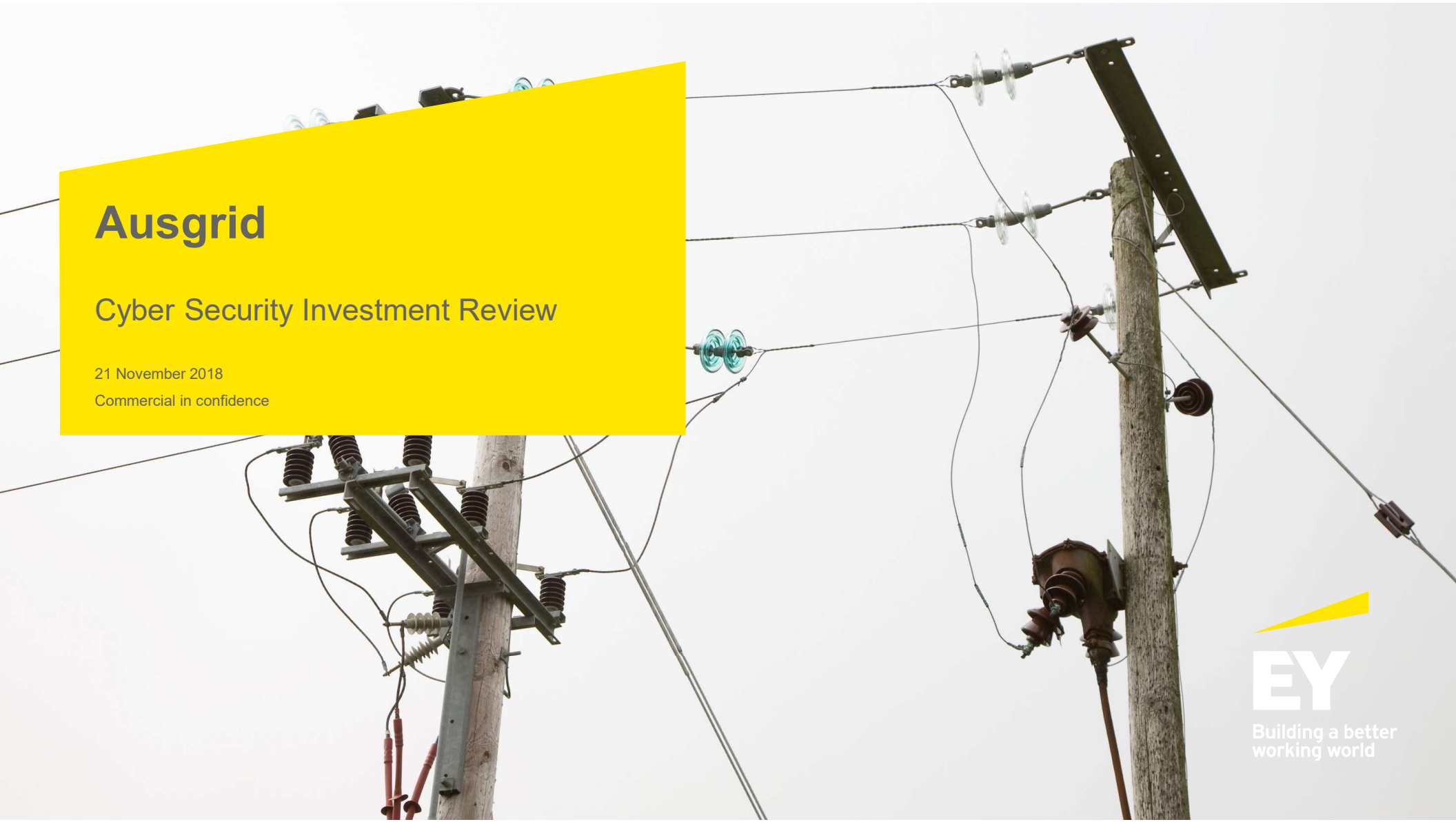
Revised Proposal Attachment 5.19.1 EY Cyber Investment Review PUBLIC

January 2019



Ausgrid

Cyber Security Investment Review

21 November 2018

Commercial in confidence

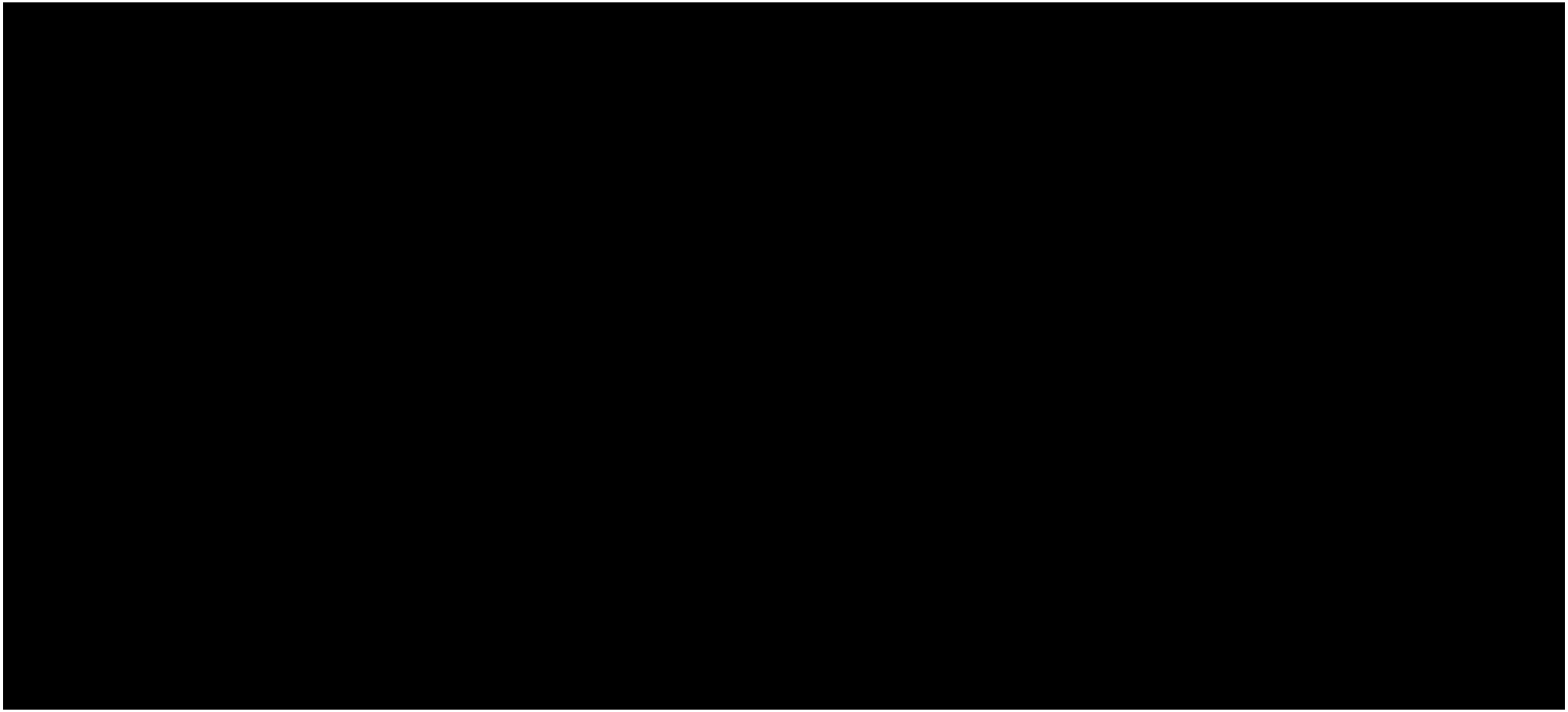
Building a better working world

Contents

1

[redacted]

2 Recent and emerging cyber regulatory changes will have a material impact on Ausgrid



3

[redacted]

[redacted]

Total risk reduction from these cyber risks has been quantified at **$1.75 Billion****

*[redacted]

***Per Ausgrid's Cyber Risk Model.*

4

[redacted]

As the **sole distributer** to 20% of Australia's GDP and 15% of Australia's population, ***Ausgrid is uniquely critical*** to the infrastructure of Australia.

[redacted]

Per the Licencing Conditions, Ausgrid must use **best industry practice for electricity network control systems.**

[redacted]

[redacted]

It is projected that **annual cyber spend will increase globally** in the next 5 years* due to:

- Increase in **frequency and complexity of cyber attacks** targeting energy and utilities
- Enforcement of increasingly **stricter compliance regulations**
- Shift in delivery of cyber capabilities to **subscription-based business models**

[redacted]

See Appendix IV for detail of projections.

1 [redacted]

1

[redacted]

1

[redacted]

[redacted]

**Assumes one half of the current proposed spend for the Cyber Transformation Program for the Calendar Year 2019.*

1

[redacted]y

[redacted]

**Leading approach includes all of the Foundational capabilities detailed on page 9.*

2

[redacted]

[redacted]

2 Global trends indicate that increasingly stringent cyber regulations are likely to have a material impact on Ausgrid

United States

North American Electric Reliability Corp. Critical Infrastructure Protection (NERC CIP) standards, are a set of standards and requirements for securing the assets responsible for operating the bulk power system. NERC CIP standards aim to mitigate the risk of a cyber security incident on the power grid by **software integrity and authenticity, vendor remote access, information system planning, vendor risk management and procurement controls.**

NERC CIP standards **continue to evolve and have widened in scope** to include operational devices in generating plants and substations. For large utilities this has led to a tenfold increase in the number of devices that need to be protected. Violations of NERC CIP standards can reach up to **$1 million a day.** [redacted]

Europe

The European Union adopted a new **NIS directive** on 6 July 2016, which focuses on increasing the cyber security capabilities in the member states.

- By establishing local authorities, each country in EU-28 will be responsible for creating a national strategy to adopt the NIS Directive.
- Enhancing cooperation on cybersecurity among the member states allows for efficient coordination, as well as detection and incident response at EU level.

In addition**, Italy launched its own National Framework for cyber security** based heavily on the US framework of improving critical infrastructure cybersecurity, to ensure international harmonization

Furthermore, General Data Protection Regulation (GDPR) was adopted in 2016 and came into effect in May 2018. It is focused on how network operators operate, handle, process and protect personal data.

- As per GDPR, the data used for profiling and managing load needs to be anonymized by removing personal data, while retaining the information that provides insights into demand for better decision-making.
- National Regulators will have the authority to issue stringent fines and penalties for infringements. Fines for non-compliance with certain GDPR provisions can be up to €20m or 2% of a company's total worldwide annual revenues.

Australia

Critical Infrastructure Act: The Critical Infrastructure Act 2018 was passed and commenced on 11 July 2018. The Acts seeks to manage the national security risk of espionage, sabotage and coercion arising from foreign involvement in Australia's critical infrastructure. The key mechanisms under the Act to achieve its objectives are the establishment of a register of the interest, control and operational information regarding critical infrastructure assets and providing the Minister of Home Affairs with the power to issue directions to an owner or operator of a critical infrastructure asset to mitigate national security risks.

IPART's licensing conditions set the legal requirements to which Ausgrid must comply in order to maintain the authority to operate. These sets of requirement gives details of Ausgrid responsibilities in performing optimally and meeting customers' needs. Per the conditions:

> *Except to the extent that the Licence Holder is undertaking steps in accordance with, and for the duration of, a Protocol agreed with the Commonwealth Representative, the Licence Holder. (a) must, by using best industry practice for electricity network control systems, ensure that operation and control of its distribution system, including all associated ICT infrastructure, can be accessed, operated and controlled only from within Australia, and that its distribution system is not connected to any other infrastructure or network which could enable it to be controlled or operated by persons outside Australia.*

3 [redacted]

3

[redacted]

3 Ausgrid is uniquely critical, playing a significant role in powering Australia's economic engine

Ausgrid is the sole distributor supplying Sydney, the Central Coast and the Hunter Valley with the electricity that is essential to our economic activity, our institutions and our way of life.

Ausgrid powering Australia's economic growth

15% of Australia's population

16% of Australia's jobs

1.5m Homes

20% of Australia's GDP

105 Hospitals

37% of Australia's ICT industry

37% of Australia's financial services industry

15% of Australia's construction industry

12 Sporting stadiums

40 Main concert hall theatres

1,238 Schools & **5** Universities

43m travellers a year at Australia's busiest airport

3

[redacted]


[redacted]

3

[redacted]

3

[redacted]

3

[redacted]

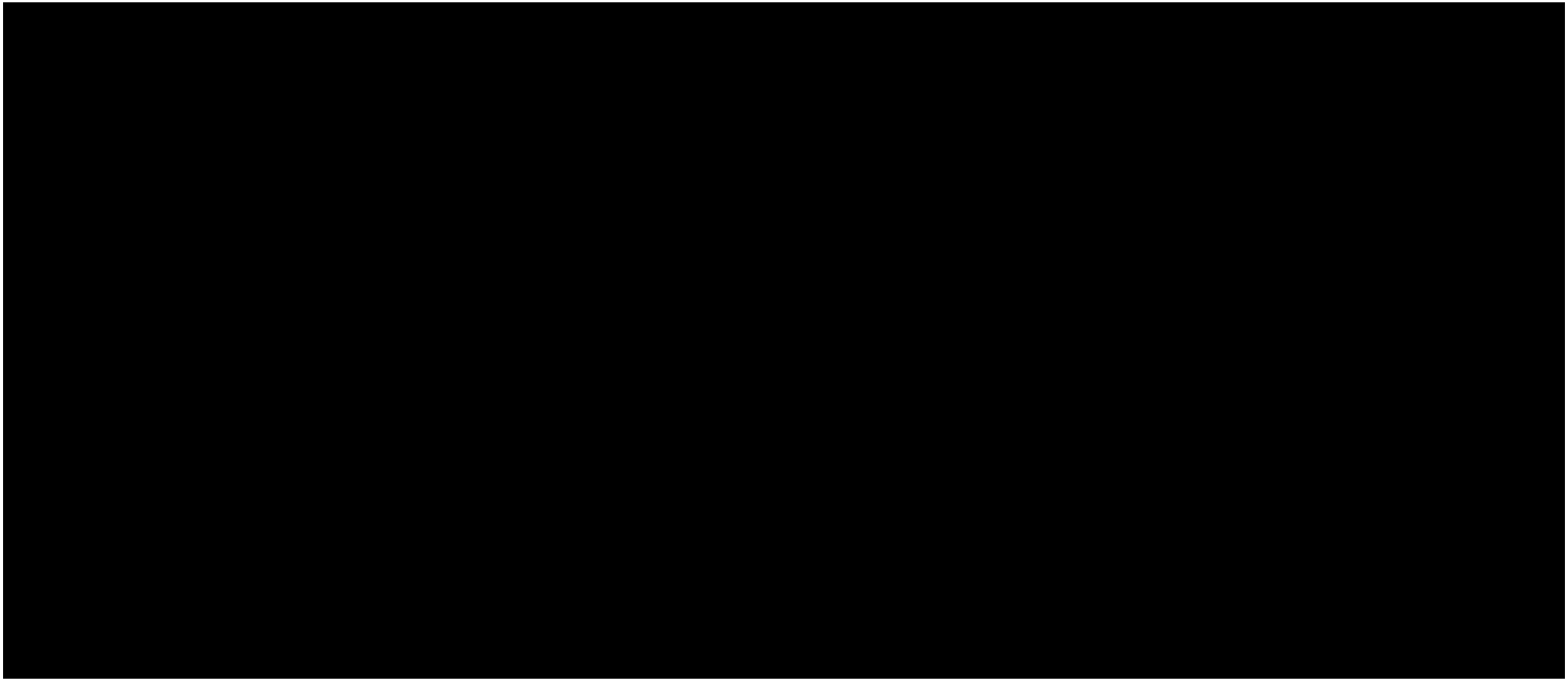
3

[redacted]

4 [redacted]

4

[redacted]


[redacted]

4

[redacted]

5 Appendix V – References

5 The following reports and analysis were used to develop our recommendation

- Gartner, "*Forecast: Information Security, Worldwide, 2016-2022, 2Q18 Update*"
- Gartner, "*Forecast: IT Spending, Worldwide, 1Q18 Update*"
- Gartner, "*IT Key Metrics Data", December 2015*
- Gartner, "*Market Trends: The Transformative Impact of SaaS on the Software Market",* 2018
- IDC, "*Worldwide Spending Semi-annual Security Spending Guide, 2017H2*"
- IDC, *"Determining How Much to Spend on IT Security",* 2015
- Computer Economics, *"IT Spending and Staffing Benchmarks 2018/2019: IT Budget and Cost Metrics by Industry and Organization Size",* 2018
- EY, "*Global Information Security Survey, 2018 – 2019*"
- Energy Decisions Group, "*Cyber Security Resource Allocation: Budgets and Staffing at US Electricity Producers and Utilities*", 2015
- CISO Lens, "*CISO Lens Benchmark Survey*", 2018
- SANS Institute, "*IT Security Spending Trends 2016"*

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organisation 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. For more information about our organisation, please visit ey.com.

ey.com