Cybersecurity and the impact on international business

2018 AAA International Midyear Meeting

EY
Building a better working world

Introduction

- Vickie Papapetrou is a Senior Manager in the Advisory Services practice of EY.
- Over 11 years of experience in information security currently based in Los Angeles, CA, having just returned from a 3 year secondment in London supporting organizations across Europe, Middle East, India and Africa.
- Certified Information Systems Security Professional (CISSP) and Certified Information Privacy Professional (CIPP) and is a trained ISO 27001 Lead Auditor and Implementer.
- Experience working clients in various sectors helping assess, design and implement security programs aligned with leading standards to mitigate business risk.

How is the world changing for international businesses?

Cybersecurity is a priority issue from board level down.

There is a growing focus on what is going wrong where cyberspace meets the physical world:

- Customers having their personal details stolen and used is unacceptable
- The theft of intellectual property is detrimental to prosperity
- Data losses and the subsequent remediation costs are a huge burden
- The hacking and manipulation of media, communications, government administration and defense systems is seen as a significant threat to national security.

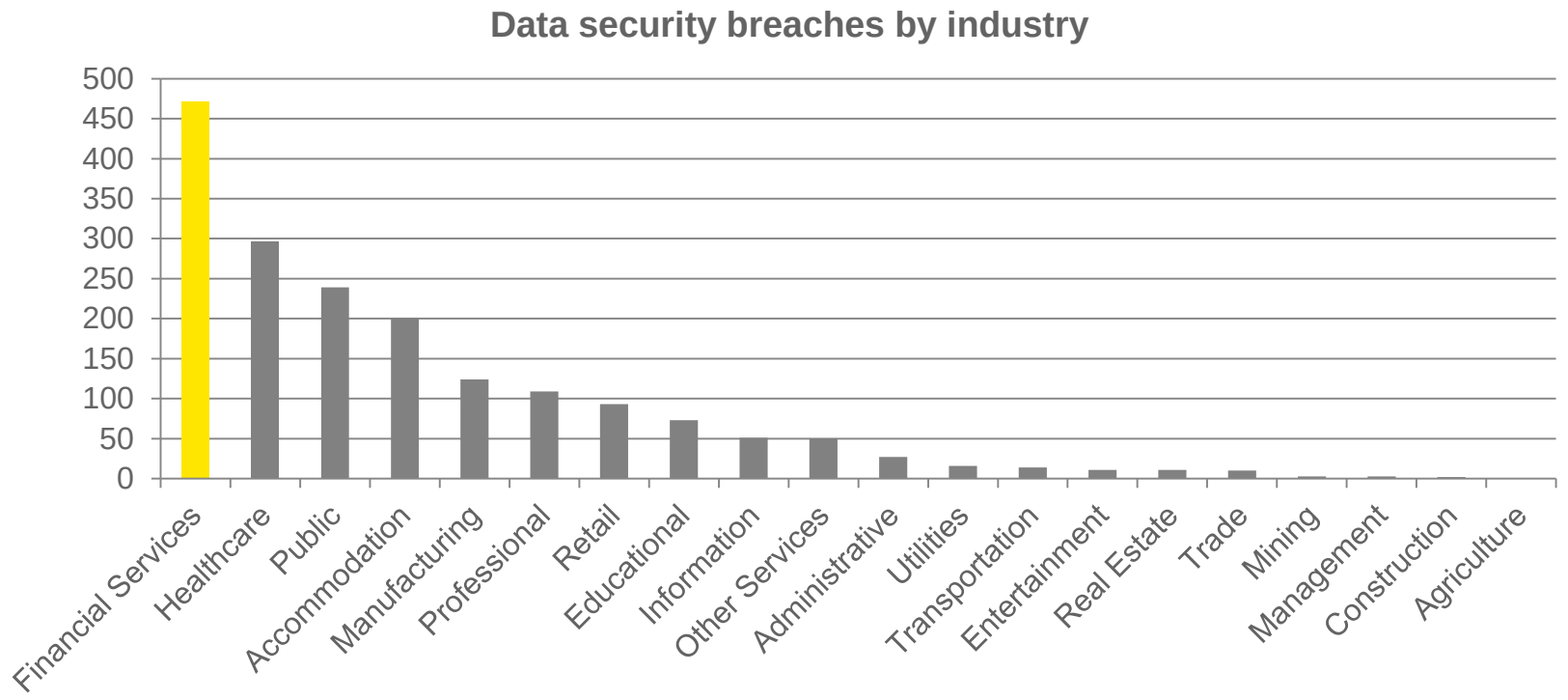
Operating in a digital world invites new challenges and threats

- Smart devices and services can deliver unintended consequences and a mass vulnerable data
- Social media is ‘always on’ and information widely shared, without a full appreciation of privacy and security
- Information is increasingly stored in the cloud or with third parties, resulting in less control, increased risk and a more complex cyber ecosystem
- Human behaviors are changing in positive and negative ways
- New legislation and regulations are forcing changes in processes which can open up new vulnerabilities and widen the attack surface of the organization

Impact of cyber attacks by industry

Financial services sector continues to be a cyber target

The industries most affected by data security breaches in 2016 were financial services, healthcare and public industries.



Source: Verizon 2017 Data Breach Investigations Report

Drivers for change: beyond the threat

Regulators and policymakers are increasing pressure

- **SEC** – cybersecurity guidance update — *April 2015; September 2015; September 2016*
- **FFIEC** Assessment tool designed to help financial institutions not only identify their level of risk to a cyber-attack but also to gauge their ability to manage and control their own specific threat levels — *June 2015; September 2016*
- **National Association of Insurance Commissioners (NAIC)** – adopted Principles for Effective Cybersecurity – Insurance Regulatory Guidance — *April 2015*
- **FINRA –** risk management-based approach to cybersecurity permits firms to tailor their approach to the individual circumstances and the changing threats each firm faces. The framework and standards discussed can inform firms' thinking at a programmatic as well as individual control level — *February 2015*
- **New York State Department of Financial Services** — the department encourages all institutions to view cybersecurity as an integral aspect of their overall risk management strategy, rather than solely as a subset of information technology — *December 2014*
- **President's working group** – resident Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts — *December 2014*
- **Cyber Risks and the Boardroom Conference** — to that end, board oversight of cyber-risk management is critical to ensuring that companies are taking adequate steps to prevent and prepare for the harms that can result from such attacks — *June 2014*
- **Federal Housing Finance Agency** — issues Advisory Bulletin on regulatory expectations — *May 2014*
- **NIST Framework** – developed by the National Institute of Standards and Technology in response to Presidential Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity— *February 2014*
- **FFIEC** highlighted key focus areas for senior management and boards of directors, specifically, developing risk management processes commensurate with the risks and complexity of the institutions — *June 2013*
- **COBIT 5 framework** assists in identifying maturity of policies, processes, and procedures or other aspects to govern and manage enterprise information technology — *April 2012*

Increased regulatory compliance is the new normal

GDPR will change how we handle data

1 Harmonisation and some progress

- Risk-based approach
- Pan-European lead DPA

2 Wider scope

- Wider definition of personal data
- Processing children data under 16 require parental consent

3 Increased obligations

- Privacy by Design
- DP Officer

4 Strengthened rights of individuals

- Right to erasure
- Data portability

5 Increased enforcement, fines, liability

- Regulatory fines up to 4% of annual worldwide turnover

6 Larger role for European Data Protection Board

- Tasked with making sure the regulation is applied around the EU.

Cybersecurity regained: preparing to face cyber attacks

20th Global Information Security Survey 2017-18

- EY's 20th Global Information Security Survey (GISS) captures the responses of nearly **1,200** C-suite leaders and Information Security and IT executives/managers, representing most of the world's largest and most-recognized global organizations.
- Responses were received from 59 countries and across nearly all industries.
- This publication can be found on the EYARC site in the featured publications.

Understanding the threat landscape

Common, advanced and emerging threats and associated attack methods

The threat landscape

Common

These attacks exploit known vulnerabilities using freely available hacking tools, with little expertise required to be successful.

Advanced

Advanced attacks exploit complex and sometimes unknown (“zero-day”) vulnerabilities using sophisticated tools and methodologies.

Emerging

These attacks focus on new attack vectors and vulnerabilities enabled by emerging technologies, based on specific research to identify and exploit vulnerabilities.

Common threats/attacks

- **Description:** Exploiting known vulnerabilities using freely available hacking tools, with little expertise required to be successful
- **Typical threat actors:** Unsophisticated attackers, such as disgruntled insiders, business competitors, hacktivists and some organized crime groups
- **Examples:**
  - Unpatched vulnerability on a website, exploited using a freely available exploit kit
  - Generic malware delivered through a phishing campaign, enabling remote access to an endpoint
  - Distributed denial of service (DDoS) attack for hire with a basic ransom demand

Advanced threats/attacks

- **Description:** Exploiting complex and sometimes unknown (“zero-day”) vulnerabilities using sophisticated tools and methodologies
- **Typical threat actors:** Sophisticated attackers, such as organized crime groups, industrial espionage teams, cyber terrorists and nation states
- **Examples:**
  - Spear phishing attacks using custom malware
  - “Zero-day” vulnerabilities exploited using custom-built exploit code
  - Rogue employees “planted” to undertake deep reconnaissance/ espionage
  - Vendors/suppliers exploited as a way to gain access to ultimate target organization

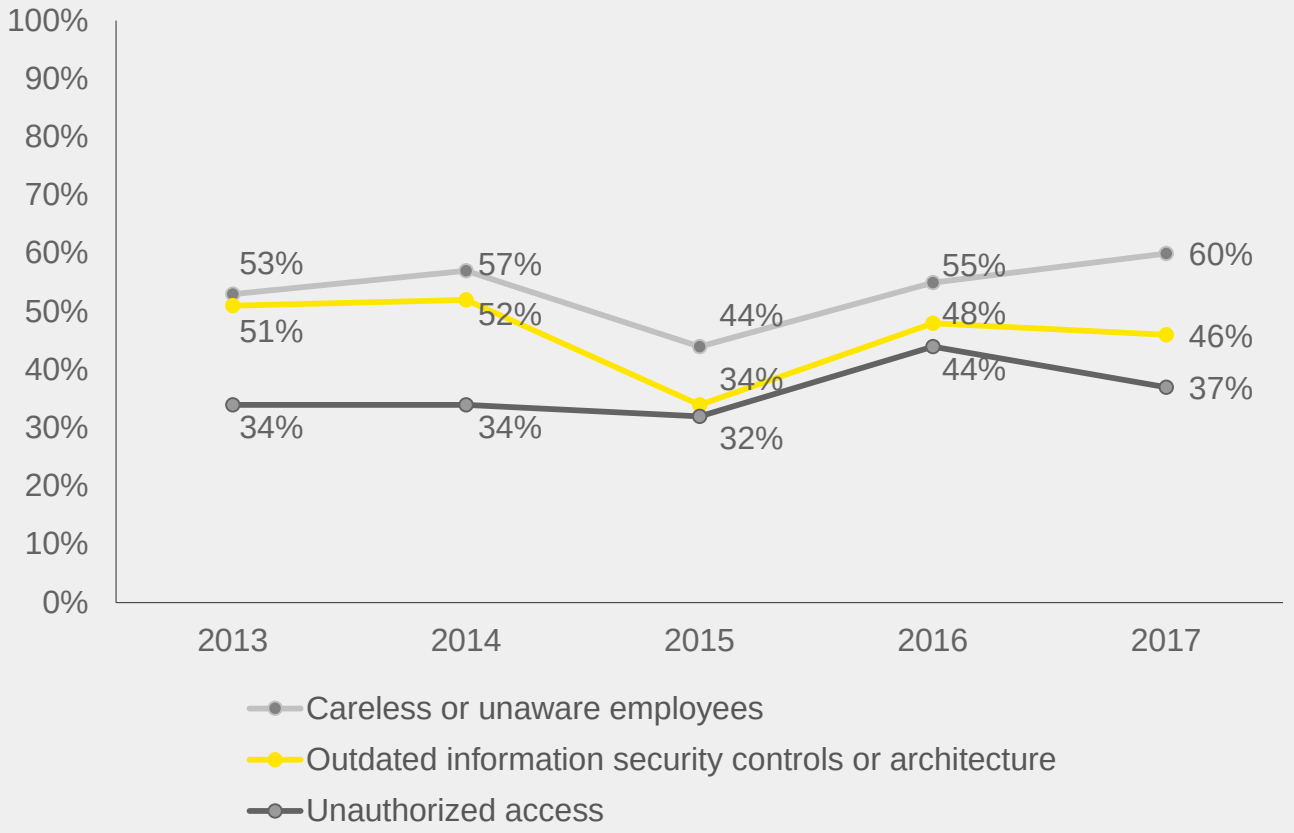
Common
Advanced
Emerging

Emerging threats/attacks

- **Description:** Focus on new attack vectors and vulnerabilities enabled by emerging technologies, based on specific research to identify and exploit vulnerabilities
- **Typical threat actors:** Sophisticated attackers, such as organized crime groups, industrial espionage teams, cyber terrorists and nation states
- **Examples:**
  - Exploiting vulnerabilities on “smart” devices to gain access to data and/or control systems
  - Leveraging security gaps created with the convergence of personal and corporate devices into one network
  - Using advanced techniques to avoid detection and/or bypass defenses

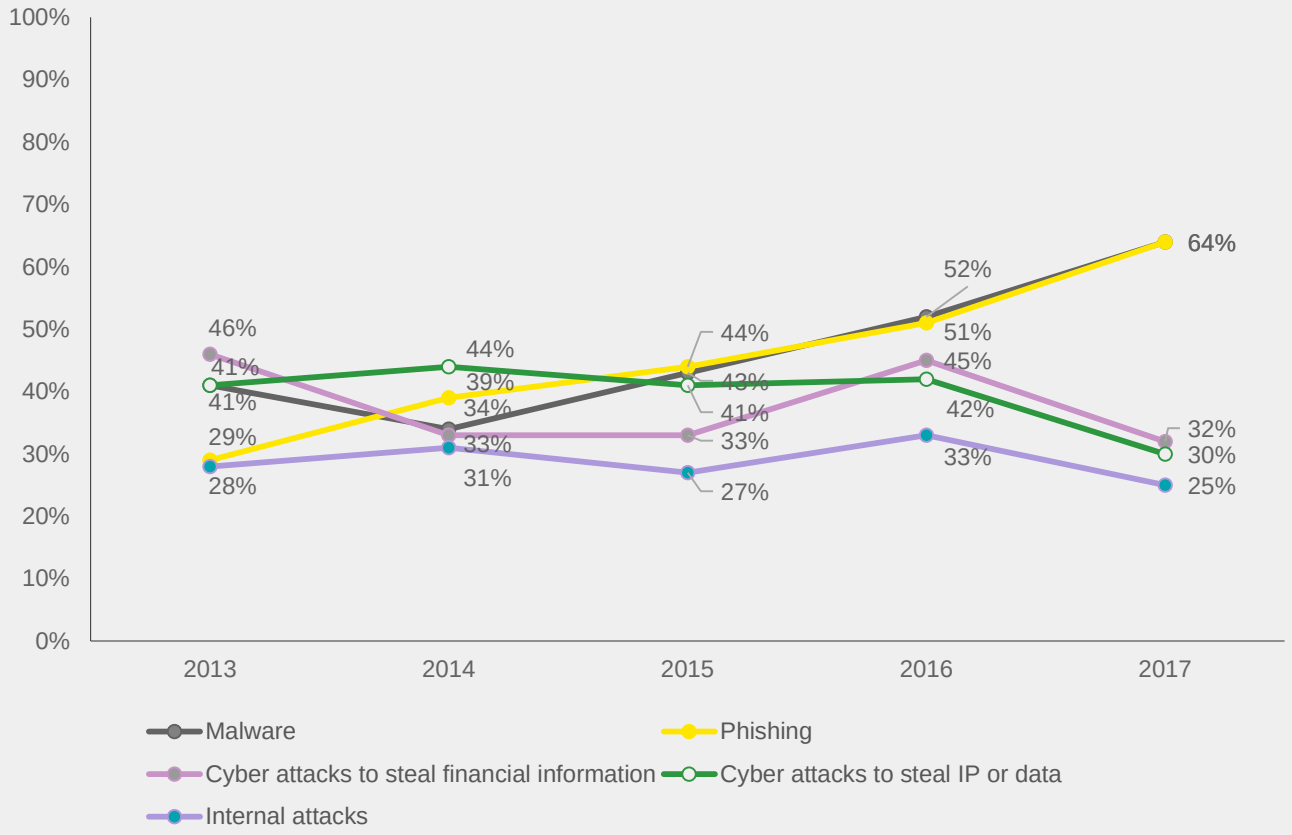
Vulnerabilities perceived to have most increased risk exposure have shifted a little between 2013-2017

- Careless or unaware employees are still seen as the greatest, and increasing, vulnerability.
- Unauthorized access has reduced as a vulnerability.



Threats perceived to have most increased risk exposure have shifted a little between 2013-2017

- Malware and phishing are seen as the greatest type of threats.



Likely sources of attack

- Employees and criminal syndicates are seen as the greatest immediate threats.
- For many organizations, the most obvious point of weakness will come from an employee who is careless – followed (in third place) by an employee with malicious intent.
- Organizations are also increasingly concerned about poor user awareness and behavior around mobile devices.
- The potential damage from losing a single smart device is understood to be increasing by 50% of respondents.

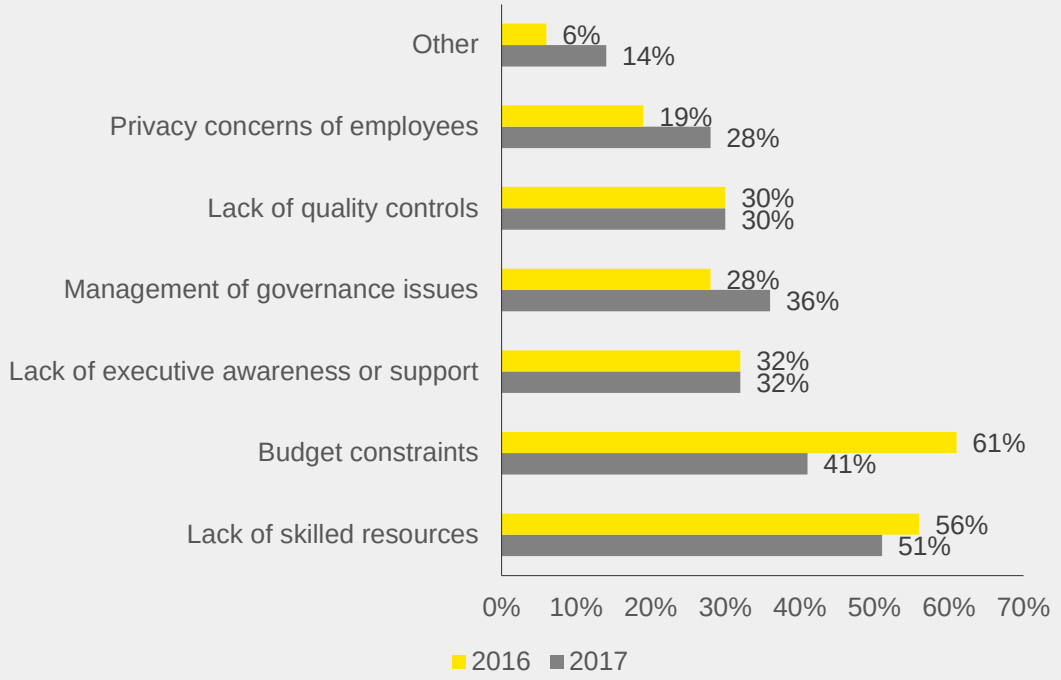
77%
of respondents consider a careless member of staff as the most likely source of attack

56%
consider a criminal syndicate as the most likely source of attack

47%
consider a malicious employee as the most likely source of attack

The Internet of Things (IoT) continues to complicate matters

- The IoT is the source of a broad range of threats that many organizations are now struggling to better understand.
- Here are the identified obstacles that are slowing down adoption of IoT devices:



Confronting cyber threats

Confronting cyber threats

- All organizations are now digital by default, and need to operate with the cultures, technology and processes of the internet era.
- The integration and growth of the Internet of Things (IoT) is vastly increasing and complicating the networked landscape.
- Cyber attackers can be either indiscriminate or highly targeted.
- Cyber attackers can be well-camouflaged: companies need to be able to identify the threat even when it adopts the colors of its immediate environment.

The scale of the threat is expanding dramatically: by 2021, the global cost of cybersecurity breaches will reach US$6 trillion by some estimates, double the total for 2015.

Cybercrime Report 2017 Edition, Cybersecurity Ventures, 19 October 2017

While cybersecurity budgets are increasing, most organizations require more to manage the risk effectively

- Mounting threat levels require a more robust approach to cybersecurity.
- Most organizations continue to increase their spending on cybersecurity, though not all.
- The vast majority believe they need up to 50% more cybersecurity funding to enable the cybersecurity function to be in line with the existing risk tolerance of the organization.
- 76% of survey respondents said the cybersecurity budget would increase if they suffered a damaging breach.

59%
of respondents this year say their budgets increased over the last 12 months

87%
say they need up to 50% more funding to meet requirements

Only 12%
expect an increase of over 25% in their cybersecurity budget

Organizations struggle to interpret the harm from attacks, resulting in lower budgets than required

- 64% said an attack that did not appear to have caused any harm would be unlikely to prompt an increase in the organization's cybersecurity budget.
- Harm is generally being done by an attack even it is not immediately obvious.
- Organizations should assume that all attacks cause harm – they just may not have discovered the damage yet.

Only 4%

of organizations are confident that they have fully considered the information security implications of their current strategy, and that their risk landscape incorporates and monitors cyber threats, vulnerabilities and risks.

Conclusion

To close, here are actions all organizations should take

Common attacks

Organizations need to be able to prevent common attacks through good basic cybersecurity.

Example activities

- Establish effective governance
- Identify what matters most
- Understand the threats
- Define your risk appetite
- Focus on education and awareness
- Implement basic protections

Advanced attacks

Organizations need to focus on improving their ability to detect and respond to the more sophisticated and dangerous attacks.

Example activities

- Be able to detect an attack
- Be prepared to react
- Adopt a risk-based approach to resilience
- Implement additional automated protections
- Challenge and test regularly
- Create a cyber risk management life cycle

Emerging attacks

Organizations need to understand the emerging threats and how they should impact strategic decision-making, while making focused investment in cybersecurity controls.

Example activities

- Build security into the development life cycle
- Enhance threat monitoring

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.

About EY's Advisory Services
EY Advisory believes a better working world means helping clients solve big, complex industry issues and capitalize on opportunities to grow, optimize and protect their businesses.

A global mindset, diversity and collaborative culture inspires EY consultants to ask better questions, create innovative answers and realize long-lasting results.

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

EYG no. 06575-173GBL

ED None

ey.com/giss