Why wait for a cyber catastrophe to prepare for a cyber attack?

EY
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 2017–18

Preparing to confront cyber threats

The power and utilities (P&U) sector is going through one of the most transformative stages since its inception. Behaviors are shifting, governments and consumers alike are demanding cleaner energy, and new technologies are driving a more decentralized and increasingly digital model. How utilities succeed in making the transition will depend on how they manage their most important risks. High on this agenda is the need to improve cybersecurity.

The P&U Global Information Security Survey (GISS) investigates the most important cybersecurity issues facing utilities today. Our findings suggest that while utilities continue to prioritize cybersecurity – and are making good progress in identifying and resolving vulnerabilities – they are more worried than ever about the breadth and complexity of the evolving threat landscape.

Mounting threat levels have pushed utilities to take a more robust approach, but there is significant room for improvement.

The GISS reveals that only 6% of P&U respondents are confident that they have fully considered the information security (IS) implications of their current strategy and that their risk operating model incorporates and monitors cyber threats, vulnerabilities and potential impacts.

All respondents (100%) say their cybersecurity function does not fully meet their needs and yet only 9% expect an increase of more than 25% in their cybersecurity budget. In addition, only 17% prioritize protection of non-IT "crown jewel" assets and almost a quarter (23%) still do not have a security operations center.

Often, the people responsible for security struggle to articulate the risk with senior management in order to obtain additional investment. This reinforces the need to elevate security to an enterprise-level risk and become an integral part of the utility's overall strategy.

To build resilience, utilities must assume the worst can happen

According to the GISS, employees, hacktivists and state-sponsored attackers are seen as the greatest immediate threats. The rise of microgrids and distributed energy resources, as well as an increasingly fragmented energy value chain, often spanning numerous countries, make it difficult to understand and manage the risk, including where responsibility ultimately lies. It's not surprising, therefore, that a majority (58%) of P&U respondents find it hard to monitor the perimeter of their ecosystem versus only 36% across all sectors.

Key findings

1. Leadership and governance around cybersecurity is lacking

27% say there is a lack of executive awareness and support, which is challenging the effectiveness of cybersecurity

6% say their boards include a member directly responsible for cybersecurity

2. Better links are needed between cybersecurity, strategy and planning

6% say they have fully considered the IS implications of their organization's current strategy and plans

53% do not appreciate or have only partially considered IS implications, risks and threats in their current strategy and plans

3. Inadequate operating models are exacerbated by budget pressures

100% say their cybersecurity function does not fully meet their needs

29% need at least a 25% increase in annual funding to achieve management's desired level of risk tolerance

4. The rise of digital and the IoT are not being sufficiently addressed

77% say poor user awareness and behavior around mobile devices are major risks for their organization

63% do not have a role within the security function focused on web-enabled devices and the IoT

5. Robust response plans are needed

64% have had a recent significant cybersecurity incident

85% do not have a robust incident response program that includes regular crisis scenario testing

Read our other insights at **ey.com/riskpulse** to learn what your peers are saying about key risks. Contact us to find out about how our risk and cybersecurity professionals can help.

Power and utilities: Global Information Security Survey 2017–18

Understanding the complex cyber threat landscape

The first step for utilities seeking to enhance their security ability is to develop a better understanding of the threats they face and what they mean for the business.

Enterprise domain and IT-related risks

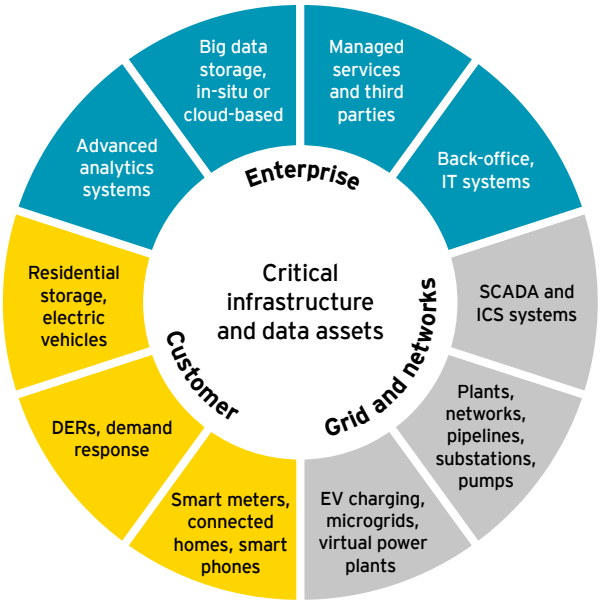
Threats associated with the collection, storage and analysis of big data and the growing interdependencies between physical assets and information and operations technology (IT and OT) systems have elevated the importance of security as an enterprise risk.

Grid and network infrastructure risks

The increasingly connected and complex nature of industrial control systems (ICS), including supervisory control and data acquisition (SCADA), makes them challenging to secure and vulnerable to cyber threats. In addition, the growth in smart electric, gas and water networks and associated digitally-enabled technologies are creating new points of entry for cyber attackers.

Customer domain risks

Growth in disruptive behind-the-meter technologies is further expanding the cyber attack surface across the P&U ecosystem. The use of smart metering data to enhance billing systems, better understand consumption patterns and ultimately improve user experience also increases the amount of data. This multi-ownership of data is making management of privacy even more challenging.



Fighting back against the threat

Utilities may feel more confident about confronting the threats that have become familiar in recent years, but they still lack the capability to deal with more advanced, targeted assaults. To be cyber resilient, utilities must embrace an enterprise-wide risk management strategy that includes a multilayered approach across a robust framework.

At the heart of this framework is a risk-enabled culture with effective governance, exceptional leadership and the right talent. A risk-enabled utility advances strategic thinking on cyber risks across the P&U ecosystem and implements an agile and resilient operating model to prepare for and respond to cyber attacks, deploys technology an innovation to continually improve and focuses. on managing the risks that matter most.

Cybersecurity is everyone's business

Understanding the threat landscape gives utilities clarity over when and why they have moved into stress, and allows them to pre-empt the development of a full-on crisis. Fighting back builds on this by giving utilities the skills and confidence to deal with stress and crisis more effectively, with tools and processes that provide a framework for responding to attackers.

Having a robust response plan is the final piece. Utilities capable of employing a well thought-out and tested cyber breach response plan in which everyone understands their responsibilities will de-escalate the crisis much more quickly.

By pulling these strands of cybersecurity together, utilities can respond in a more agile and resilient way, even in the face of significant and increasing risk. Decision makers across the entire C-suite should understand that cybersecurity needs to be treated as an enterprise-level risk. Much as a safety culture encompasses shared attitudes, perceptions and values that drive an organization to "do the right thing," utilities need to create a security culture of awareness and vigilance that is equally embedded.

> "The cyber attack surface has significantly increased through advances in automation and connected devices. Combined with the commercialization of attack tools that were once limited to a nation state's arsenal, you have the ingredients for significant disruption."
>
> **Matt Chambers**, EY Global P&U Protecting the Enterprise Lead

Contact the EY Global Protecting the Enterprise team:

Matt Chambers (Houston, US)	+1 713 750 5944	matt.chambers@ey.com
Alex Campbell (London, UK)	+44 74 3743 4117	acampbell2@uk.ey.com
Georgina Crundell (Brisbane, Australia)	+61 7 3011 3186	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.

EYG no. 00440-184GBL

BMC Agency
GA 1006665

ED None.

ey.com/riskpulse