

Cyber attacks in the energy industry

Government's role in protecting national critical infrastructure



EY

Building a better
working world



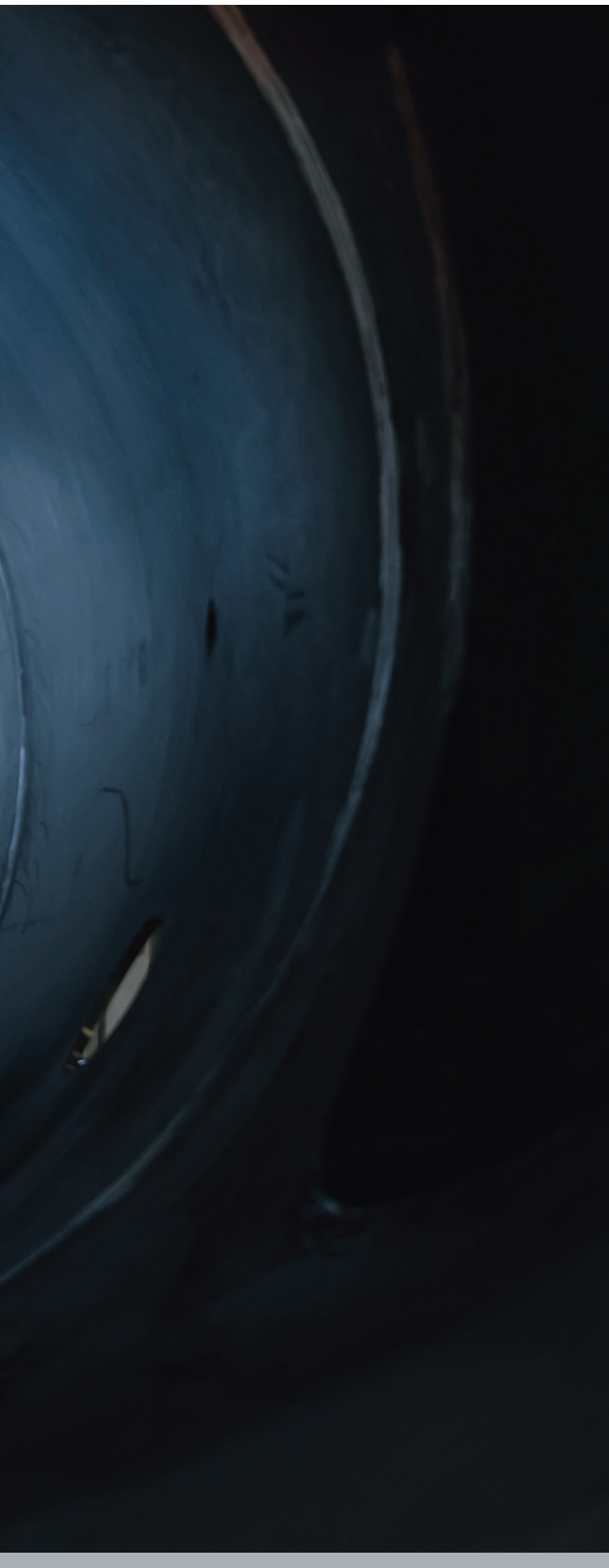


Table of contents

Executive summary	04
Section 1: How risks and government response are evolving	08
Section 2: Energy sector and governments: how the past is impacting the protection of critical infrastructure	12
Section 3: An effective governance approach for the protection and accountability of critical infrastructure across the energy sector and their respective governments	16
Section 4: A cohesive approach for the energy sector and government to manage cyber risks and implement compliance requirements	22
Conclusion	26
Call to action	28
References	30
Key contacts	31

Executive summary





It has become evident that hybrid warfare is the new reality, inextricably linking governments and cybersecurity. The number of attacks against the energy industry and critical national infrastructure is rising dramatically, in quantity, magnitude and impact.¹ Most countries now recognize cyber as an element of national power and have used it to gain a strategic advantage to support asymmetric operations to demonstrate the capability to target critical infrastructure. In addition, new and emerging technologies have added complexity to the issue, as governments and organization alike scramble to address the potential risks and benefits of artificial intelligence (AI), generative AI (GenAI) and quantum computing that have seen rapid adoption and acceleration.

Lastly, as per the EY Global Board Risk Survey 2023, board members are reporting that cybersecurity is among their top three risks. However, on some energy sector-specific boards, cybersecurity only ranks within the top 10 risks. This arguably shows the significant gap between the energy industry and others in their maturity in addressing this risk and thus in protecting critical national infrastructure.




In recent years, some countries have taken significant steps, although largely reactive in nature, to improve the regulation, resources and support available to private companies to enhance cybersecurity. Unfortunately, the energy industry and their respective government regulators are uncertain about how well the cybersecurity risk to critical infrastructure can be managed by each organization, given the historically low priority the energy industry has placed on cybersecurity. Through this, it can be argued that without any national governance, intervention and supporting resources, this would place the energy industry and critical national infrastructure at risk from a cyber attack.²

Governments must determine the right balance of oversight without impacting the ability of energy industry companies to deliver safe and profitable services to their customers. By providing a balanced regulation through proactive intervention, governments will be enabled to provide the right mix of regulatory oversight and support, while allowing companies the flexibility to take a risk-based approach based on threats, likelihood of attack, potential impact and available resources. Pioneering organizations are building methodologies that consider not only the business environment, but also the government's intervention through regulation and cybersecurity standards, and the risk landscape.

While no organization is immune to cyber attacks, organizations with a strong risk management framework incorporating balanced and focused government regulations and standards are likely to be more cyber resilient. A risk-based approach to cybersecurity allows organizations to focus on protecting high-value assets and mitigating assessed risks, thereby reducing the attack surface and potential impact. While there is still much work to be done, there is a role for each nation's government to relieve some

of the burden from private energy owners and operators for protecting national critical infrastructure. Governments must provide regulatory frameworks that enable the protection of critical infrastructure from cyber attacks. This white paper also argues that the use of commercial incentives and shared accountability of potential issues and incidents will improve the cybersecurity posture of the energy industry. This can be achieved through collaborative and proactive interventions which could create a sense of control and uniform protections across their identified critical infrastructure.



In conclusion, smart and effective governance will be a catalyst for effective protection and accountability of critical infrastructure via a balanced approach for managing cyber risks and implementing compliance requirements between the energy sector and government.

Section 1

How risks and government response are evolving

This same event led Nordex SE to shut down its IT systems and Deutsche Windtechnik to lose control of monitoring of nearly

2,000

wind turbines for at least a day.



Cyberattacks on energy
companies in the
US and Canada have
increased by almost

71%

from 2021 to 2022.

Given the complexity and prevalence of legacy assets in the industry's asset base, the energy sector has always been an attractive target for increasingly sophisticated cybercriminals. In the last few years, the number of cyber attacks on energy companies in the US and Canada has increased by almost 71% from 2021 to 2022.³ As per the Microsoft Digital Defense Report 2023, the number of cyber threat actors has expanded, particularly to the Global South to more parts of Latin America and sub-Saharan Africa.⁴ Therefore, the corresponding impacts, such as financial loss, loss of life, regulatory and reputational, are mounting. The ransomware costs globally are expected to reach US\$265b by 2031, up from US\$20b in 2021.⁵ New and sophisticated adversaries are using the latest technology to increase the speed and scale of their attacks, especially with the rapid adoption of AI.

It is not possible to escape from cyber warfare in today's world. As the pace of change continues, the potential to expose organizations to data loss, breaches and disruption will continue to evolve. Recent cyber attacks have emphasized the critical role of cybersecurity in ensuring the stability and functioning of essential services. In 2021, Colonial Pipeline experienced a ransomware attack which disabled its IT computer systems. Out of an abundance of caution, the company temporarily shut down the pipeline, which was responsible for transporting 45% of fuel demand to the US East Coast, resulting in fuel shortages and panic buying in affected states.⁶ Moreover, the recent war in Ukraine has shown new 21st century cyber warfare. In February 2022, as Russia's invasion of Ukraine began, a satellite outage believed to be caused by Russia or its proxies knocked out communication and control of thousands of Enercon's wind turbines. This rendered 11 gigawatts of power to operate without any monitoring. This same event led Nordex SE to shut down its IT systems and led Deutsche Windtechnik to lose control of monitoring, impacting nearly 2,000 wind turbines for at least a day.

To counter the increased risk, the energy industry has ramped up investment in cybersecurity in recent years, driven by tightening regulatory and compliance pressures to ensure resilience against attacks and failures. Cybersecurity technology offerings have helped companies efficiently identify vulnerabilities and develop key controls like privileged access management, threat detection and response. However, the industry is still struggling to develop effective cyber resilience due to a fragmented technology environment.

The EY 2023 Global Cybersecurity Leadership Insights Survey reveals that only 35% of energy companies believe that their organization is well positioned to take on the threats of tomorrow, compared with 48% of other industries.

An ecosystem-led approach to business today also presents a significant cybersecurity challenge due to lengthening supply chains. The EY 2023 Global Cybersecurity Leadership Insights Survey reveals that 57% of energy cyber leaders agree that there is no such thing as a secure perimeter in today's digital ecosystem. In 2020, a major software company in the US, SolarWinds experienced a cyber attack, which led to a wide-ranging cyber intrusion. The nation state hackers were able to gain access to the IT systems, networks and data of several government agencies and organizations using SolarWinds' Orion platform.⁷

These cyber attacks have underscored the need for regulatory enhancements and public-private collaboration to mitigate future risks and safeguard critical infrastructure. For instance, in the aftermath of a cyber attack on Colonial Pipeline, the Transportation



Security Administration in the US revised its cybersecurity directives. These new directives call on pipeline and transport companies to develop a cybersecurity implementation plan, put an incident response plan in place for handling potential attacks and establish a long-term assessment program to test and audit cybersecurity measures. In addition, the US-based Cybersecurity and Infrastructure Security Agency (CISA) has also published specific recommendations and guidelines for the organizations to identify and eliminate the exploited components of their supply chain.



57%

of energy cyber leaders agree there is no such thing as a secure perimeter in today's digital ecosystem.

The US and Israel created a joint cybersecurity force to invest

US\$4m

in critical infrastructure cybersecurity projects, with an additional

US\$10m

to be funded by the private sector.

The nature of these risks requires that governments to collaborate with the private sector to develop regulations, policies and procedures to effectively confront and eliminate cyber threats. In May 2021, the US signed an executive order aimed at improving the nation's cybersecurity and protecting federal government networks. The order outlined measures to enhance cybersecurity standards, information sharing and incident response. It also sought to modernize federal IT systems and emphasize the importance of international collaboration and partnerships to strengthen global cybersecurity.⁸ The US and Israel created a joint cybersecurity force to invest US\$4m in critical infrastructure cybersecurity projects, with an additional US\$10m to be funded by the private sector.⁹ Additionally, the European Union (EU) and the Association of Southeast Asian Nations (ASEAN) have jointly agreed to mitigate cybersecurity threats and strengthen cyber capacity-building measures by sharing best practices.¹⁰

An aerial photograph showing a large array of blue solar panels installed in a field. The panels are arranged in rows and are surrounded by lush green vegetation. A large yellow rectangular area is overlaid on the left side of the image, containing the text for this section.


Section 2

Energy sector and their government: how the past is impacting the protection of critical infrastructure



The energy sector has traditionally been a mature, commodity-driven industry with established products, specialized technologies and ways of doing business. These critical infrastructure systems were designed and built decades ago, using now legacy operational technology (OT) that lack modern security features. Over the past several years, there has been exponential growth in the deployment of digital assets and innovation that has been rapidly adopted by the business (such as the Industrial Internet of Things and AI), further complicating the issue between legacy OT systems and new technology all operating in the same organization. However, energy companies still lag other industries in scaling these digital initiatives and building out its cyber resilience. According to the EY Digital Investment Index Survey 2022, more than two-thirds of energy companies are yet to realize the full benefit of AI, the Internet of Things (IoT) and advanced cyber defense mechanisms.

The energy industry faces major challenges, from the original equipment manufacturers (OEM) whose legacy OT environments are very difficult to change or update. Modernization efforts driven by digital transformation, have led to the integration of legacy systems with newer technologies, which have brought through further security vulnerabilities. Moreover, the pressure to transition to new clean energy sources is forcing a shift toward more distributed networks, enabled by digital technologies. The widespread adoption of cloud computing and IoT has increased opportunities for cybersecurity breaches.



The EY 2023 Global Cybersecurity Leadership Insights Survey reveals that nearly 70% of energy firms believe new technologies (such as, cloud, IoT, AI and ML) will pose the biggest cybersecurity risks in the next five years. Hence, new technology adoption can increase the risk of a cyber attack causing disruption of services, damage to equipment, data breaches and potential threats to public safety and national security.

Given the current global instability, cyber warfare and political tensions, energy infrastructure has become a prime target for nation-state attackers. Several countries have suffered high-profile cyber attacks in recent years¹¹, forcing governments across the globe to recognize the need to protect their critical national assets through further regulations. Some countries have launched their own cybersecurity initiatives to safeguard their critical national infrastructure. For instance:

- ▶ The EU reviewed and adopted the Network and Information Security (NIS2) and Critical Entities Resilience Directive in 2022, with a baseline for cybersecurity risk management and reporting obligations across critical sectors (including energy).¹²
- ▶ The Netherlands Cybersecurity Innovation Fund (CIF-NL) aims to stimulate cybersecurity innovation. The grant is for the (further) development of cybersecurity solutions. The projects are characterized by their focus on enhancing the national security of the Netherlands through highly targeted and specific solutions.¹³

- ▶ Greece has established a National Cybersecurity Authority (NCSA), to be enacted as a legal entity under Public Law, which aims to coordinate and implement a comprehensive cybersecurity strategy for the nation. The authority will enhance capacities and supervisory roles, aligning with EU commitments, and cover a broad spectrum, including public and commercial sectors.¹⁴
- ▶ In March 2023, the US has implemented a new cybersecurity strategy to protect critical infrastructure by investing in innovative technologies and bringing in best-in-class technologies through international partnerships.¹⁵
- ▶ North American Electric Reliability Corporation (NERC) has designed Critical Infrastructure Protection (CIP) standards to secure the assets of bulk electric systems.¹⁶
- ▶ The Albanese government of Australia is set to empower small and medium businesses against cyber threats through the 2023-2030 Australian Cyber Security Strategy. Recognizing the vulnerability of these businesses to cyber incidents, the strategy will introduce new support initiatives, backed by a US\$7.2m commitment for a voluntary cyber health-check program. This program enables businesses to conduct a free, tailored self-assessment of their cybersecurity maturity, providing access to educational tools. Small and medium enterprises (SMEs) with higher risk exposure can also benefit from a more advanced third-party assessment to enhance security across national supply chains.¹⁷
- ▶ The National Cybersecurity Authority (NCA) in Saudi Arabia issued several cybersecurity regulations that all government entities and critical national infrastructures need to comply with.¹⁸
- ▶ In August 2023, the Azerbaijan government announced its first five-year strategy on information security and cybersecurity strategy for 2023 to 2027. Within this strategy, Azerbaijan has expressed interest in investing in foreign-run ICT training centers. The Azerbaijani government is looking to expand its technical training resources with American academic and technical partners.¹⁹

- ▶ Australian Energy Sector Cyber Security Framework (AESCSF) assesses the cybersecurity maturity across the country's energy sector.²⁰ Along with the new "2023-2030 Australian Cyber Security Strategy," that has dedicated a section to "Strengthen cybersecurity obligations and compliance for critical infrastructure."



However, these regulations are mostly fragmented, and largely compliance or directive driven. According to the *EY Global Information Security Survey 2021*, more than half of energy cybersecurity leaders (54%) state that achieving compliance is the most stressful part of their job. Several international standards such as ISA99, ISO 62443 and NIST, define a common set of procedures for implementing security practices and assessing cybersecurity performance, but these standards are more than a decade old and were not originally designed considering the current technology interactions or protocols, or adoption of emerging technologies (such as AI), which has strained the boundaries of these standards.

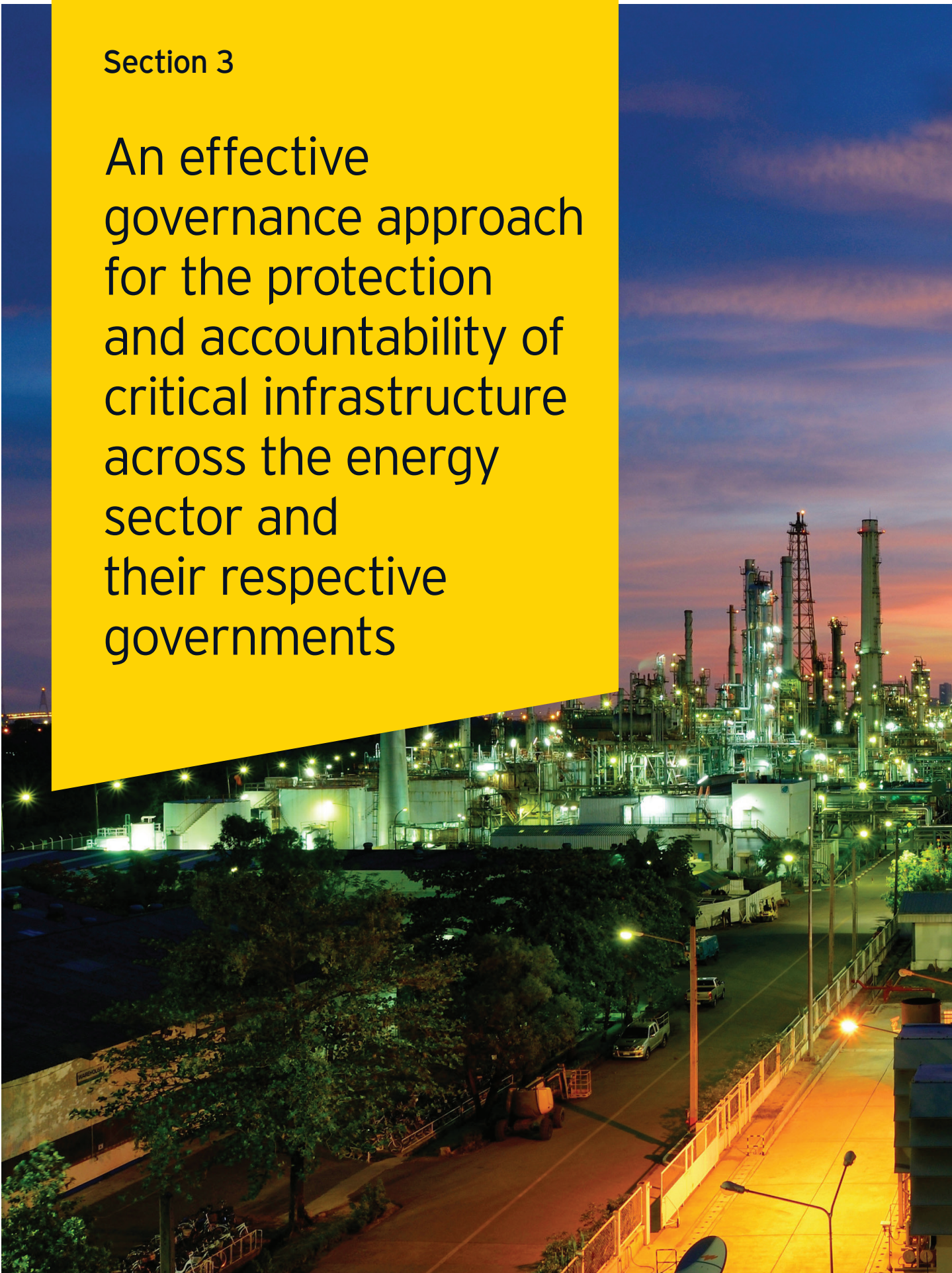
Simply meeting cyber regulatory obligations is no longer enough. Expectations from boards, regulators and other stakeholders are higher.

Almost half (45%) of the board members surveyed for the latest EY Global Board Risk Survey said they expect a cyber attack or data breach to have a severe impact on their organization over the next 12 months – but only 40% understand the biggest cyber risks they face.

Therefore, along with companies embedding risk-based thinking from the onset of all their projects, governments would also need to level up their approach toward managing, monitoring and mitigating the continuously increasing, sophisticated cyber attacks.

Section 3

An effective governance approach for the protection and accountability of critical infrastructure across the energy sector and their respective governments





Despite the ever-increasing regulation and interventions made by each country's government, there have been more successful attacks than ever. A new, dynamic and multi-stakeholder approach is required by the governments to provide cyber resilience to critical national infrastructure. The approach needs to balance the energy industry's need for operational efficiency, with the imperative of safeguarding national security and public welfare.

There have been calls for global initiatives to address the issue, but given the geopolitical tensions on the subject, for now it will ultimately come down to the individual country to provide the catalyst for change.²¹ Parallels can be drawn to data privacy which initiated at scale with the EU Global Data Protection Regulation (GDPR), before being widely adopted as the gold standard globally by many governments, with nuances for each country.²² Interestingly, in September 2023, the International Criminal Court (ICC) announced the decision to investigate and prosecute any hacking crimes that violated existing international law, just as it does for war crimes committed in the physical world.²³ Such penalties and charges will certainly gain attention of the organization's boards and executives.

However, there are also other initiatives for governments to consider in increasing cyber resilience of their critical national infrastructure:

Provide tax-based or other incentives to companies that invest in cybersecurity

Offering grants or tax subsidies for cyber defense projects can encourage companies to invest in research, training and technology, making the cyber investment more financially viable for organizations. For instance, Australia's Technology Investment Boost regulation aims to help small businesses (with an annual turnover of US\$50m or less) by providing an additional business tax deduction of 20% on technology investments, particularly in cybersecurity.²⁴ Furthermore, the US Federal Energy Regulatory Commission (FERC) has issued an order to provide incentive-based rate treatment for utilities to encourage investment in advanced cybersecurity technology and participation in information-sharing programs. This would allow utilities to defer their cybersecurity costs and include them in their rate case as a regulated asset. Japan is also considering the provision of tax incentives to defense contractors who enhance cybersecurity measures to safeguard sensitive industry information from state-supported cyber threats. The proposal, set to be legislated in 2023, could apply to thousands of companies, including smaller suppliers, meeting criteria such as adopting effective antivirus software and implementing two-step authentication.²⁵

Offer assistance and resources to help companies comply with cybersecurity regulations

Regulatory bodies should make it easier for organizations to navigate compliance requirements and focus on building their cyber capabilities. For instance, the US government has announced an investment of US\$27b, under the Bipartisan Infrastructure Law, to upgrade and modernize the country's electric grids to further resistant to cyber attacks. Similar models can be drawn from the Qatar FIFA World Cup Cybersecurity Framework, which was a capability-driven regulation that helped accelerate the adoption and maturity of cybersecurity within critical organizations before the World Cup.²⁶ The US Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Security Agency (NSA) and Department of the Treasury have released new guidance for OT vendors and critical infrastructure facilities regarding risk from open-source software (OSS). This will help promote a better understanding of OSS, its implementation in OT and ICS environments and best practices for its secure usage.²⁷

Establish a collaborative and shared responsibility framework

To safeguard the critical energy infrastructure, various stakeholders including government entities, regulatory bodies, energy companies and other relevant parties, would need to engage in a coordinated effort to address cybersecurity challenges. By eliminating silos and enhancing communication by creating platforms for information sharing, the government can respond more effectively to



the growing threat landscape. For example, the US government established a new cyber defense center, Joint Cyber Defense Collaborative (JCDC), comprising federal agencies, private companies and state and local governments.²⁸ Furthermore, operational collaboration models such as DOE's Energy Threat Analysis Center, Defense Industrial Base Collaborative Information Sharing Environment (DCISE) and NSA's Cybersecurity Collaboration Center (CCC) also enable actionable and timely exchange of information directly with the private sector.

Secure the supply chain

Governments could assist in securing the supply chain of critical national infrastructure organizations by providing testing and certification of critical OT components. This should be done in a way that would incentivize OEMs in making sure the products are better secured during the manufacturing process and provide a fundamental technology layer for the critical systems. For example, governments must use certain products that have been certified to a particular Evaluation Assurance Level under the Common Criteria framework. These international guidelines provide documents defining the criteria and evaluation methods for certifying specific technologies. Moreover, the testing is funded by the vendors and evaluated by competent and independent licensed laboratories.²⁹ There is ISA/IEC 62443 which provides a series of international standards define requirements and processes for implementing secure ICS/OT systems, through a common set of guidelines and procedures for key stakeholders such as product suppliers, integrators and service suppliers, to secure the control systems.³⁰



Collaborate with national laboratories and universities for advanced cyber research

Governments could develop national laboratories that would enable an organization to establish a digital twin of a particular critical system or even a wider ecosystem. This would allow for advanced research and testing of security architecture, configuration, in a safe environment to stress test the systems cybersecurity. In addition, governments could complement this with a cyber range that effectively replicates cybersecurity attacks, and essentially “fire” these attacks at the digital twin for enhanced testing of cyber resilience. The US DOE’s Office of Cybersecurity, Energy Security, and Emergency Response (CESER) announced US\$39m funding for nine new national laboratory projects to advance the cybersecurity of distributed energy resources. Further, collaboration with academies and universities can help enable the sector to benefit from advanced cybersecurity research, including threat analysis, vulnerability assessments and technology development. The Canadian government has granted US\$1.2m to Waterloo University to develop an enhanced cybersecurity system using checkpoint technology to identify the threats in the energy supply chain.³¹

Building a future-ready cyber workforce

Governments should focus on providing financial aid, scholarships or sponsorships for employees pursuing cybersecurity education to encourage skill development within the organization. For instance, the Qatar government has partnered with the SANS institute (a private company specializing in information security, cybersecurity training

and selling certifications) and created working groups to provide free cybersecurity training, threat alerts and IOC (indicators of compromise) for companies that participate.³²

Global collaboration to establish guidelines and standards for state-sponsored cyber attacks

International collaboration can promote a more secure and stable energy infrastructure, by creating a framework that outlines appropriate responses, boundaries and expectations when it comes to cyber activities affecting the energy sector. For instance, the BIRD Cyber Program is a collaborative effort between the US Department of Homeland Security Science and Technology Directorate and Israel’s National Cyber Directorate (INCD) to bolster the cyber resilience of critical infrastructure in both countries. The US and Denmark have also announced a partnership to reduce cybersecurity vulnerabilities and build cyber resilience within Ukraine’s critical infrastructure. The US CISA and the Ukrainian State Service of Special Communications and Information Protection also signed a memorandum of cooperation to strengthen collaboration on shared cybersecurity priorities.

Therefore, governments and industry associations can collaboratively provide exclusive opportunities to energy companies to build strong cybersecurity capabilities and encourage investment in cyber defenses. Creating platforms that incentivize organizations to share threat intelligence and collaborate on cyber threats can help develop a more resilient cybersecurity ecosystem.

Section 4

A cohesive approach for the energy sector and government to manage cyber risks and implement compliance requirements





Organizations need to take the right steps to identify and manage the risks associated with their businesses and protect against cyber attacks to minimize any impact on business operations. Cyber risk quantification can help build this resilience. It's a more rigorous, evidence-based way of evaluating and quantifying cyber risk that can help energy companies mature their cybersecurity programs. It gives leaders the ability to proactively identify the most relevant threats and prioritize finite resources in a constrained environment. Importantly, cyber risk quantification helps CISOs confidently take their seats, armed with the tools to articulate the value of cybersecurity investment to the C-suite in a way that is relevant to the CFO, COO and other business leaders.

With the increasing number of IoT devices, industrial cybersecurity also requires renewed attention from regulators. Several countries have introduced technical requirements to enhance security controls over OT and IoT devices. For instance, the European Commission introduced a new Cyber Resilience Act in September 2022, establishing minimum security requirements for connected devices and making manufacturers responsible for ensuring that their products are digitally secure.³³ The US reintroduced the Cyber Shield Act in March 2021, which would create security standards for IoT devices based on the recommendations of an advisory committee made up of cybersecurity experts from the government, academia and the private sector.³⁴

Australia is also considering making mandatory a suite of voluntary regulations that would outline a set of minimum cybersecurity requirements for consumer-grade smart devices.³⁵

New technologies which help companies analyze data, optimize supply chains and assess risks, also calls for the need of specific legislations to regulate their use. For instance, the EU has introduced a legal framework for AI with clear requirements and obligations for developers, deployers and users. Further, the commission has proposed an AI Act to classify the applications into three major risk categories: unacceptable subject to complete ban (such as government-run social scoring), high-risk subject to specific legal requirements (such as a résumé-scanning tool that ranks job applicants) and limited or no risk which will be unregulated. US has also issued an Executive Order to mandate safety testing of AI systems, promote privacy-preserving techniques, address algorithmic bias, and foster AI innovation. It also aims to promote international cooperation on AI standards and its responsible use.

Organizations need to explore the feasibility and effectiveness of blockchain-based security solutions to prevent ransomware attacks.

Using blockchain's decentralized, distributed ledger with encrypted transactions can help companies preserve the authenticity of data and prevent data breaches. In addition, a Software Bill of Materials (SBOM), such as a running list of applications and installed



software, can help companies detect and mitigate the potential cyber attacks in the global software supply chains. This mandate will enable companies to identify the components that are disallowed within a compliance framework such as PCI-DSS, SOX and HIPAA. In May 2021, US administration issued a cybersecurity executive order for all software vendors to include an SBOM of their respective companies, when commercially interacting with any firm. In response to this order, three US government agencies, Department of Defense, NASA and General Services Administration, proposed new rules for their contractors that would require them to develop and maintain an SBOM for any software used to deliver a contract.³⁶

Original equipment manufacturers are now working with the energy companies to be compliant with the government standards. For example, a technology company, ABB has signed a contract with European utility, Energias de Portugal (EDP), to improve its



plant control systems to increase efficiency, output and reliability, and also enhance the security of energy plant controls to ensure that the facilities comply with the NIS2 regulations.³⁷ Further, Siemens Energy has partnered with AWS to offer industrial cybersecurity, analytics and storage solutions for energy companies.³⁸ The company also launched an NIS compliance 4.0 solution to help critical infrastructure operators comply with the NIS directive and follow the best practices.³⁹

Intergovernmental organizations such as United Nations (UN) and North Atlantic Treaty Organization (NATO) can also play a critical role in enhancing cyber defense capabilities of their member countries. The organizations can establish a mechanism for rapid response for cyber incidents and information sharing to help member countries in identifying and mitigating cyber attacks. Recently, in the aftermath of the Russian-Ukraine crisis, the EU and NATO have announced plans to

intensify their collaboration for addressing cyber threats. The organizations will continue to work together for enhancing situational awareness and building cyber capacity across the member states.⁴⁰

As the world increasingly embraces digital transformation and the global geopolitical situation remains in a constant flux, governments need to establish robust guidelines to empower energy companies for building cyber resilience.

The task at hand is for regulators to stay informed about the evolving digital landscape, be proactive in identifying threats and foster an environment where industries are willing to engage in collaborative partnerships.


Conclusion



Digital transformation and the swift adoption of advanced technologies around the world is creating an even larger and more complex attack surface for adversaries to exploit. This is further exacerbated, as adversaries learn to leverage advanced digital technologies and sophisticated capabilities to exploit the OT and ICS systems in critical infrastructure. Moreover, unstable geopolitical situations have enabled the escalation of state-sponsored cyber attacks on critical infrastructure around the world. Despite the increasing cyber regulations and the addition of some resources and programs, cyber attacks are continuously rising. Therefore, building a robust regulatory environment – ensuring not only compliance but also a safe cyber ecosystem – is crucial for governments to protect their critical infrastructure.

The transition of regulators from strict enforcers to enablers will be a significant shift in the right direction. Although it's important to introduce and enforce strict compliance requirements for companies supporting critical infrastructure, we must do it in a way that enables companies to take a risk-based approach. Offering tax incentives, shared platforms and cyber investment programs can help companies build cybersecurity capabilities and meet their compliance requirements. Governments also have the responsibility to put the right frameworks in place to help develop cybersecurity talent and address critical shortages, particularly in the very specialized but exponentially growing area of OT cybersecurity. Moreover, governments need to adopt a collaborative approach to understand risks associated with the rapidly changing digital environment. They must comprehend the potential risk that a technology or digital transformation could pose and take risk-informed mitigation actions. This will help create an open environment for organizations to collaborate and share information at both country and industry levels.

Organizations need to embrace more of a risk-based approach toward cybersecurity to protect their high-value information assets and mitigate the potential risks. It is essential for companies to implement holistic and effective cyber governance, risk and compliance programs that includes cyber risk assessments, thorough vulnerability assessments, penetration testing and critical assets configuration reviews. Further, adopting a more rigorous, evidence-based approach of evaluating and quantifying cyber risk can also help energy companies mature their cybersecurity programs. It will help CISOs direct the cybersecurity resources to the right risks in a timelier manner.



In conclusion, in order to combat increasing cyber threats while enabling energy companies to be creative and develop new energy sources, it is paramount to build cyber resilience capabilities in critical national infrastructure, using a more proactive approach, with advanced regulatory frameworks put in place by the government through increased collaboration with public and private sector organizations.



Call to action

A new, dynamic and multi-stakeholder approach is required by the governments to provide cyber resilience to critical national infrastructure. The approach needs to balance the industry's need for operational efficiency, with the imperative of safeguarding national

security and public welfare. These are the top seven actions firms and governments alike need to consider while creating and implementing a cyber resilience ecosystem for critical national infrastructure:

1

Provide tax-based or other incentives to companies that invest in cybersecurity

Offering grants or tax subsidies for cyber defense projects can encourage companies to invest in research, training and technology, making the cyber investment more financially viable for organizations.

2

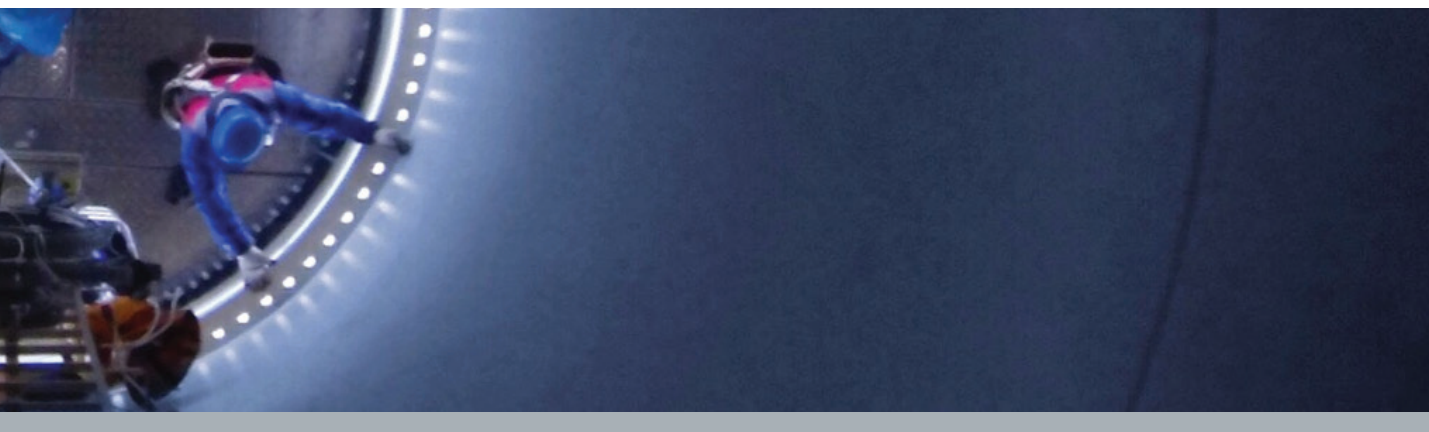
Offer assistance and resources to help companies comply with cybersecurity regulations

Regulatory bodies should make it easier for organizations to navigate compliance requirements and focus on building their cyber capabilities. This can be achieved through consolidation of legislation and regulation, also while emphasizing the move to a more risk-based approach.

3

Establish a collaborative and shared responsibility framework

To safeguard the critical national infrastructure, various stakeholders, including government entities, regulatory bodies, energy companies and other relevant parties, would need to engage in a coordinated effort to address cybersecurity challenges. By eliminating silos and enhancing communication by creating platforms for information sharing, the government can respond more effectively to the growing threat landscape.



4

Secure the supply chain

Governments could assist in securing the supply chain of critical national infrastructure organizations by providing testing and certification of critical OT components. This would accelerate the OEMs in making sure the products are better secured and provide a fundamental secure technology layer for the critical systems.

5

Collaborate with national laboratories and universities for advanced cyber research

To take a further step, governments could provide national laboratories that would enable an organization to establish a digital twin of a particular critical system or even a wider ecosystem. This would allow for testing cyber architecture, configuration, and even change of a digital environment in a safe environment to stress test the cybersecurity.

6

Building future-ready cyber workforce

Governments should provide an educational framework that will focus on the urgent needs to develop cyber IT and OT talent to meet the growing demand. They should also consider options such as providing financial aid, scholarships or sponsorships for employees pursuing cybersecurity education to encourage skill development within the organization.

7

Multilateralism to establish guidelines and standards to address state-sponsored cyber attacks

International collaboration can promote a more secure and stable energy infrastructure, by creating a framework for multilateralism that outlines appropriate responses, boundaries and expectations when it comes to cyber activities affecting critical national infrastructure.

References

1. "Energy Sector: More attacks in 2022 than ever before," Power and Beyond, Energy sector: More cyber attacks in 2022 than ever before (power-and-beyond.com), assessed on 14 November 2023.
2. "Collaboration is key to energy sector cyber defense," Security Magazine, Collaboration is key to energy sector cyber defense | Security Magazine, assessed on 14 November 2023.
3. "Extremists keep trying to trigger mass blackouts – and that's not even the scariest part," Politico, Extremists keep trying to trigger mass blackouts – and that's not even the scariest part – POLITICO, accessed on 14 November 2023.
4. "Microsoft Digital Defense Report 2023," Microsoft, Microsoft Digital Defense Report 2023 (MDDR) | Microsoft Security Insider, assessed on 14 November 2023.
5. "What is the real cost of a data breach?," RiskXchange, What Is The Real Cost Of Data Breach? | RiskXchange, assessed on 14 November 2023.
6. "Ransomware cyberattack shuts down major US pipeline, company says," ABC News, Ransomware cyberattack shuts down major US pipeline, company says - ABC News (go.com), assessed on 14 November 2023.
7. "The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal," Business Insider, What Is the SolarWinds Hack and Why Is It a Big Deal? (businessinsider.com), assessed on 14 November 2023.
8. "Executive Order on Improving the Nation's Cybersecurity," White House, Executive Order on Improving the Nation's Cybersecurity | The White House, assessed on 14 November 2023.
9. "BIRD - Israel-U.S. Binational Industrial R&D Foundation, to Invest \$3.85M in Critical Infrastructure Cybersecurity Projects," PR Newswire, BIRD - Israel-U.S. Binational Industrial R&D Foundation, to Invest \$3.85M in Critical Infrastructure Cybersecurity Projects (prnewswire.com), assessed on 14 November 2023.
10. "ASEAN-EU Statement on Cybersecurity Cooperation," European Union External Action, ASEAN-EU Statement on Cybersecurity Cooperation | EEAS (europa.eu), assessed on 14 November 2023.
11. "Ukraine, Israel, South Korea top list of most-targeted countries for cyberattacks," The Record, Ukraine, Israel, South Korea top list of most-targeted countries for cyberattacks (therecord.media), assessed on 14 November 2023.
12. "The Critical Entities Resilience Directive (CER)," CER, The Critical Entities Resilience Directive (CER) (critical-entities-resilience-directive.com), assessed on 14 November 2023.
13. "Cybersecurity Innovation Fund (CIF-NL)," RVO Netherlands, Cybersecurity Innovation Fund (CIF-NL) (rvo.nl), assessed on 20 December 2023.
14. "Greece Plans National Cybersecurity Authority to Combat Rising Hacker Threats," The Cyber Express, National Cybersecurity Authority Proposed In Greece (thecyberexpress.com), assessed on 20 December 2023.
15. "National Cybersecurity Strategy," White House, National-Cybersecurity-Strategy-2023.pdf (whitehouse.gov), assessed on 14 November 2023.
16. "What Is NERC CIP: The Ultimate Guide," Industrial Defender, What Is NERC CIP: The Ultimate Guide | Industrial Defender OT/ICS Cybersecurity Blog, assessed on 14 November 2023.
17. "Small businesses to receive cyber security boost," Ministry of Treasury, Small businesses to receive cyber security boost | Treasury Ministers, assessed on 20 December 2023.
18. "National Cybersecurity Authority Legislation," National Cybersecurity Authority, National Cybersecurity Authority (nca.gov.sa), assessed on 14 November 2023.
19. "Information and Communications Technology," International Trade Administration, Azerbaijan – Information and Communications Technology (trade.gov), assessed on 20 December 2023.
20. "AESCSF framework and resources," AEMO, AEMO | AESCSF framework and resources, assessed on 14 November 2023.
21. "How Geopolitics Impacts the Cyber-Threat Landscape," Gartner, How Geopolitics Impacts the Cyber-Threat Landscape (gartner.com), assessed on 14 November 2023.
22. "Statement ahead of the 5th anniversary of the General Data Protection Regulation," European Union, 5th anniversary of the General Data Protection Regulation (europa.eu), assessed on 14 November 2023.
23. "The International Criminal Court Will Now Prosecute Cyberwar Crimes," Wired, The International Criminal Court Will Now Prosecute Cyberwar Crimes | WIRED, assessed on 14 November 2023.
24. "Small business technology investment boost and skills and training boost," Australian Taxation Office, www.ato.gov.au/General/New-legislation/In-detail/Direct-taxes/Income-tax-for-businesses/Small-Business-Technology-Investment-Boost-and-Small-Business-Skills-and-Training-Boost/, accessed 20 October 2023.
25. "Japan plans cybersecurity tax break for defense contractors," Nikkei Asia, Japan plans cybersecurity tax break for defense contractors - Nikkei Asia, assessed on 20 December 2023.
26. "QATAR – CYBERSECURITY SECTOR," International Trade Administration, Qatar – Cybersecurity Sector (trade.gov), assessed on 14 November 2023.
27. "CISA Releases its Open Source Software Security Roadmap," CISA, www.cisa.gov/news-events/alerts/2023/09/12/cisa-releases-its-open-source-software-security-roadmap, accessed 21 October 2023.
28. "JCDC: New Center Comprised of Federal Agencies, Private Sector, State and Local Governments Join Forces to Prevent Cyberattacks," Net Centrics, netcentrics.com/jcdc-joint-cyber-defense-collaborative-to-prevent-cyberattacks/, accessed 30 October 2023.
29. The Common Criteria, www.commoncriteriaportal.org/, accessed 16 October 2023.

30. "ISA/IEC 62443 Series of Standards," International Society of Automation, www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards, accessed 5 November 2023.
31. "Protecting Canada's energy infrastructure and supply chain from cyber attacks," University of Waterloo, Protecting Canada's energy infrastructure and supply chain from cyber attacks | Waterloo News | University of Waterloo (uwaterloo.ca), assessed on 14 November 2023.
32. "SANS Institute elevates cyber resilience in Qatar with SANS Doha September 2023," Tahawultech, SANS Institute elevates cyber resilience in Qatar with SANS Doha September 2023 | TahawulTech.com, assessed on 14 November 2023.
33. "EU Cyber Resilience Act," European Commission, EU Cyber Resilience Act | Shaping Europe's digital future (europa.eu), assessed on 14 November 2023.
34. "SENATOR MARKEY AND REP. LIEU REINTRODUCE LEGISLATION TO IMPROVE THE CYBERSECURITY OF INTERNET OF THINGS TECHNOLOGY," Senator Ed Markey, Senator Markey and Rep. Lieu Reintroduce Legislation to Improve the Cybersecurity of Internet of Things Technology (senate.gov), assessed on 14 November 2023.
35. "Govt to make its voluntary IoT cybersecurity standards mandatory," Innovation Australia, Govt to make its voluntary IoT cybersecurity standards mandatory (innovationaus.com), assessed on 14 November 2023.
36. "Executive Order on Improving the Nation's Cybersecurity," White House, Executive Order on Improving the Nation's Cybersecurity | The White House, assessed on 14 November 2023.
37. "ABB to upgrade control systems at two of EDP's power plants in Spain," ABB Group, ABB to upgrade control systems at two of EDP's power plants in Spain, assessed on 14 November 2023.
38. "Siemens Energy Takes Next Step to Protect Critical Infrastructure," Siemens Energy, Siemens Energy Takes Next Step to Protect Critical Infrastructure (siemens-energy.com), assessed on 14 November 2023.
39. "NIS compliance 4.0," Siemens, NIS Compliance ENG (siemens.com), assessed on 14 November 2023.
40. "The European Union and NATO intensify cooperation on addressing cyber threats," European Union External Action, www.eeas.europa.eu/eeas/european-union-and-nato-intensify-cooperation-addressing-cyber-threats_en, accessed 7 November 2023.

Key contacts

Saulius Adomaitis

EY Global Oil & Gas Leader
saulius.adomaitis@ae.ey.com

Mobin Khan

EY MENA Energy Leader
mobin.khan@ae.ey.com

Nilanshi Chhabra

Cybersecurity Energy Knowledge, Senior
Ernst & Young LLP (India)
nilanshi.chhabra@gds.ey.com

Jim Guinn

EY Americas Cybersecurity Leader
jim.guinn@ey.com

Jason Green

EY Canada Cybersecurity Energy Partner
jason.green1@ey.com

Alexander Amaya

US Cybersecurity Energy, Senior Manager
Ernst & Young Middle East (Dubai Branch)
alexander.amaya1@ae.ey.com

Kevin Dugas

US Cybersecurity Senior Manager
Ernst & Young LLP
kevin.dugas@ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

The MENA practice of EY has been operating in the region since 1923. Over the past 100 years, we have grown to over 8,000 people united across 26 offices and 15 countries, sharing the same values and an unwavering commitment to quality. As an organization, we continue to develop outstanding leaders who deliver exceptional services to our clients and who contribute to our communities. We are proud of our accomplishments over the years, reaffirming our position as the largest and most established professional services organization in the region.

© 2024 EYGM Limited.

All Rights Reserved.

EYG no.

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com