www.pwc.com/cybersecurity

Moving forward with cybersecurity and privacy – What Does The Media/Cyber Environment Look Like Now…and What's Next?

Including Key findings from The Global State of Information Security® Survey 2017 Customized for the Content Protection Summit

December 7, 2016

pwc

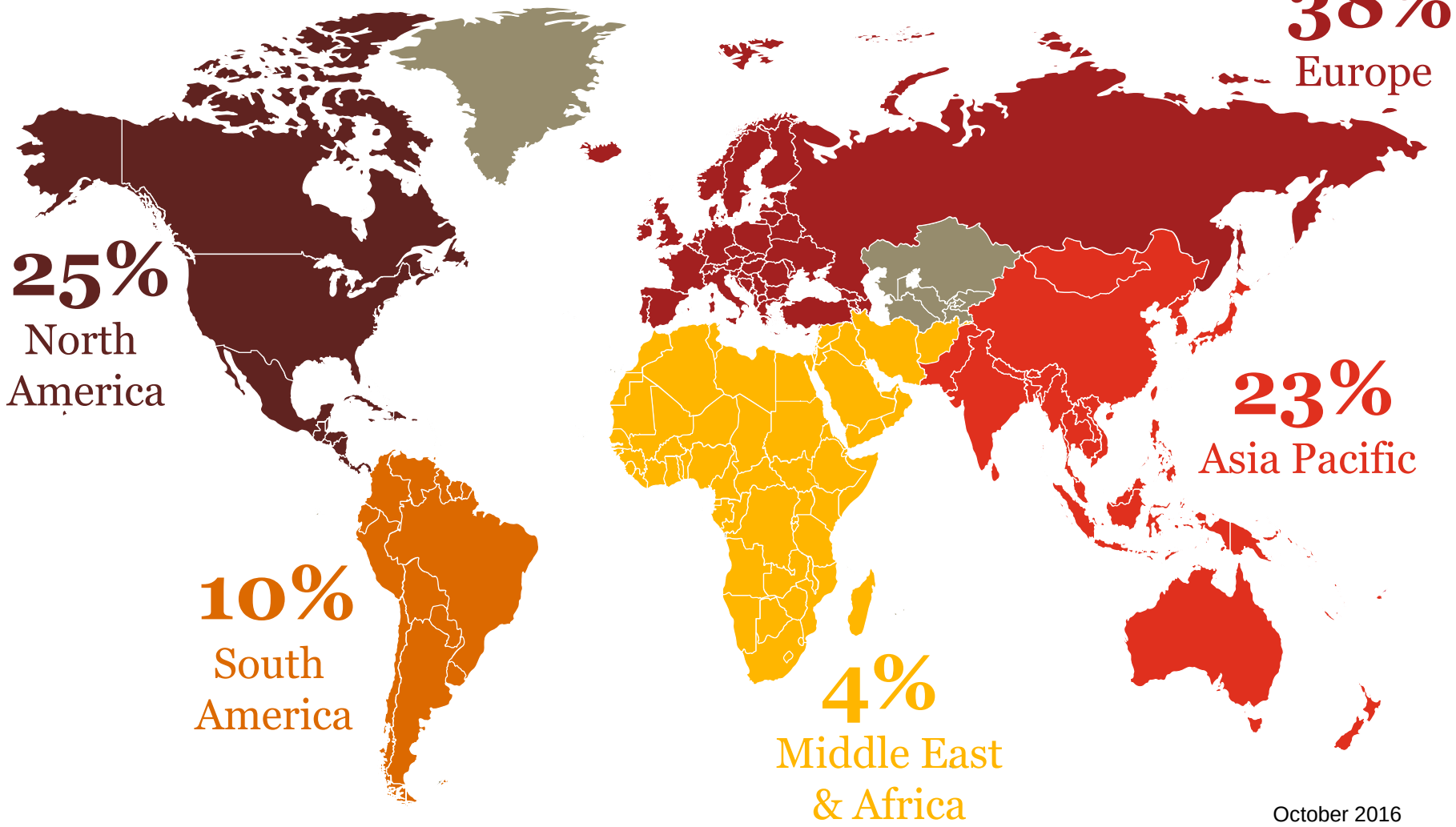
Methodology

The Global State of Information Security® Survey 2017, a worldwide study by PwC, *CIO* and *CSO*, was conducted online from April 4, 2016 to June 3, 2016.

- PwC's 19th year conducting the online survey, 14th with *CIO* and *CSO*
- Readers of *CSO* and *CIO* and clients of PwC from 41 countries
- Responses from 275 CEOs, CFOs, CIOs, CISOs, CSOs, VPs and directors of IT and security practices
- Forty-one percent (41%) of respondents from companies with revenue of $500 million+
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Twenty-five percent (25%) of respondents from North America, 38% from Europe, 23% from Asia Pacific, 10% from South America and 4% from the Middle East and Africa
- The margin of error is less than 1%; numbers may not add to 100% due to rounding
- Figures in this report are based on respondents in the entertainment, media and communications industry

A survey of 275 entertainment, media and communications respondents from 41 nations.

Respondents by region of employment

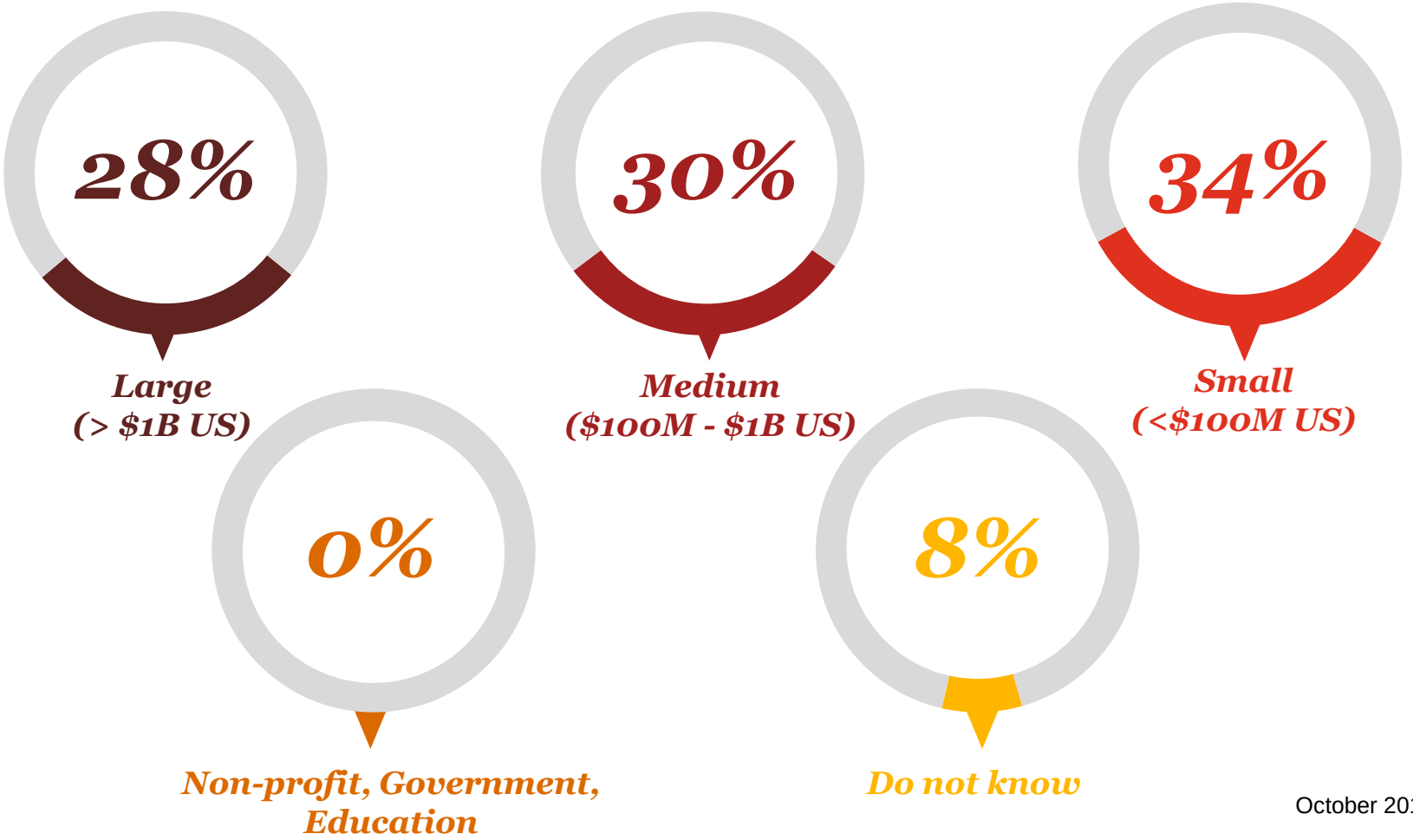


A mix of business and IT security executives are represented.

Respondents by title

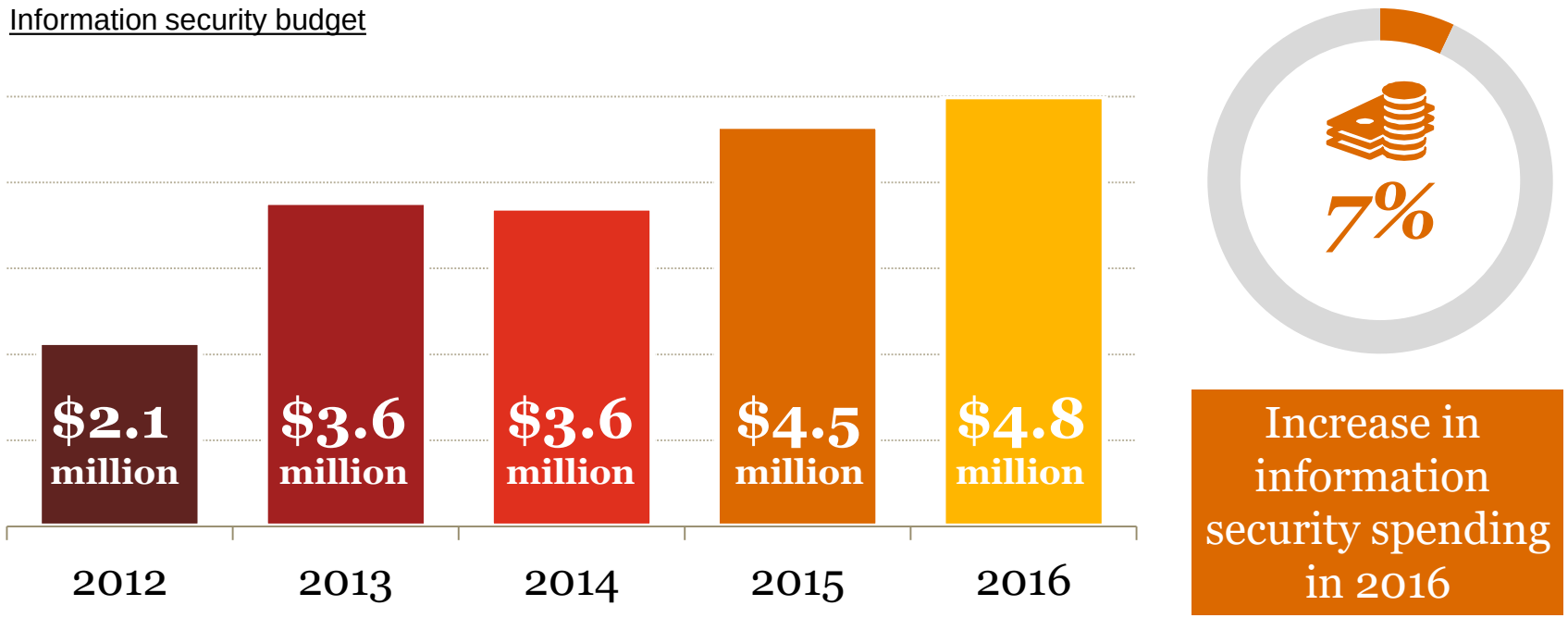
A range of organizations by annual revenue.

Respondents by company revenue size



*Entertainment, media & communications (EMC) respondents continue to boost information security spending.**

Information security budgets have increased 35% since 2014. In 2016, security spending climbed 7% over the year before and IT budgets were up 9%.



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

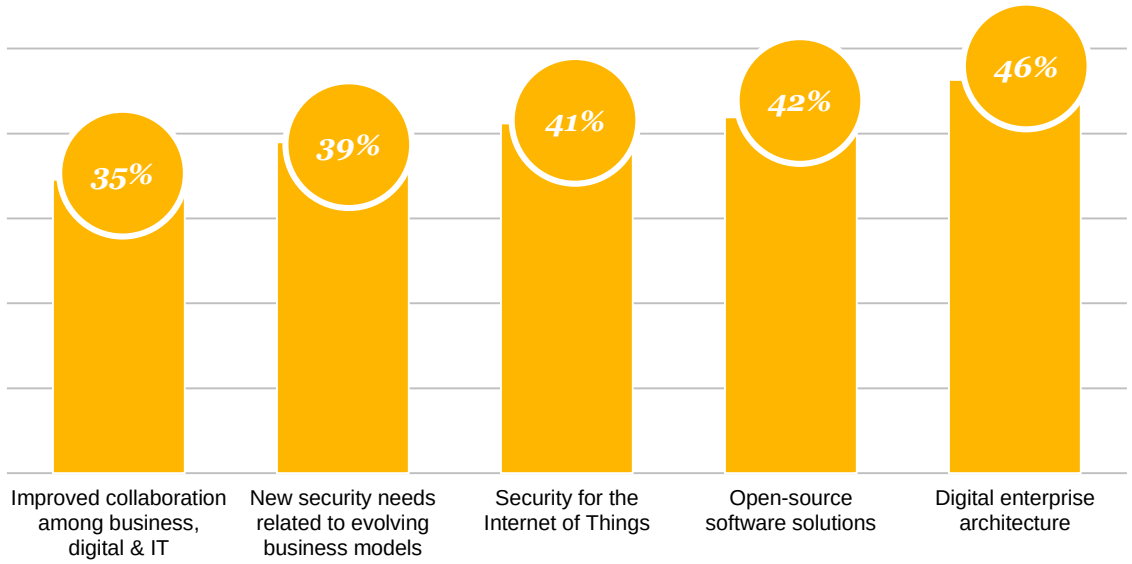
Question 7: “What is your organization's total information technology budget for 2016?” Question 8: “What is your organization’s total information security budget for 2016?”

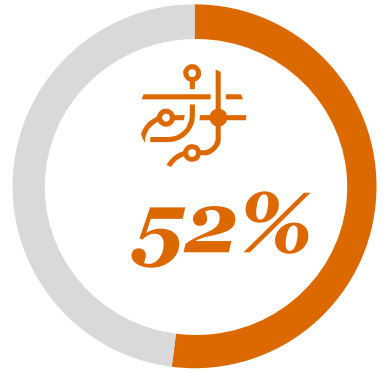
October 2016

Respondents who say digitization drives security spending are focusing on broad strategies for digital ecosystems.

Top spending priorities in 2016 include digital enterprise architecture, open-source software and security for the Internet of Things.

Information security spending priorities for 2016





Say digitization has led to a rise in security spending

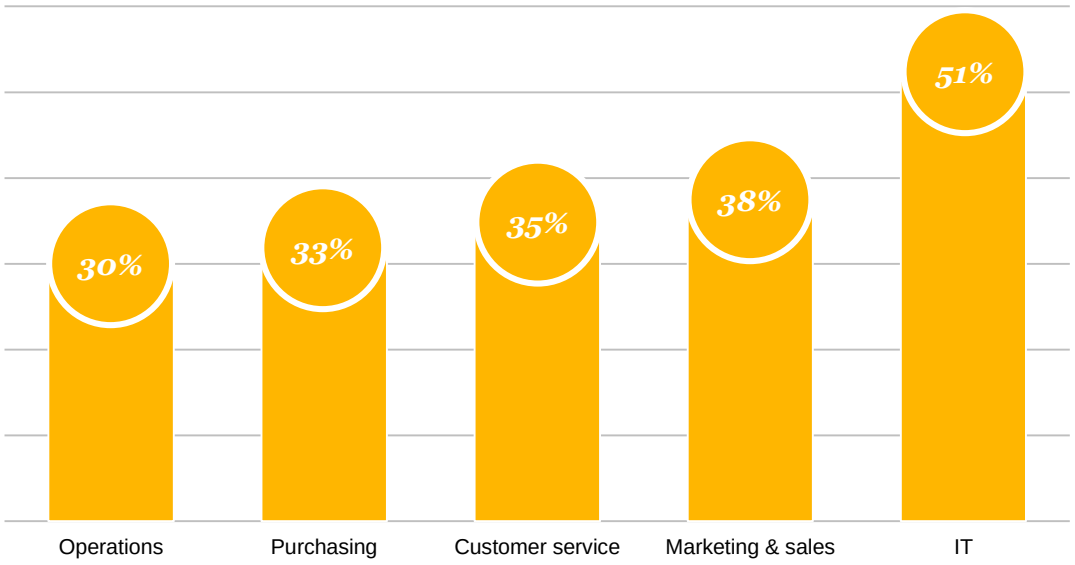
Question 10a_2017: “What types of security safeguards does your organization plan to invest in over the next 12 months?” Question 10_2017: “What impact has digitization of the business ecosystem had on your organization’s security spending?”

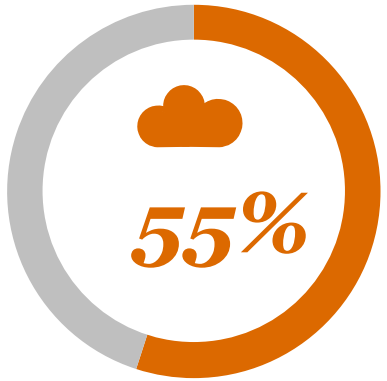
October 2016

As trust in cloud models deepens, EMC companies are starting to run more sensitive business functions in the cloud.

Although IT systems are most likely to be run in the cloud, one-third or more respondents entrust providers with marketing and sales, customer service and purchasing functions.

Business functions run in a cloud environment





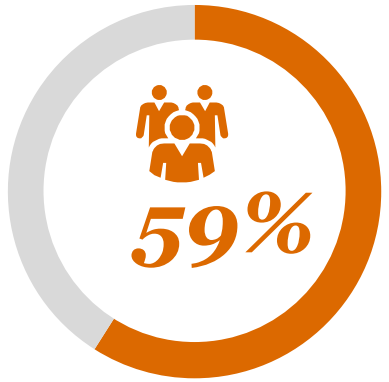
Of all IT services are delivered via cloud service providers

Question Q15_2017: “What business function areas does your organization run in a cloud environment?” Question Q16_2017: “Currently, what percentage of your organization’s IT services is delivered via cloud service providers?”

Organizations use managed security services to enhance and expand complex cybersecurity capabilities.

EMC respondents have implemented managed security services for initiatives such as authentication, data loss prevention, and identity and access management.

Types of managed security services used



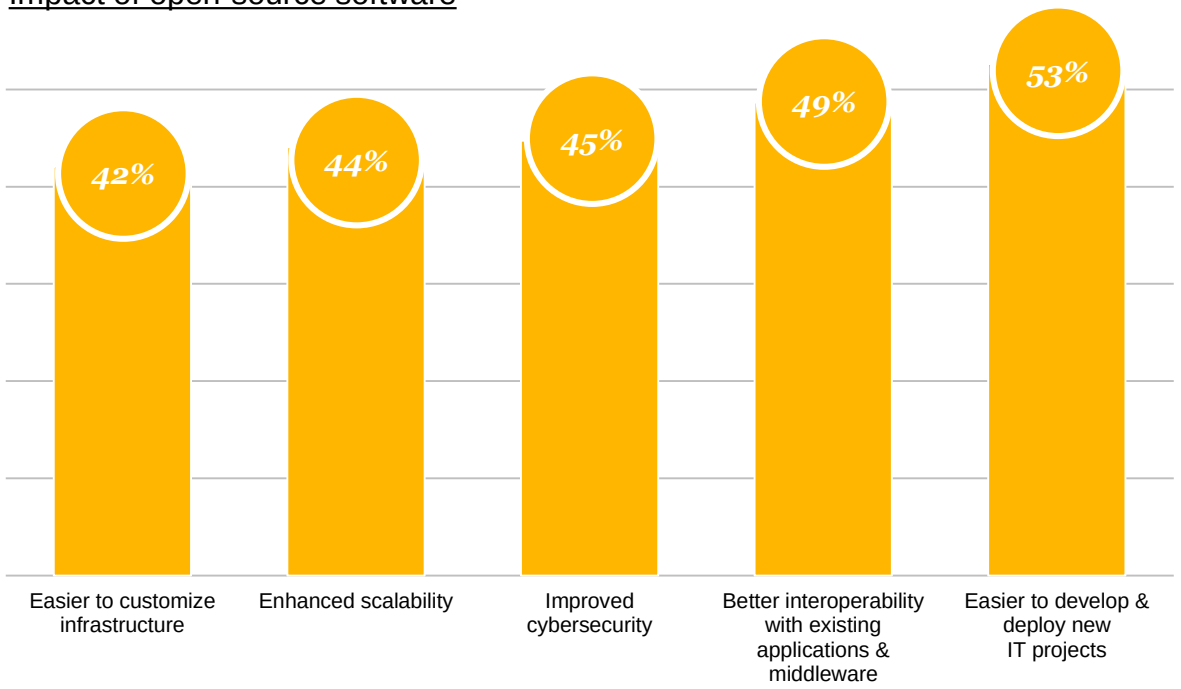
Use managed security services for cybersecurity & privacy

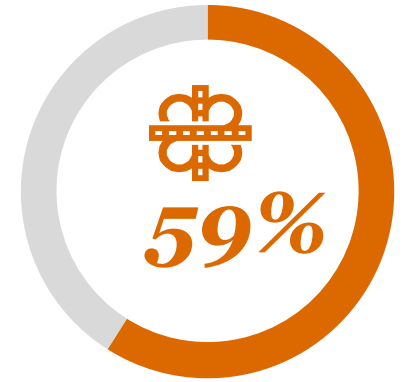
Question 20_2017: “Does your organization use managed security services in its cybersecurity and privacy programs?” Question 20a_2017: “Which of the following managed security services does your organization use?”

EMC businesses are deploying open-source software to more efficiently deliver IT services and improve interoperability.

More than half of EMC respondents use open-source software, and of these, 45% say open-source has improved their cybersecurity program.

Impact of open-source software





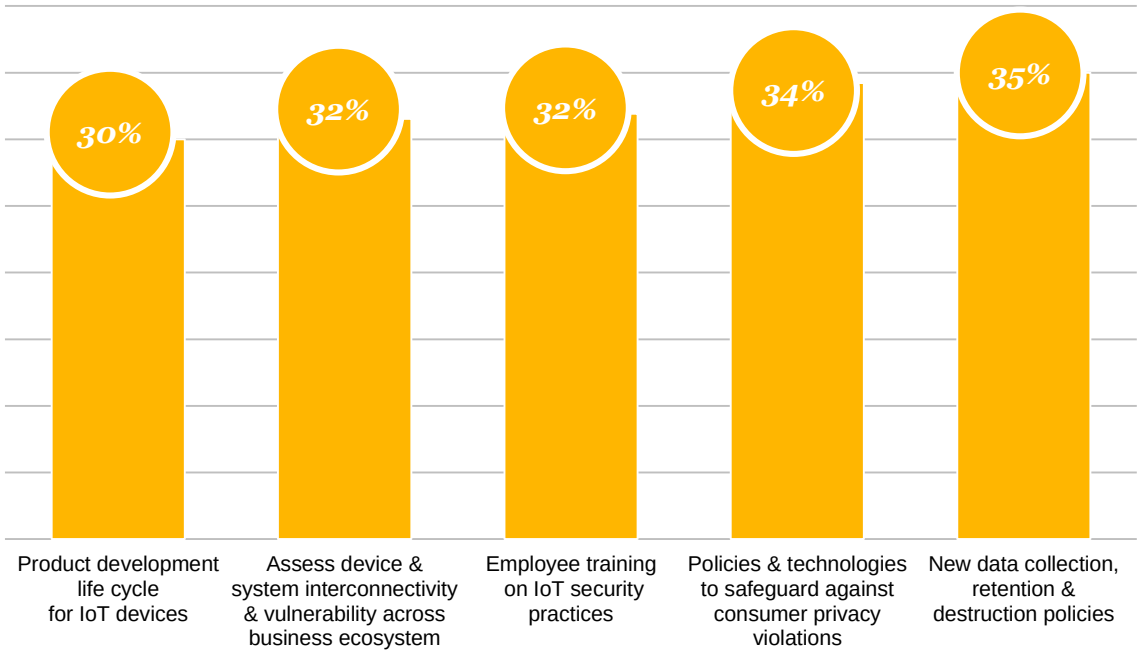
Use open-source software

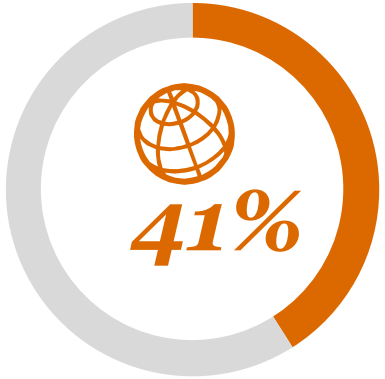
Question 21_2017: “Does your organization use open-source software in place of/in addition to traditional enterprise software infrastructure and middleware?” Question 21a_2017: “What impact has the use of open-source software had on your organization?”

Many organizations are updating cybersecurity safeguards to address risks associated with the Internet of Things.

Key priorities include data-governance policies, consumer data privacy protection and employee training for IoT security practices.

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





Are investing in security for the Internet of Things

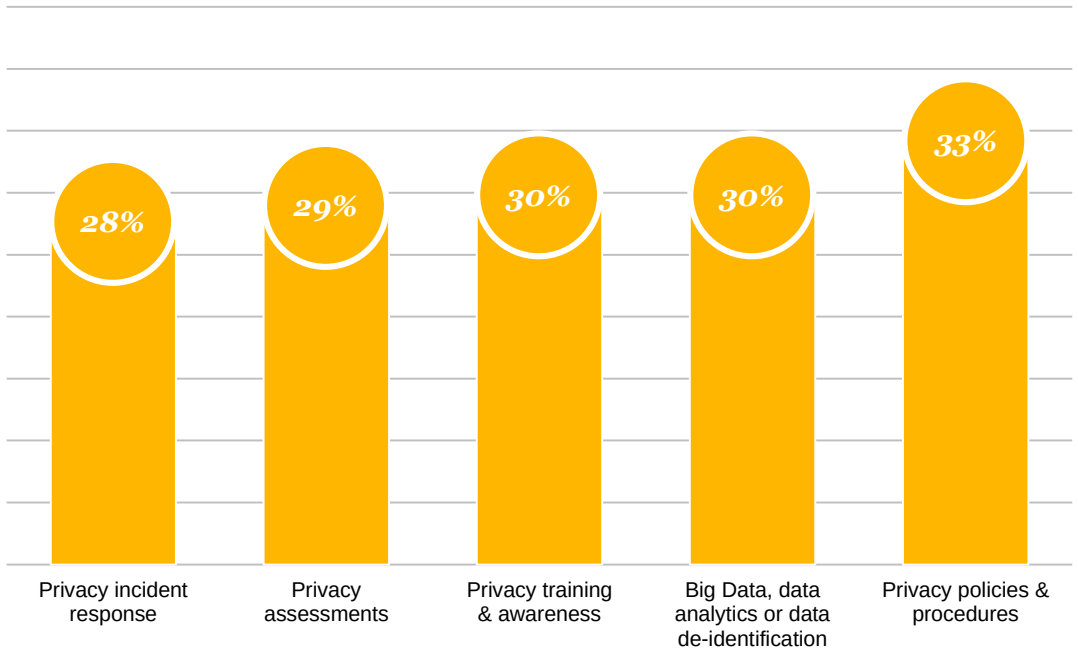
Question 25_2017: “What policies, technologies and people skills does your organization plan to implement over the next 12 months to address the cybersecurity and privacy risks associated with the Internet of Things (IoT)?” Question 10A_2017: “What types of security safeguards does your organization plan to invest in over the next 12 months?”

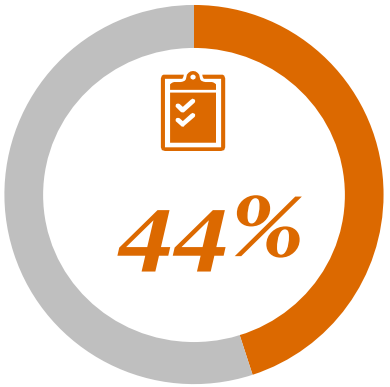
October 2016

As data privacy becomes an increasingly critical business requirement, companies are updating privacy policies.

EMC respondents are also emphasizing privacy training for employees and are revising their data-management programs.

Top privacy initiatives for 2016



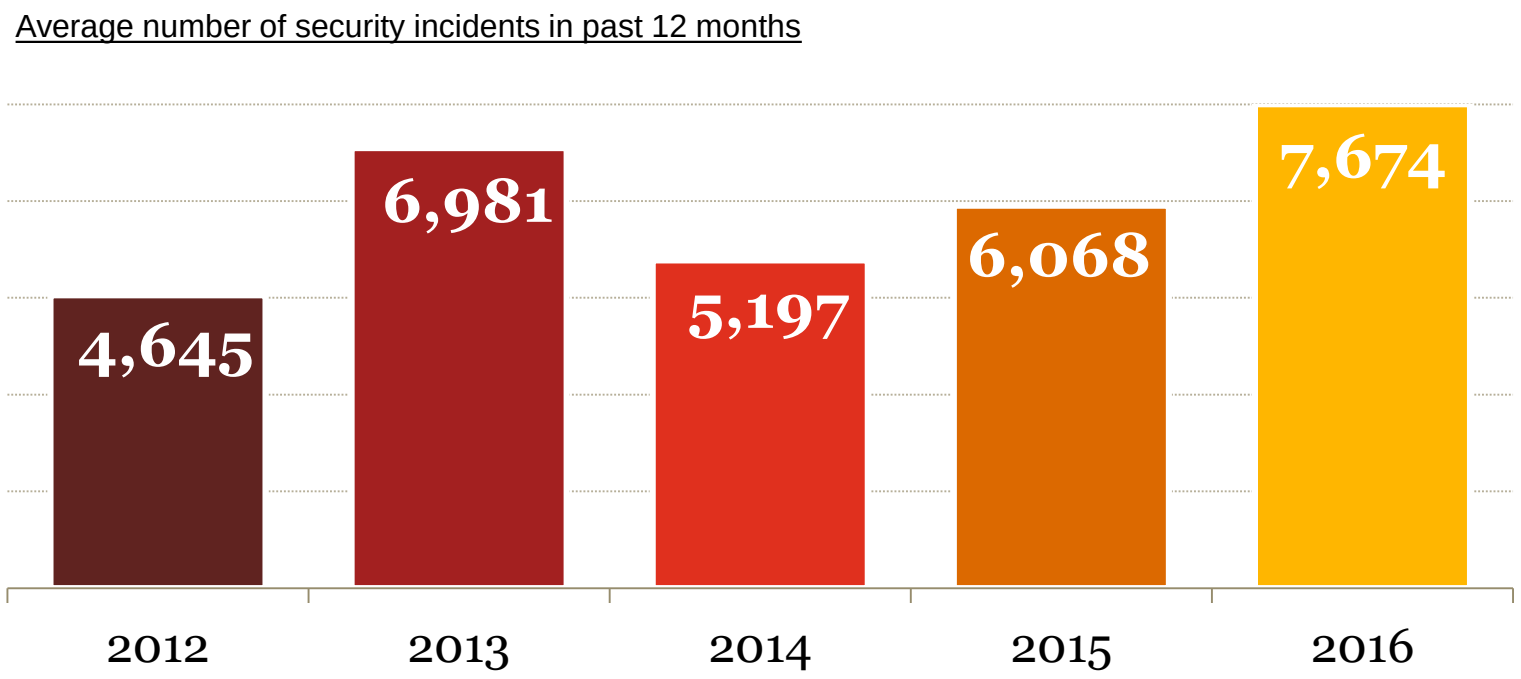


Limit collection, retention & access to personal information

Question 24_2017: “Which of the following projects, if any, will your privacy function address over the next 12 months?” Question 10a_2016: “Which safeguards does your organization currently have in place?”

*The number of detected information security incidents has increased steadily since 2014.**

Overall, detected incidents climbed 26% in 2016. Average total financial losses as a result of these incidents soared 81% over the year before.



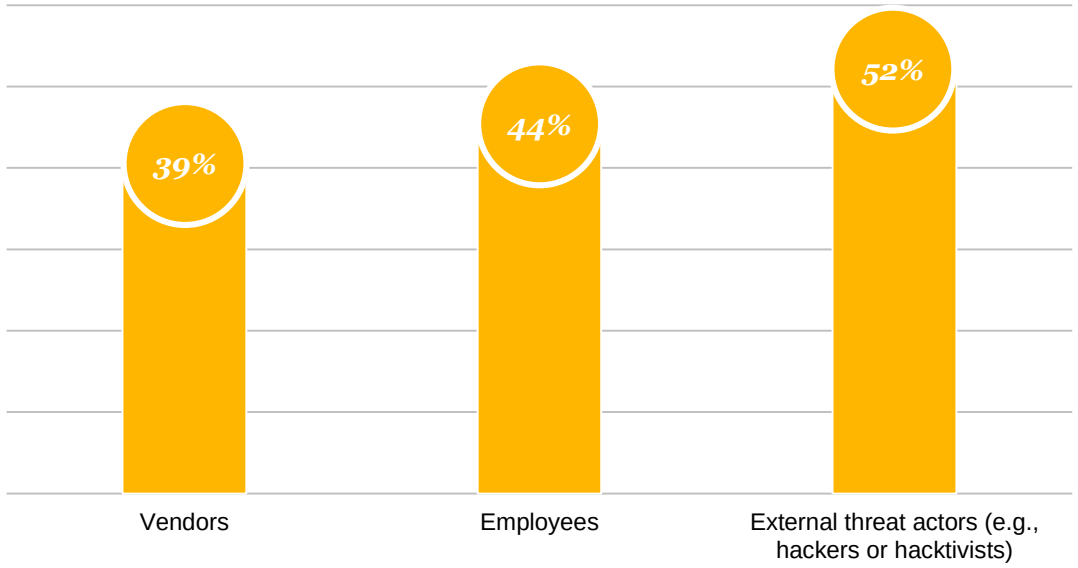
* A security incident is defined as any adverse incident that threatens some aspect of computer security.

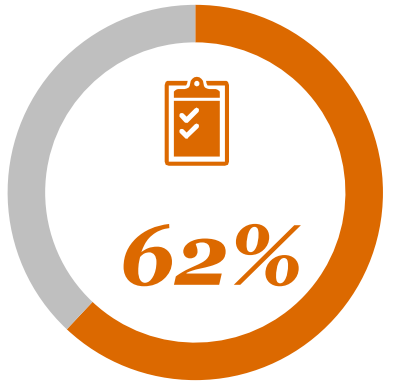
Question 18: “What is the number of security incidents detected in the past 12 months?” Question 22A: “Estimated total financial losses as a result of all security incidents.

EMC respondents believe that external threat actors like hackers and hacktivists are most likely to lift digital content.

Respondents say that third-party vendors are least likely to steal digital content, while 44% point the finger at employees.

Awareness of parties involved in theft / loss of digital content prior to launch





Have adequate in-house security expertise to secure Internet content distribution

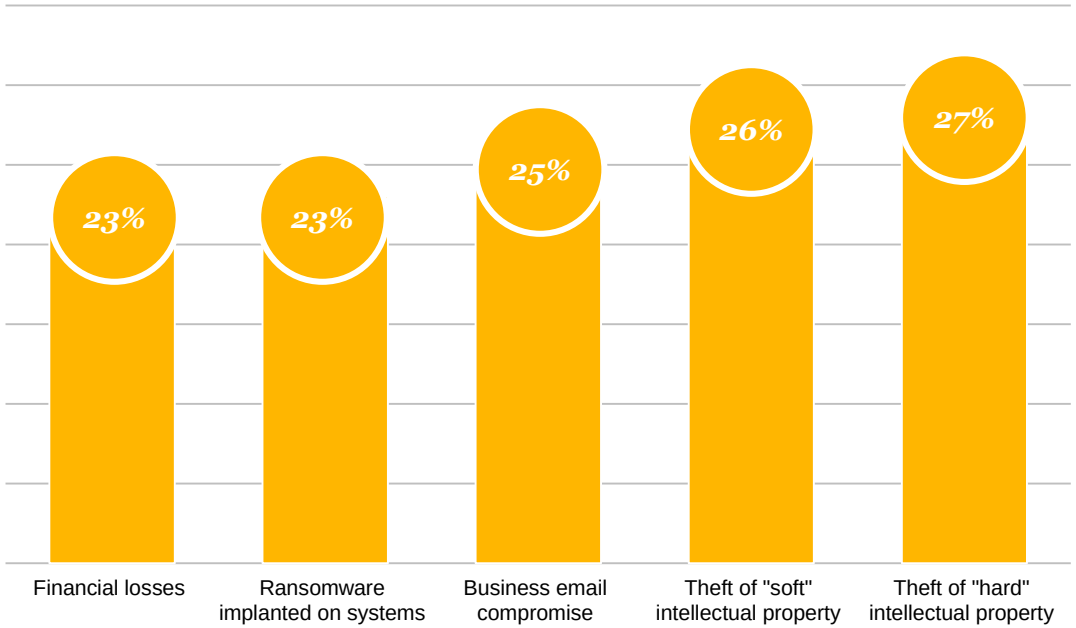
Question 1ENT: “Do you have adequate in-house security expertise to secure Internet content distribution?” Question Q2a/b/cENT: “Are you aware of any employees / vendors / external threat actors being involved in or responsible for the theft or loss of digital content prior to a major launch window (e.g., theatrical, DVD, streaming media)?”

October 2016

Business email compromise and ransomware emerge as growing business impacts, while phishing is the top vector.

Large organizations are more likely to fall victim to phishing (social engineering): 48% of businesses with revenues of more than $1 billion reported this type of incident.

Business impacts of security incidents



Cite phishing (social engineering), making it the No. 1 vector of incidents this year.

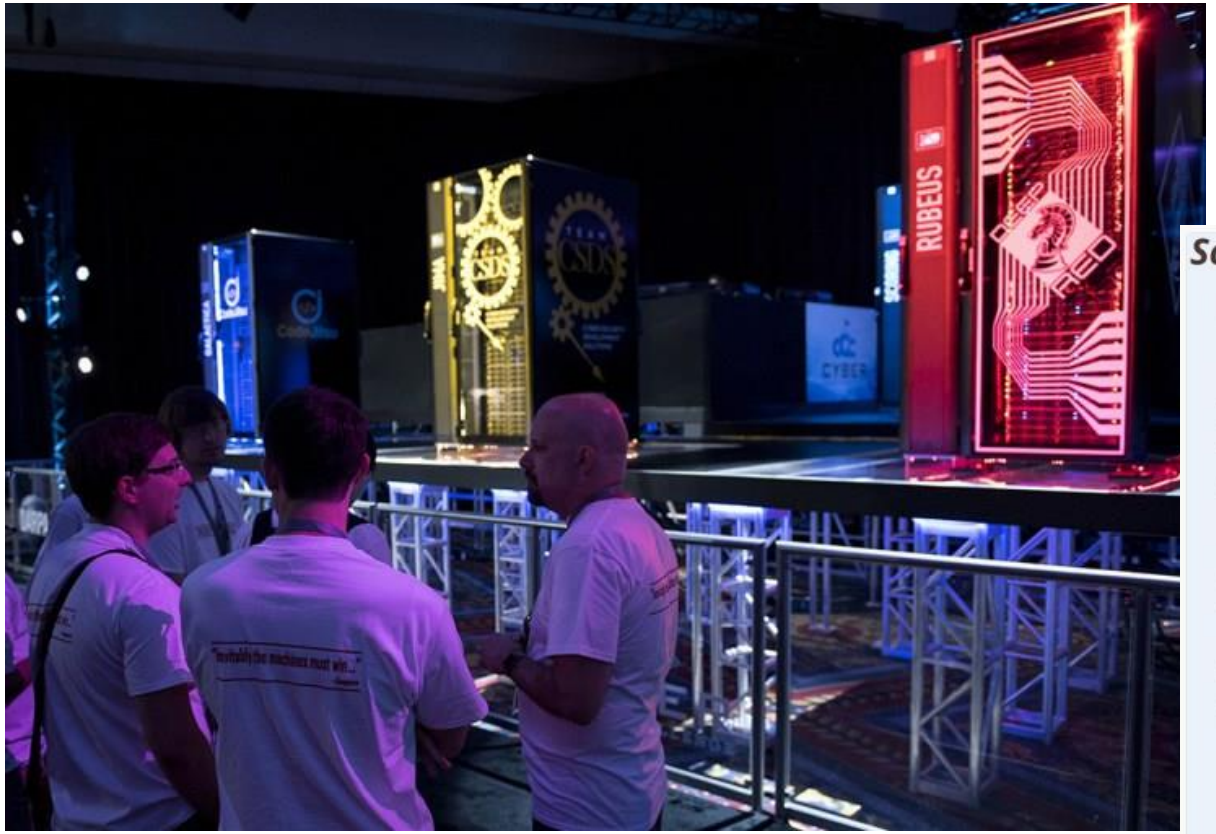
Question 22: “How was your organization impacted by the security incidents?” Question 19: “How did the security incident(s) occur?”

But I Really Want to Talk About the Future – Where to Next?

- Drone Security

But I Really Want to Talk About the Future – Where to Next?

- Artificial Intelligence and Self Defending Networks

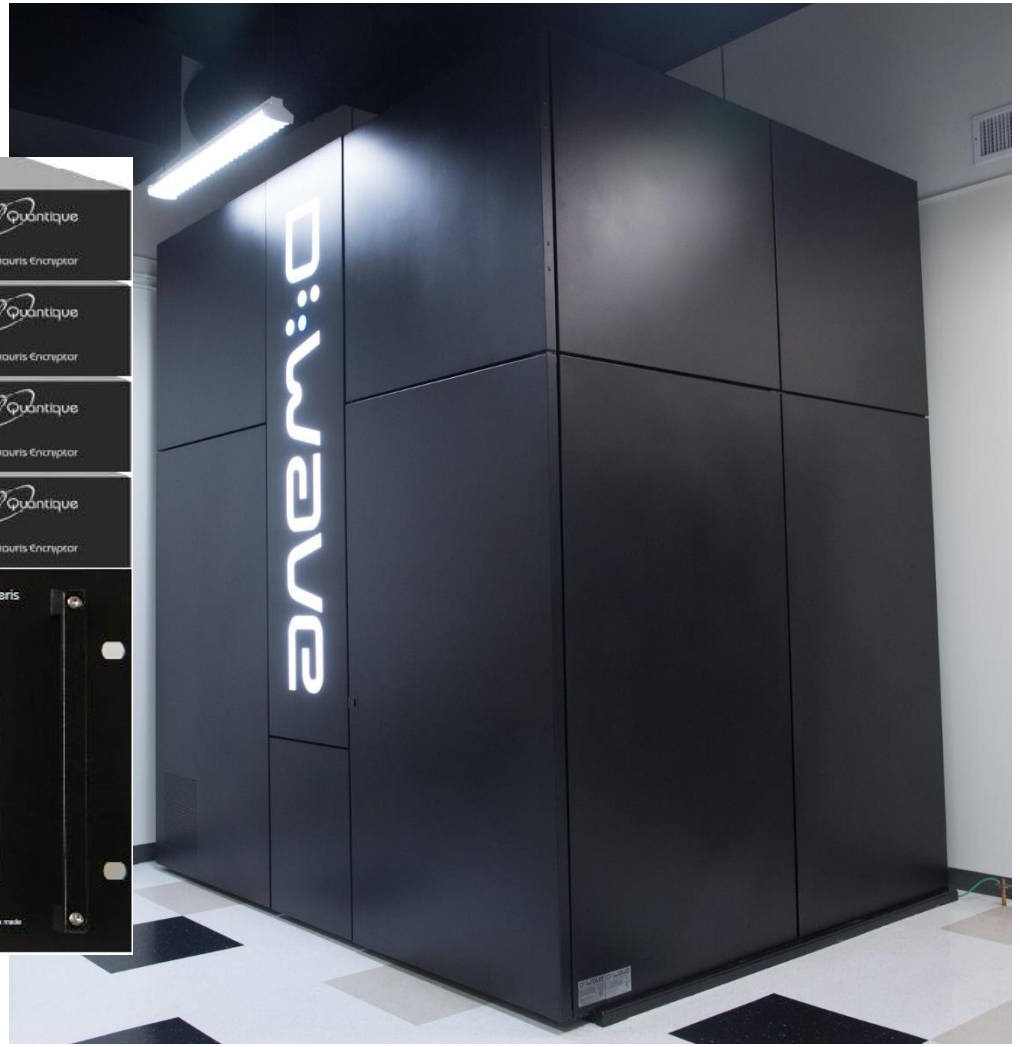


Scoreboard

place	score	team
1	15	PPP
2	14	b1o0p
3	13	DEFKOR
4	12	HITCON
5	11	KaisHack GoN
6	10	LC↯BC
7	9	Eat Sleep Pwn Repeat
8	8	binja
9	7	pasten
10	6	9447
11	5	!SpamAndHex
12	4	Shellphish
13	3	Dragon Sector
14	2	侍
15	1	Mayhem

But I Really Want to Talk About the Future – Where to Next?

- Quantum Computing – The End of Security As We Know It



For more information, please contact:

Wendy Frank
Principal, Cybersecurity, Privacy and Risk Practice
wendy.l.frank@pwc.com

Visit www.pwc.com/gsiss2017 to further explore the data.