## Agenda

<table>
<thead>
<tr>
<th></th>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Overview</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>Today’s attacks on the digital world</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>How attacks unfold</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>Why are you still so vulnerable?</td>
<td>14</td>
</tr>
<tr>
<td>5</td>
<td>The shift to “Active Defense”</td>
<td>17</td>
</tr>
<tr>
<td>6</td>
<td>Using cybersecurity as a digital enabler</td>
<td>19</td>
</tr>
<tr>
<td>7</td>
<td>How can EY help?</td>
<td>22</td>
</tr>
</tbody>
</table>
Overview
Our 18th global annual survey of the most important cybersecurity issues facing business today

► 1,755 respondents from organizations in 67 countries around the world and across all key sectors participated in the survey between June and September 2015.

We found that:

► Organizations are making progress in improving the way they respond to today’s cyber threats and attacks, but …

► There is a need for considerable improvement as the world becomes increasingly more digital and attackers increase in sophistication and persistence.
The digital world offers many benefits and opportunities, however, the risks have been underestimated.

The Power & Utilities (P&U) sector is currently undergoing major transformation driven by the introduction of smart meters and data networks across the energy value chain.

For organizations to recognize the current challenges and to understand what they need to do to get ahead of cybercriminals, they need to think fully about each of the following four areas:
Today’s attacks on the digital world
How is the world changing for you?

Energy supply chain transformation
Integration of new smart grid technologies for real-time energy transmission and distribution management with smart metering systems and associated customer business processes is revolutionizing the end-to-end value chain.

Enterprise transformation
P&U companies are rethinking their business models for winning in the market by being more innovative and offering a richer customer and employee experience through a variety of channels.
GISS 2015 findings

19%
of P&U responders say that they do not have an information security strategy

Compared with … 13%
across all sectors

32%
of respondents say lack of executive awareness or support is a major obstacle or reason that challenge their information security operation’s contribution and value to the organization

46%

55%
of P&U respondents say they do not have a security operations center (SOC)

Compared with … 47%
across all sectors
Apply a cyber lens to everything you do

Dimensions of the enterprise

**Strategy, innovation and growth**
- Drive agility and innovation
- Align the operating model for the digital world
- Engage the landscape without boundaries
- Understand threats and opportunities

**Customer experience**
- Enhance customer experiences leveraging technology
- Collect intelligence across touch points and media channels
- Deepen customer relationships and insights
- Leverage technology to better integrate among functions

**Supply chain and operations**
- Establish a more agile digital supply network
- Manage in-house and third-party providers
- Leverage new technologies to enhance operations
- Respond quickly to market changes

**Technology**
- Streamline the digital ecosystem
- Fully enable digital systems
- Balance digital innovation with IT maintenance
- Integrate front-office apps with back-end systems

**Risk and cybersecurity**
- Manage risk as business transforms
- Keep pace with increasing privacy risks and cyber attacks
- Understand broader risks of new technologies
- Provide digital trust and privacy

**Finance, legal and tax**
- Automate processes and controls
- Digitize invoices and documents
- Evaluate digital tax operating model effectiveness
- Address legal and regulatory requirements

**People and organization**
- Create a diverse culture of innovation and ideation
- Redesign the organization to fit the digital age
- Transform knowledge across the organization
- Integrate digital technologies to empower people
**How can you manage the attacks?**

**Key risk management principles ...**

1. **Focus on what matters most**
   - Align to your unique business and risk culture

2. **Measure and report**
   - Include qualitative statements and quantitative measures

3. **Comprehensive in nature**
   - Cover all risk types, current and forward-looking

4. **Allocation of risk appetite**
   - Allocate based on the appetite of business units and risk types

5. **Integrate with business planning**
   - Prepare for regulators seeking evidence

**... applied to cyber risk**

1. **Know your critical assets**
   - Identify assets most vulnerable to cyber attack (e.g., critical infrastructure, personal data)

2. **Make cyber risk more tangible**
   - Define cyber risk and underlying metrics clearly. Not just IT but across the enterprise.

3. **Align with existing risk frameworks**
   - Bring financial, operational, regulatory, customer, reputation and other frameworks together

4. **Make cyber risk relevant to the business**
   - Link organizational-level risks to individual BUs and their assets (e.g., convergence of IT/OT)

5. **Embed risk appetite in investment decisions**
   - Prioritize investment where critical, empower businesses to make informed local decisions
How attacks unfold
In order to identify that things are “not quite right,” it is first necessary to know your environment, how it is evolving and the security implications.

- Increase in organization attack surface through large number of interconnected devices (e.g., meters)
- Convergence of information technology and operational technology
- Uncertainty on privacy of personal energy consumption data

Energy supply chain transformation

- Cross-channel, cross-platform sharing of sensitive data
- Consumerization – bring your own device – can blur organizational boundaries
- Cloud-based services and third-party data storage

Enterprise transformation
Smart metering cyber threats

Smart meters introduce considerable benefits across the energy life cycle ...

... however, there are significant cyber threats organizations and consumers will be exposed to.

Larger attack surface compared to traditional IT system due to potentially millions of networked end-points in the “wild,” i.e., meters in households

Cyber threats

- Device tampering
- HAN drive-by attacks
- WAN layer attacks
- Fraudulent pre-pay top-ups
- Remote disconnection spoofing/replay
- Personal data leakage
- Insider threat

Household

- Other devices
- In-home display
- Smart electricity meter
- Smart gas meter

Wide Area Network (WAN)

- Two communication service providers

Market participants

- Utilities (electricity and gas)
- Network operators
- New market participants (e.g., energy efficiency advisors)
Who or what do you consider the most likely source of an attack? (select all that apply)

- Employee: 70% (P&U), 56% (All sectors)
- Hacktivists: 61% (P&U), 54% (All sectors)
- Criminal syndicate: 52% (P&U), 59% (All sectors)
- State-sponsored attacker: 48% (P&U), 35% (All sectors)
- Lone wolf hacker: 47% (P&U), 43% (All sectors)
- External contractor working on-site: 42% (P&U), 36% (All sectors)

Multiple responses allowed
Why are you still so vulnerable?
The three As
How to get ahead of cybercrime

To get ahead of cybercrime, in 2014 we suggested that organizations adopt a three-stage improvement process:

► **Activate** – (a foundational approach)
  - Organizations need to establish and improve the solid foundations of their cybersecurity

► **Adapt** – (a dynamic approach)
  - Organizations are constantly changing and cyber threats are evolving: cybersecurity needs to adapt to changing requirements

► **Anticipate** – (a proactive approach)
  - Organizations need to make efforts to predict what is coming so they can be better prepared for the inevitable cyber attacks
The three As today
P&U progress and gaps

Activate
- Only 11% say that their information security function fully meets the organization’s needs. (12% – all sectors)
- 59% say their information security budget needs to rise by up to 50% to keep in line with risk tolerance. (69% – all sectors)
- 52% do not have a data protection program or only ad hoc policies or processes in place. (37% – all sectors)
- 31% do not have an identity and asset management program. (18% – all sectors)

Adapt
- 54% of organizations do not currently have a role or department in their information security function that is focusing on emerging technology and its impact. (54% – all sectors)
- Only 21% would rate their security monitoring as mature or very mature. (34% – all sectors)
- 55% say that lack of skilled resources is challenging information security’s contribution and value to the organization. (57% – all sectors)

Anticipate
- 44% do not have a threat intelligence program, with a further 26% only having an informal approach. (36% and 30% respectively across all sectors)
- In evaluating their ecosystem, only 11% look beyond their suppliers to their suppliers’ suppliers (fourth parties). (12% – all sectors)
- 83% say that poor user awareness/behavior is the main risk associated with mobile devices. (79% – all sectors)

In 2015: not enough measures in the current environment
In 2015: no mechanisms to adapt to change
In 2015: slow proactive approach to neutralize sophisticated attacks
The shift to “Active Defense”
What is “Active Defense”? And how do you build it?

► “Active Defense” sends out intelligent feelers to look for potential attackers, analyze and assess the threat, and neutralize the threat before it can damage your organization’s critical assets.

► To build it:

► Professionally analyzed Cyber Threat Intelligence can identify likely attackers, infer their most likely targets within your business and develop hypotheses about how those attacks will unfold.

► Active Defense practitioners use disciplined processes to analyze available information, draw relevant conclusions and take action.

► By implementing and executing an iterative cycle with built-in mechanisms for continuous learning and improvement, the organization can realize gains in efficiency, accountability and governance capabilities.

31% of responders say that their SOC has a dedicated individual(s) focusing solely on cyber threat intelligence

15%
Using cybersecurity as a digital enabler
Cybersecurity as the digital enabler

- Cybersecurity is not an inhibitor in the digital world; rather it helps make the digital world fully operational and sustainable.
- Cybersecurity is the key to unlocking innovation and expansion.
- A tailored organization and risk-centric approach to cybersecurity will adjust the balance of the digital world back towards sustainability and safety, to help better protect your organization and create trust in your brand.

If the answer to any of these statements is “yes,” you should consider an **Active Defense** approach:

- We have an SOC, but are still not finding evidence of advanced attackers.
- We have an SOC, but we still had a major breach.
- We have an outsourced SOC, but my intellectual property and businesses systems are not truly secure.
What does your organization require to build trust in a digital world?

- Knowledge of what can hurt the organization and disrupt achieving your strategy
- Clear identification of your critical assets, or “crown jewels”
- Cyber business risk scenarios that paint an accurate picture of how an attack can progress
- A board and senior executives who can accurately determine the risk appetite for the organization
- An assessment of current cybersecurity maturity, and a comparison to the maturity level that is actually required to meet the risk appetite
- An improvement road map
- Tailored threat profiling and advanced Cyber Threat Intelligence
- A more advanced SOC: in-house, co-sourced or outsourced
How can EY help?
Is your cybersecurity ready to support your digital business?

► Do you understand the specific threats and vulnerabilities in your digital world?
► Have you done the work and thinking required to determine how that threat landscape applies to your organization and strategy?
► Do you know how to set your risk appetite, to determine the acceptable and unacceptable loss and harm from potential incidents, and prioritized cybersecurity measures around this?

If the answer is “no” to any of the above, EY can help.
Want to learn more?

- **Cyber program management**: identifying ways to get ahead of cybercrime
  
  [www.ey.com/CPM](http://www.ey.com/CPM)

- **Security Operations Centers**: helping you get ahead of cybercrime
  
  [www.ey.com/SOC](http://www.ey.com/SOC)

- **Achieving resilience in the cyber ecosystem**
  
  [www.ey.com/cyberecosystem](http://www.ey.com/cyberecosystem)

  Published December 2014

- **Using cyber analytics to help you get on top of cybercrime**
  
  [www.ey.com/3SOC](http://www.ey.com/3SOC)

- **Managed SOC**: EY’s Advanced Security Center: world-class cybersecurity working for you
  
  [www.ey.com/managedSOC](http://www.ey.com/managedSOC)

- **Cyber threat intelligence**: how to get ahead of cybercrime
  
  [www.ey.com/CTI](http://www.ey.com/CTI)

  Published November 2014

- **Cybersecurity and the Internet of Things**
  
  [www.ey.com/IoT](http://www.ey.com/IoT)

- **Unlocking the value of your program investments**
  
  [www.ey.com/prm](http://www.ey.com/prm)

- **Get ahead of cybercrime**: EY’s Global Information Security Survey 2014
  
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.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2016 EYGM Limited.
All Rights Reserved.

EYG no. DX0377
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