The Need for a New IT Security Architecture:
Global Study on the Risk of Outdated Technologies

Sponsored by Citrix

Independently conducted by Ponemon Institute LLC

Publication Date: February 2017

The Need for a New IT Security Architecture: Global Study on the Risk of Outdated Technologies

Ponemon Institute, February 2017

Part 1. Introduction

The Need for a New IT Security Architecture: Global Study on the Risk of Outdated Technologies, sponsored by Citrix and conducted by Ponemon Institute, reveals global trends in IT security risks and reasons why security practices and policies need to evolve to deal with threats from disruptive technologies, insider risk and compliance. Changes in the workplace and problems managing IT security are also increasing risks to organizations.

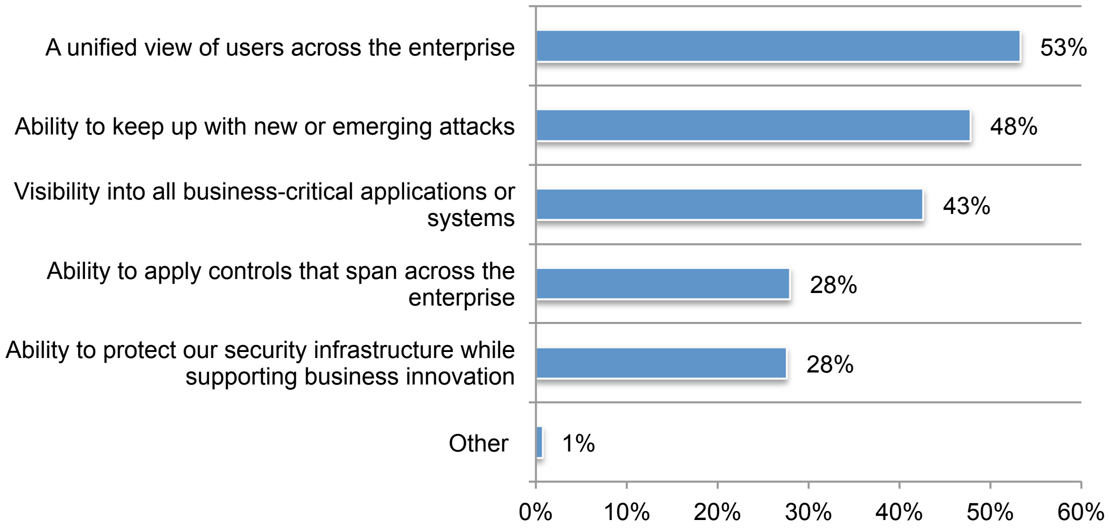
We surveyed 4,268 IT and IT security practitioners in Australia/New Zealand, Brazil, Canada, China, Germany, France, India, Japan, Korea, Mexico, the Netherlands, the United Arab Emirates, the United Kingdom and the United States. This report presents the consolidated findings.

This is the second of three reports that present the findings of this global study. In this report, we discuss the findings that concern risks created by outdated and inefficient IT security technologies

Organizations are at risk because they often do not have a unified view of users across the enterprise. According to Figure 1, the new IT security architecture should provide a unified view of users across the enterprise, according to 53 percent of respondents. Almost half (48 percent of respondents) say they want to be able to keep up with new or emerging attacks. Not as critical is the ability to apply controls that span across the enterprise and the ability to protect their security infrastructure while supporting business innovation (both 28 percent of respondents).

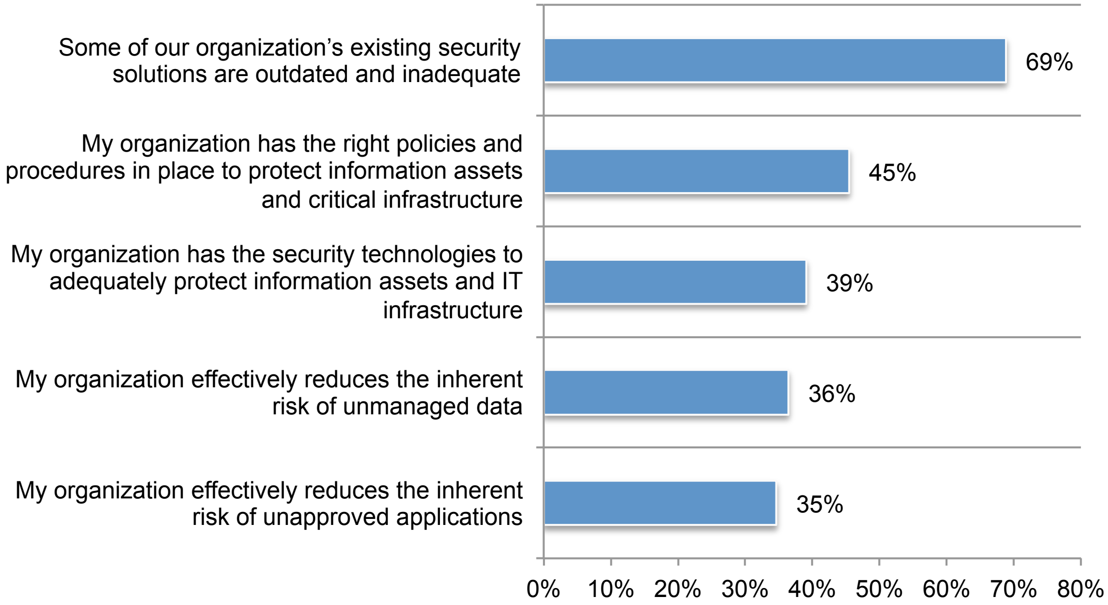
Almost half of the respondents (48 percent) say their current security infrastructure does not facilitate compliance and regulatory enforcement with a centralized approach to controlling, monitoring and reporting of data or they are unsure.

Figure 1. What are the top two goals of a new IT security framework in your organization?
Two choices permitted



Outdated and inadequate security solutions put organizations at risk. As shown in Figure 2, 69 percent of respondents believe some of their organization's existing security solutions are outdated and inadequate. As a result, they give their organization poor marks on reducing the inherent risk of unmanaged data (only 36 percent of respondents agree), reducing the risk of unapproved applications (only 35 percent of respondents), having the security technologies to adequately protect information assets and IT infrastructure (only 39 percent of respondents) and having the right policies and procedures in place to protect information assets and critical infrastructure (only 45 percent of respondents).

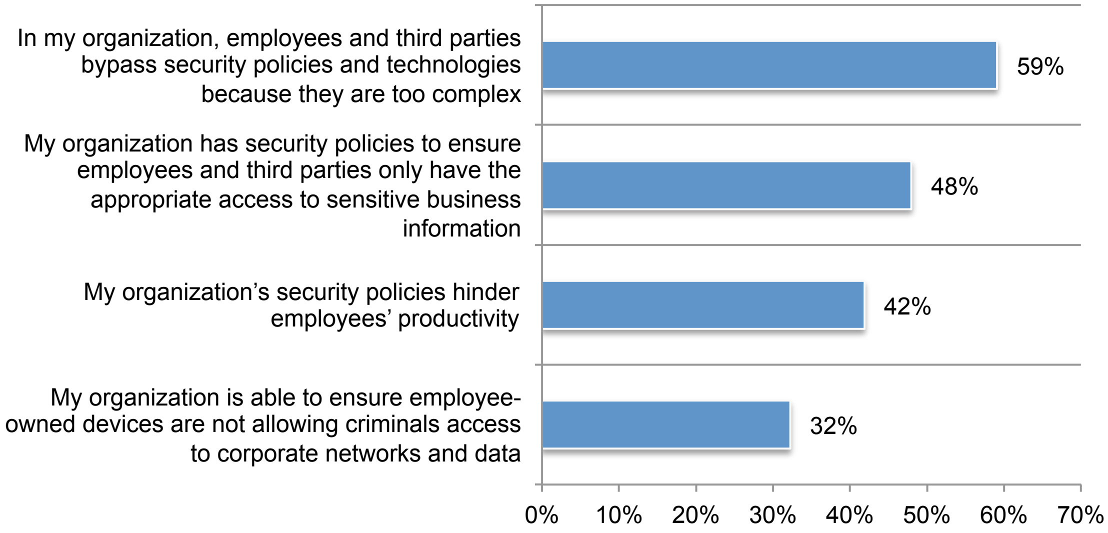
Figure 2. Perceptions about security technologies
Strongly agree and Agree responses combined



Security solutions and policies are not effective in addressing insider risk. As shown in Figure 3, only 32 percent of respondents are confident that employees' devices are not allowing criminals access to their corporate networks and data. Less than half (48 percent of respondents) say their organization has security policies in place to ensure that employees and third parties only have the appropriate access to sensitive business information.

Another area of risk is the perception that employees and third parties bypass security policies and technologies because they are too complex (59 percent of respondents). This is often the case because their organizations' security policies hinder employees' productivity (42 percent of respondents).

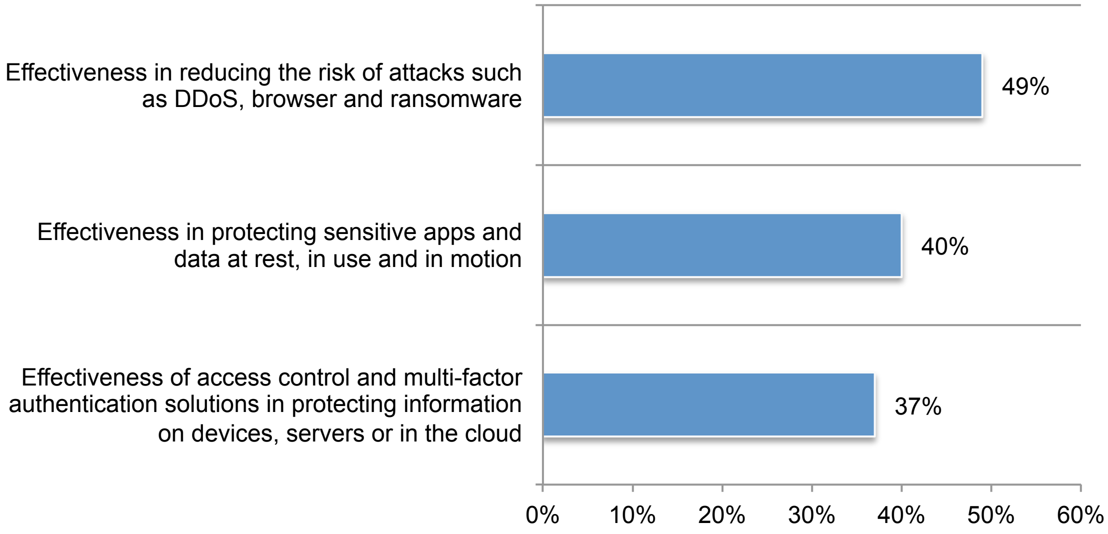
Figure 3. Perceptions about the insider risk
Strongly agree and Agree responses combined



We asked respondents to rate the effectiveness in reducing risk to information assets on a scale from 1 = low effectiveness to 10 = high effectiveness. Figure 4, presents the highly effective responses.

Organizations struggle to reduce risks to information assets. As shown in Figure 4, only 37 percent of respondents say their organization is highly effective in using access control and multi-factor authentication solutions to protect information on devices, servers or in the cloud. Only 40 percent of respondents rate their organizations' effectiveness as high in protecting sensitive apps and data at rest, in use and in motion, and less than half (49 percent of respondents) rate their effectiveness as high in reducing the risk of attacks such as DDoS, browser and ransomware.

Figure 4. Effectiveness in reducing risks to information assets
7+ responses on a scale of 1 = low effectiveness to 10 = high effectiveness



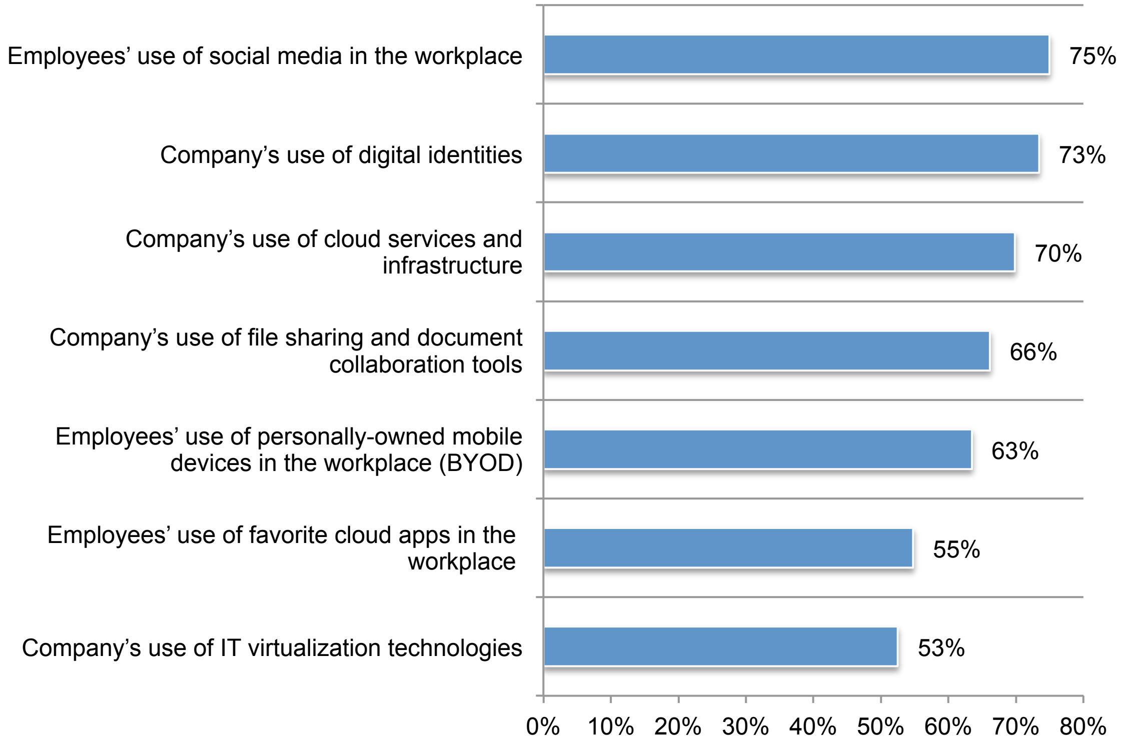
Trends in IT security risks due to disruptive technologies

We asked respondents to rate the potential negative impact of risks due to disruptive technologies on a scale from 1 = no negative impact to 10 = significant negative impact. Shown in the figures below are the most significant risks (7+ responses) rated by participants in this research. The findings reveal that these risks are very significant.

Employees' use of social media is expected to pose the greatest risk. Figure 5 lists seven disruptive technologies that could pose risks to the IT security infrastructure**.** As shown, the most negative impact is expected to be created by employees' use of social media in the workplace (75 percent of respondents). Other employee-related risks include use of personally-owned mobile devices in the workplace (63 percent of respondents) and use of favorite cloud apps in the workplace (55 percent of respondents).

Respondents also expected organizations' increasing use of certain disruptive technologies to have a negative impact. These include the use of digital identities[1] (73 percent of respondents), the use of cloud services and infrastructure (70 percent of respondents), the use of file sharing and document collaboration tools (66 percent of respondents) and the use of virtualization technologies (53 percent of respondents).

Figure 5. Trends in disruptive technology risks
7+ responses on a scale of 1 = no negative impact to 10 = significant negative impact

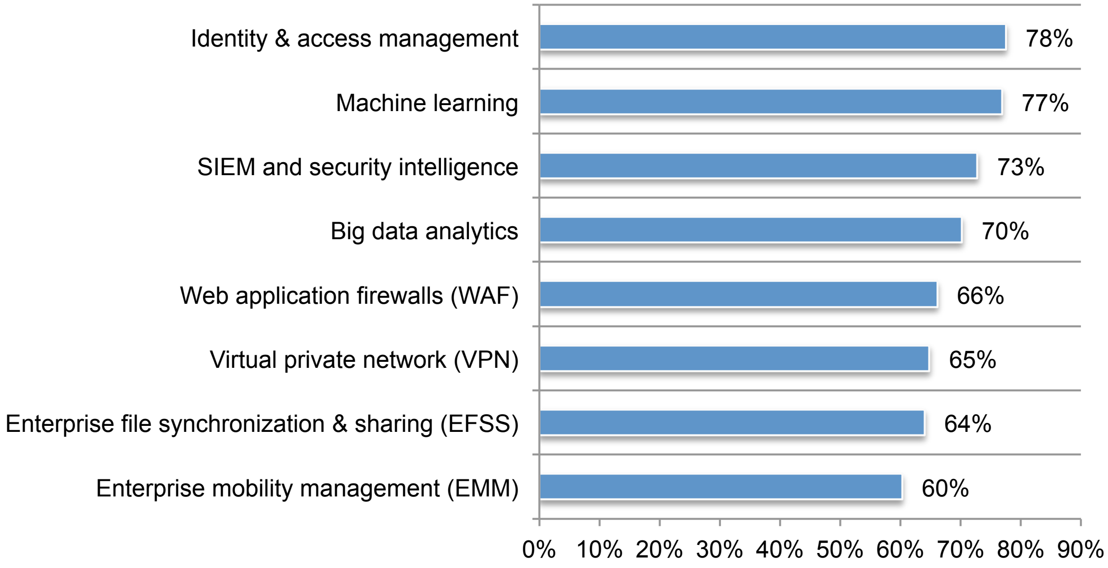


[1] A **digital identity** is information on an entity used by computer systems to represent an external agent. That agent may be a person, organization, application or device. ISO/IEC 24760-1 defines **identity** as a "set of attributes related to an entity". Source: Wikipedia

We also asked respondents to rate the importance of specific technologies in terms of their ability to reduce security risks over the next two years on a scale from 1 = low importance to 10 = high importance. Shown in the figures below are the most important technologies (7+ responses) rated by participants in this research.

Identity and access management (IAM) and machine learning are considered the most important technologies to reduce security risks. What technologies will organizations depend upon most in the next two years? According to Figure 6, 78 percent rate IAM as very important, and 77 percent of respondents rate machine learning as critical. Other important technologies include SIEM and security intelligence (73 percent of respondents), big data analytics (70 percent of respondents), Web application firewalls (WAF) (66 percent of respondents), virtual private network (VPN) (65 percent of respondents), enterprise file synchronization and sharing (EFSS) (64 percent of respondents) and enterprise mobility management (EMM) (60 percent of respondents).

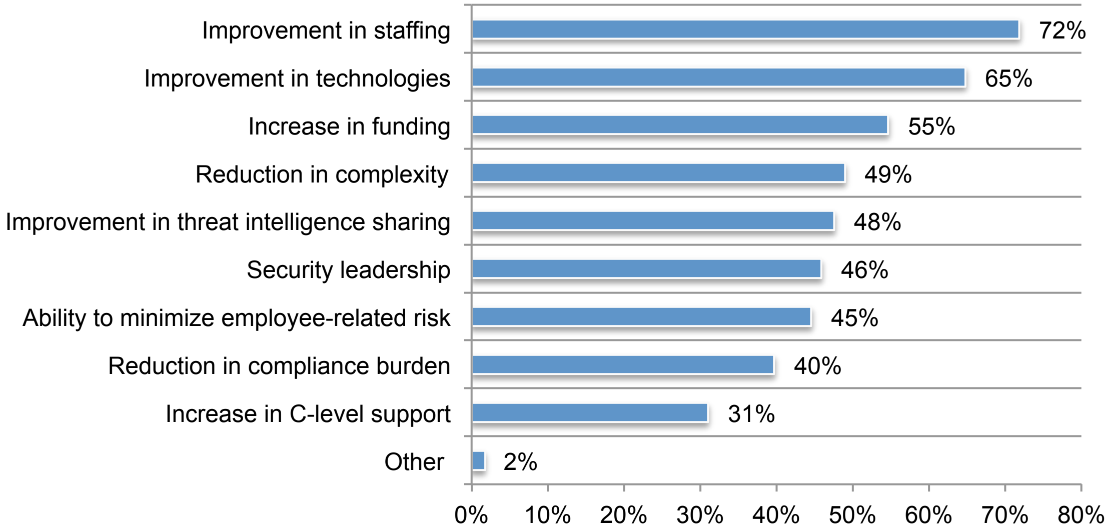
Figure 6. Trends in the most important technologies to reduce security risks
7+ responses on a scale of 1 = low importance to 10 = high importance



Achieving a better IT security infrastructure

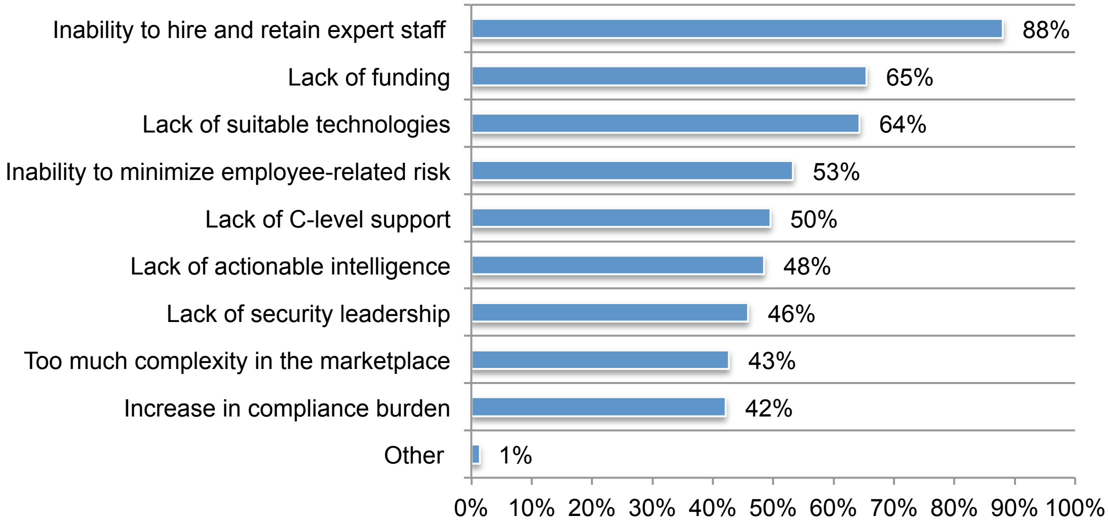
Improvements in staffing and technologies will improve security posture. As shown in Figure 7, the two most important goals are to improve the expertise and quality of staff (72 percent of respondents) and to improve the technologies they invest in (65 percent of respondents). Also important is an increase in funding (55 percent of respondents), reduction in complexity (49 percent of respondents) and improvement in threat intelligence sharing (48 percent of respondents).

Figure 7. Business goals that improve security posture
More than one choice permitted



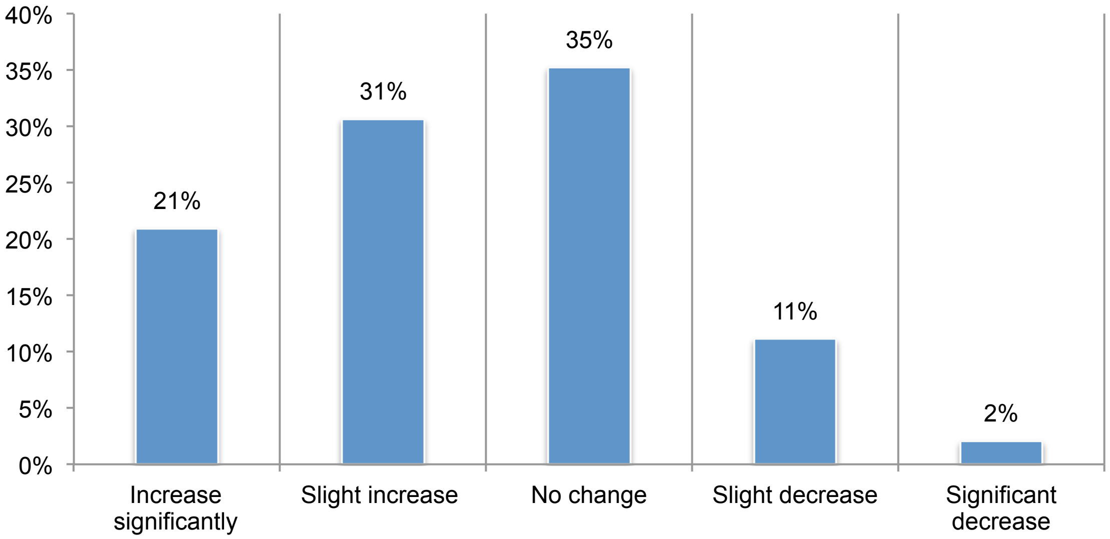
Security posture is affected by the inability to hire and retain staff. As discussed above, organizations can improve their security posture by improving their staffing and technologies. By not achieving these goals, as shown in Figure 8, 88 percent of respondents say the lack of expert staff will decrease the organization's security posture, and 64 percent of respondents say a lack of suitable technologies has a negative effect on security posture. Other factors that have a negative impact on security posture are lack of funding (65 percent of respondents), lack of C-level support (50 percent of respondents) and lack of actionable intelligence (48 percent of respondents).

Figure 8. What decreases overall security posture?
More than one choice permitted



Companies will receive a slight increase in budgets. Lack of funding is considered a barrier to having a strong security posture. On average, the organizations represented in this research will spend about $13 million on IT security in 2017. For most (66 percent of respondents), this represents a slight increase (31 percent) or no change in the IT security budget (35 percent), as shown in Figure 9.

Figure 9. Budgets will increase or stay the same



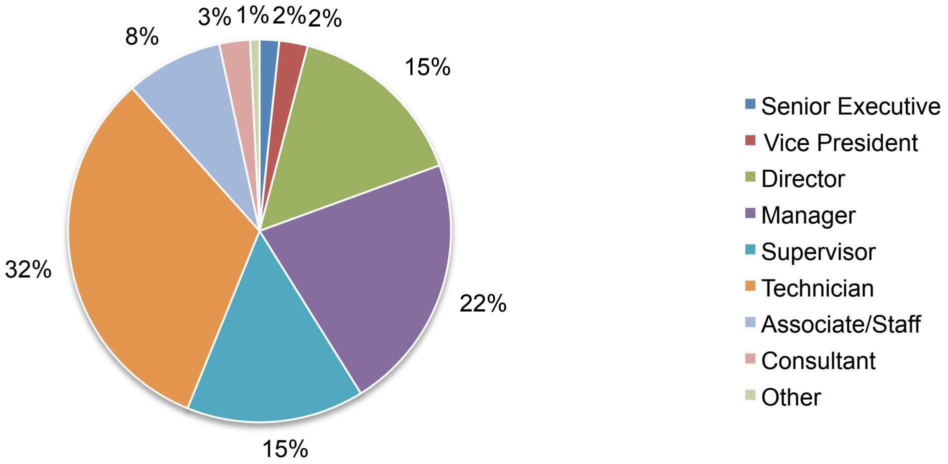
Part 2. Methods

A sampling frame composed of 119,088 IT and IT security practitioners in Australia/New Zealand, Brazil, Canada, China, Germany, France, India, Japan, Korea, Mexico, the Netherlands, the United Arab Emirates, the United Kingdom and the United States were selected for participation in this survey. As shown in Table 1, 4,917 respondents completed the survey. Screening removed 649 respondent surveys. The final sample comprised 4,268 respondent surveys (or a 3.6 percent response rate).

Table 1. Sample response	Freq	Pct%
Total sampling frame	119,088	100.0%
Total returns	4,917	4.1%
Rejected surveys	649	0.5%
Final sample	4,268	3.6%

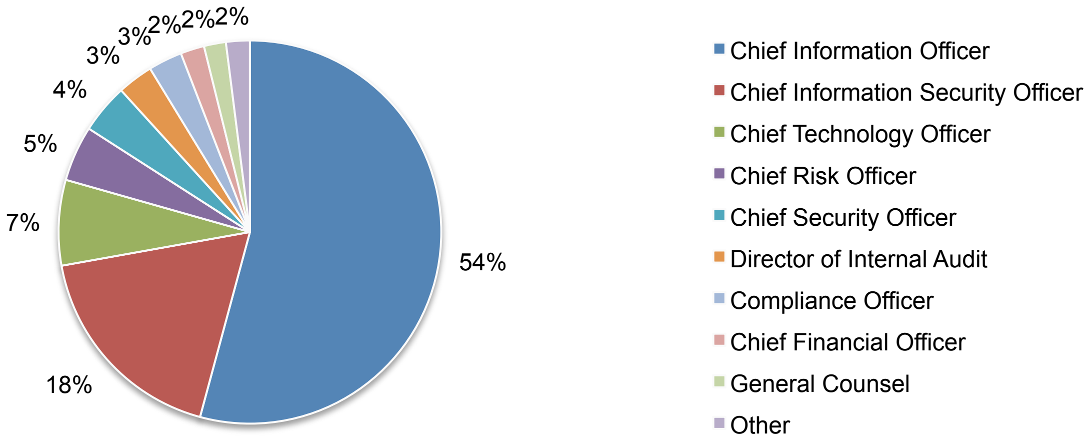
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half of the respondents (56 percent) are at or above the supervisory levels.

Pie Chart 1. Position level within the organization



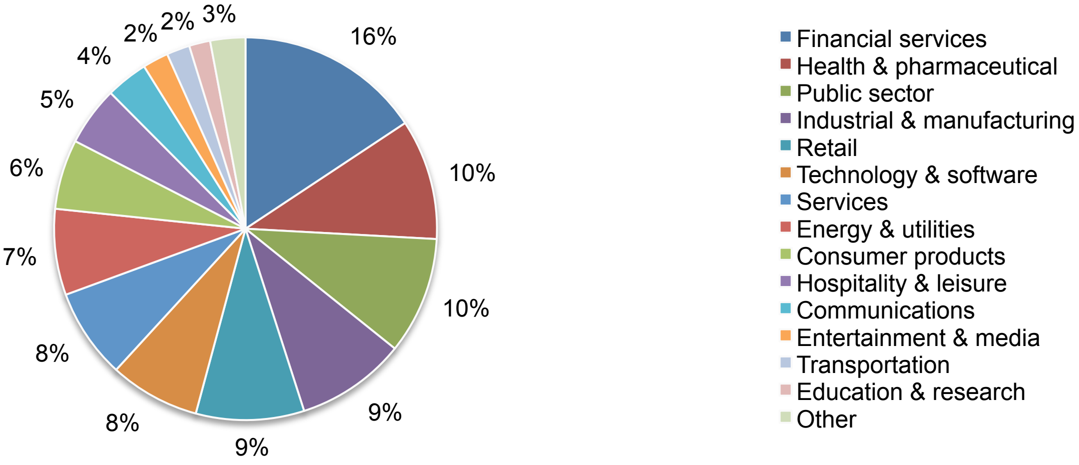
As shown in Pie Chart 2, 54 percent of respondents report directly to the CIO, 18 percent report to the CISO and 7 percent report to the CTO.

Pie Chart 2. The primary person reported to within the organization



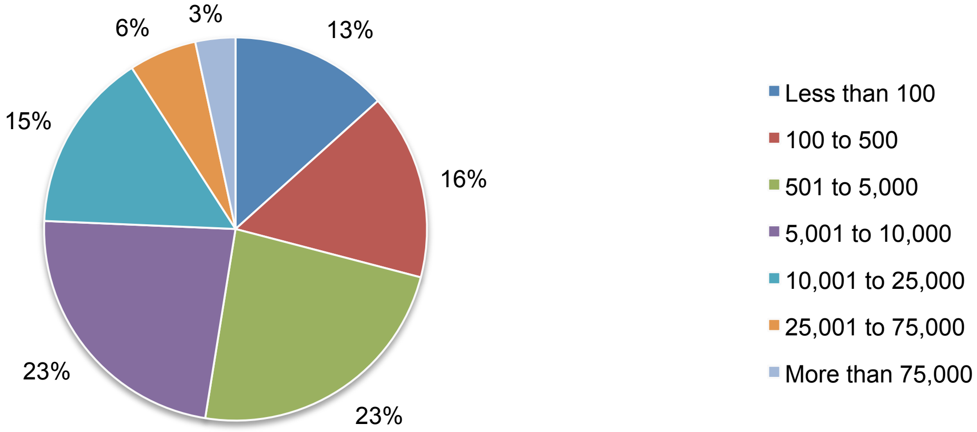
Pie Chart 3 reports the primary industry focus of respondents' organizations. This chart identifies financial services (16 percent of respondents) as the largest segment, followed by health and pharmaceuticals (10 percent of respondents) and public sector (10 percent of respondents).

Pie Chart 3. Primary industry focus



According to Pie Chart 4, 47 percent of the respondents are from organizations with a global headcount of more than 5,000 employees.

Pie Chart 4. Worldwide headcount of the organization



Please write to research@ponemon.org or call 800.877.3118 if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advance responsible information and privacy-management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.