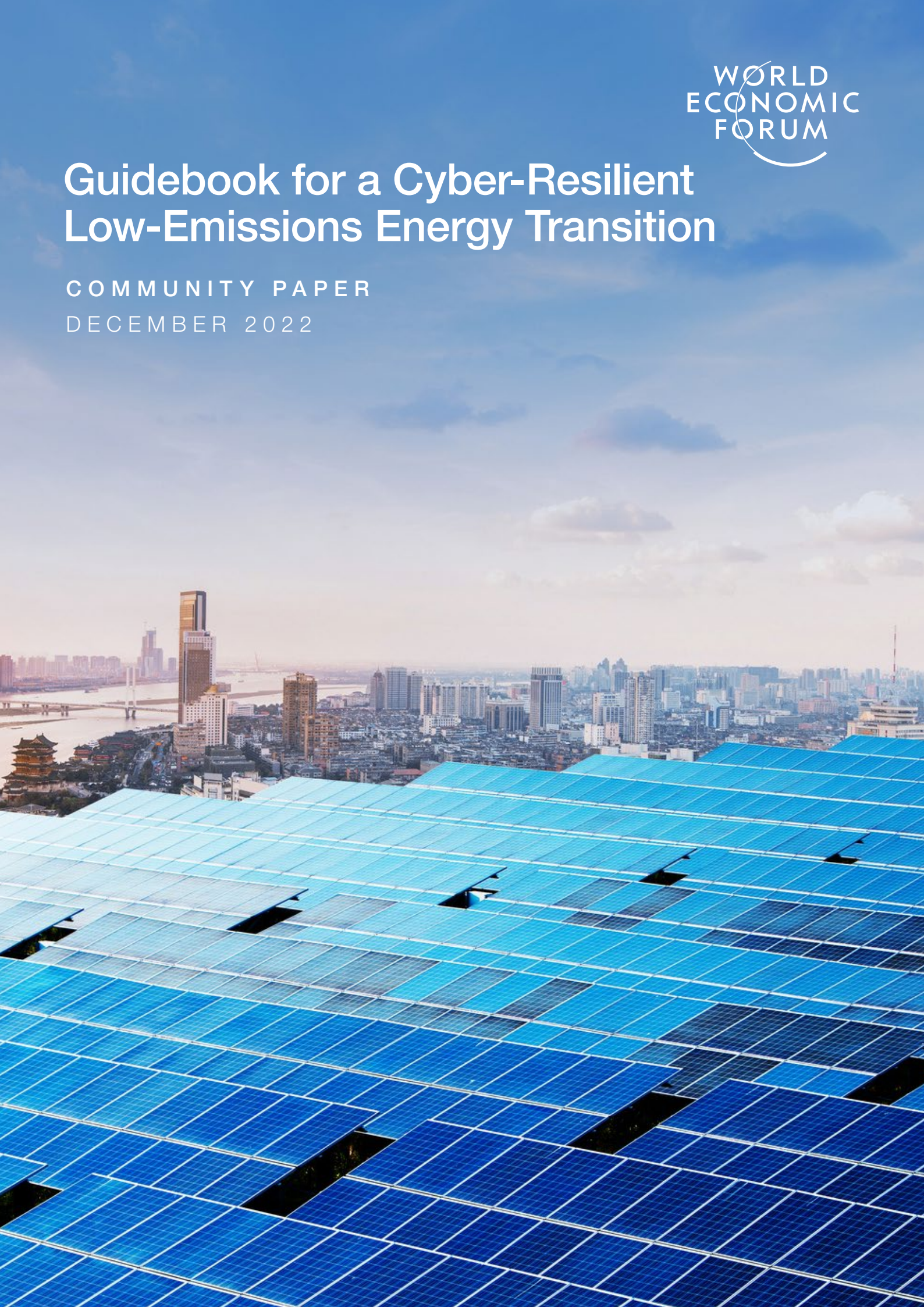
WORLD ECONOMIC FORUM

Guidebook for a Cyber-Resilient Low-Emissions Energy Transition

COMMUNITY PAPER

DECEMBER 2022



Images: Getty Images, Unsplash

Contents

Executive summary

As it moves to greener energy sources, the energy sector needs to build cybersecurity into its transition journey.

Countries and companies worldwide are ramping up their investments in renewable energy solutions to achieve a greener low-emissions future. As the energy sector embarks on the transition journey towards greener energy sources, new business models that rely on digital, connected and intelligent technologies emerge.

The shift to greener energy sources is being driven by three main digital enablers:

- Digitalization of the infrastructure to increase the efficiency of conventional technologies and optimize business performance
- Innovation using emerging technologies such as the industrial internet of things (IIoT) and artificial intelligence (AI) to help organizations improve their analytic and predictive capabilities, and ultimately take informed and automated decisions
- Adoption and integration of new assets and decentralized energy systems, such as wind and solar power, renewable hydrogen and biofuels, that rely on digital devices to function

While such digital enablers provide transformative business and operational value, they also expand and introduce additional cybersecurity threats. From the offset, to better respond to cyber risks and avoid offsetting all of this provided value, organizations need to embed cybersecurity into the design of technologies, but also in their strategic and operational plans.

To ensure that cyber resilience moves from a business cost to a business enabler, organizations need to be prepared to mitigate cyber risks that may disrupt their business operations and gains. To encourage an effective and resilient energy transition, this guidebook proposes a set of principles that will help senior leaders to build cybersecurity into their organization's transition journey:

1. Prepare the new energy system structure to meet emerging threats
2. Invest capital for long-term benefits
3. Navigate the regulatory landscape
4. Establish cyber-resilient governance for the energy transition
5. Build the foundation for an innovative business environment
6. Develop strong human capital

These principles complement the six energy transition readiness dimensions, outlined by the World Economic Forum`s Energy Transition Index, which set out the interdependencies of energy system transformation with the relevant macroeconomic, political, regulatory and social factors. The extent to which organizations integrate cybersecurity into their energy transition readiness dimensions and perform on the six principles will determine whether they will advance or impede progress on a low-emissions future.

Introduction

Cyber resilience should be integrated from the outset into energy transition projects to ensure a low-emissions future is achieved.

Achieving a low-emissions future is a global priority, with a collective need to pave the way "for future ambition to effectively tackle the global challenge of climate change".[1]

Countries and companies around the world aim to reduce CO_2 emissions by 40% by 2030, compared to levels from 2020. Investments in renewable energy solutions reached $755 billion in 2021, which represents a 27% increase from the previous year.[2] Europe, for example, expects renewable energy sources to account for 54% of the integrated energy system mix and, when combined with hydropower, reach almost 70%.[3]

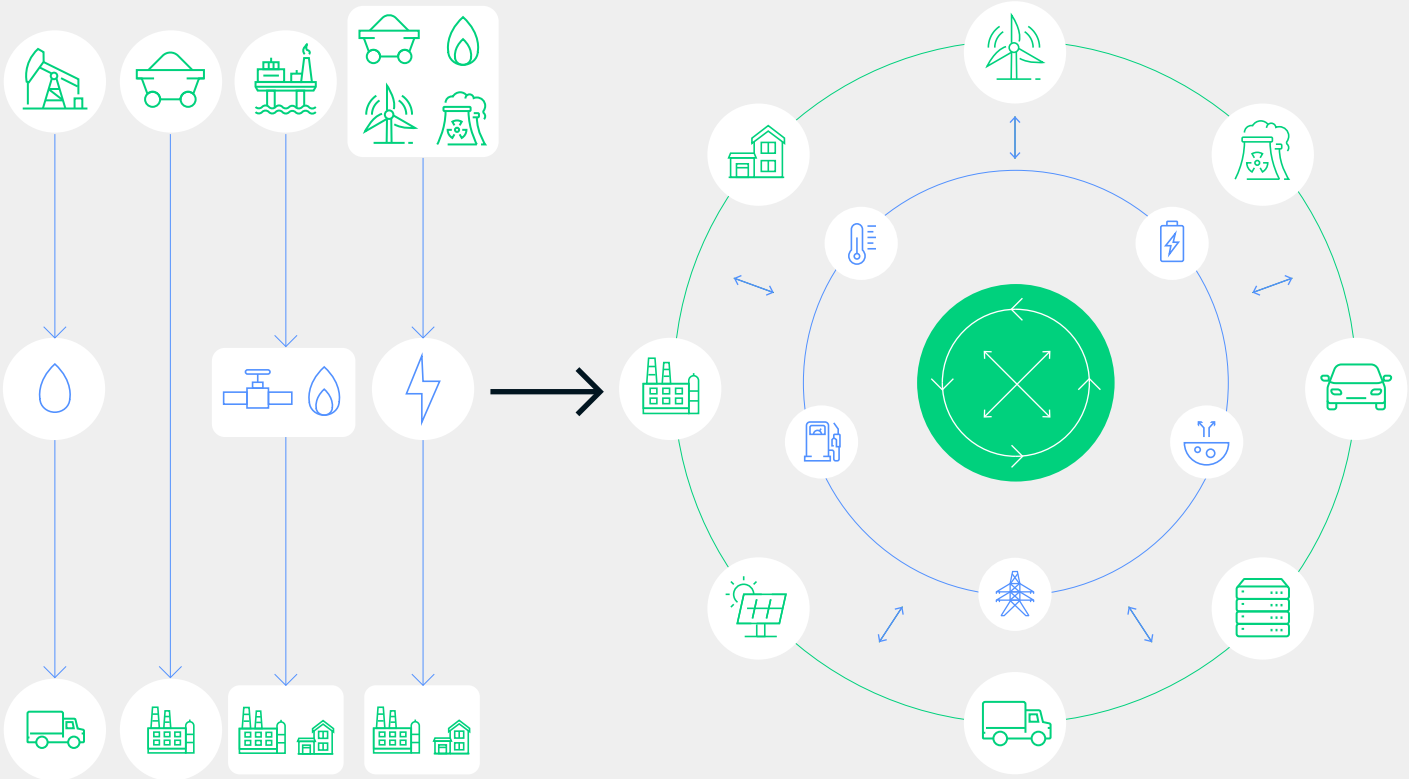
This transition to greener sources is transforming the energy system and integrating energy flows to reduce operational and financial costs, but it also makes the energy ecosystem more complicated.

The ongoing energy transition adds a layer of complexity to the energy sector's responsibility to ensure an uninterrupted and reliable supply of energy to other critical infrastructure, local economies and citizens. The combined need for reduced emissions and continuous energy delivery is driving rapid changes and altering the way companies and countries must think about energy security and resilience.

FIGURE 1 **Towards an integrated energy system**

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

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



Source: *EU Energy System Integration Strategy,* 2020

Power and utility companies are increasingly digitalizing their operations to optimize the end-to-end value chain. The shift to low-carbon energy sources relies heavily on three main digital enablers:

- Digitalization of the infrastructure to increase the efficiency of conventional technologies and increase business performance
- Innovation using emerging technologies such as IIoT and AI to help organizations improve their analytic and predictive capabilities, and ultimately take informed and automated decisions
- Adoption and integration of new assets and decentralized energy systems, such as wind and solar power, renewable hydrogen and biofuels, that rely on interconnected equipment to operate

While such enablers allow for optimization of operations and processes, they expand and introduce new cybersecurity risks.[4] More digitalization can translate into an expansion of the attack surface, which also means a higher exposure to offensive cyber capabilities and cyber incidents.

Continued climate and efficiency benefits unlocked by the energy transition depend on the acceptance by governments and customers that transition technologies do not present a risk to the reliability of energy supply and delivery. Cyberattacks that disrupt energy systems could impede this transition.

Among the many cybersecurity issues that energy organizations currently face, three particular cyber challenges stand in the way of the energy transition:

1. The expansion and convergence of the digital footprint and threat landscape between information technology (IT) and operational technology (OT), with greater connectivity of the critical energy infrastructure and rapid adoption of emerging technologies to speed up the energy transition journey.
2. The rise of complex and sophisticated supply-chain attacks involving highly interconnected partners, including suppliers, vendors and stakeholders with different levels of cyber readiness and cyber hygiene.
3. The escalation of cyberattacks in the industry threatens business operations and public safety, as stressed by 80% of cyber leaders on the Cybersecurity Outlook Report.[5]

On top of these issues, recent global energy and geopolitical crises increase the pressure to ensure a secure and safe energy transition. Prior to the Ukraine crisis, at least 21 gas producers were victims of cyberattacks targeting the production, exportation and distribution of liquified natural gas.[6] Such attacks not only disrupt operations, but also have the potential to cause harm to the environment, and even result in loss of life.[7] In addition to physical damage, security breaches bear significant financial and reputational costs for the industry.

This guidebook is intended to help organizations and their cyber leaders manage the energy transition while embedding cybersecurity and resilience into corporate processes and the design of green technologies. To help leaders adopt a holistic approach to achieving a low-carbon future, it delivers six guiding principles with recommendations to address cyber threats that can compromise the shift to renewable energy production and transmission.

> **The transition to a low-emissions economy is well underway. Never has it been clearer that the future of energy will depend on digital networks and digitized equipment – and that these systems must be resilient against cyberattacks.**
>
> Leo Simonovich, Vice-President and Global Head, Industrial Cyber and Digital Security, Siemens Energy, USA

> **Environmental challenges coupled with an unprecedented geopolitical backdrop have put an emphasis on the need to transition to sustainable energy systems at pace. While the technologies underpinning this transition are being deployed, due care must be given to ensure security is not an afterthought, else we risk building systems with inherent vulnerabilities that can be exploited by malicious actors.**
>
> Akshay Joshi, Head of Operations, Centre for Cybersecurity, World Economic Forum

1 Why prioritize cyber in the energy transition?

Cyber threats can disrupt the business operations and gains of the energy transition.

Many organizations still fail to regard cybersecurity as a business priority. If anything, it is often viewed as a cost rather than an investment. To illustrate, one in three C-suite energy executives state that their organization would need to be affected by a major cyber incident before "it would spend any more time or money" on its cyber defences.[8]

But such a reactive mindset could leave organizations vulnerable to malicious attacks and exposed to the cyber threats that can disrupt business operations and gains.

To ensure a reliable and resilient energy transition, the World Economic Forum developed the Energy Transition Index,[9] which sets out the interdependencies of energy system transformation with the relevant macroeconomic, political, regulatory and social factors. Among other things, this index identifies six enabling dimensions to ensure and encourage transition readiness.

FIGURE 2 **Transition readiness: enabling dimensions**

Source: *World Economic Forum, Fostering Effective Energy Transition: 2021 Edition*

> The extent to which cyber is integrated into each of the six dimensions can determine whether organizations will advance or impede the progress of energy transition.

Each of these six dimensions can also be viewed through the cyber lens. In fact, incorporating cybersecurity into these dimensions is vital to building and maintaining a resilient energy system. Put differently, the extent to which cyber is integrated into each of the six dimensions can determine whether organizations will advance or impede the progress of energy transition.

- The **energy system structure** dimension encompasses elements such as maturity of the energy system and power generation mix, as well as fossil fuel dependency. Both the expansion of renewables and the performance of existing energy systems will rely on digital technologies – and will be more reliable if strong cybersecurity measures are in place.

- The **capital and investment** dimension considers the ability to invest and the availability of capital, as well as the proportion of energy investments directed towards energy efficiency. From the cyber perspective, this translates into the ability to invest in cybersecurity tools and resources, including cybersecurity talent, to reduce the risks and ensure an adequate level of protection for operational infrastructure and assets.

- The **regulation and political commitment** dimension covers commitments to emission-reduction policies and frameworks. Such commitments, in part, require the use of new technologies that offer greater energy efficiency, but also introduce new cybersecurity risks. These new technologies need to be designed in such a way as to ensure a balance between security, innovation and compliance with cybersecurity standards.

- The **institutions and governance** dimension measures the credibility, trust and support for government institutions. This dimension shows a positive correlation with the regulatory environment and is vital for trustworthy public and private collaborations to ensure that effective cybersecurity practices are in place to respond to and mitigate systemic risks. It also includes activities such as information sharing and government incentives to ensure a resilient energy system.

- The **infrastructure and innovative business environment** dimension takes into account the availability of technology that allows for the development of ambitious energy programmes and innovation of the business environment. An innovative business environment can be sustained only if security is embedded into the very design of technologies and applications ushering in the transition, so as to mitigate the new risks and securely harness the benefits. This means proactively revising reference architectures and technical standards that are either impractical or of limited value in new paradigms such as software-as-a-service (SaaS), remote operation and dependency on cloud computing.

- The **human capital and consumer participation** dimension considers workforce impact and qualifications. As energy systems become digitized, organizations need to invest in human capital development and prioritize cyber skills and educating employees. The shortage of cybersecurity awareness and skilled cybersecurity personnel often constrains the maturity of workforce within the energy sector.

2

How to cybersecure the energy transition

A set of principles has been developed to ensure a cybersecure energy transition journey.

Energy companies are increasingly digitalizing their operations to optimize the end-to-end value chain. Digitalization is integral to most energy transition strategies, and unavoidably brings a higher exposure to cyberattacks.

To encourage an effective and resilient energy transition, organizations need to embed cybersecurity into the design of technologies, but also into corporate strategies, processes and operations.

The following principles are designed to support organizations and their cyber leaders to build cybersecurity into their organization processes and operations while driving their strategic goals and ensuring a cybersecure energy transition journey:

1. **Prepare the new energy system structure to meet emerging threats**
2. **Invest capital for long-term benefits**
3. **Navigate the regulatory landscape**
4. **Establish cyber-resilient governance for the energy transition**
5. **Build the foundation for an innovative business environment**
6. **Develop strong human capital**

3 Cybersecure energy transition principles – adoption guidelines

Each principle is defined with additional information and brief guidance to help organizations and cyber leaders ensure the effective, cybersecure implementation of the energy transition.

3.1 Prepare the new energy system structure to meet emerging threats

Securing the energy transition requires investing in and embedding cybersecurity into technologies and corporate strategies to harness the benefits of digital transformation.

The energy sector is no stranger to cyberthreats that can upend the production, distribution and storage of energy sources. In recent years, attacks against the Colonial Pipeline[10] and oil terminals across European ports[11] made headlines. As cyberattacks increase in frequency, sophistication and complexity, energy executives have voiced serious concerns over the damage and disruptions resulting from future incidents.

> Many of the risks can be mitigated by building systems with cybersecurity and cyber resilience in mind.

In the context of the energy transition, moving from isolated systems, legacy infrastructure and operational technology to digitally networked greenfield and brownfield energy systems supported by innovative emerging technologies requires a cybersecurity upgrade. Digitized assets offer new efficiencies and allow for the emergence of new business models. At the same time, operating an ever more sophisticated IIoT raises cybersecurity challenges. That said, many of the risks can be mitigated by building systems with cybersecurity and cyber resilience in mind. For example, failure to embed monitoring and detection capabilities in advance may leave companies unable to determine the extent of an attack underway.

Organizations should:

- **Build resilience and security by design into operations, starting with proper access, authorization and authentication management.** It is best practice to restrict access for a given role to the minimum necessary to complete the work. Such restrictions can help prevent accidental data losses in addition to hardening networks against intentional attacks. Given the number of employees and service providers requiring data access, careful definition of roles and proper management of the identity life cycle reduce the proliferation of cybersecurity threats.
- **Develop capabilities in incident response and threat detection to prepare for potential attacks.** Leaders and chief information security officers (CISOs) must continuously exercise these capabilities to meet the needs of connected and evolving assets being deployed to address the energy transition. Many CISOs do not have an up-to-date record of the fleet of assets and resources their organizations operate with. Without a baseline of known devices, identifying malicious devices and actions is more difficult. Those aspiring to build monitoring and detection capabilities can begin by creating asset-management practices that can scale up at the same pace as their organization's energy transition. Automated data collection through endpoint sensors enables monitoring and controls to reduce emissions and increase efficiency. Increasingly, core capabilities such as up-to-date asset inventories

and ways to easily link associated disparate datasets in real time are needed to support the needs of engineering, compliance, trading, maintenance and security. Focusing on resilient sources of truth, like industrial data operations and digital twins maximizes investment in aligned secure operations

- **Collaborate with, and seek support from, government cybersecurity offices and ecosystem partners.** This includes academia, government entities and cross-sectoral organizations such as Information Sharing and Analysis Centers (ISACs) and other experts. Participation in collaboration and information-sharing as well as resilience-planning programmes strengthens cybersecurity, both for individual companies and for the broader energy ecosystem. Governments and sector-level organizations should consider expanding the participant group for resilience exercises to reflect the growing importance of renewable energy and decentralized generation models.

- **Understand and capitalize on the use of emerging technology** by making solutions and technologies easy for teams to identify and use, and by creating automatic tasks. Ensuring that the company's technology stack can securely complete all workflows – and working to anticipate the solutions needed for new workflows – makes teams more cooperative with CISO guidance on cybersecurity. It is also good practice to automate routine tasks performed by the cyber-defence team. For example, if a business experiences frequent changes in the inventory of assets connected to company networks, automating asset inventory will help to provide the cyber-defence team with up-to-date information and clear visibility into the availability and employment of corporate assets.

CASE STUDY 1

Cognite observes containerization of supervisory parts in industrial control systems

Operational technology (OT) security professionals are increasingly moving towards a containerized architecture of the supervisory parts of industrial control systems (ICS), with sensors and other legacy equipment remaining in the field. This emerging architectural trend is gaining adoption in renewables, distributed energy and smaller-scale projects in onshore oil and gas.

The architecture enables asset operators to scale common automation architecture and data governance across the enterprise, supports detection, response and recovery activities at scale, and can support more centralized maintenance and operation among geographically distributed assets. In contrast to traditional automation, assets can be patched in real time without it affecting operations and new vendor features can be pushed after being tested in a containerized test bed. Containerized ICS enables unified security services for monitoring, discovery and protection in a way that traditional on-premises proprietary control systems have not supported at scale.

The adoption of containerized ICS can be a significant accelerator in moving real-time and asset data into a common industrial data operations layer. With this data in the cloud, it is much easier to support the identity management and access control needed for off-premise energy value chain data consumers, such as the operational and maintenance experts, trading, compliance, safety and data scientists that need granular and secured data access to perform their roles.

While containerizing ICS has a number of security and operational benefits, adopting containerized ICS requires: investment in architecture to support data persistence; developing OT security teams with container experience; staffing up centralized oversight management and orchestration; site-to-cloud connectivity improvements; and implementing virtualized test beds to support this constant update cycle.

3.2 Invest capital for long-term benefits

The energy transition will be driven by investment. Embedding cybersecurity by design both protects and reduces future investments.

Putting the world on a path to achieve the energy transition requires a substantial increase in clean energy assets and new technologies. These involve relatively high upfront investments that unlock steady returns in the long run resulting from a reduction in the environmental footprint. Though scenarios diverge, annual average clean energy financing represents between $2,250 billion and $4,000 billion, of which 70% is expected to come from private developers, consumers and financiers.[12]

Building and embedding cybersecurity into these energy systems by design increases the upfront capital costs yet reduces the overall risk to facilities and supply chains and ultimately can reduce variables ranging from staffing to re-architecting systems and even insurance premiums. Currently, quantifying cyber risks remains a challenge due to numerous contributing factors including human error and the multiplication of cyberthreats such as ransomware. The difficulty of quantifying cyber risk extends to cyber insurance, meaning companies struggle to implement the financial strategies designed to mitigate risk. Many energy companies are gaining capabilities in terms of calculating and communicating the cost of cyber risks. This cost is key in creating an economic business case that corporate boards understand, which leads ultimately to their support of higher-impact security investments.

> Investments in cyber resilience are still scarce, with 97% of oil and gas organizations investing less than 1% of their revenue on cyber-resilience initiatives.

While investment in innovative technologies will always involve some level of risk, cybersecurity should be a basic consideration for any energy-transition project. Energy systems should be designed to not only reduce cyber vulnerabilities that may be of human or technical origin, but to also allow for a quick containment of, and recovery following, an incident. For that reason, systems should be segmented to limit the propagation of a breach when one occurs.

"Secure by design" should not be regarded as a one-time effort to fight cyberthreats. Cybersecurity and cyber resilience present a moving target, and part of "security by design" is ensuring systems will be adaptable to the changing digital environment – and that the personnel and budget exist to implement such updates. New technologies being adopted in energy support an ability to secure assets throughout their life cycle with significantly decreased operational impacts. For example, an emergent trend towards a cloud-first automation strategy can address some of the main challenges of traditional on-premises automation. These include: disparate architectures and naming conventions by site; minimal capability to monitor OT environments at scale; and long test/patch cycles.

Corporate executives need to **shift from a cost-based to a protect-the-investment-based discussion**. Any initiative that secures the energy transition is a long-term investment**.** Complying with security standards or regulations is now an entry requirement for market access. Security measures can become a vector of trust with markets (shareholders, consumers) and authorities, demonstrating a credible commitment to protecting investments. For more sophisticated investors, the presence or absence of cybersecurity considerations may affect the creditworthiness of a project or company. Cybersecurity is an investment that builds reliable service and a reputable brand and, as such, translates into business opportunity.

That said, for many organizations in the energy sector, investments in cyber resilience are still scarce, with 97% of oil and gas organizations investing less than 1% of their revenue on cyber-resilience initiatives.[13] Organizational leadership can and should move beyond a compliance approach by ensuring that security is built into the organizational culture, operations and technology solutions.

Organizations should:

- **Make cyber resilience a business imperative** of the energy transition strategy, and part of the corporate story. Executive leadership needs to be aware of the risks that affect their organization, ecosystem and customer landscapes. Cyber leaders should educate and proactively communicate with executives and the board to convey cyber resilience as a business risk. To seek support and investment, it is necessary to explain that a cyber incident is a "when" and not an "if" by using scenarios and real-world examples of the potential current and future disruptive impacts. Showing that cyberattacks are constant, escalating and innovative may help leadership executives better understand the exposure of their respective organizations to cyber risk and prioritize investments accordingly to integrate cyber resilience by design.
- **Invest in forward-looking technology roadmap** and make smart investments in technology that will become the legacy environment of tomorrow. Cybersecurity that was an afterthought or retrofit in past design

cycles has created difficult technical challenges for current practitioners. Considering forward compatibility can help reduce future costs for creating and maintaining enterprise-wide cybersecurity. This forward-leaning design focus could consider architecture that supports data persistence, developing OT security teams with container experience, staffing centralized oversight management and orchestration, site-to-cloud connectivity improvements and implementing virtualized test beds to support this constant update cycle. Considering this investment in greenfield projects can also reduce security-related automation costs tied to regulatory compliance – such as incident reporting – and monitoring systems designed for industrial operating environments.

– **Set cyber resilience as mandatory when performing business investments** by collaborating within and beyond the security organization to reach a high-resilience standard. When newly acquired companies join a large organization, integrating their work sites, technologies and personnel into the enterprise-wide cybersecurity programme will be necessary. Such integration requires both technical and social skills – ideally establishing a relationship that enables newcomers to feel empowered, not threatened, by the focus on stronger security. Likewise, when working with suppliers or downstream customers, managing a common position to ensure all participants collaborate and meet robust cybersecurity standards is a mutual benefit.[14]

CASE STUDY 2

Energias de Portugal (EDP) raises cyber awareness for long-term business investments

In a period of true transformation and transition for the energy sector, cybersecurity issues become a driver that influences this evolution. To improve, modernize and innovate business services, ensuring the trust and security of the service becomes paramount.

The evolution and growth of electric vehicle (EV) charging stations essentially using IoT components is a prime example. With the introduction of these stations and to ensure their secure use, the EDP cybersecurity team invested in a security assessment of previously installed charging stations.

While the results of the security assessment did not identify any highly critical issues, some of the models evaluated presented a set of vulnerabilities of medium severity. These results were decisive in educating and increasing the awareness of the key people responsible for managing the charging station services. Moreover, it led to the involvement of the cybersecurity team in the production of technical specifications and necessary security requirements for the renovation and acquisition process for new electric vehicle charging stations. These exercises contributed to the creation of two checklists of security controls: one for IoT components in general, and the other a technically specific list for EV charging stations.

3.3 Navigate the regulatory landscape

Reduce risk by understanding political and regulatory insights. International political commitments and domestic policy mandates made by governments shape the technologies and business models required to advance and secure the energy transition.

Cybersecurity is a global risk that crosses borders and industries. Efforts to mitigate cyber risks are mostly fragmented at the level of national regulatory frameworks. This means that along with the global pace of technological change and dynamic business models driving the energy transition, a country's political landscape will drive the policy frameworks and regulatory structures that affect an energy company's business and investment decisions. A government's commitment to reduce emissions, or mandates to deploy clean energy technologies on an international basis, are often shaped by a wide range of domestic factors, such as the country's energy mix and infrastructure base, as well as its national security interests, economic and social needs, and climate ambitions. This will require a vastly different approach to digital technology adoption, regulation and cybersecurity.

Governments, policy-makers and regulators have been active in moving forward with policies and regulations that cover cybersecurity as a key part of their energy transition initiatives. With regulatory compliance often being a burden for cyber leaders, as confirmed by 54% of oil and gas organizations, it is important, to navigate and help improve the regulatory landscape.[15]

Organizations should:

- **Plan ahead for political and regulatory risk.** Physical energy assets are long-term investments that deliver returns over decades. However, with the rapid proliferation of cyberthreats, their functioning and resiliency can come under threat. Energy companies, therefore, must ensure that their investments can evolve with the rapid pace of digitalization – changing management needs will arise at the pace of regulatory changes. Each national or regional regulatory environment brings unique challenges and opportunities for the energy transition, but all will see changes over the expected lifespan of energy infrastructure. The regulatory environment can shift rapidly depending on changes in political and policy environments, or major incidents such as the Colonial Pipeline attack.

- **Understand the global and local regulatory and policy environment and how these structures are shaped,** which, in turn, can make it less challenging for leaders to mitigate and understand the systemic risk as they consider new investments in physical and digital assets, business model projections and cybersecurity requirements. For instance, the European Union has set cyber resilience as a priority for the energy transition, taking a systemic approach by proposing a set of new policies that include the revised Network and Information Security Directive (NIS2)[16] and the Cyber Resilience Act,[17] to be adopted by and translated for each EU member state regulatory environment. Similarly, through the Cybersecurity and Infrastructure Security Agency (CISA), the United States' new policies have expressly addressed cyber resilience in mission-critical industries such as energy.

- **Use the regulatory process as an opportunity to work with government officials and ecosystem players.** Regulators often seek input from industry leaders and CISOs on new regulatory proposals and policies before they are implemented. Organizations should use their leaders to communicate clearly to authorities throughout each stage of the regulatory process to make sure the upcoming regulatory framework will be **achievable, actionable and sustainable.** Meanwhile, public-sector leaders can encourage private-sector adoption by basing regulatory frameworks on pricing, penalties and/or credit to convince organizations to address energy transition and security.

- **Leverage international commitments and domestic policies to guide future cybersecurity needs.** Nationally determined contributions (NDCs) to the 2016 Paris Climate Accord indicate the intentions governments bring to their future energy infrastructure. Likewise, government reports and other domestic policies signal the type of energy system governments will support. Companies can use these signals to infer the level of digital sophistication and cybersecurity that will be required to manage critical infrastructure. Policy incentives and regulatory requirements typically align with policy targets, giving financial reasons to attend to these signals.

CASE STUDY 3

Schneider Electric plays an active role in the evolution of cybersecurity policies

The constant onslaught of cyberattacks has forced governments throughout the world to introduce new approaches to the shoring up of their digital defences and economies. In many cases, key players such as the European Union, the US and China have introduced new regulatory measures to ensure improved cybersecurity for citizens and businesses.

That said, Schneider Electric views this ever-evolving regulatory landscape as an opportunity to continuously improve its posture and raise its defence levels across its value chain. The company promotes the use of internationally accepted cybersecurity standards and information-sharing frameworks in every region in which it operates to enhance the level of trust between industries and governments. Schneider Electric also plays an active part in the evolution of cybersecurity policies, by participating in over 30 globally recognized external organizations focused on advancing the regulatory environment from standards development organizations, trade associations and non-governmental organizations globally to advance the interests of customers and industry.

In this complex regulatory environment, processes and products need to evolve as quickly as possible in order to stay ahead of governmental expectations and continue the improvement of security posture for the organization's customers and partners.

3.4 Establish cyber-resilient governance for the energy transition

In an integrated and distributed energy ecosystem, navigating multiple stakeholders and existing regulations, and anticipating new rules across national and regional governments, is a must to secure access to markets.

Many energy industry governance[18] models and institutions originated during eras when the most common business models involved centralized energy production and distribution. The energy transition is upending these decades-old paradigms by enabling new models, such as distributed generation and producer-consumers. Keeping up with these changes may strain existing governance or require institutional change.

Scaling cybersecurity along with the energy transition requires strengthening and, in some cases, reimagining the institutions and governance models that dictate security requirements for infrastructure. Ultimately, **effective governance models and institutions are built on trust**. Their role is to **establish clear rules and responsibilities** for regulators, policy-makers and the energy sector, especially when it comes to navigating the full ecosystem, incident reporting and information sharing to enable a "chain of trust" of entities.[19]

Incident reporting and data sharing requires companies to understand: how, when and with whom to share information; the legal implications and protections afforded to participating companies sharing information with the government or regulatory bodies; how data is protected and anonymized, used and shared throughout the ecosystem; how to access synthesized and actionable intelligence after it is compiled.

Organizations should:

- **Ensure organizational design supports cybersecurity.** Organizations should design an internal governance structure that addresses cybersecurity on an enterprise-wide basis. Throughout planning, design and operations, cybersecurity should be embedded as a value and practice. Cyber resilience is a shared responsibility guided and coordinated by the CISO and is not the responsibility of any single individual. This includes defining clear ownership and responsibilities across all internal and external stakeholders, and integrating cybersecurity practices into business operations, decision-making and energy ecosystem partnerships.
- **Understand the existing and global frameworks** available to adopt and implement cyber resilience. Technical and legal frameworks are needed to cover how cyber-resilience data will be shared, handled, stored and then distributed back to energy and private-sector companies. Ensure that information sharing produces actionable intelligence in near real

time. If companies fear that information sharing will produce negative legal repercussions or fines, they will be more reluctant and slower to share information. Incident-reporting and information-sharing requirements differ significantly from country to country and sector to sector. In general, energy companies should monitor and detect threats, and then share data with the locally appropriate governments, private-sector partners such as suppliers, and industry incident-reporting non-profits, such as ISACs.

– **Build monitoring, detection and response capacities.** Organizations should ensure they have the technologies, personnel and capabilities to meet regulatory requirements. They should request and discuss different forms of support and incentives to scale solutions and resources to meet government regulations. Governments are poised to require reporting requirements for energy companies that have detected a possible or attempted breach to their IT and OT systems. Often, CISOs will be required to report these incidents within 24 or 36 hours after they occur. This means that CISOs must have the capabilities to monitor, detect and respond to anomalous behaviour on their networks rapidly and accurately to fulfil a regulator's reporting requirements.

– **Develop relationships before incidents occur**. Should a cyberthreat occur, it should not be the first time an energy company CISO has engaged with government officials, regulators and independent information-sharing organizations. Rather, organizations should work closely with government officials and regulators **before potential cyberthreats** to ensure incident reporting and information-sharing systems are well understood. Such planning will help to mitigate vulnerabilities early and respond to incidents more rapidly in real time. Tabletop exercises can strengthen cross-sector and public-private relationships and resilience.

CASE STUDY 4

Siemens Energy and the Global Resilience Federation cooperate on information sharing

Being able to quickly understand threats is critical to security and resilience. Information sharing helps energy-sector organizations blunt the potency of known attack methods and identify new threats. ISACs have been built to serve subsectors and industry verticals. As the energy sector is transformed by digitization and the energy transition, information-sharing efforts in the energy sector also need to evolve to embrace new classes of energy companies that are more distributed and interconnected.

To secure digitized and digitally native operational technologies (OT) and cyber-physical systems, organizations need the capability to share OT threat data – not only with their peer organizations and asset operators, but also with equipment manufacturers and other supply-chain partners across the full spectrum of energy companies. To share information at speeds that keep pace with threats, organizations must build stronger capabilities to identify anomalous activity and automate information sharing.

With that need in mind, Siemens Energy and the Global Resilience Federation are launching a new initiative aimed at developing next-generation information-sharing capabilities that bridge industry silos and emphasize automated threat detection. This initiative will work towards the goal of sharing IT and OT threat information at machine-like speeds – fast enough to be relevant for the early detection of novel threats.

Using advanced capabilities and built-for-purpose industrial cybersecurity technologies, the initiative addresses cybersecurity challenges exacerbated by the energy transition. The aim of the initiative is to build greater awareness of threats and create collaboration to address new risks to the rapidly evolving energy ecosystem.

3.5 Build the foundation for an innovative business environment

The availability of cybersecurity solutions and expertise is a constraint for many post-transition energy businesses.

Policy-makers, investors and energy companies each have a shared interest in sustaining a market where high-quality cybersecurity skills, services and technologies are readily available to support the energy transition. Strategically, energy companies must view **cybersecurity as a key enabler essential to ensure and accelerate business performance, rather than a cost to be minimized**. This shift in mindset is gradually unfolding, with forecasts predicting that cybersecurity spending in the energy sector will reach $10 billion by 2025.[20] Ideally, companies should clearly communicate to their business partners about their cyber-risk management approaches, allowing cyber-mature organizations to differentiate themselves from the competition. Finding ways to demonstrate cybersecurity as a unique selling proposition to potential investors, partners and customers will eventually allow leaders to create and sustain an innovative business environment and send clearer price signals about the market value of cybersecurity.

To ensure the resilience of energy systems today, businesses must take tactical steps to reduce cyber risk, with minimal operation disruptions, while keeping an eye on costs and supply-chain complexity. The reliance on and number of active third-party suppliers is growing, with the 20 most prominent energy organizations in North America working, on average, with more than 3,600 suppliers.[21] Yet energy organizations have very little oversight of suppliers' levels of cybersecurity protection and capabilities, with only 67% undergoing warranted due diligence checks.[22] Energy executives must therefore work with their CISOs and business unit managers to manage investment, procurement and supply-chain risk both internally and with third parties to incorporate cybersecurity into all facets of the business.

Organizations should:

- **Make cybersecurity a core competency.** Organizations should determine how they will measure risk and prioritize the most relevant and efficient risk-management practices. Companies beginning their cybersecurity journey need to focus on the risks that would present the greatest impact to their organizations. Energy companies that can demonstrate exceptional cyber hygiene, consistent adherence to a technology standards regime, and their own investments in cybersecurity technology and protocols may be able to market cybersecurity as a unique selling proposition or indicator of reliability.
- **Focus on basic hygiene** as a first step to demonstrate commitment to high cybersecurity standards. Many companies have not yet implemented relatively simple and low-cost security measures such as two-factor authentication that can make a big difference to corporate security. Once the basics have been covered, energy-sector leaders should focus on more sophisticated protocols including establishing a security operations centre (SOC) capable of monitoring and detecting OT and IT threats.
- **Support clear cybersecurity standards.** Private-sector leaders reduce business risk and strengthen cybersecurity by working with regulators and original equipment manufacturers (OEMs) to identify approved technology vendors. Without clear guidance from governments, companies struggle to make long-term investments that meet their business needs but also comply with security protocols.
- **Adopt standard technology and procurement frameworks,** such as NIST or the ISA/IEC 62443 series of cybersecurity standards, to help streamline procurement and compliance requirements. Complying with or following international and well-understood standards will help regulators, OEMs and suppliers meet rigorous cybersecurity protocols while allowing energy companies to deploy affordable and reliable technologies that best support their business.
- **Focus on supply-chain security.** A vast interdependent network of physical and digital technologies is being deployed and procured as energy companies expand into new businesses models. However, each of these procured or contracted technologies poses a potential cyber vulnerability. Attackers will target weak links in supply chains in order to compromise the other entities comprising the network. As internal cybersecurity matures, organizations should consider how to manage third-party risks.[23] Companies and suppliers must align and share information on cyber vulnerabilities to ensure the robustness of their respective products and services.

“Companies beginning their cybersecurity journey need to focus on the risks that would present the greatest impact to their organizations.

CASE STUDY 5

Repsol develops a flexible yet robust approach to third-party cybersecurity

Repsol has followed a flexible yet robust third-party cybersecurity management approach. Different supply-chain cybersecurity risk scenarios are treated according to their third-party type, including:

- IT and digital providers
- OT providers with remote or physical access to ICS
- Business providers receiving and keeping sensitive information from Repsol
- Business providers that are critical for maintaining normal business operations

In the search for security and agility, Repsol has also defined clear processes for each scenario. These include:

- A specific internal triage questionnaire, which helps qualify the risk potential of the contract (independent of provider), assigning a risk tier level
- If the tier is medium or high, providers are assessed through security rating tools and questionnaires, according to the type of service
- If the tier is high, certifications are required, additional evidence may be requested and penetration testing could be undertaken
- Depending on the tier level and type of contract, specific clauses are included by default into the final contract with security requirements
- Ensuring that different cases are treated differently is vital to making the process scalable and helps contract holders accept an additional step in the procurement process

3.6 Develop strong human capital

Addressing human capital deficits is the key to improving and ensuring cybersecurity in the energy sector.

Organizations interested in improving cybersecurity increasingly cannot find the needed expertise at affordable price points. Recent reports show that there are more than 3.5 million unfilled cybersecurity positions. This talent shortage becomes a cost and a burden for organizations. According to a Fortinet study, 80% of organizations have experienced one or more security breaches that resulted from a lack of cybersecurity skills or awareness.[24] In addition to the cyber-talent gap, companies also face difficulty in retaining their cyber workforce due to the stress and burnout caused by mounting threats.

Expanding the talent pool of cybersecurity expertise would help scale up and secure the energy transition. Organizations need to develop and support strategies that address end-to-end HR planning.

Organizations should:

- **Work closely with HR and business partners on an ongoing basis to expand, enable and bridge the cyber-talent gap.** Companies should value and retain their **existing talent pool** and seek to generate interest for cyber positions among their employees and contractors. For example, OT personnel could be upskilled to meet the new cybersecurity demands of their role. Organizations should bridge the talent gap within the industry through internal training programmes or by participating in partnerships aimed at job training. Industry surveys indicate that, although many companies report an unmet demand for cybersecurity talent, few companies offer adequate cybersecurity training to meet their own needs.
- **Build a cyber culture to ensure that** cybersecurity is everyone's business in the organization. Cyber hygiene should be an ongoing effort enforced by **periodic training** or **regular phishing campaigns** to increase education and awareness about secure procedures. Another approach to promoting a cyber-aware culture is to require all customer-facing staff, such as those in sales or maintenance roles, to obtain and display a cybersecurity competency badge that assures customers the person entering their site has the proper level of endpoint security and awareness. This serves both to sustain a cyber culture and to build trust with clients.

– **Build an end-to-end talent management programme** where leaders are able to understand what skills will be needed tomorrow, make use of the pools that produce talent, and have a plan for individual growth and retention. In the latter case, mechanisms should be put in place to map employee profiles – in particular, those either at risk of leaving their current position or the most promising ones. Organizations should also devise key employee retention plans and programmes.

CASE STUDY 6

People as a key element in the transformation of cybersecurity at Ecopetrol

In recent years, Ecopetrol has developed a comprehensive cybersecurity strategy to improve its digital security posture. As part of this strategy, culture has been established as a priority to improve the general awareness of employees and the corporate mentality towards cybersecurity risks at the company. Transforming and strengthening cybersecurity culture and behaviours establishes three pillars: 1. training (the development of new skills); 2. mobilization (driving and appropriating change); and 3. communication (encouraging understanding and cyber-savvy behaviours).

As part of the strategy of transformation and reduction of cyber risk, during the past year Ecopetrol has carried out some relevant actions:

1. Established a Science, Technology and Innovation month, where cybersecurity played a vital role in raising awareness about cyber risks. Various pieces of content were designed and distributed to more than 9,000 collaborators, 25,000 contractors and officials of the subsidiaries of the Ecopetrol group on important topics such as phishing, secure passwords, good practice in corporate emails and the use of information repositories. The company also created and strengthened a network of 300-plus champions or cyber guardians around the Ecopetrol group, with cybersecurity campaigns aimed at key processes in regard to, for example, exploration, projects, health, safety and the environment.

2. Generated innovative cybersecurity-related themes such as “the magic or thinking of Disney villains”, “in the minds of hackers” and “social engineering”.

3. Held face-to-face conversations in different locations with more than 1,600 employees to promote the prevention of digital risks and the impact of cybersecurity in OT environments, using clear and simple language to explain the relevance of digital security in the day-to-day operations of the company.

Ecopetrol is transforming the perception and culture of cybersecurity, making it innovative, close and essential in the work and home environments. For this, the processes, resources and support of senior management have been consolidated to implement short- and medium-term actions that make people the “human firewall” – the first and most relevant protection against digital threats.

Conclusion

Building secure, reliable, low-emissions energy infrastructure is an essential task. Companies are shifting their business model to design a sustainable future with digital enablers: digitalization; the adoption of emerging technologies; and the integration of new assets and decentralized energy systems.

Regardless of the obvious benefits, the sustainability of such a model relies on its resilience over time. Security should therefore be an integral part of the strategy to achieve a low-emissions energy transition.

With recent highly publicized cyberattacks, cybersecurity has become a top concern among leaders. However, it remains a burden rather than a strategic asset. The extent to which this mindset is reversed and cyber is integrated into the business value proposition will determine whether organizations will advance or impede the progress of the energy transition.

The performance of existing energy systems will depend on digital technologies and will be more reliable if strong cybersecurity measures are in place. An innovative business environment can be sustained only if security is embedded in the very design of technologies and applications ushering in the transition so as to mitigate the new risks and securely harness the benefits.

Energy-sector leaders should seek to invest in cybersecurity tools, resources and talent to manage their attack surface, reduce the risks and ensure an adequate level of protection for their operational infrastructure and assets. Finally, governments and energy-sector leaders must work together to create a strong ecosystem for cybersecurity that supports the sector. With approaches that encourage resilience and embrace security by design, leaders can ensure that cybersecurity enhances each of the enabling dimensions critical to energy transition readiness.

Contributors

Lead Authors

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

Andrew Gumbiner
Adviser, Policy Strategy, Siemens Energy, Germany

John La Rue
Adviser, Policy Strategy, Siemens Energy, Germany

Natasa Perucica
Research and Analysis Specialist, Centre for Cybersecurity, World Economic Forum, Switzerland

Elisabeth Williamson
Platform Fellow, Centre for Cybersecurity, World Economic Forum, Switzerland

Acknowledgements

Working Group chair

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

Community

The World Economic Forum would like to extend its sincere thanks to the cyber leaders who contributed their valuable insights and perspectives to this Community Paper. The following individuals led in-depth discussions as part of the action group dedicated to Securing the Energy Transition.

Edgardo Arrieta Arteta
Ecopetrol, Colombia

Neelakarun Asari
HCL Technologies, India

Ali H. Asseri
Saudi Aramco, Saudi Arabia

Christophe Blassiau
Schneider Electric, France

Jose Manuel Cabrera Pozuelos
Repsol, Spain

Giovanni Cock
Ecopetrol, Colombia

Stefan Deutscher
Boston Consulting Group, Germany

Javier Garcia Quintela
Repsol, Spain

Rosa Kariger
Iberdrola, Spain

Sigmund Kristiansen
Aker BP, Norway

Paulo Moniz
Energias de Portugal (EDP), Portugal

Luis Filipe Morais
Galp, Portugal

Rishi Muchalla
Check Point Software Technologies, Canada

Mark Orsi
Global Resilience Federation, US

Haider Pasha
Palo Alto Networks, US

Susan Peterson Sturm
Cognite, US

Amir Abdul Samad
PETRONAS, Malaysia

Leo Simonovich
Siemens Energy, US

Swantje Westpfahl
Institute for Security and Safety, Germany

Olivera Zatezalo
Suncor Energy, Canada

The World Economic Forum also wishes to acknowledge the contribution of Anders Rimstad, Chief Security Officer, Aker, Norway, to the action group's activities.

Endnotes

1. United Nations Climate Change, "COP27", 2022: https://unfccc.int/event/cop-27 (accessed 30 November 2022).
2. BloombergNEF, "Energy Transition Investment Trends 2022", January 2022: https://assets.bbhub.io/professional/sites/24/Energy-Transition-Investment-Trends-Exec-Summary-2022.pdf (accessed 11 November 2022).
3. European Commission, "Renewable Technologies in the EU Electricity Sector: Trends and Projections", 2017, https://publications.jrc.ec.europa.eu/repository/handle/JRC109254 (accessed 30 November 2022).
4. U.S. Department of Energy, "Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid", October 2022: https://www.energy.gov/sites/default/files/2022-10/Cybersecurity%20Considerations%20for%20Distributed%20Energy%20Resources%20on%20the%20U.S.%20Electric%20Grid.pdf (accessed 11 November 2022).
5. World Economic Forum, "Global Cybersecurity Outlook 2022", January 2022: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf (accessed 11 November 2022).
6. Robertson, J. and Chapa, S. "Hackers Targeted U.S. LNG Producers in Run-Up to Ukraine War", Bloomberg, 7 March 2022: https://www.bloomberg.com/news/articles/2022-03-07/hackers-targeted-u-s-lng-producers-in-run-up-to-war-in-ukraine (accessed 29 November 2022).
7. DNV, "The Cyber Priority: The State of Cyber Security in the Energy Sector", May 2022: https://brandcentral.dnv.com/fr/gallery/10651/files/original/e45ef6c8-fb14-4b0c-98f3-caa889584cd9.pdf?_ga=2.12780983.1849343128.1665572575-996463403.1665572575 (accessed 11 November 2022).
8. Ibid.
9. World Economic Forum, "Fostering Effective Energy Transition: 2021 Edition", April 2021: https://www3.weforum.org/docs/WEF_Fostering_Effective_Energy_Transition_2021.pdf (accessed 11 November 2022).
10. Bing, C. and Kelly, S., "Cyberattack Shuts Down U.S. Fuel Pipeline 'Jugular,' Biden Briefed", Reuters, 8 May 2021: https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/ (accessed 11 November 2022).
11. Staden-Coats, R. and Gupta, E., "Cyberattack Causes Chaos at Key European Oil Terminals", S&P Global, 3 February 2022: https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/oil/020322-cyberattack-causes-chaos-at-key-european-oil-terminals (accessed 11 November 2022).
12. Gupta, S. and Lam, S., "How Digital Transformation Must Go in Hand With Cyber Resilience", EY, 26 November 2021: https://www.ey.com/en_vn/oil-gas/how-digital-transformation-must-go-in-hand-with-cyber-resilience (accessed 11 November 2022).
13. Ibid.
14. Kariger, R. and Blassiau, C., "Cybersecurity in the Energy Industry: Why Working Together across the Value Chain Is Vital for Resilience", World Economic Forum, 1 November 2022, https://www.weforum.org/agenda/2022/11/cybersecurity-energy-sector-trust-value-chain/ (accessed 11 November 2022).
15. Ayoub, R., "How Oil and Gas Security Leaders Can Smooth the Transformation Path", EY, 30 September 2021: https://www.ey.com/en_lu/oil-gas/how-oil-and-gas-security-leaders-can-smooth-the-transformation-path (accessed 11 November 2022).
16. Think Tank, "The NIS2 Directive: A High Common Level of Cybersecurity in the EU", European Commission, 16 June 2022: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333 (accessed 11 November 2022).
17. European Commission, "Cyber Resilience Act: New EU Cybersecurity Rules Ensure More Secure Hardware and Software Products", 15 September 2022: https://digital-strategy.ec.europa.eu/en/news/new-eu-cybersecurity-rules-ensure-more-secure-hardware-and-software-products (accessed 11 November 2022).
18. Note that "governance" here means the set of relationships between governments and energy sector organizations. Corporate governance – the set of relationships of subcomponents and individuals within a given company – is a related concept also important to cybersecurity but is not the meaning used in the World Economic Forum enabling dimensions.
19. World Economic Forum, "Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain", December 2020: https://www3.weforum.org/docs/WEF_Securing_the_Electricity_Value_Chain_2020.pdf (accessed 11 November 2022).
20. GlobalData, "Cybersecurity Spending in the Energy Industry Will Rise to $10 Billion by 2025 as Digitalization Brings Risks as Well as Rewards", 14 July 2022: https://www.globaldata.com/media/thematic-research/cybersecurity-spending-energy-industry-will-rise-10-billion-2025-digitalization-brings-risks-well-rewards-says-globaldata/ (accessed 11 November 2022).
21. Livingston, S., Slaughter, A. and Zonneveld, P., "Managing Cyber Risk in the Electric Power Sector", Deloitte Insights: https://www2.deloitte.com/content/dam/insights/us/articles/4921_Managing-cyber-risk-Electric-energy/DI_Managing-cyber-risk.pdf (accessed 11 November 2022).
22. Refinitiv, "Refinitiv Due Diligence, Third-Party Risk Reports": https://www.refinitiv.com/content/dam/marketing/en_us/documents/brochures/refinitiv-due-diligence-third-party-risk-reports-brochure.pdf (accessed 11 November 2022).
23. World Economic Forum, "Advancing Supply Chain Security in Oil and Gas: An Industry Analysis", 2021: https://www3.weforum.org/docs/WEF_Advancing_Supply_Chain_Security_in_Oil_and_Gas_2021.pdf (accessed 29 November 2022).
24. Fortinet, "2022 Cybersecurity Skills Gap": https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf?utm_source=pr&utm_campaign=report-2022-skills-gap-survey.

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