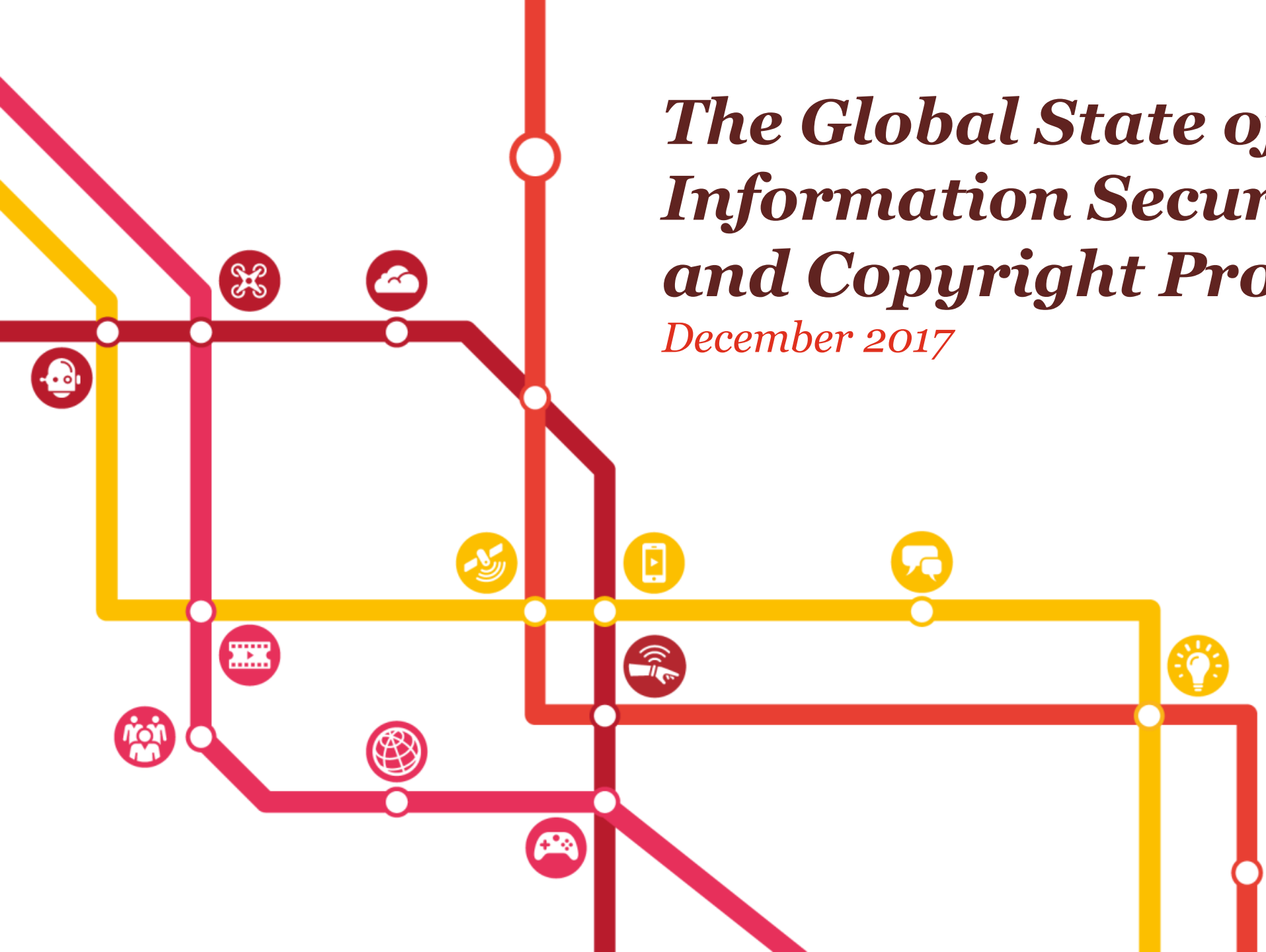


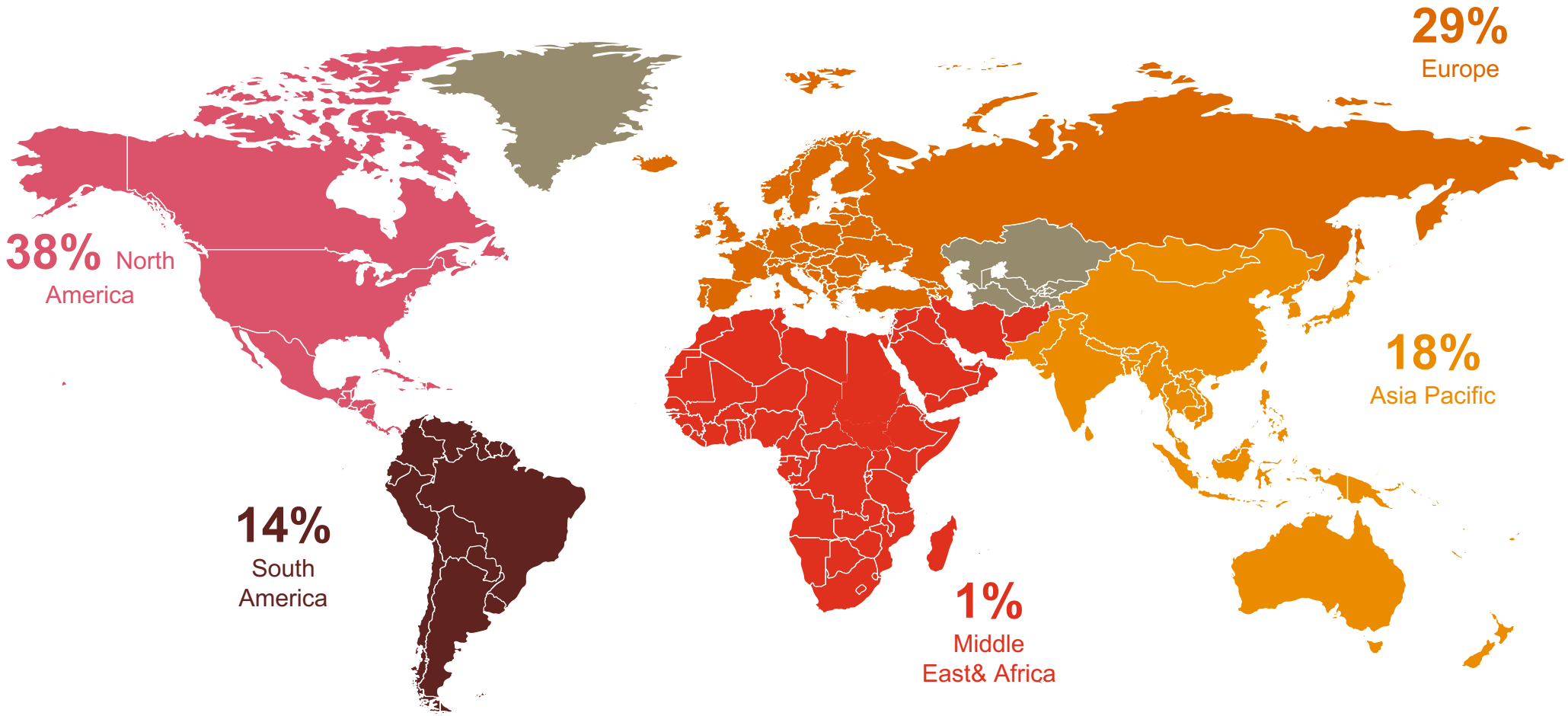
The Global State of Information Security and Copyright Protection

December 2017

pwc

Information Security

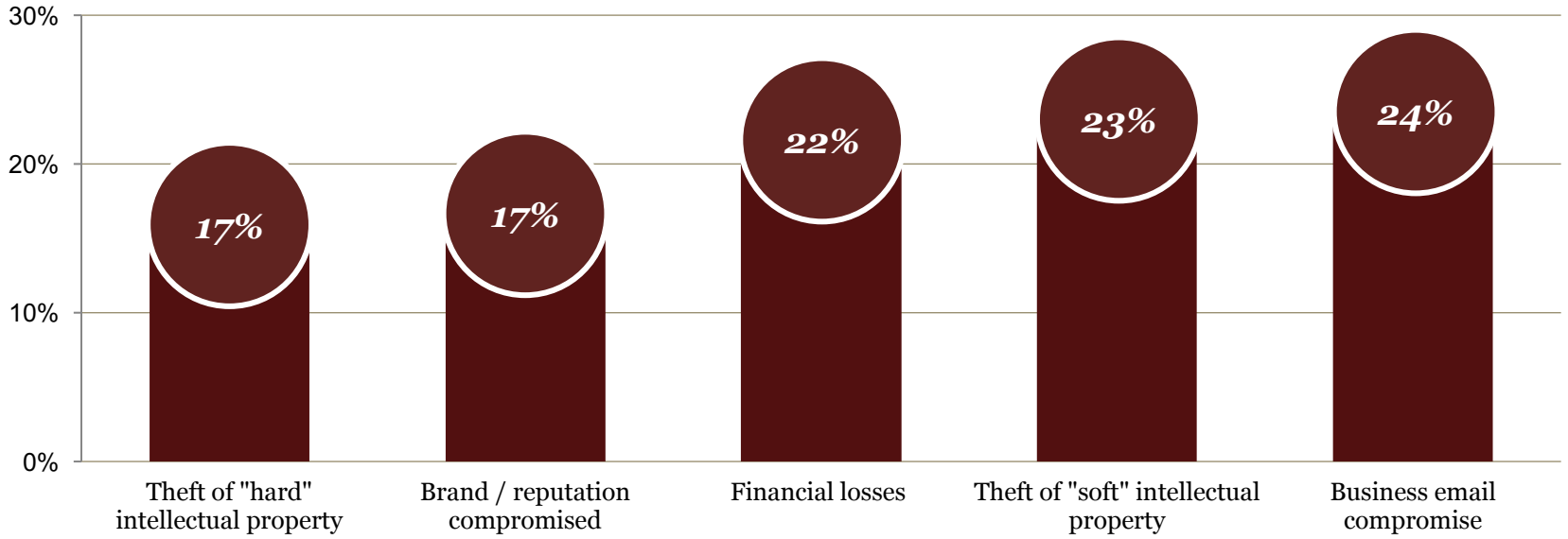
Survey Includes: 9,500 Respondents from 122 Countries



Security incidents continue to be a top business impact

Recently, cyber extortion, where a cyber criminal threatens to publically embarrass or threaten a company to secure large sums of money, has become an increasingly common approach taken by threat actors as evidenced in the case of film/television production and distribution companies and a number of hospitals. Thus, financial losses as a business impact of an incident may begin to climb.

Business impacts of security incidents



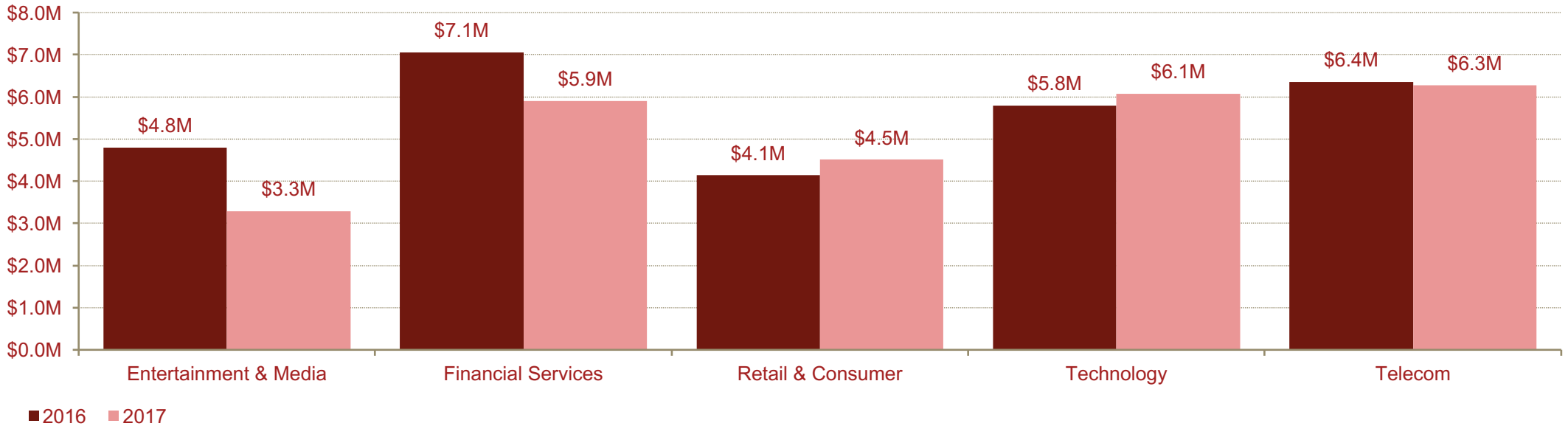
Cite mobile device exploitation as the cause of security incidents, overtaking phishing attacks as the top threat vector

Question 22: “How was your organization impacted by the security incidents?”
Question 19: “How did the security incident(s) occur?”

Information Security Budgets

Respondents in the Entertainment & Media industry saw information security budgets drop an average of 31%, while those in Financial Services reported an average decrease of 17%. Only 3 of 12 sectors reported increases in information security budgets.

Average information security budgets by industry



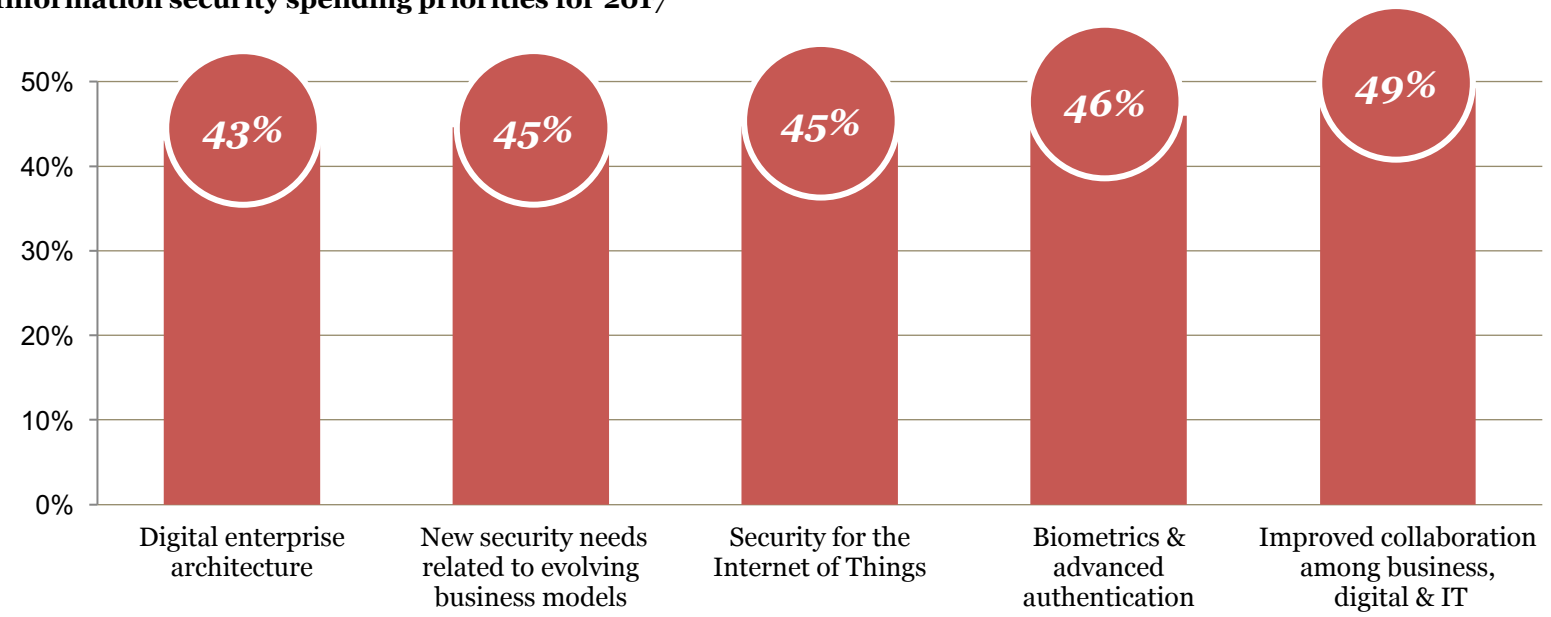
* Information security budget refers to funds specifically and explicitly dedicated to information security, including money for hardware, software, services, education and information security staff.

Question 8: "What is your organization's total information security budget for 2017?"

This year, organizations are prioritizing spending on broad strategies to strengthen their digital ecosystems

Security priorities in 2017 emphasize internal collaboration and new security safeguards for evolving business models. Biometrics and advanced authentication has notably increased as an investment priority compared to 2016 (+3% YoY).

Information security spending priorities for 2017



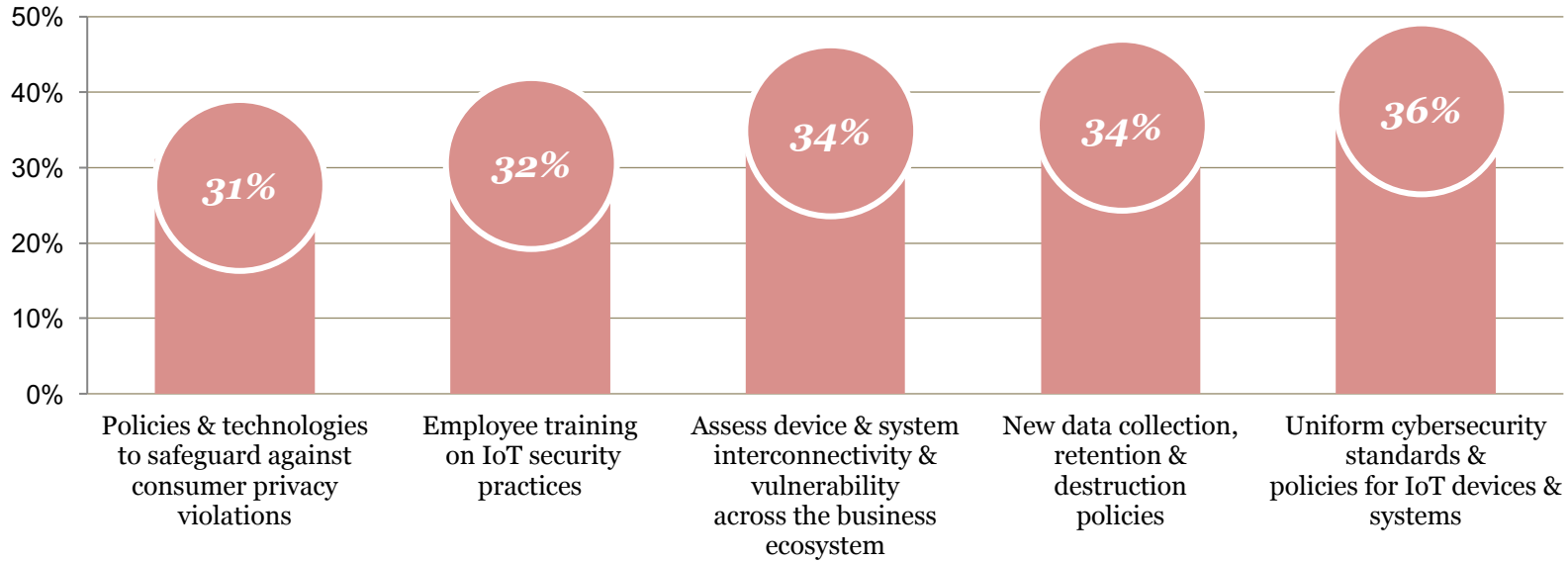
Say digital transformation has increased information security spending

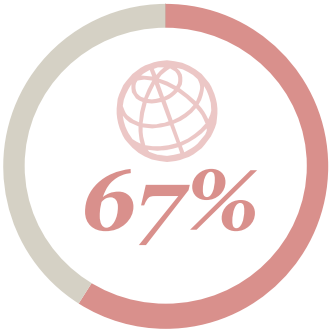
Question 10a_2017: "What types of security safeguards does your organization plan to invest in over the next 12 months?"
Question 10_2017: "What impact has digitization of the business ecosystem had on your organization's security spending?"

As Internet of Things becomes more ubiquitous, organizations are investing in revamping their security policies

Consumers are demanding products with an emphasis on cybersecurity and privacy. This is reflected in key IoT investment areas including policies and technologies to protect consumer privacy, as well as data governance policies.

Policies, technologies & people skills being implemented for the Internet of Things





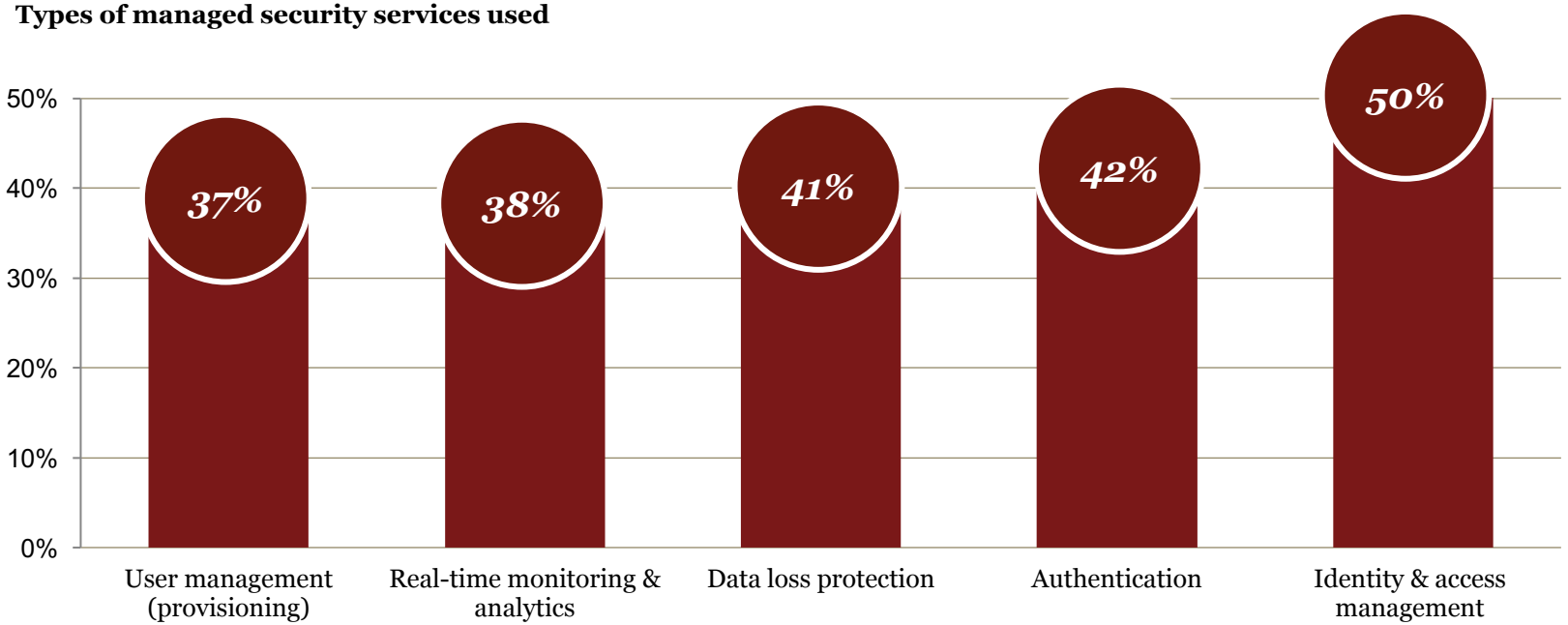
Have an IoT security strategy in place or are currently implementing one (+5% YoY)

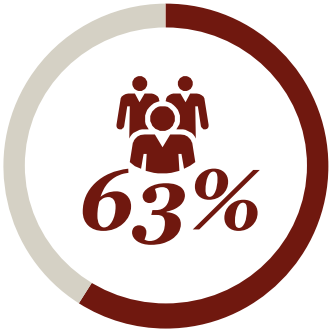
Question 25_2017: "What policies, technologies and people skills does your organization plan to implement over the next 12 months to address the cybersecurity and privacy risks associated with the Internet of Things (IoT)?"
Question 17_2015 Does your organization have a security strategy for the convergence of information, operational, and consumer technologies (also known as the Internet of Things)?

Respondents are embracing managed security services to extend and enhance their cybersecurity capabilities

Organizations say they rely on managed security services for highly technical initiatives such as identity & access management, authentication and data loss protection.

Types of managed security services used



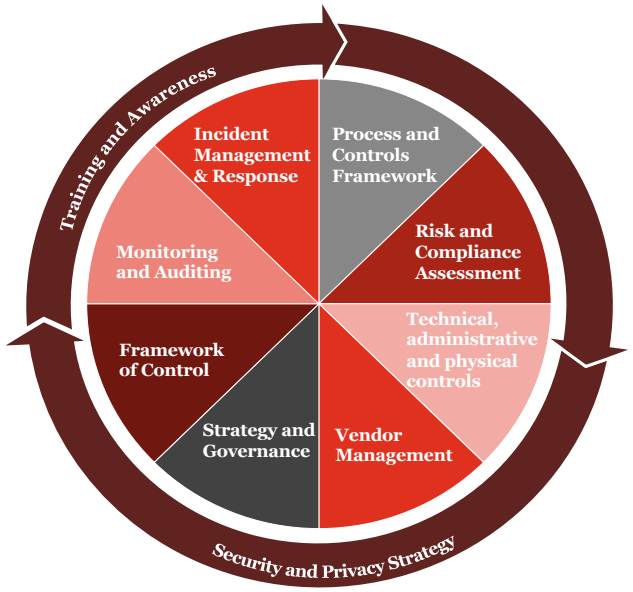


Use managed security services for cybersecurity & privacy

Question 20_2017: "Does your organization use managed security services in its cybersecurity and privacy programs?"
Question 20a_2017: "Which of the following managed security services does your organization use?"

What can you do to improve your Information Security and Privacy stance?

At a macro level, you can improve your information security posture in the following ways:



Assess: *Assessing your privacy and compliance risks, programs, and capabilities to help you develop strategies to better align your program to the organization's broader business objectives and threat landscape.*

Design & Implement: *Design and implement comprehensive, defensible privacy and compliance programs and technologies to enable you to better protect your customer data, provide greater trust and transparency to consumers, and streamline compliance initiatives and costs.*

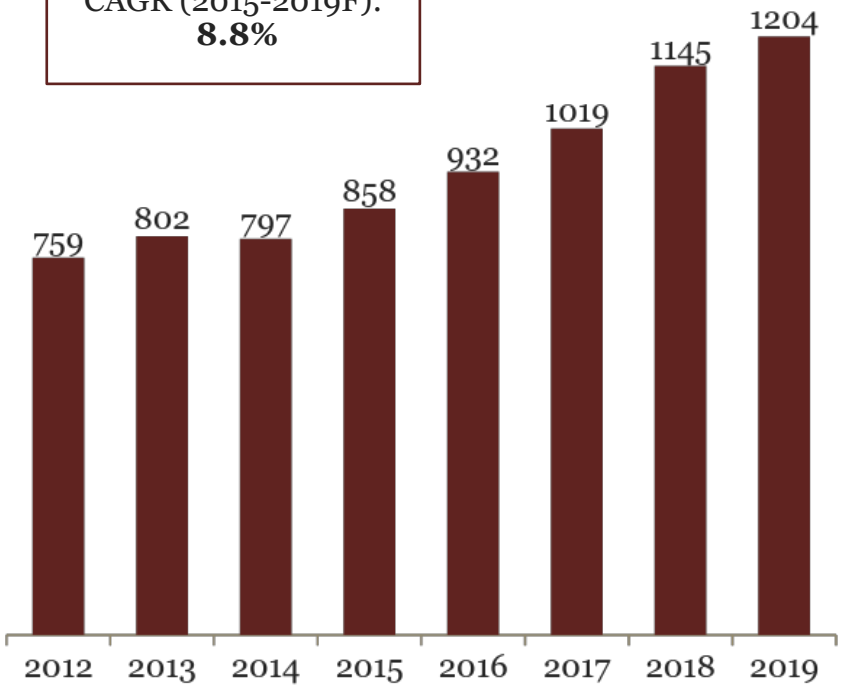
Operate & Sustain: *Manage dynamic information protection and privacy risks and compliance obligations on an ongoing basis by providing operational support in the form of regular assessments or health checks, recurring regulatory assessments, co-sourced/outsourced program support, and staff augmentation services.*

Copyright Protection

Copyright Owner: Pain Points

With the emergence of new technologies, piracy has continued to increase year-over-year. This as resulted in revenue losses of over $32 billion for content owners.

Pirated file sharing – North America (Petabytes, 2012-2019F)



Source: Cisco Virtual Network Index

1.1 bn

takedown notices received by a large Online Service Provider in 2016

Source: 2016 Google Transparency Report

$32 bn

loss of revenue to content owners annually in the US due to piracy

Source: 2017 PwC Projection

191 bn

film and television piracy site visits globally during 2016

Source: Muso Piracy Report 2017

60%

Piracy consumers use streaming services to illegally obtain digital content in 2016

Source: Muso Piracy Report 2017

Infringement Activity in a Diverse Ecosystem

Infringement and Piracy activity continues to increase due to the continuously evolving technology landscape and a dynamic ecosystem

Emergent technology is driving increased infringement activity...

Mobile

Computing

Broadcasting

Streaming

...and taking enforcement actions against Service Providers is a constant game of whack-a-mole.

Complex ecosystem

- **Disparate systems & data**
- **Diverse & distributed environments across cloud & ground**

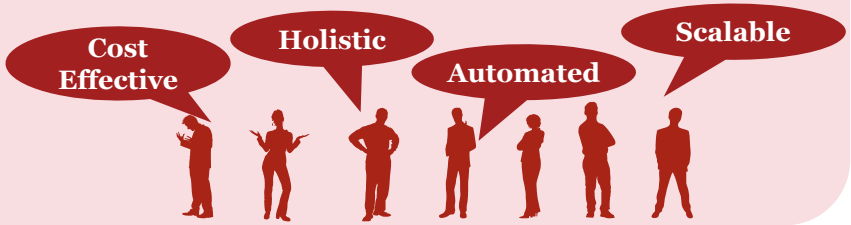
This results in significant challenges for Copyright owners to protect their revenue

Music

Movies/TV

Games

...which in turn is increasing demands for technology solutions.



This calls for a broader strategy

With 60% of online users preferring to use streaming services such as Kodi add-ons and torrent sites, the insatiable demand for easy to consume content has resulted in approx. **$32 billion in 2016 US revenue losses** to the movie, music, TV, gaming and software industries.

Based on our Information Security findings, the 59% increase in Security spending is a welcome signal in the fight to protect digital assets but to be effective you need a broader strategy.

A holistic Copyright Protection strategy should incorporate:

1. An automated technology solution that actively searches for, identifies, and grades pirated content across the regular, deep, and dark web with minimal human analysis and enables enforcement actions.
2. Policies and procedures that protect digital assets from hacks, leaks, third party misuse and abuse.
3. Access to aggregated data about piracy trends, threat actors and vectors, and mitigation methods.
4. Data Analytics around who is pirating based on available meta-data to build intelligence around the demographics and geolocations where piracy is being seeded, distributed, and consumed.
5. Reach/market to those consuming pirated content and attempt to convert to paying audience – attempt to convert 10%.

How should you go about protecting your digital assets?

Using automated tools search the public, deep and dark web to identify allegedly infringed content.

Using technology review alleged infringed content and evaluate if it has been used fairly or infringement has likely occurred.

Using technology review the allegedly infringed content and grade the likelihood that infringement has occurred using advanced analytics.

Upon review and approval, Service Providers should be notified of subscriber copyright infringement incidences with a request to remove alleged infringed content or stop infringing behavior.

Include proactive monitoring to reduce incidents and ensure high availability utilizing multi-skilled support staff, service level monitoring and reporting.

Thank you.

Wendy Frank
Principal, Strategic Technology, PwC
601 S Figueroa St
Los Angeles, CA 90017
Office: +1 (213) 217-3615
wendy.l.frank@pwc.com

Namir Khan
Director, Strategic Technology, PwC
1075 Peachtree St, Suite 2600
Atlanta, GA 30309
Office: +1 (678) 419-3220
namir.khan@pwc.com