

Is cybersecurity about more than protection?



Building a better working world

The better the question. The better the answer. The better the world works.

Power and utilities: Global Information Security Survey 2018-19

Sustaining and enhancing trust in the digital utility

The power and utilities (P&U) Global Information Security Survey (GISS) investigates the most important cybersecurity issues facing utilities today. Analysis of 68 responses from P&U executives shows that many utilities are increasing the resources they devote to security but remain deeply concerned about the potential scale and severity of adverse events. Utilities need to focus on both protecting the enterprise and enabling the business through new technologies to become more agile, innovative and confident. But this cannot come at the expense of the trust that they have built with key stakeholders over many years: utilities need to sustain and enhance trust with customers, regulators, investors and employees as they embark on new growth strategies and prepare for the risk and security challenges of tomorrow.

Protect, optimize, enable

As cybersecurity continues to impact the board agenda, utilities can enhance trust and build confidence by addressing three key challenges:

- 1. Protect the enterprise** – focus on the identification of critical assets across the enterprise, grid and customer domains and implement risk-informed layers of defense. The GISS reveals that well over a third (38%) of P&U respondents have a nonexistent or obsolete identity and access management program.
- 2. Optimize cybersecurity** – stop low-value activities, increase efficiency and reinvest funds in emerging and innovative technologies, such as data analytics and robotic process automation (RPA), to enhance existing protection. Almost half (47%) of P&U respondents indicate a need for an increase of more than 25% in their cybersecurity budget to achieve management's desired level of risk tolerance.
- 3. Enable growth** – implement security by design as a key success factor for the digital transformations that most utilities are now going through. Only 14% of P&U respondents are confident that they have fully considered the security implications of their current strategy and that their risk operating model incorporates and monitors cyber threats, vulnerabilities and potential impacts.

Key findings

1. Leadership and governance around cybersecurity is lacking.

26% say a lack of executive awareness of management/governance issues limits the value of their security function.

26% say their boards include a member directly responsible for cybersecurity compared with 40% across all industries.

2. As incidents rise, strategies and planning become paramount.

58% have had a recent significant cybersecurity incident.

56% do not consider or have only partially considered security implications in their current strategies and plans.

3. Inadequate operating models are exacerbated by budget pressures.

95% say their cybersecurity function does not fully meet their needs, and almost half (49%) still do not have a security operations center.

47% need at least a 25% increase in annual funding to achieve management's desired level of risk tolerance.

4. A skilled cyber workforce is essential to keep pace with evolving utility threats.

28% say a lack of skilled resources limits the value that the security function adds to their organization.

44% say their organization is unlikely to detect a sophisticated cyber attack compared with 38% across all industries.

5. Robust response plans are needed.

71% say they don't have cyber insurance compared with 65% across all sectors.

28% have a nonexistent or obsolete incident response program.

Read our other insights at [ey.com/riskpulse](https://www.ey.com/riskpulse) to learn what your peers are saying about key risks. Contact us to find out how EY risk and cybersecurity professionals can help.

Power and utilities: Global Information Security Survey 2018-19

Confidence and trust

The P&U industry is undergoing unprecedented transformation, and how risk is managed will become critical to unlock the strategic upside of disruption. With the expansion of digital and the internet of things, it is becoming increasingly challenging for utilities to monitor their complete ecosystem. At the same time, utilities need to derive actionable intelligence from their data by investing in the tools and skills that will enable them to embrace disruption with confidence, build trust with stakeholders, and create business value and market differentiation.

Efficient and effective security

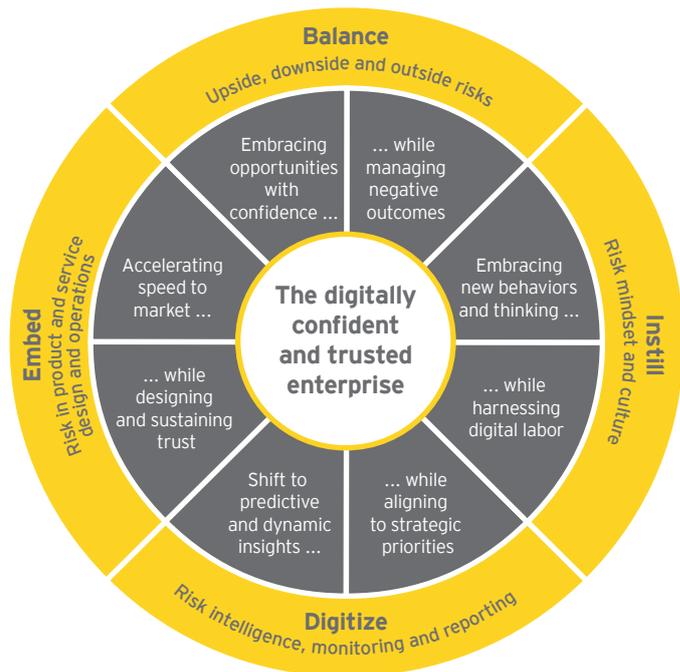
New and emerging technologies are playing a crucial role in utilities' evolution. Digital technologies, such as cloud services, data analytics and RPA, are expected to have significant impacts on utility businesses and the future of risk and cybersecurity.

Cloud computing is becoming more prevalent as legacy systems are replaced due to significant advantages in scalability and upgrading, as well as business continuity and disaster recovery. With this shift, the right governance, risk and compliance measures need to be put in place to ensure cloud security. Almost three-quarters (73%) of P&U respondents expect to spend more on cloud cybersecurity in the next year compared with 57% across all industries.

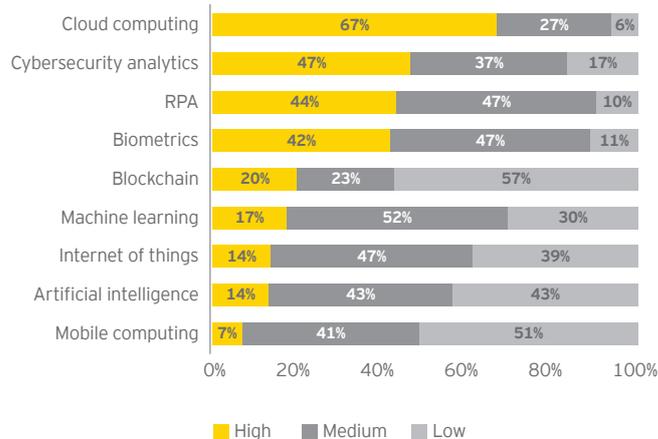
Data analytics and increasingly automated processes will enable utilities to detect unusual behavior and respond to alerts more effectively, helping to reduce risk and improve security. More than half (56%) of P&U respondents plan to spend more on cybersecurity analytics in the next year compared with 48% across all industries.

RPA combined with security orchestration and automation can enhance the efficiency and sustainability of risk and compliance reporting by improving time-consuming processes in collecting, compiling, cleansing and summarizing large amounts of data. Almost half (45%) of P&U respondents expect to spend more on RPA security in the next year compared with only 25% across all industries.

Adopting a more agile risk management framework, enabled and facilitated by new technologies, will allow utilities to respond to changing circumstances and take advantage of increased efficiencies and reduced costs to improve performance.



Cybersecurity investment priorities in the next year*



*Fields may not add to 100% due to rounding.

"As we navigate the digitization of operations, trust with customers, regulators, employees and investors will become a critical building block in pursuit of growth. Establishing, sustaining and increasing trust needs to be at the heart of everything we do."

Matt Chambers, EY Global P&U Trust by Design Lead

Contact the EY Global P&U Trust by Design Team:

Matt Chambers
(Houston, US)
+1 713 750 5944
matt.chambers@ey.com

Jamey Sample
(Denver, US)
+1 415 894 8137
jamey.sample@ey.com

Alex Campbell
(London, UK)
+44 74 3743 4117
acampbell2@uk.ey.com

Georgina Crundell
(Brisbane, Aus)
+61 401 142 209
georgina.crundell@au.ey.com

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 organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2019 EYGM Limited.
All Rights Reserved.

EYG no. 012847-18Gbl

BMC Agency
GA 1009890

ED None

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

ey.com/riskpulse