The Need for a New IT Security Architecture:
Global Study on Compliance Challenges & Security Effectiveness in the Workplace

Sponsored by Citrix

Independently conducted by Ponemon Institute LLC

Publication Date: March 2017

The Need for a New IT Security Architecture: Global Study on Compliance Challenges & Security Effectiveness in the Workplace

Ponemon Institute, March 2017

Part 1. Introduction

The Need for a New IT Security Architecture: Global Study, which was 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 posing increased risk to the organization.

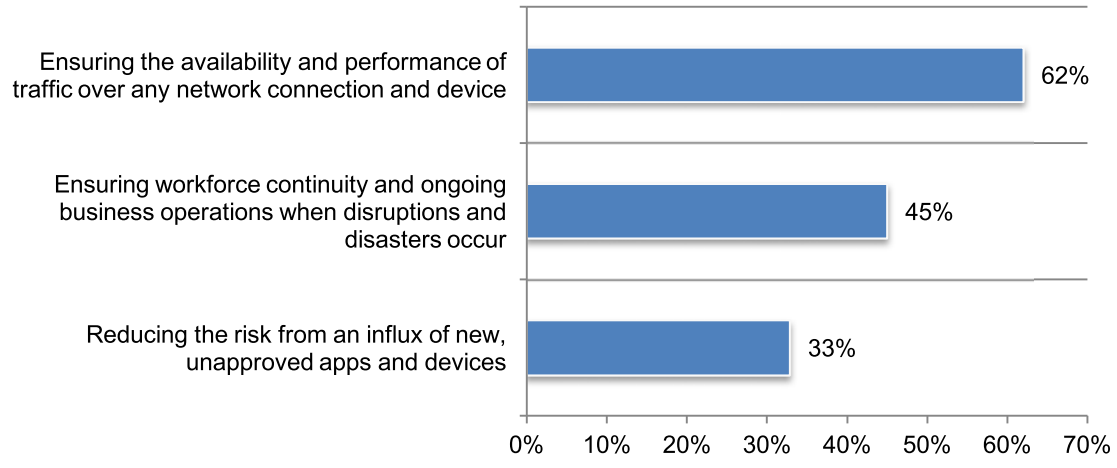
We surveyed 4,268 IT and IT security practitioners in Australia/New Zealand, Brazil, Canada, China, Germany, France, India, Japan, Korea, Mexico, the Netherlands, the United Arab Emirates, the United Kingdom and the United States. The consolidated findings are presented in this report.

This is the third of three reports that present the findings of this global study. In this report, we discuss the findings that concern risks created by compliance with regulations, especially compliance with the EU's General Data Protection Regulations (GDPR). According to the research, 74 percent of respondents say that complying with the GDPR will have a significant and negative impact on their organizations, such as large potential fines and the increased territorial reach of the regulations. The study also addresses the influx of unapproved applications and devices as well as organizational dysfunction created by differences among generations in the workplace.

Trends in security effectiveness in the workplace

Organizations admit challenges in reducing the risk from unapproved apps and devices. As shown in Figure 1, only one-third of respondents rate their effectiveness as high (7+ responses) in reducing the risk from an influx of new, unapproved apps and devices. Respondents say their organizations are more effective in ensuring workforce continuity and ongoing business operations when disruptions and disasters occur (45 percent of respondents) and ensuring the availability and performance of traffic over any network connection and device (62 percent).

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



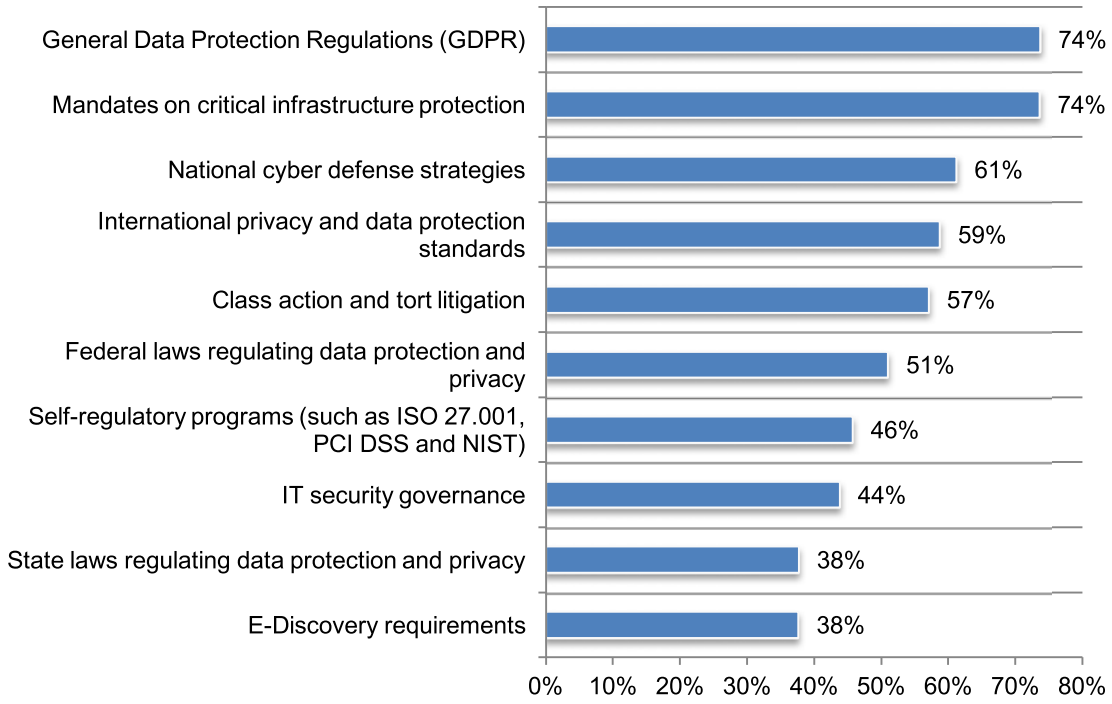
Trends in compliance risk

A new IT security framework is needed to address the challenges of international regulations. Less than half of the organizations represented in this research (48 percent of respondents) believe their security infrastructure facilitates compliance and regulatory enforcement with a centralized approach to controlling, monitoring and reporting data. As a result, respondents are concerned about how their organizations will address the risks associated with the introduction of new international privacy and security regulations and cybersecurity mandates.

In this study, we asked respondents to rate the potential negative impact of 10 trends in compliance 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.

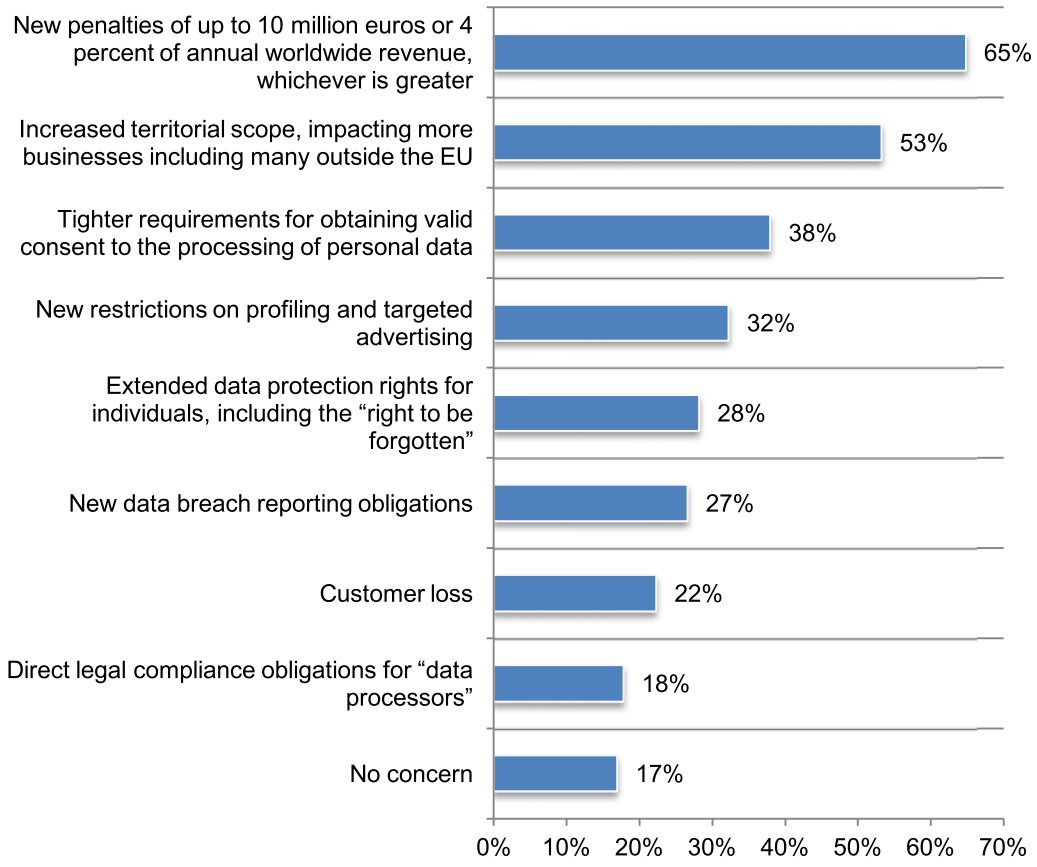
As shown in Figure 2, the findings reveal that respondents are most concerned about complying with the EU's General Data Protection Regulations (GDPR), mandates on critical infrastructure protection, national cyber defense strategies and international privacy and data protection standards. Respondents are also concerned about class action and tort litigation and the potential negative impact they will have on their organizations.

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



Organizations worry about potential fines if they are not in compliance with GDPR. While 67 percent of respondents are aware of GDPR, only about half of organizations represented in this research have allocated budgets and started to prepare for these new regulations. Figure 3 reveals the concerns of those respondents who are aware of the GDPR. The biggest concern is the potential fine of up to 10 million euros or 4 percent of annual worldwide revenues, whichever is greater. Another major worry is that their businesses outside the EU will also be impacted by the regulations. Only 17 percent of respondents have no concern.

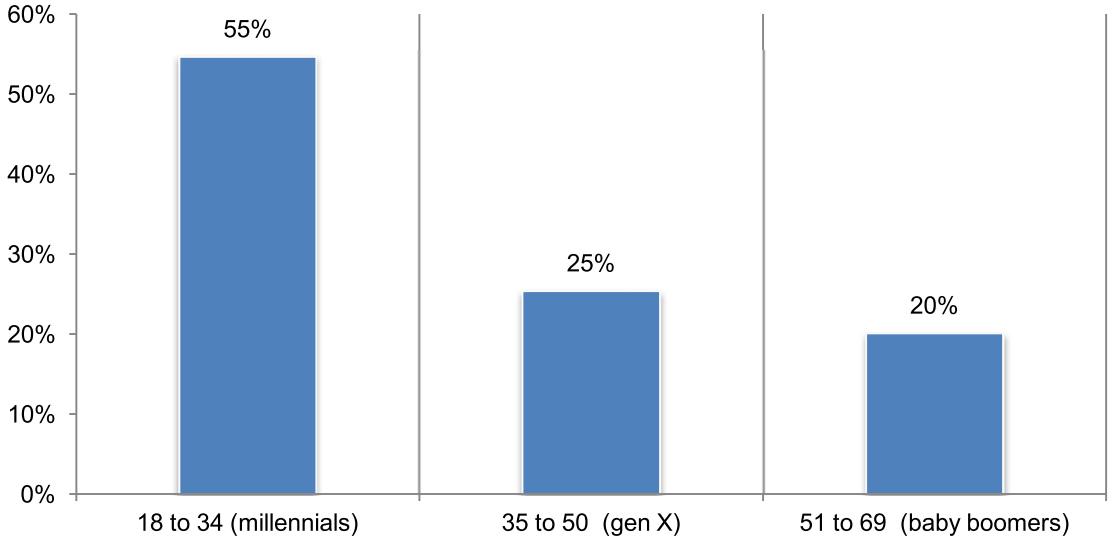
Figure 3. Concerns about compliance with GDPR
Three choices permitted



The risk of generational differences in the workplace

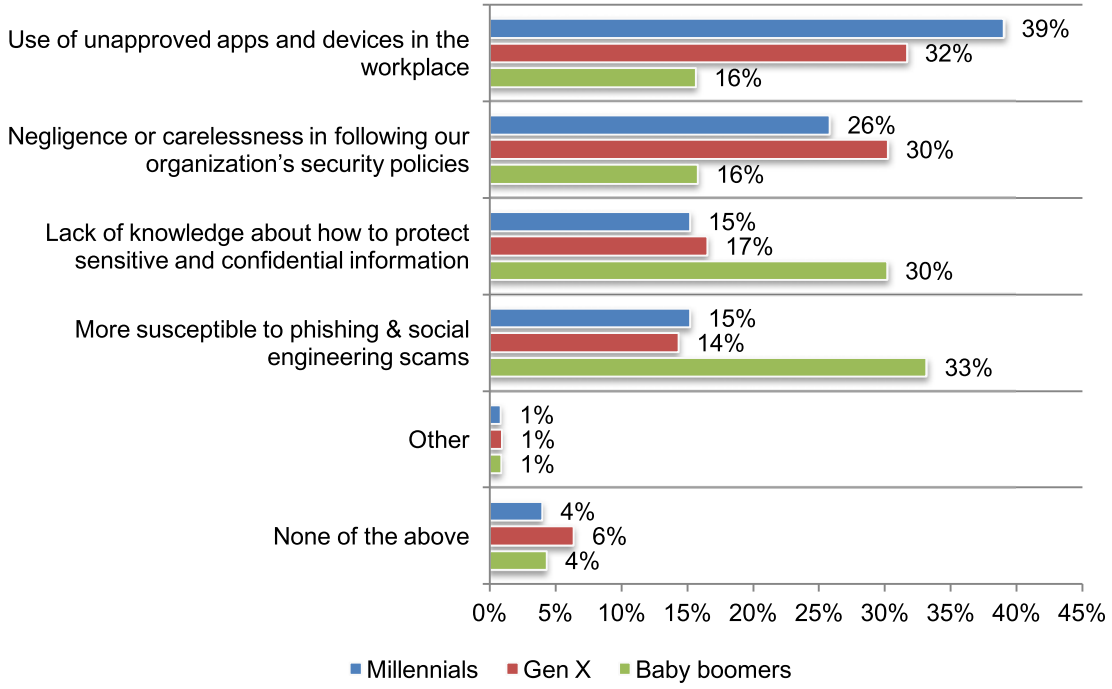
Millennials pose the greatest risk to sensitive information. According to Figure 4, millennials (age 18 to 34) pose the greatest risk followed by gen X (age 35 to 50). Baby boomers (age 51 to 69) pose the least amount of risk.

Figure 4. Which age group poses the greatest risk to sensitive and confidential data in the workplace?



Millennials and gen X are most likely to use unapproved apps and devices in the workplace. Figure 5 shows the greatest risks created by individuals from all three generations. The most interesting differences among the generations is the likelihood that millennials and gen X are the most likely to circumvent security policies and use unapproved apps and devices (39 percent and 32 percent of respondents, respectively). In contrast, baby boomers are more susceptible to phishing and social engineering scams (33 percent of respondents), or they tend not to know how to protect sensitive and confidential information (30 percent of respondents).

Figure 5. What are the greatest risks posed by millennials, gen X and baby boomers?



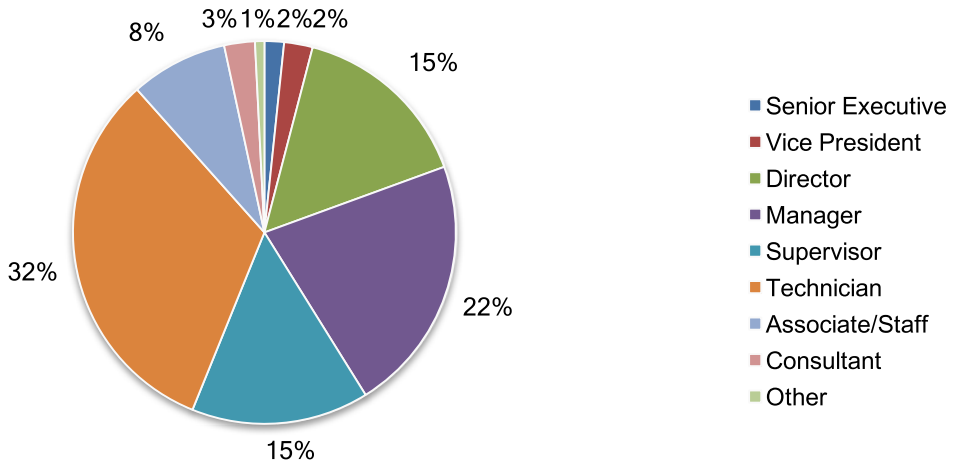
Part 2. Methods

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 respondents' 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%

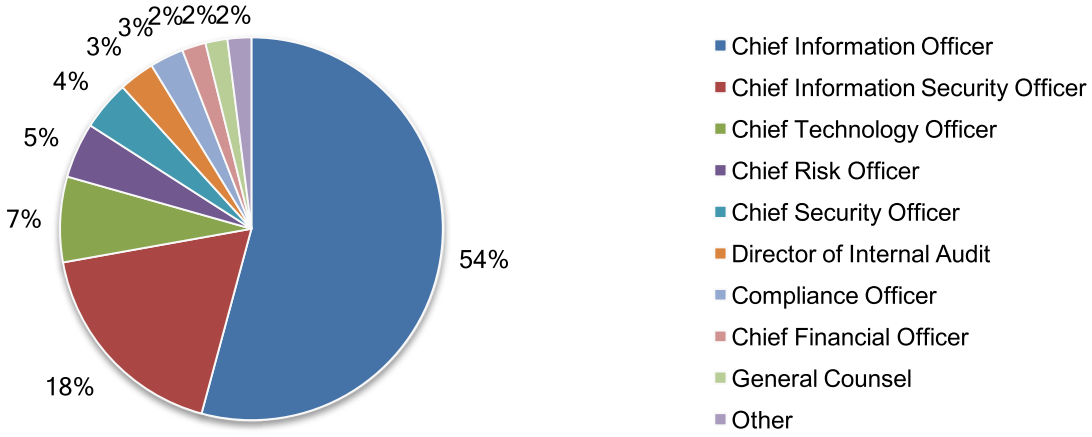
Pie Chart 1 reports the respondents' position levels within participating organizations. By design, more than half of the respondents (56 percent) are at or above the supervisory level.

Pie Chart 1. Position level within the organization



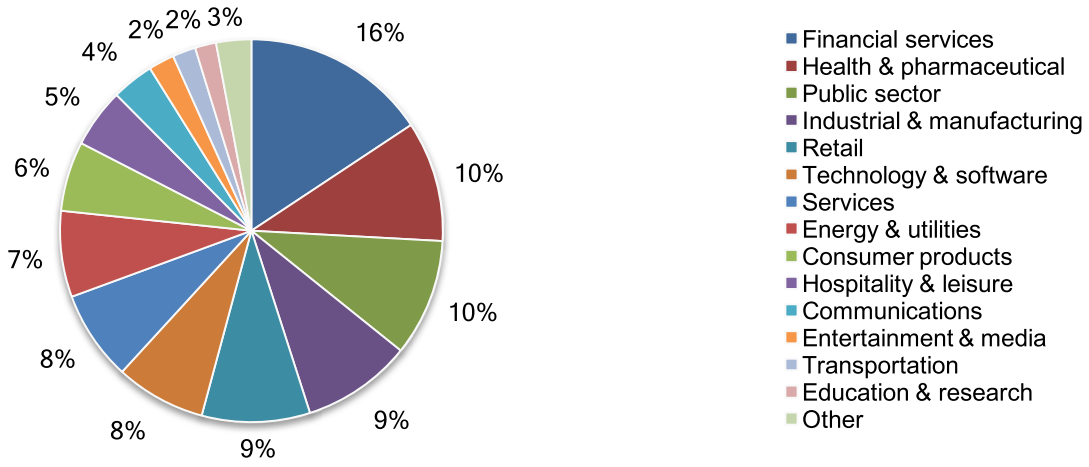
As shown in Pie Chart 2, 54 percent of respondents report directly to the CIO, 18 percent report to the CISO and 7 percent report to the CTO.

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



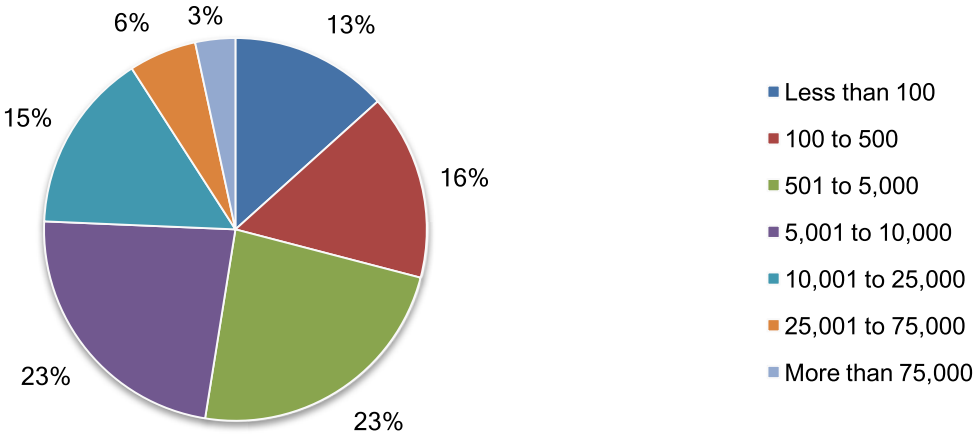
Pie Chart 3 reports the primary industry focus of respondents' organizations. This chart identifies financial services (16 percent of respondents) as the largest segment, followed by health and pharmaceuticals (10 percent of respondents) and the public sector (10 percent of respondents).

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.