The Need for a New IT Security Architecture: Global Study

Sponsored by Citrix

Independently conducted by Ponemon Institute LLC

Publication Date: January 2017

The Need for a New IT Security Architecture: Global Study

Ponemon Institute, January 2017

Part 1. Introduction

The Need for a New IT Security Architecture: Global Study 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 in order to deal with threats from disruptive technologies, cyber crime and compliance. Changes in the workplace and problems managing IT security are also increasing risks to the organization.

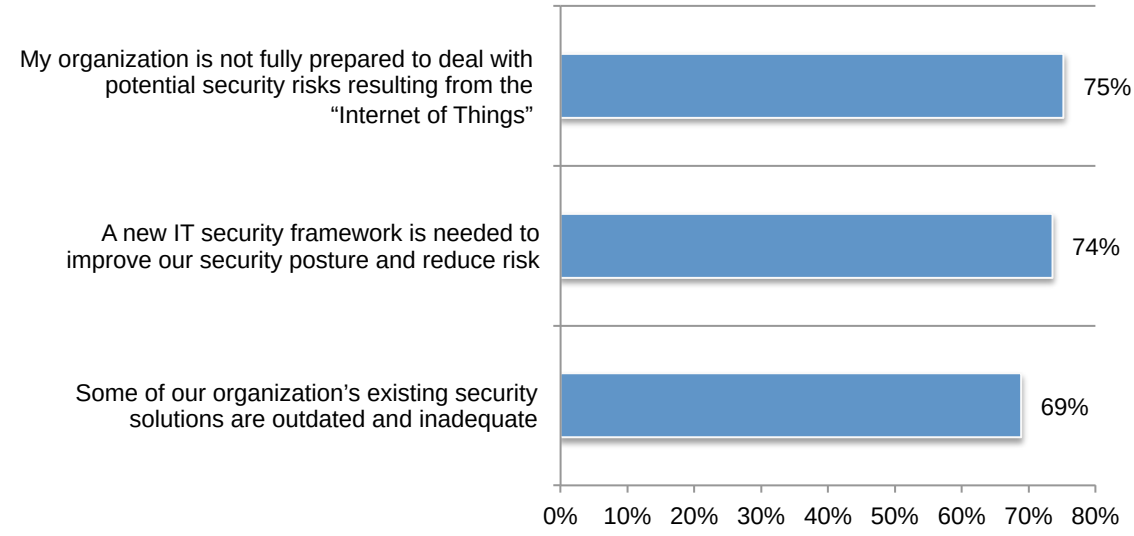
We surveyed 4,268 IT and IT security practitioners in Australia/New Zealand, Brazil, Canada, China, Germany, France, India, Japan, Korea, Mexico, Netherlands, United Arab Emirates, United Kingdom and the United States. The consolidated findings are presented in this report.

This is the first of three reports that present the findings of this global study. In this report, we discuss the findings that concern risks created by cyber crime, employee negligence and organizational dysfunction and the technologies respondents believe are most effective at dealing with these risks.

Organizations are concerned they will not be able to manage emerging risks because of outdated security solutions. As shown in Figure 1, 69 percent of respondents say their organization's existing security solutions are outdated and inadequate. What is needed, according to 74 percent of respondents, is a new IT security framework to improve their security posture and reduce risk. A new strategy is especially important in order to manage such potential risks from the Internet of Things (75 percent of respondents).

Figure 1. Why companies are at risk

Strongly agree and Agree responses combined

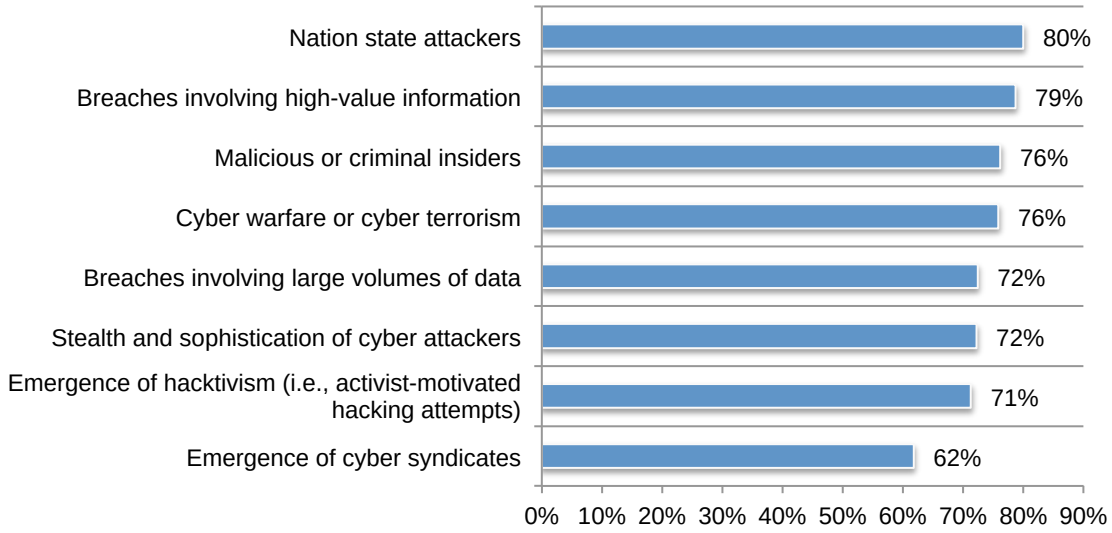


Trends in IT security risk

We asked respondents to rate the potential negative impact of eight cyber crime risks, 10 human factor risks and seven organizational factor risks 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 most risks, with the exception of globalization of the workforce, are very significant.

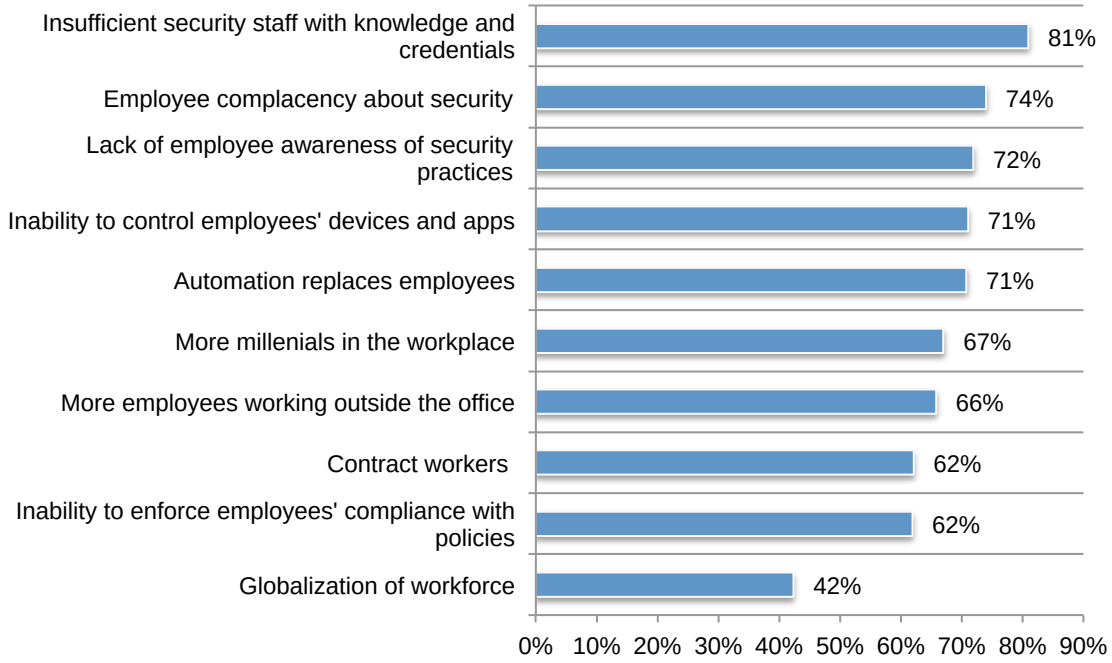
The top cyber crime risks are nation state attackers (80 percent of respondents), breaches involving high-value information such intellectual property and trade secrets (79 percent of respondents), malicious or criminal insiders (76 percent of respondents) and cyber warfare or cyber terrorism (76 percent of respondents).

Figure 2. Trends in cyber crime risk
7+ responses on a scale of 1 = no negative impact to 10 = significant negative impact



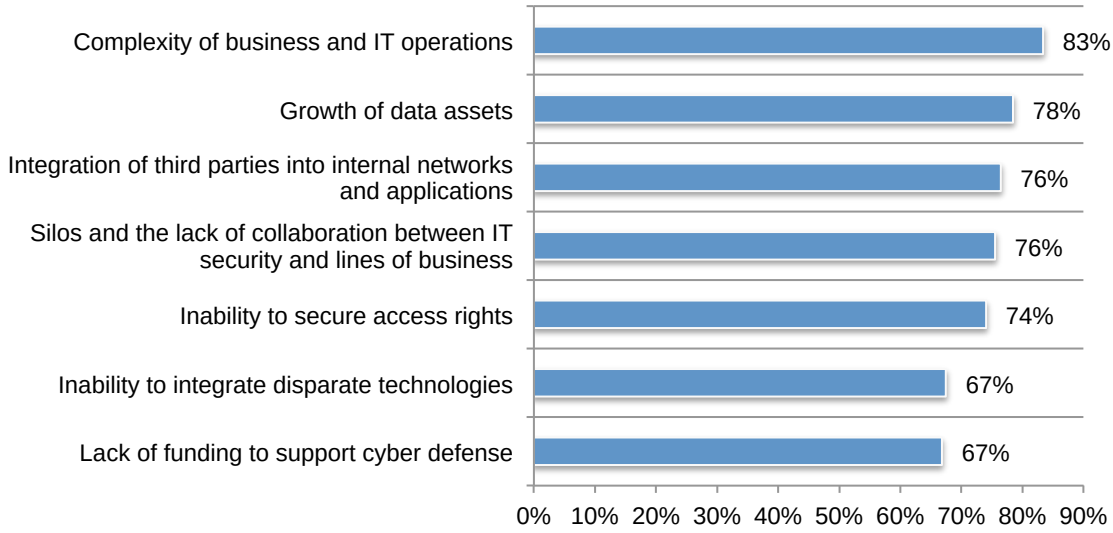
The workplace is changing and so are the human factor risks. While 81 percent of respondents are concerned about the inability to hire and retain security staff with knowledge and credential, employee behaviors are creating risks that pose a significant risk. These are employee complacency about security (74 percent of respondents), lack of employee awareness of security practices (72 percent of respondents) and the inability to control employees' devices and apps (71 percent of respondents).

Figure 3. Trends in the human factor risk
7+ responses on a scale of 1 = no negative impact to 10 = significant negative impact



Complexity of business and IT operations is a significant security risk. According to 83 percent of respondents, too much complexity is making organizations more vulnerable to security threats. Other trends are the growth of data assets (78 percent of respondents) and the process of integrating third parties into internal networks and applications.

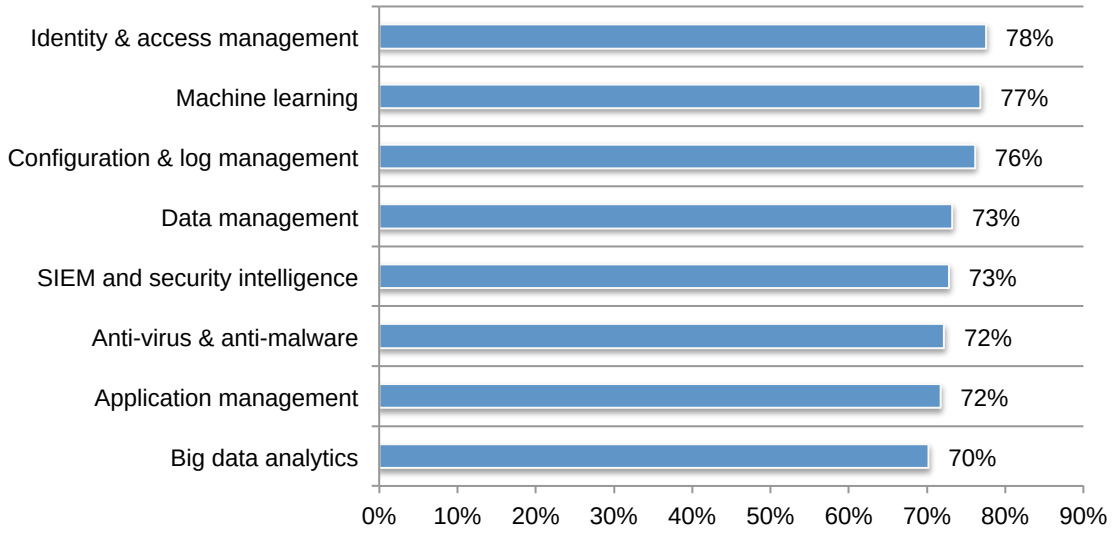
Figure 4. Trends in the organizational factor risk
7+ responses on a scale of 1 = no negative impact to 10 = significant negative impact



Certain technologies are needed for a new IT security infrastructure. As discussed above, respondents believe their organizations' IT security solutions are outdated and failing to mitigate the risks of cyber crime, employee behavior and organizational problems. We asked respondents to rate the importance of technologies on a scale from 1 = low importance to 10 = high importance. Shown in Figure 5 are the 7+ responses.

The most important technologies are identity & access management (78 percent of respondents), machine learning (77 percent of respondents) and configuration & log management (76 percent of respondents).

Figure 5. The most important technologies for a new IT security infrastructure
1 = low importance to 10 = high importance, 7 + responses reported



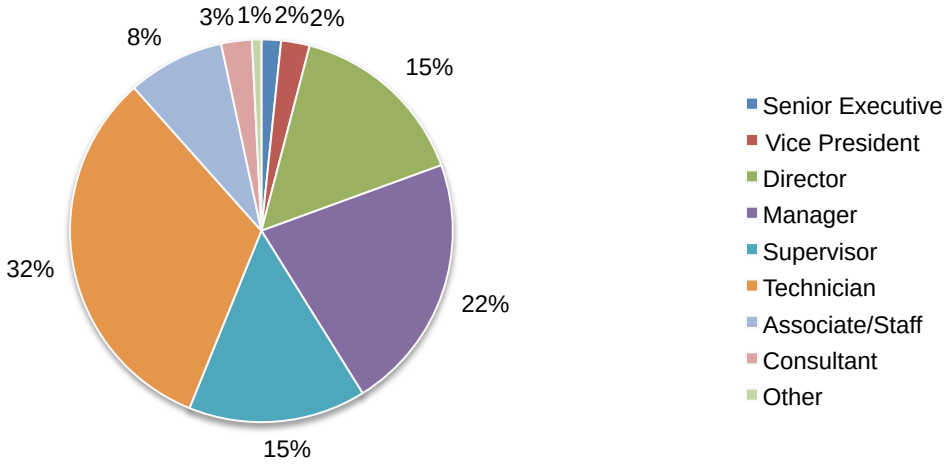
Part 2. Methods

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, Netherlands, United Arab Emirates, 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 was 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%

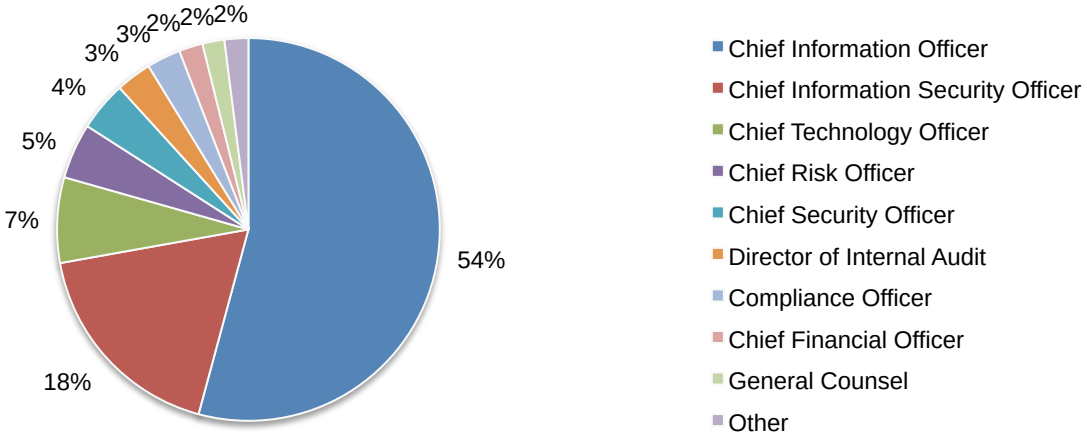
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half of the respondents (56 percent) are at or above the supervisory levels.

Pie Chart 1. Position level within the organization



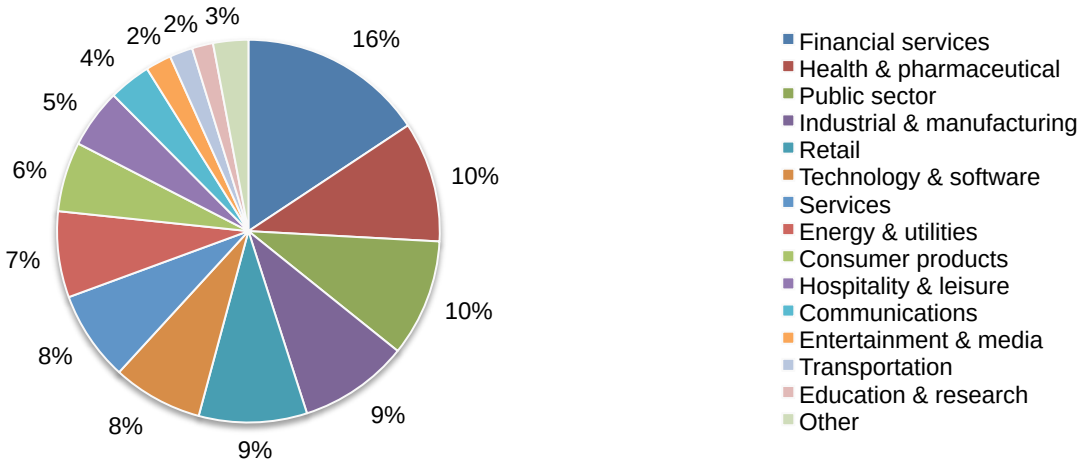
As shown in Pie Chart 2, 54 percent of respondents report directly to the CIO, 18 percent report to the CISO and 7 percent report to the CTO.

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



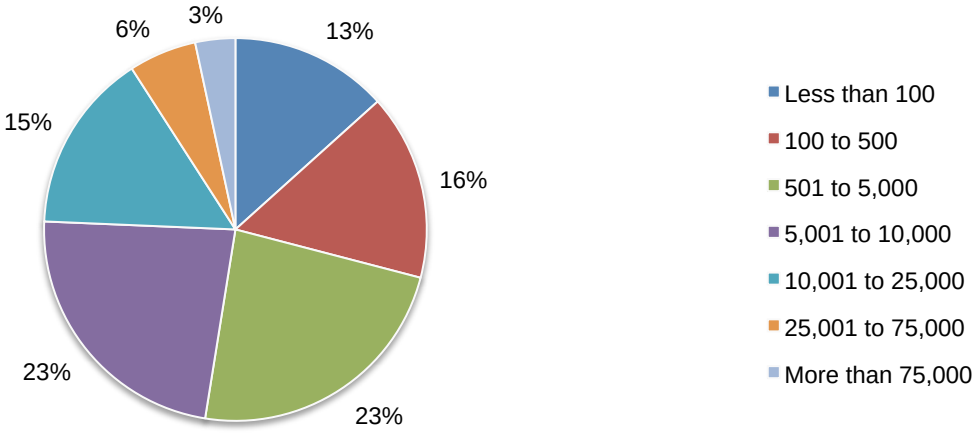
Pie Chart 3 reports the primary industry focus of respondents' organizations. This chart identifies financial services (16 percent of respondents) as the largest segment, followed by health and pharmaceuticals (10 percent of respondents) and public sector (10 percent of respondents).

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.