Risk Snapshot
Smart Grids

Smart Grids, or electricity networks that intelligently integrate the actions of any connected user–from producers and consumers to prosumers–are enabling the transformation of traditional electricity systems. Increasing numbers of Internet of Things (IoT) devices deployed within electricity networks allow connected users take advantage of real time data to automate decision making and contribute to accelerating the energy transition.[1]

Despite the immense positive potential of IoT technologies to catalyse efficient and sustainable use of electricity–connecting critical infrastructure like the electricity grid to the industrial IoT ecosystem creates new vulnerabilities, potentially resulting in system wide power outages and causing severe negative externalities. Just about everything depends on availability of electricity, including water supply, transport and communication.

Increasing collaboration between multiple stakeholders including, but not limited to, utilities, manufacturers, energy service providers, telecom companies, IT providers and insurance carriers to develop and share best practices and security protocols can help reduce some of the risks and maximise the benefits of Smart Grids.

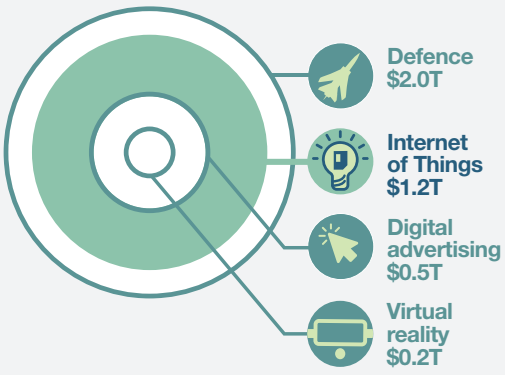
This document offers a brief snapshot illustrating the benefits of adopting IoT in the electricity ecosystem while recognizing that cyber vulnerabilities can compromise critical infrastructure with unintended consequences to the public.

The World Economic Forum has closely worked with the electricity industry to develop best cyber resilience practices contained in the report *Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards*.

Transformation of the electricity industry

Worldwide spending on IoT is forecast to reach $1.2 trillion[2] in 2020. Utilities rank fourth amongst the industries that are forecast to spend the most on IoT.[3]

Estimated global spending in 2022[4]

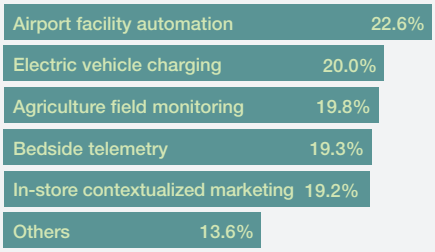


IoT devices embedded within the wider electricity ecosystem enable increased access to and control of electric power. In addition, through the gains in transparency and visibility, Smart Grids empower operators and consumers to influence the efficiency, sustainability and safety of their electricity production, transmission and consumption.

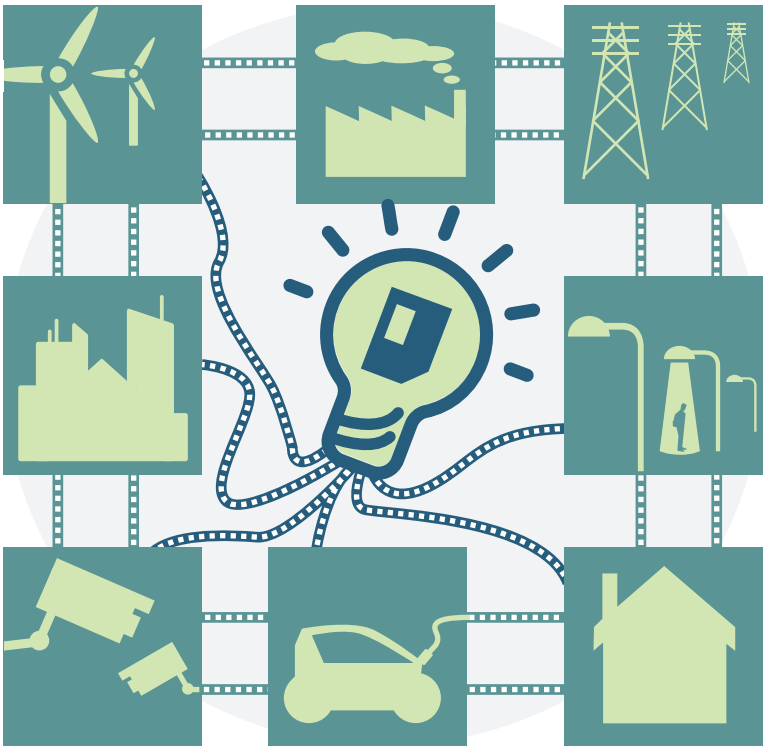
Traditional one-way electricity flows

Fastest spending growth: top 10 IoT use cases 2017-2022

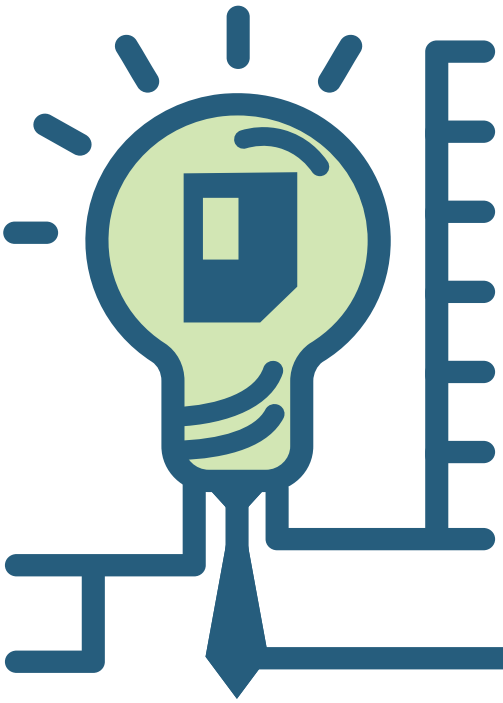
Electric vehicle charging is located within the IoT use cases expected to deliver the fastest spending growth over the 2017-2022 forecast period.[5]



Multi-directional Smart Grid



Smart Grid Benefits

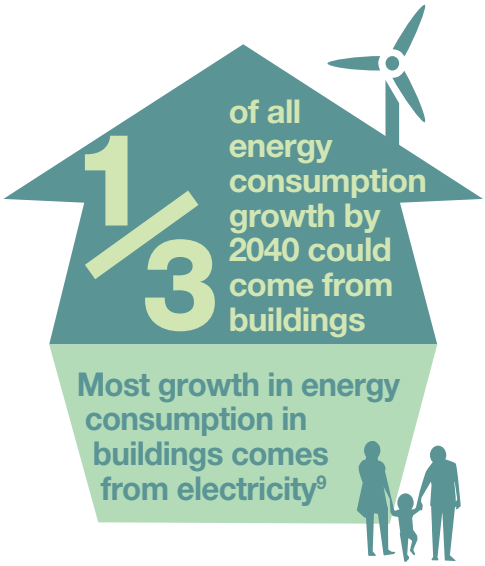


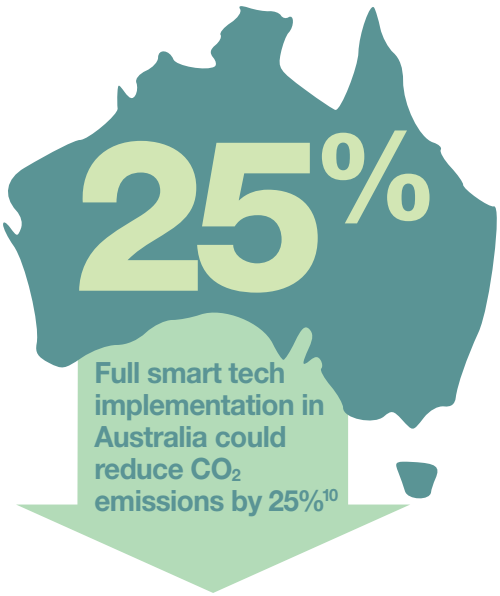
- Detailed information to optimize generation, transmission and consumption
- Efficient management of resources and introduction of renewables
- Reduced reliance on new or inefficent generation
- Greater control over time-based usage
- Faster detection and restoration of service
- Cost savings due to reduced onsite visits and predictive maintenance
- Emergence of new business models

Key findings from the Forum's report on building a flexible and resilient electricity grid indicate that real-time supply and demand platforms, potentially worth $191 billion for the power industry, could deliver a value of $632 billion to society – higher than any other individual digital initiative. This value derives primarily from cost savings to the customer and from reduced carbon emissions.[6]

By 2040 electricity will make up 40% of the expected end-user energy consumption.[7]

As a result of the expected electrification of sectors such as transport and heating, peak electricity demand is predicted to increase significantly by 2050. IoT technologies could potentially reduce peak demand increases by up to 24% across some major regions of the world.[8]





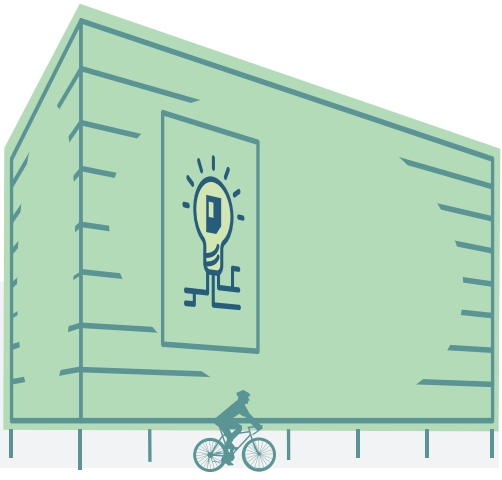
Individuals play a key role in electricity consumption. Faster and better implementation of smart meters can help them monitor–and decrease–energy use.

IoT will be used within distribution systems, including to monitor flows within power substations as well as from transformers to building entries.

The Edge, Amsterdam

The Edge building uses smart grid technologies to create adaptable and intelligent work spaces.

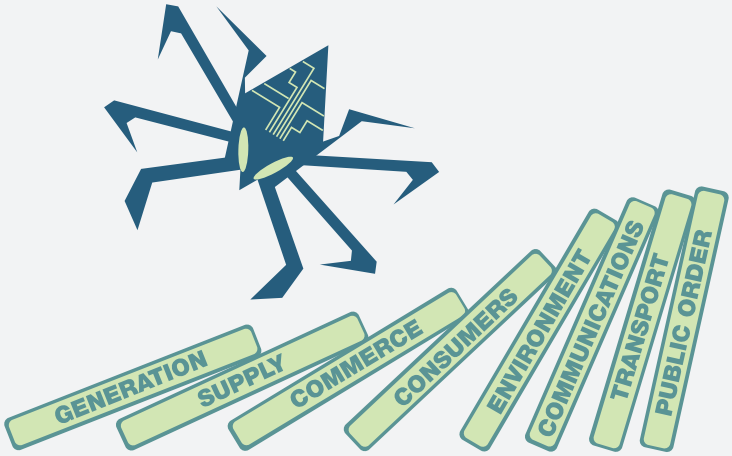
Over ten years, The Edge will save 42 million kg of CO_2 compared with a "normal" building.[11] It is considered the greenest, most intelligent building in the world.



What is at stake?

The increasing use of IoT technologies improves efficiency and facilitates enhanced operation of power systems, but the interconnectedness that results from the integration of cyber-physical systems in critical infrastructures creates new vulnerabilities requiring specific cyber resilience strategies. According to Kirstjen M. Nielsen, former Secretary of Homeland Security of the United States: "Hyperconnectivity means that your risk is now my risk and that an attack on the 'weakest link' can have consequences on us all."[12] Increasing dependence on data-driven automated systems could introduce new types of physical risks, as well as significant financial and economic threats.

The Cyber Attack Cascade



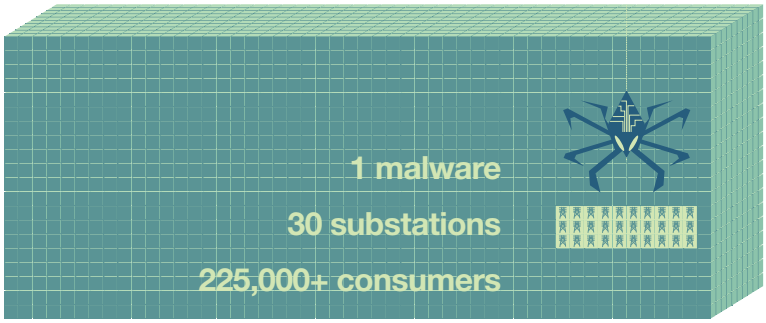
Operators of critical infrastructure face risks that, if exploited by a capable attacker, can have cascading effects that may result in economic loss, industrial disruption, and, in some cases, even the loss of lives.

Resilience is the key to fostering more secure systems. What measures is your company currently implementing?

The World Economic Forum provides Principles and Guidance for Boards

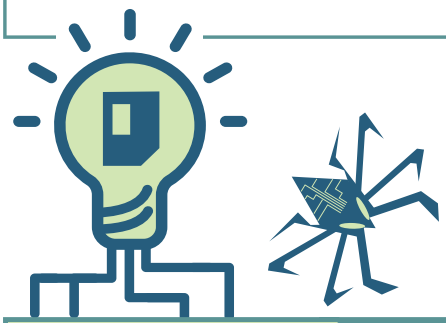
Connectivity is outpacing security

Ukraine cyberattack 2015[14]



Global Risks Report — The five risks most likely to happen in the next 10 years[13]

1. Extreme weather events
2. Failure of climate change mitigation and adaptation
3. Major natural disasters
4. Massive incident of data fraud or theft
5. Large-scale cyberattacks



Smart Grid features pose reciprocal threats

Interoperability	Propagation of failures
Multiplicity of access	Opportunity
Data traffic	Exploitation/privacy risk
Complexity	Range of attacks Likelihood of error

Just about everything depends on the availability of electricity

Cyber resilience is a challenge for all organizations, but it is of particular importance for the electricity ecosystem.

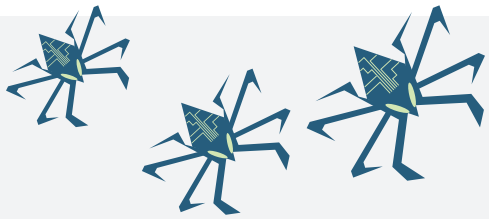
A large-scale blackout would have socioeconomic ramifications for households, businesses and vital institutions.[15]

WORLD ECONOMIC FORUM

Cost of cyberattacks on the Smart Grid

The University of Cambridge Centre for Risk Studies and Lloyd's released a report in 2015 that analyzed a hypothetical cyberattack on the U.S. power grid.

It predicted financial losses between $243 billion to more than $1 trillion, with insured losses of between $21.4 billion and $71.1 billion, depending on the severity of the power outage.[16]



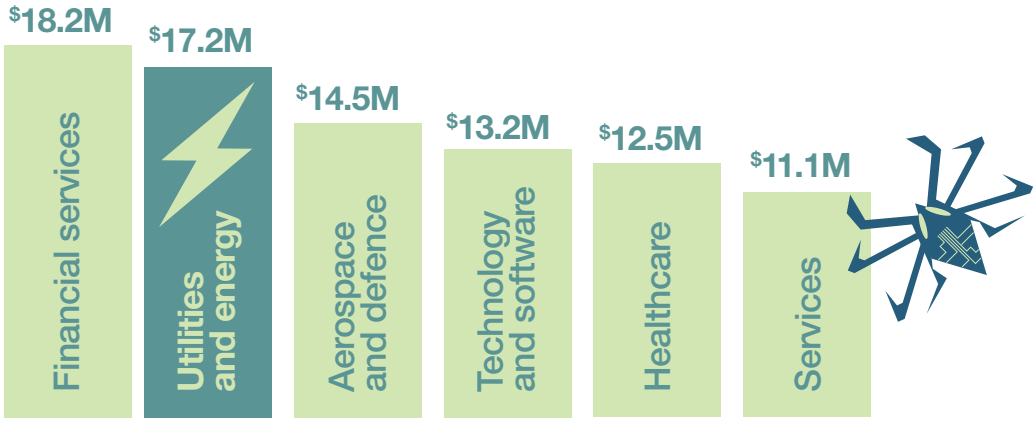
Fukushima nuclear disaster clean-up **$188B**

8% of cybercrime losses insured

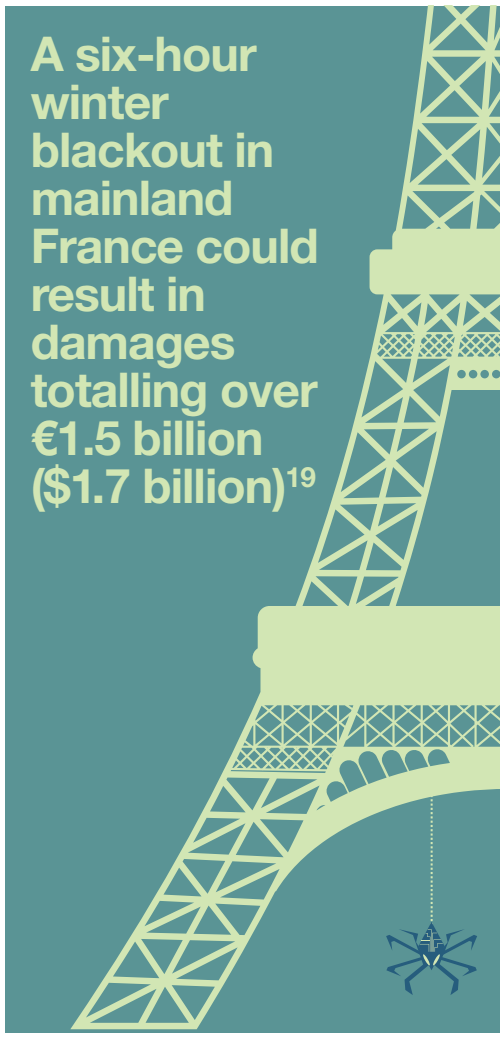
92% of cybercrime losses uninsured[17]

Estimated cost of hypothetical US grid cyberattack clean-up[17]

$1,000B



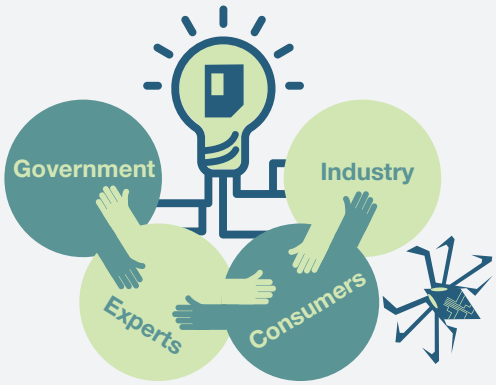
Average annualized cybercrime cost per company, by industry sector.[18]



A six-hour winter blackout in mainland France could result in damages totalling over €1.5 billion ($1.7 billion)[19]

Where to next?

Long-term mitigation strategies require a multi-dimensional and holistic approach. If a single cyber attack can affect multiple stakeholders, then the **stakeholders need to work together** to manage the risk.[20]



Society often bears the cost of cyberattacks. What are you doing to improve your organization's cyber resilience?

Mitigation strategies

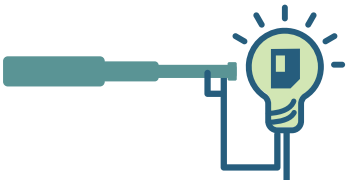
In April 2018 the Forum published the *Industrial Internet of Things Safety and Security Protocol*. This first of its kind policy framework generates an understanding of how risk and insurance can facilitate the improvement of industrial IoT security design, implementation and maintenance practices. It also sets forth a universal set of security best practices that should be incorporated in all industrial IoT deployments.

Sample IIoT safety and security best practices[21]

Line of business IIoT device safeguards

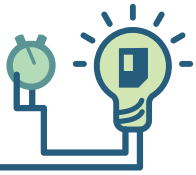
- Risk-assessment models
- Device integrity and availability
- Patches and updating
- Software development lifecycle
- Vulnerability disclosures
- Segmentation
- Encryption
- Privacy
- Interoperability
- Root of trust

Internal governance and risk management



- Board oversight
- Top-level accountability
- Ongoing testing
- Information sharing
- Cyber resilience
- Ongoing assessment
- Track/address legacy
- Incident response

Record-keeping and metrics



- Performance indicators
- Metrics

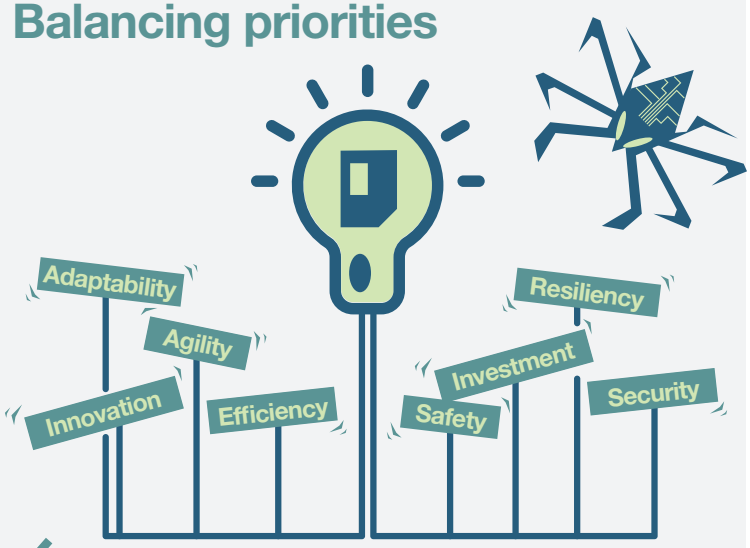
What is your organization doing to establish a culture of cyber awareness?

The World Economic Forum provides Principles and Guidance for Boards

Did you know?

Insurance claims data shows two-thirds of incidents are the direct result of employee behaviour–for example, negligence leading to lost devices–and additional human factors, such as talent shortage, skill deficits and employee engagement.[22]

Balancing priorities



Evidence-based policy

Cybersecurity operates in an arena seen as intangible, complex, ambiguous, contested, and not conducive to agreed standards. More robust evidence-based cybersecurity policy-making is needed, an area that cybersecurity strategies generally don't cover.

Find out more at wef.ch/WEF-secure-IoT

Footnotes

1. International Electrotechnical Commission, "What is a Smart Grid?" https://www.iec.ch/smartgrid/background/explained.htm (link as of 02/28/19).
2. International Data Corporation (IDC). 2018. IDC Forecasts Worldwide Technology Spending on the Internet of Things to Reach $1.2 Trillion in 2022. https://www.idc.com/getdoc.jsp?containerId=prUS43994118 (link as of 11/23/18).
3. International Data Corporation (IDC). 2019. IDC Forecasts Worldwide Spending on the Internet of Things to Reach $745 Billion in 2019, Led by the Manufacturing, Consumer, Transportation, and Utilities Sector. https://www.idc.com/getdoc.jsp?containerId=prUS44596319 (link as of 01/06/19).
4. Statista. 2018. Global defense spending from FY 2008 to FY 2022. https://www.statista.com/statistics/859455/global-defense-spending/ (link as of 01/17/19).

   Statista. 2018. Forecast augmented (AR) and virtual reality (VR) market size worldwide from2016 to 2022. https://www.statista.com/statistics/591181/global-augmented-virtual-realitymarket-size/ (link as of 01/17/19).

   Statista. 2018. Forecast digital advertising from 2017 to 2023. https://www.statista.com/outlook/216/100/digital-advertising/worldwide (link as of 01/17/19).
5. International Data Corporation (IDC). 2018. IDC Forecasts Worldwide Technology Spending on the Internet of Things to Reach $1.2 Trillion in 2022. 18 June. https://www.idc.com/getdoc.jsp?containerId=prUS43994118 (link as of 01/18/19).
6. World Economic Forum. How can digital help build a more flexible and resilient electricity grid? http://reports.weforum.org/digital-transformation/building-a-more-flexible-and-resilient-grid/ (link as of 11/06/18).
7. International Energy Agency, World Energy Outlook, 2017. https://www.iea.org/weo2017/ (link as of 12/15/18).
8. Research and Markets. 2018. Smart Grids Infrastructure Market, 2018-2030. https://www.researchandmarkets.com/research/cwqb9b/global_smart?w=5 (link as of 12/10/18).
9. BP Magazine [Online]. 2018. Energy Demand by Sector. https://www.bp.com/en/global/corporate/energy-economics/energy-outlook/demand-by-sector.html (link as of 12/17/18).
10. Noja Power. 2013. Carbon emission reductions by the implementation of a smart grid. 5 April. https://www.nojapower.com.au/press/2013/carbon-emission-reductions-by-the-implementation-of-a-smart-grid.html (link as of 01/20/19).
11. Breeam. The Edge, Amsterdam. https://www.breeam.com/case-studies/offices/the-edge-amsterdam/ (link as of 12/20/18).
12. US Department of Homeland Security. 2018. Secretary Kirstjen M. Nielsen Remarks at the RSA Conference. 17 April. https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nielsen-remarks-rsa-conference (link as of 26/11/18).
13. World Economic Forum. 2019. Global Risk Report. World Economic Forum, p. 5. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf (link as of 01/28/19).
14. Dragos Inc. 2017. Crashoverride: Analysis of the Threat of Electric Grid Operations, p. 10. https://dragos.com/wp-content/uploads/CrashOverride-01.pdf (link as of 02/16/19).
15. World Economic Forum, Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards, 2019, p. 5. http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf (link as of 13/02/19).
16. Lloyd's and University of Cambridge. 2015. Lloyd's Emerging Risk Report, pp. 5, 12-16. https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-lloyds-business-blackout-scenario.pdf (link as of 01/20/19).
17. Idem.
18. Accenture. 2017. Cost of Cyber Crime Study, p. 20. https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf (link as of 01/28/19).
19. Energie Institute an der Johannes Kepler Universitat Linz. Black Simulator. Simulation parameters – 6 hour blackout starting at 17:00 on December 20 in mainland France. http://www.blackout-simulator.com/ (link as of 26/02/19).
20. World Economic Forum, Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards, 2019, p. 21. http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf (link as of 13/02/19).
21. World Economic Forum. 2018. Industrial Internet of Things Safety and Security Protocol. World Economic Forum, pp. 9-11. http://www3.weforum.org/docs/47498_Industrial_Internet_Things_Safety_Security_Protocol_WP-FINAL.pdf (link as of 02/03/19).
22. Willis Towers Watson. 2017. Cyber risk: It's a people problem too, p. 2. https://www.willistowerswatson.com/en/insights/2017/09/Cyber-risk-its-a-people-problem-too (link as of 02/10/19)

Acknowledgements

Lead Authors

Karime Kuri Tiscareno, Lead of Internet of Things, Robotics and Smart Cities, Centre for the Fourth Industrial Revolution, World Economic Forum

John Villasenor, Professor of Electrical Engineering, Public Policy and Management, UCLA School of Law

Contributors

Pierre-Alain Graf, Senior Vice-President, Global Security Business, ABB Ltd, Switzerland

Rosa Kariger, Chief Information Security Officer, Iberdrola SA, Spain

Aniello Gentile, Director Cybersecurity, Enel SpA, Italy

Agustin Valencia Gil-Ortega, of Operational Technology Cybersecurity, Iberdrola SA, Spain

Ingo Susemihl, Partner Management, Charter of Trust, Siemens AG, Germany

Brecht Wyseur, Manager, Internet of Things (IoT) Security, Kudelski Group, Switzerland

Ahmed Alketbi, Chief Information Security Officer, Dubai Electricity and Water Authority, United Arab Emirates

Abdulla Algaoud, Manager - Cyber Defense Center, Dubai Electricity and Water Authority, United Arab Emirates

World Economic Forum

Jeff Merritt, Head of Internet of Things, Robotics and Smart Cities, Centre for the Fourth Industrial Revolution, World Economic Forum

Louise Anderson, Electricity Industry Community Lead, World Economic Forum

Georges De Moura, Head of Cyber Threat and Risk Management, Centre for Cybersecurity, World Economic Forum

Daniel Dobrygowski, Head of Governance and Policy, Centre for Cybersecurity, World Economic Forum

Designed and produced April 2019 by **Design Resources Ltd**