International Energy Agency

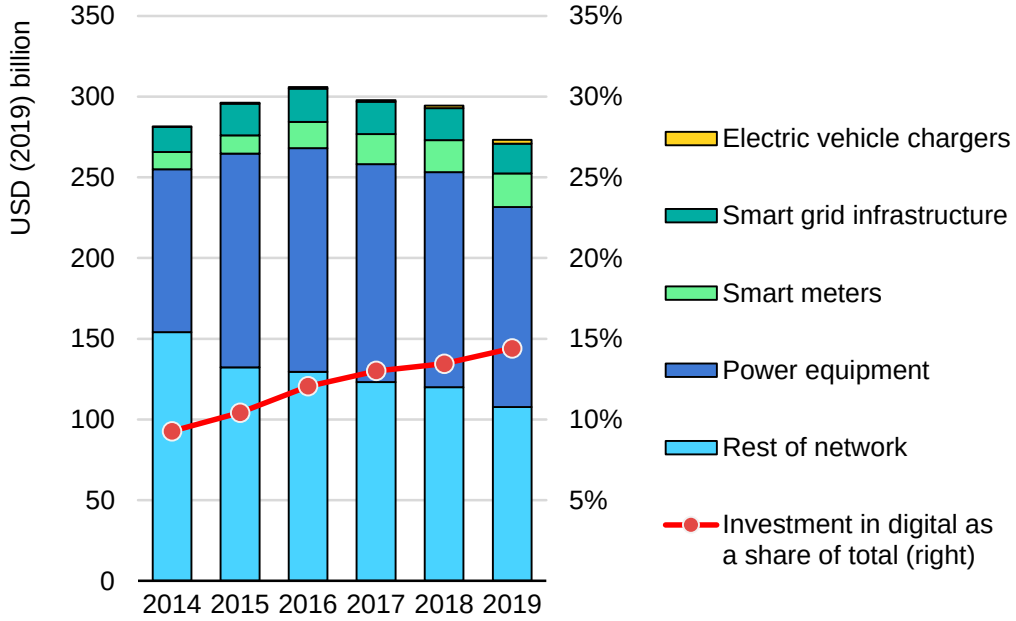
Enhancing cyber resilience in electricity systems

Part of *Electricity Security 2021*

Launch presentation – 12 April 2020

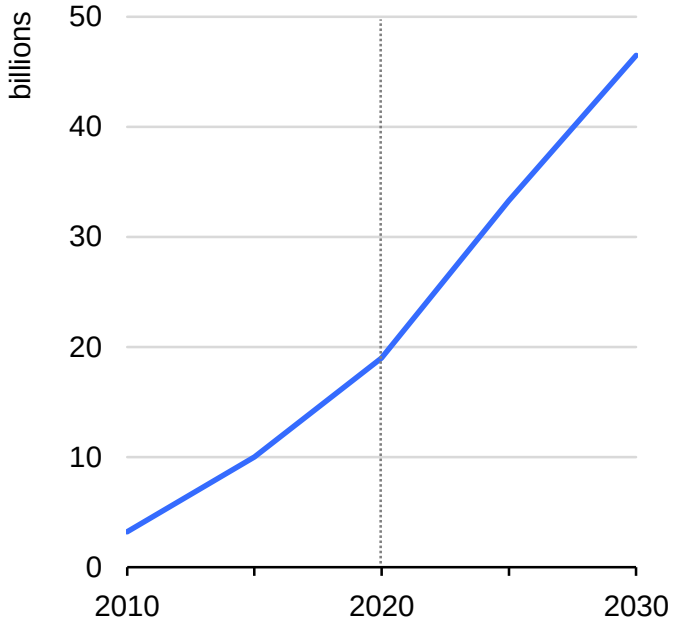
The electricity system is increasingly digitalising…

Investment in electricity networks, 2014-2019



IEA (2020), World Energy Investment.

Connected devices worldwide, 2010-2030

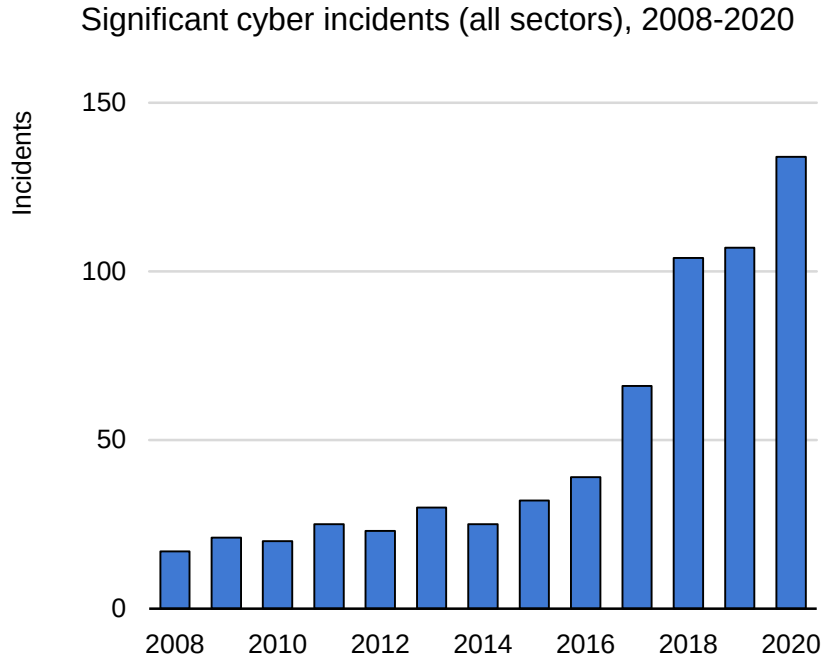


IEA 4E EDNA (2019), Total Energy Model for Connected Devices.

…bringing many benefits for electricity and clean energy transitions

Generation	Transmission & distribution	Consumers and DERs
• Improved efficiency • Predictive maintenance • Reduced downtime • Lifetime extension • Renewables forecasting	• Improved efficiency of assets and wider system operations • Predictive maintenance • Reduced downtime with faster fault localisation • Lifetime extension • Grid stability monitoring • Enhanced local flexibility options	• Demand response, including vehicle-to-grid (V2G) • Demand forecasting • Energy management • Smart buildings

But digitalisation comes with risks to cybersecurity



Note: Significant incidents are defined as cyber-attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars.
Source: Center for Strategic and International Studies (2020), Significant Cyber Incidents.

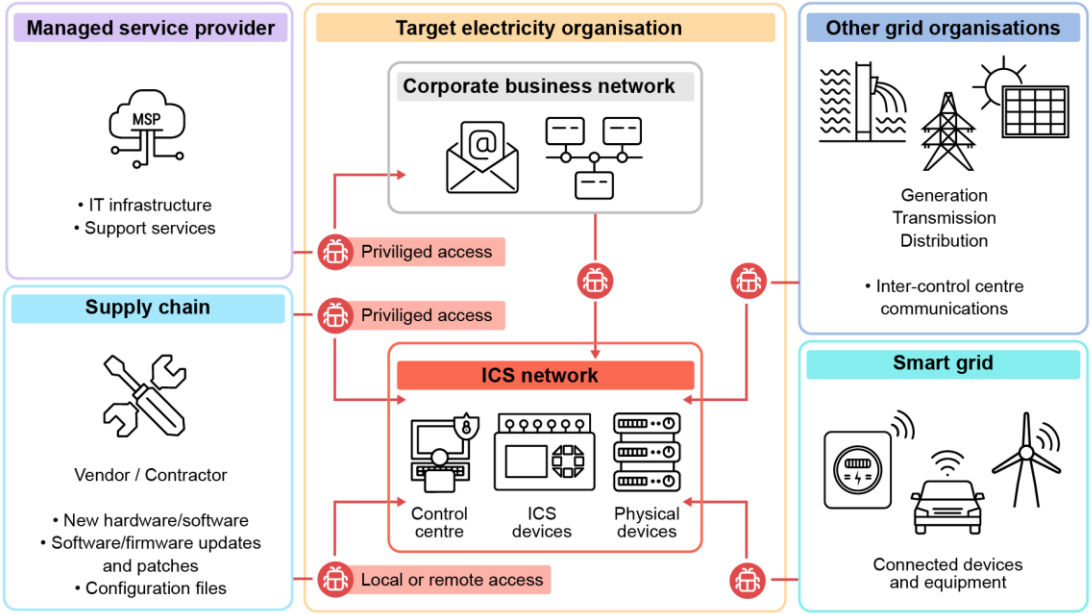
Selected electricity-related cyber incidents in 2020

- Supply chain cyberattack on IT service provider
- Ransomware attack on market operator in the UK
- Ransomware attack on Canadian utility
- Ransomware attack on Portuguese utility
- Intrusion of internal information exchange platform of European TSO association
- Ransomware attack on US equipment vendor

The threat of cyberattack is substantial and growing, and threat actors are becoming increasingly sophisticated at carrying out attacks – both in their ability to identify vulnerabilities and their destructive capabilities.

There are numerous potential cyberattack scenarios and impacts

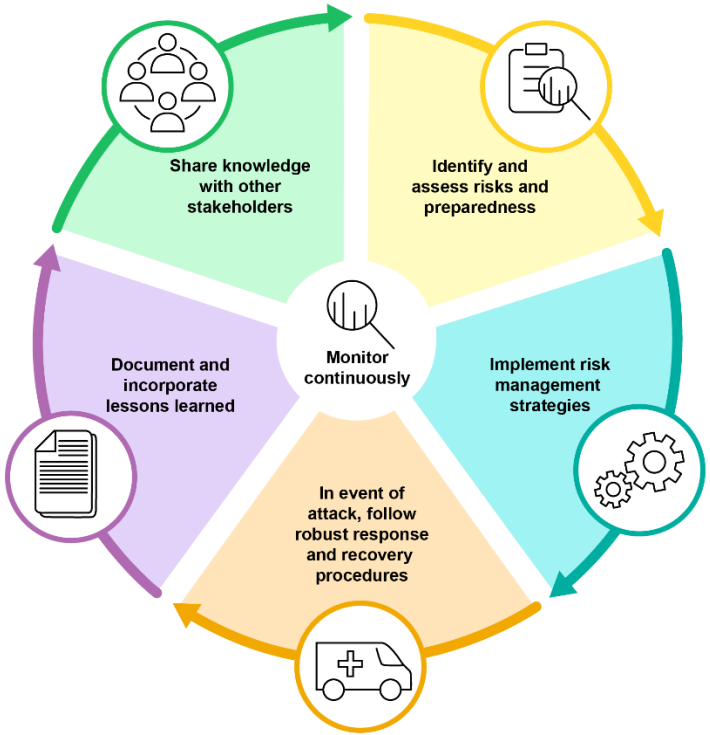
Potential ways an attacker could compromise industrial control systems



IEA analysis based on Canadian Centre for Cyber Security (2020) and US Government Accountability Office (2019).

A successful cyberattack could trigger the loss of control over devices and processes, in turn causing physical damage and widespread service disruption.

Enhancing cyber resilience is a continuous process



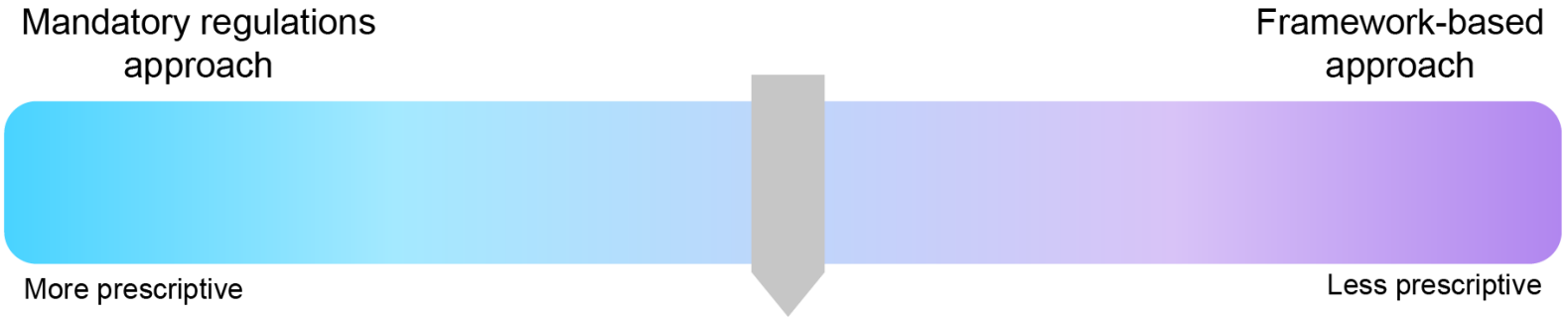
While the full prevention of all attacks is not possible, electricity systems must become more cyber resilient – to withstand, adapt to, and rapidly recover from attacks.

Policy makers are central to enhancing cyber resilience

- **Institutionalise:** set appropriate responsibilities and incentives for relevant organisations within their jurisdiction.
- **Identify risks:** ensure that operators of critical electricity infrastructure identify, assess and communicate critical risks.
- **Manage and mitigate risk:** collaborate with industry to improve readiness across the entire electricity system-value chain.
- **Monitor progress:** ensure mechanisms and tools are in place to evaluate and monitor risks and preparedness, and track progress over time.
- **Respond and recover:** enhance the response and recovery mechanisms of electricity sector stakeholders.

Tailoring policy and regulatory approaches

The regulatory spectrum for ensuring cybersecurity – the balance between prescription and outcome



Requirements to meet specific standards ensures:

+ minimum level across networks
+ streamlined monitoring for compliance
- but regulations can lag behind technology changes and focus more on compliance rather than risk

Establishing common criteria across networks allows:

+ customised approaches to achieve desired outcome
+ focus on outcomes to adapt to evolving risks
- but variable speed and level of cyber resilience risks weak link or contagion

Implementation strategies should be tailored to national contexts while considering the global nature of risks

Summary

- Digitalisation offers many benefits both for electricity systems and clean energy transitions.
- The threat of cyberattacks on electricity systems is substantial and growing.
- While the full prevention of cyberattacks is not possible, electricity systems can become more cyber resilient.
- Policy makers are central to enhancing the cyber resilience of electricity systems.
- Information sharing can enhance cyber resilience across the system for all electricity sector stakeholders.
- A wealth of existing risk management tools, security frameworks, technical measures and self-assessment approaches are available.

The IEA's participation in this event was made possible through the Clean Energy Transitions in Emerging Economies programme has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952363.