber Operational Technology	National Grid Group Plc
Robert Lee	Chief Executive Officer	Dragos
Robert Watson	Manager - Cybersecurity Program	US Cybersecurity and Infrastructure Security Agency
Scott Pinkerton	Cyber Security Programme Manager	Argonne National Laboratory
Shaharyar Khan	Research Scientist	MIT – Sloan School of Management
Shih Hsien Lim	Chief Security Officer	Singapore Power Group (SP Group)
Simon Uzunov	Deputy Head of Electricity Unit	Energy Community
Stuart Madnick	John Norris Maguire Professor of Information Technologies and Professor of Engineering Systems	MIT - Sloan School of Management
Swantje Westpfahl	Co-Director	Institute for Security and Safety (ISS)
Tim Conway	Director of SCADA and ICS	Sans Institute
Tom Wilson	SVP & CISO	Southern Company
Yuri G. Rassega	Chief Information Security Officer (CISO)	Enel

The World Economic Forum wishes to acknowledge contributions from the Energy Community. The Energy Community is an international organization which brings together the European Union and its neighbours to create an integrated pan-European energy market. A special acknowledgement also goes to Stefano Bracco at the Agency for the Cooperation of Energy Regulators and the Irish and Norwegian energy regulatory authorities. A final acknowledgement should go to Joe Weiss, Managing Partner, Applied Control Solutions for contributions.

Accenture team
Jacky Fox, Managing Director, Accenture Security

Ettore Galluccio, Principal Director, Accenture

Martino Bevacqua, Senior Manager, Accenture

World Economic Forum team
Louise Anderson, Community Lead, Electricity Industry, World Economic Forum

Filipe Beato, Lead, Centre for Cybersecurity, World Economic Forum

Georges De Moura, Head of Industry Solutions, Centre for Cybersecurity, World Economic Forum

Endnotes

1 https://www.chertoffgroup.com/blog/solarwinds-compromise-software-lifecycle-management-implications

2 http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf

3 http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf

4 Article 2 (2), Page 21 - https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

5 https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2392

6 https://ec.europa.eu/energy/topics/energy-system-integration_fr

7 https://www.iberdrola.com/sustainability/decarbonisation-european-union

8 https://www.weforum.org/reports/unlocking-technology-for-the-global-goals

9 Page 14, Items (4) and (5) - https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

10 Page 15, Items (9) and (10) - https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

11 Page 15 - Cyber risks stemming from the demand side. http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf

12 https://europa.eu/investeu/home_en

13 Article 31 (4), Page 56 - https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

14 Page 5, http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf

15 Page 3, https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508.pdf

16 https://www.algemeiner.com/2020/04/26/israel-thwarts-major-coordinated-cyber-attack-on-its-water-infrastructure-command-and-control-systems/

17 http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf

18 Article 2 (2), Page 21 - https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

19 https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2392

20 https://www.icao.int/Meetings/a39/Documents/Resolutions/a39_res_prov_en.pdf

21 https://www.icao.int/Meetings/a40/Documents/Resolutions/a40_res_prov_en.pdf

22 https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf

23 http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf

24 https://www.eei.org/issuesandpolicy/Documents/Cyber%20Mutual%20Assistance%20Program.pdf

25 https://www.csis.org/chinas-emerging-cyber-governance-system

26 https://www.fticonsulting.com/~/media/Files/apac-files/insights/white-papers/singapore-cybersecurity.pdf

27 https://www.csa.gov.sg/news/publications/ot-cybersecurity-masterplan

28 https://www.ofgem.gov.uk/system/files/docs/2019/05/riio-2_sector_specific_methodology_decision_-_core_30.5.19.pdf

29 http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem_Policy_makers_2020.pdf

30 https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

31 https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/cyber-europe-2020/

32 https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx

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