Global Insights on Document Security

Sponsored by Adobe

Independently conducted by Ponemon Institute LLC

Publication Date: June 2014

Global Insights on Document Security

Ponemon Institute, June 2014

Part 1. Introduction

Ponemon Institute is pleased to present the results of *Global Insights on Document Security*, sponsored by Adobe. The purpose of this research is to understand the challenges companies face in their document or file level security practices as a result of the adoption of such disruptive technologies as mobile devices and cloud services. To deal with a new world of mobile computing, 72 percent of respondents believe that document security can help protect the confidentiality, integrity, authenticity, access, availability and utility of information as one layered defense.

We surveyed 2,300 IT and IT security practitioners in the following countries: United States, United Kingdom, Canada, Germany, France, Singapore, Australia and Japan in 18 different industry sectors. The majority of participants are at the supervisor level or higher in their organizations.

All participants in this research are familiar with their company's document security strategy. While there are some differences among the countries, respondents are consistent in their perceptions about the risks and the importance of certain practices and processes to the protection of sensitive and confidential information.

Key takeaways from this research include the following:

BYOD creates a risk to the security of documents. The ability to minimize the risk created by mobile devices is decreased as more personally owned mobile devices are introduced into the workplace. The majority of respondents (58 percent) agree that (BYOD) in the workplace makes it difficult to place invasive controls on these devices.

Companies focus on protecting information, not the IT stack. Sixty-seven percent of respondents are in agreement that the protection of information is more critical than the IT stack.

Document security is a critical component of a layered defense. Seventy-two percent of respondents agree that document security is valuable in protecting the confidentiality, integrity, authenticity, access, availability and utility of information as one layered defense.

Restrictive and preventative controls on mobile devices are not effective. Sixty percent believe this is the case primarily because of the new types of mobile devices and cloud services. According to 40 percent of respondents they also impact these controls have on employee productivity.

Document security technologies are most important to the protection of information. Considered not as important are the enforcement of document security policies and the safe destruction of documents.

Security strategies are incorporating individual accountability as a measure to manage risk. Sixty-six percent of organizations are using a people-centric approach to safeguarding documents.

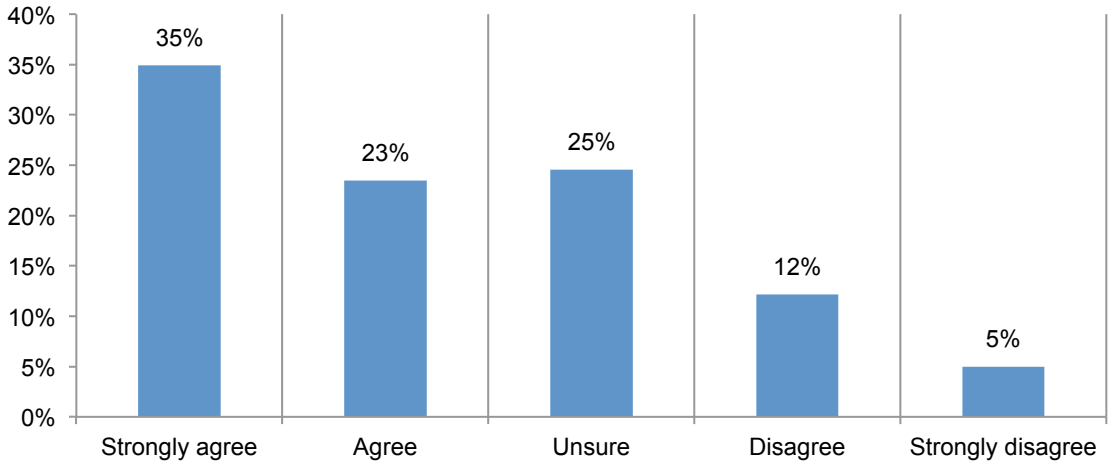
The proliferation in the use of cloud services has decreased IT's role and influence with respect to strategy and technology investments. Fifty-seven percent of respondents believe it is the lines of business, not IT that is determining the strategy and investments in technology.

Part 2. Key findings

In this section, we provide an analysis of the consolidated findings of this research.

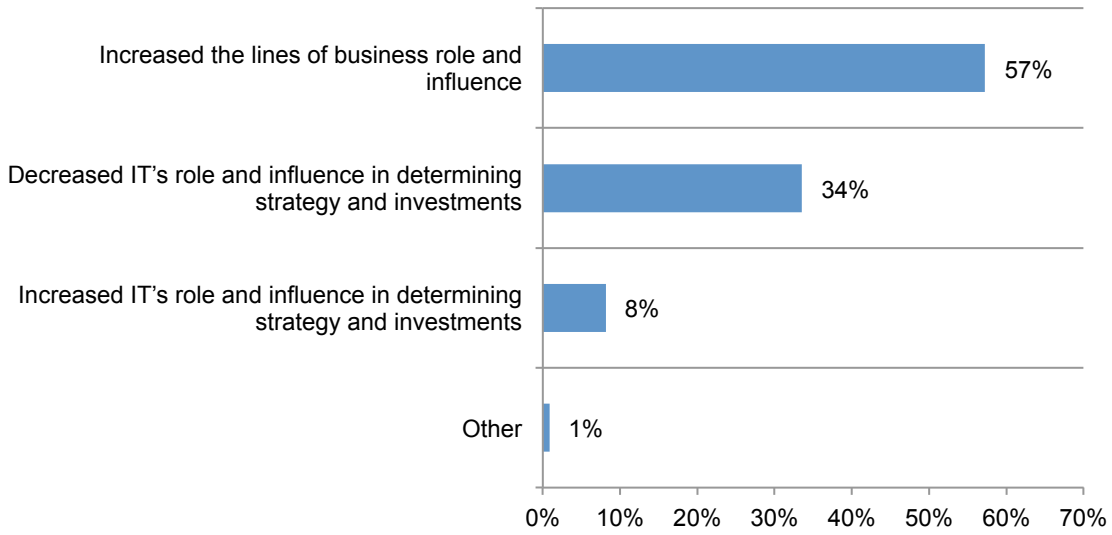
BYOD creates a risk to the security of documents. The ability to minimize the risk created by mobile devices is decreased as more personally owned mobile devices are introduced into the workplace. As shown in Figure 1, unlike with the use of company provided mobile devices, 58 percent of respondents (35 percent + 23 percent) agree that (BYOD) in the workplace makes it difficult to place invasive controls on these devices.

Figure 1. BYOD makes it difficult to place invasive controls on these devices



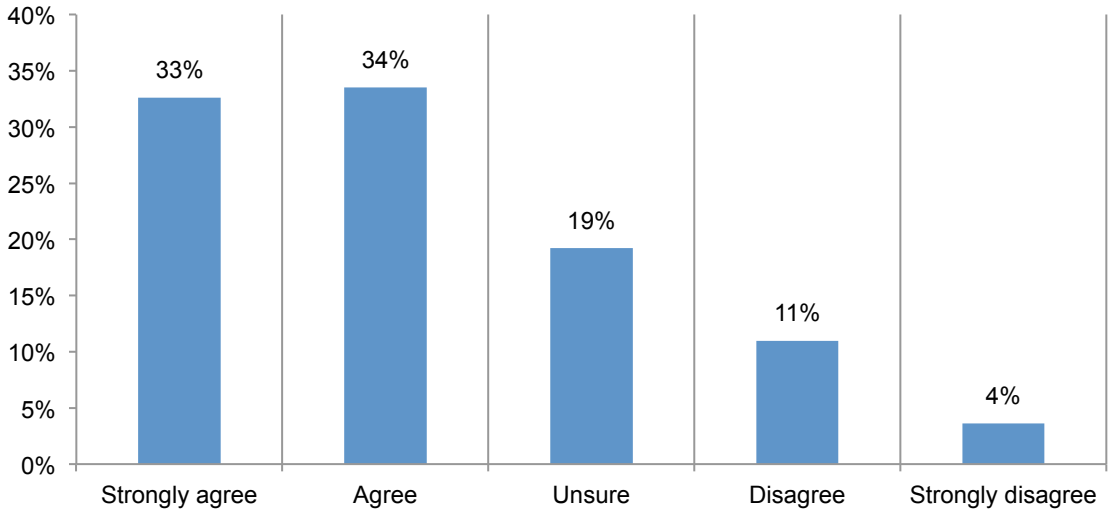
Growth in cloud services has decreased IT's role and influence. Figure 2 shows that 57 percent believe it is the lines of business, not IT that is determining the strategy and investments in technology. Thirty-four percent of respondents believe that the cloud has decreased the IT's function influence in this area. However, IT's expertise is important in ensuring the appropriate security technologies and procedures are in place. What would be ideal is to have a partnership between IT security and the business units to achieve a strong document security posture.

Figure 2. How the increased use of cloud services affected the IT function's influence



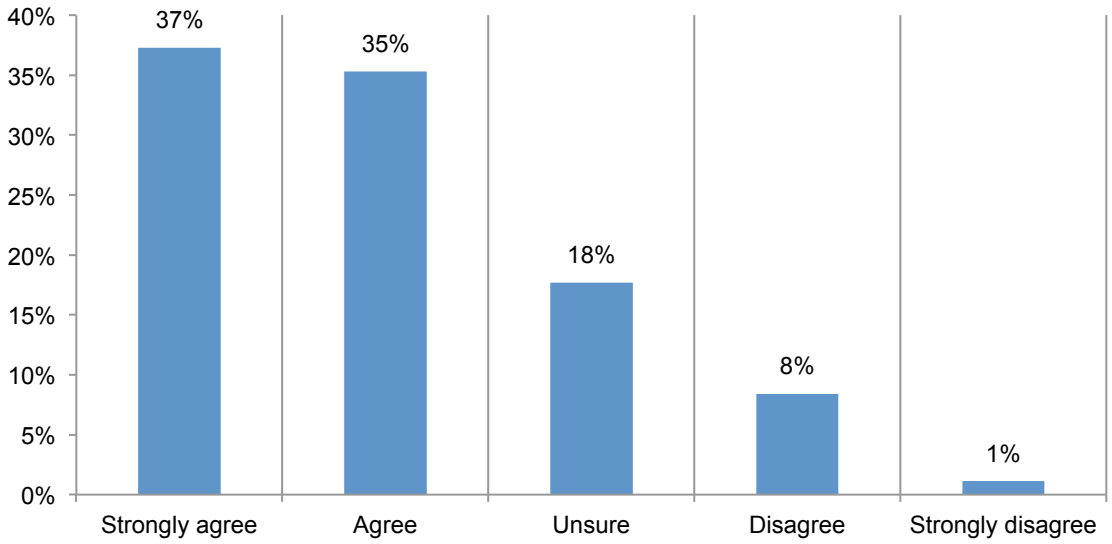
Companies focus on protecting information, not the IT stack. Sixty-seven percent of respondents (33 percent + 34 percent) are in agreement that the protection of information is more critical than the IT stack. This finding indicates that organizations are recognizing the value of their information assets (Figure 2).

Figure 3. Does your organization's security strategy focus on protecting information rather than securing the IT stack



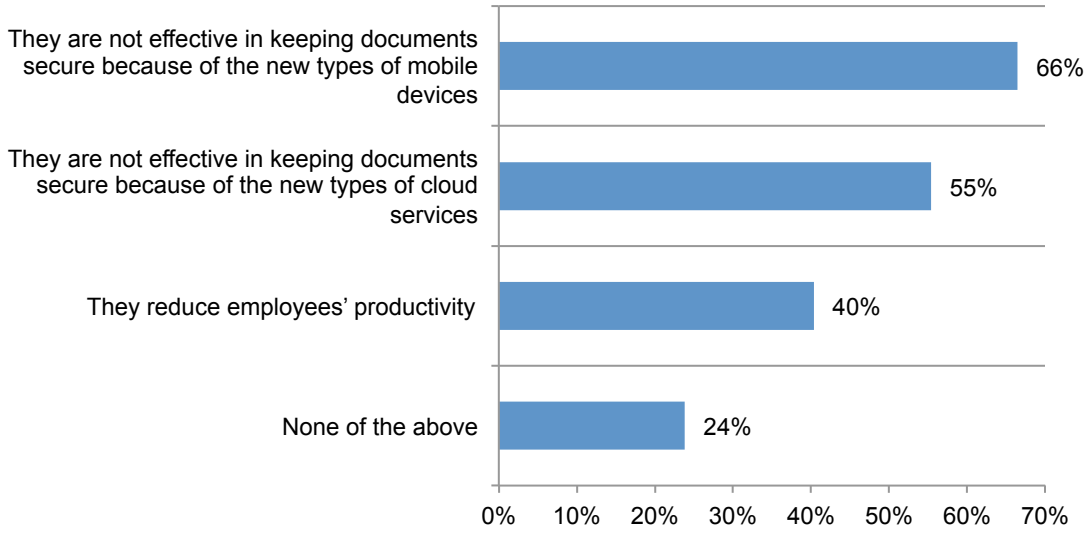
Document security is a critical component of a layered defense. Once again, this research reveals a consensus of opinion among the various countries. According to Figure 3, 72 percent of respondents (37 percent + 35 percent) agree that document security is valuable in protecting the confidentiality, integrity, authenticity, access, availability and utility of information as one layered defense.

Figure 4. Document security can help to protect the confidentiality, integrity, authenticity, access, availability and utility of information as one layered defense



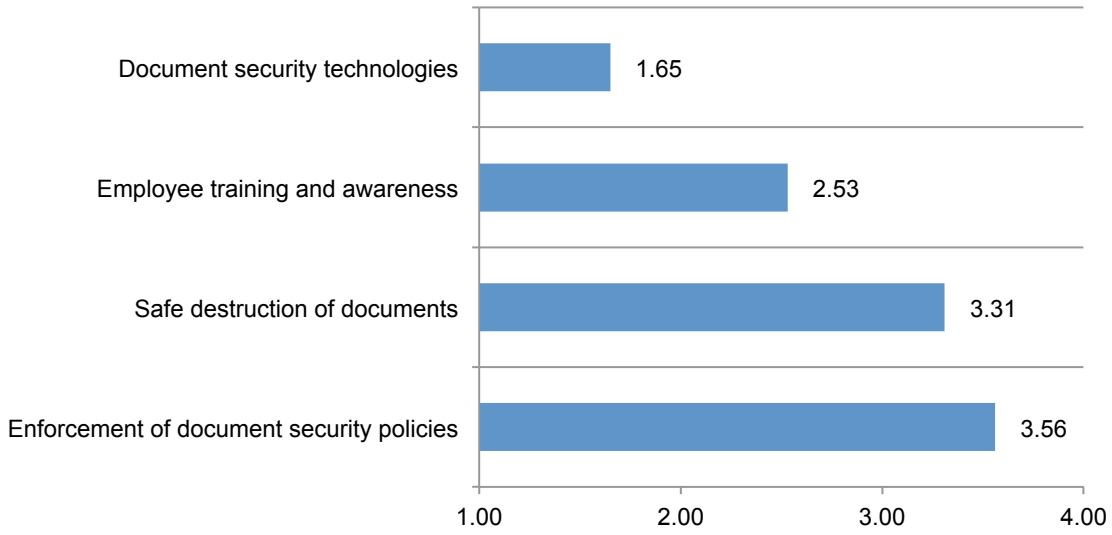
Restrictive and preventative controls on mobile devices are not effective. Sixty percent believe this is the case. As shown in Figure 4, those respondents who believe it is not effective say it is primarily because of the new types of mobile devices and cloud services (66 percent and 55 percent of respondents, respectively). Another concern, according to 40 percent of respondents is the impact these controls have on employee productivity.

Figure 5. Reasons restrictive, preventative security controls are not effective
More than one response permitted



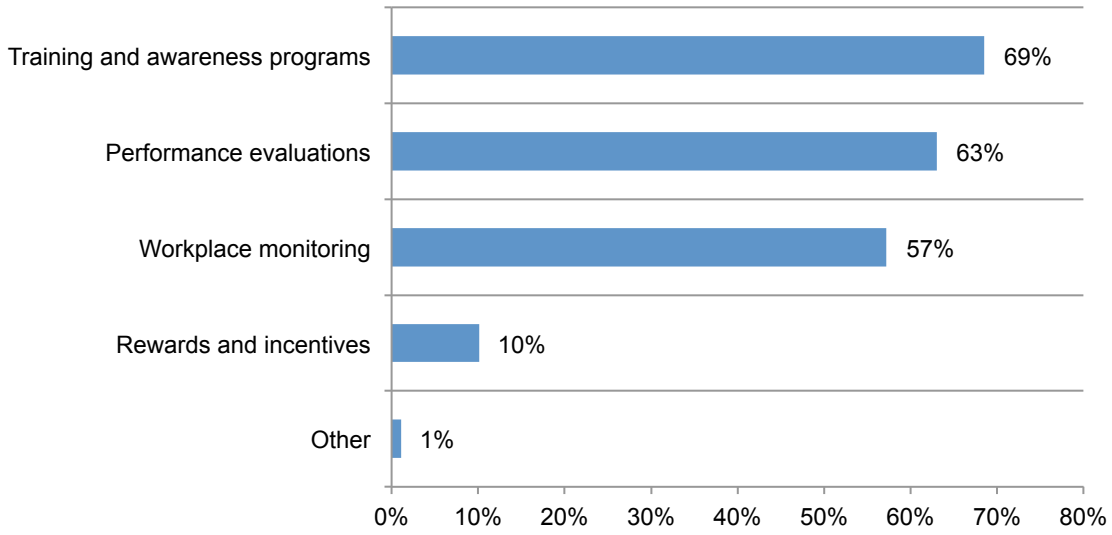
Document security technologies are most important to the protection of information. Figure 5 also reveals that employee training and awareness is critical to the protection of documents. Considered not as important are the enforcement of document security policies and the safe destruction of documents.

Figure 6. The most important steps to ensuring document security
1 = most important to 4 = least important



Security strategies are incorporating individual accountability as a measure to manage risk. Sixty-six percent of organizations are using a people-centric approach to safeguarding documents. According to Figure 6, this is mostly accomplished through training and awareness programs. This is consistent with the previous finding that training and awareness is in the top two of what companies believe is important to document security.

Figure 7. How does the security strategy incorporate individual accountability or a people-centric approach to managing risk?
Two choices permitted



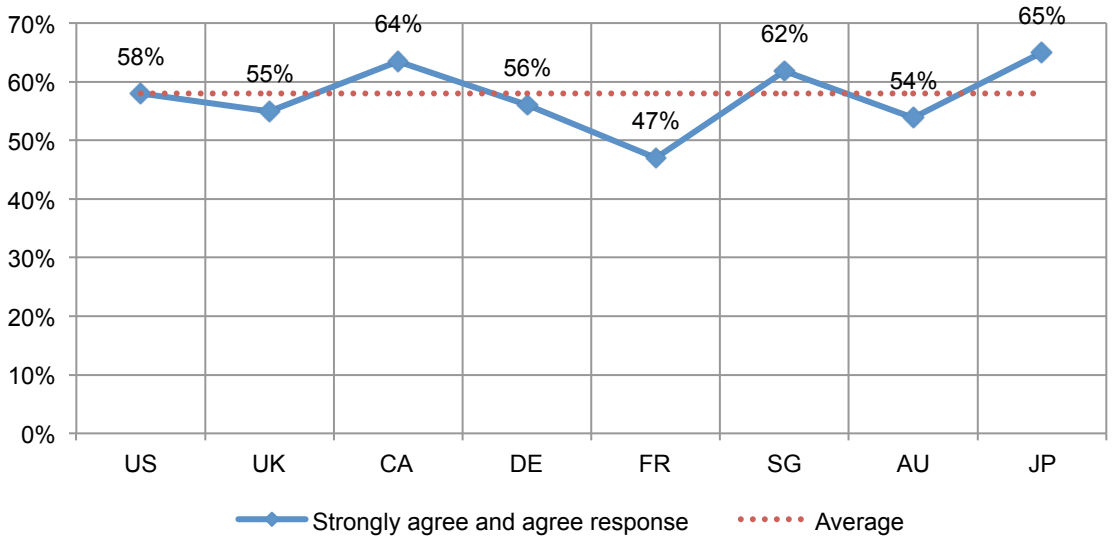
Part 3. Country Differences

In this section, we present the most interesting differences among the countries represented in this research.

BYOD creates a risk to the security of documents. Figure 8 reveals that respondents in Canada, Singapore and Japan have the highest level of agreement that the ability to minimize the risk created by mobile devices is decreased as more personally owned mobile devices are introduced into the workplace. Lowest level of perception about the ability to place invasive controls is held by respondents in France.

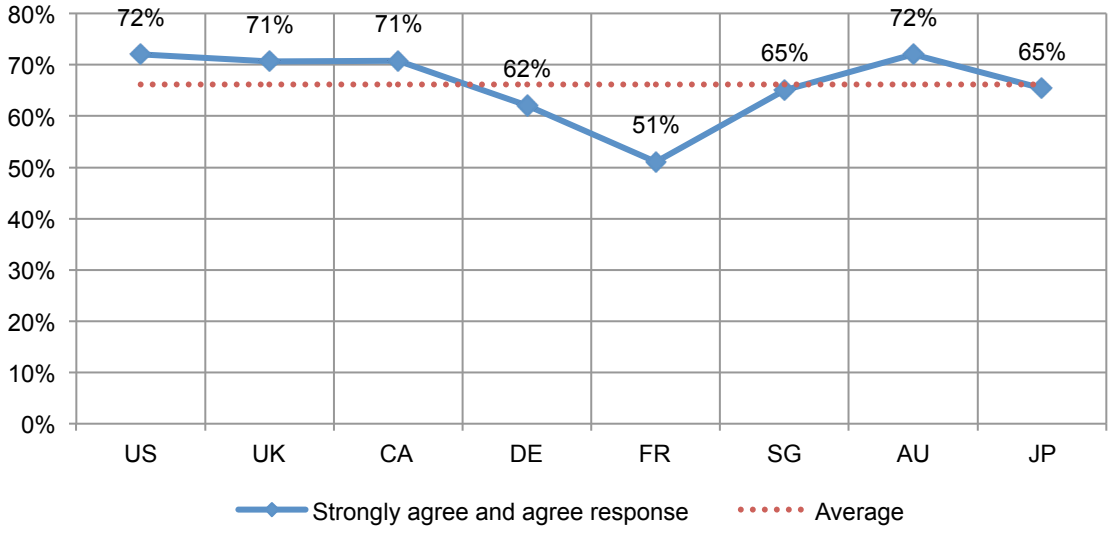
Figure 8. The use of personally owned mobile devices makes it difficult to place invasive controls on these devices

Strongly agree and agree response combined



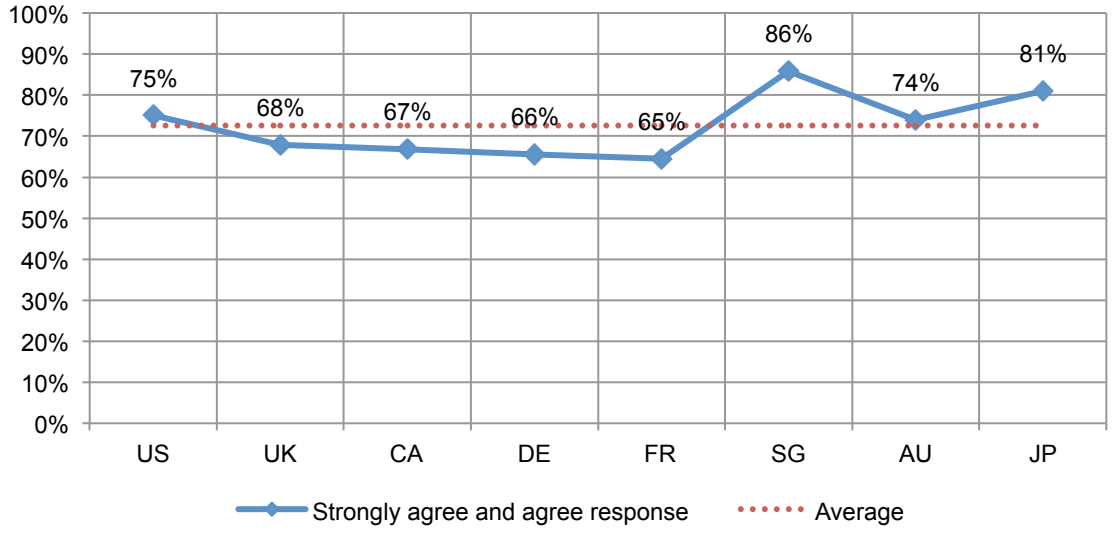
With the exception of France, a high percentage of respondents agree that their security strategy focuses on safeguarding data. As shown in Figure 9**,** the U.S., UK, Canada and Australia are most likely to address threats to information.

Figure 9. Does your organization's security strategy focus on protecting information rather than securing the IT stack?
Strongly agree and agree response combined



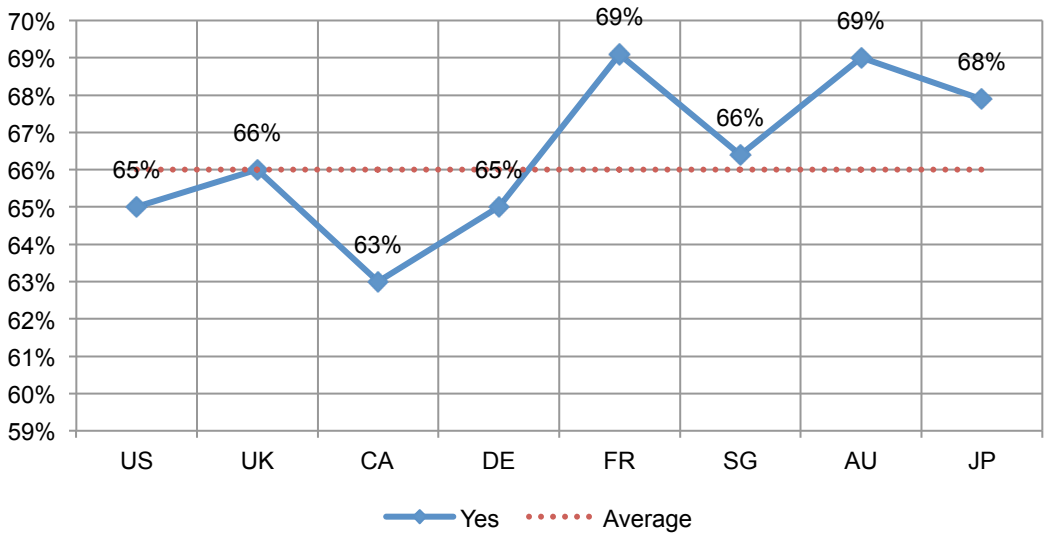
Singapore and Japan are most likely to believe in document security as a critical component of a layered defense. Respondents in the US and Australia also strongly agree and agree with the benefits of document security.

Figure 10. Document security can help to protect the confidentiality, integrity, authenticity, access, availability and utility of information as one layered defense
Strongly agree and agree response combined



Strategies that incorporate individual accountability as a risk management measure vary among countries represented in this research. Respondents in France, Australia and Japan are mostly likely to use a people-centric approach to safeguarding documents. Least likely are organizations in Canada.

Figure 11. Does your organization's security strategy incorporate individual accountability or a people-centric approach to managing risk?



Conclusion

The world and workplace is changing for document security. The findings from this research highlight some of the trends that call for a new approach to protecting sensitive and confidential information in documents. These include the following:

IT does not have as much control over disruptive technologies. The proliferation of BYOD means that increasingly IT will not be able to protect user devices. Organizations are limited in their ability to place invasive controls on mobile devices. Cloud-based services mean IT doesn't directly control the network, server, OS or applications in use.

Business units are becoming more influential in document security. However, security-savvy IT professionals should partner with end-users to share in the determination of strategy and investments in cloud services and other disruptive technologies.

Restrictive, preventative security controls are not realistic. Prevention-centric security strategies are seen as less effective. As revealed in this research there is a shift towards people-centric security strategies that emphasize individual accountability.

Training and awareness programs are critical to achieving a strong document security posture. Sixty-six percent of organizations are incorporating individual accountability as a measure to manage risk. This is mostly accomplished through training and awareness programs. Participants in this research also believe employee training and awareness is one of the most important steps to ensuring document security.

Information-centric security strategies will become more important. The findings reveal that document security is a critical component of a layered defense. Seventy-two percent of respondents agree that document security is valuable in protecting, confidentiality, integrity, authenticity, access, availability and utility of information.

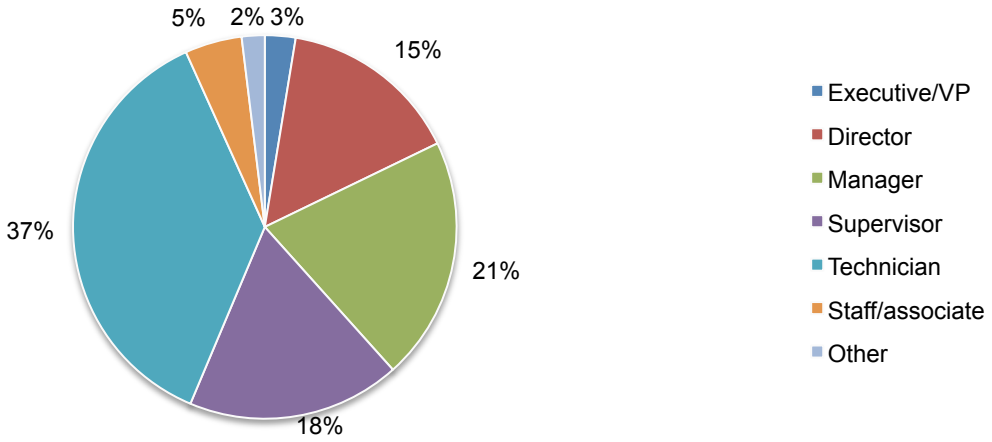
Part 4. Methods & Limitations

Table 1 reports the consolidated sample response for 8 countries. A total of 63,120 IT and IT security practitioners in 8 countries were invited to participate in this global study. A total of 2,586 respondents returned the survey. Tests for reliability and screening removed 286 surveys. The final combined sample was 2,300 surveys, yielding a 3.6 percent response rate.

Table 1. Sample response	Freq	Pct%
Sampling frame	63,120	100%
Total returns	2,586	4.1%
Rejections and screened surveys	286	0.5%
Final sample	2,300	3.6%

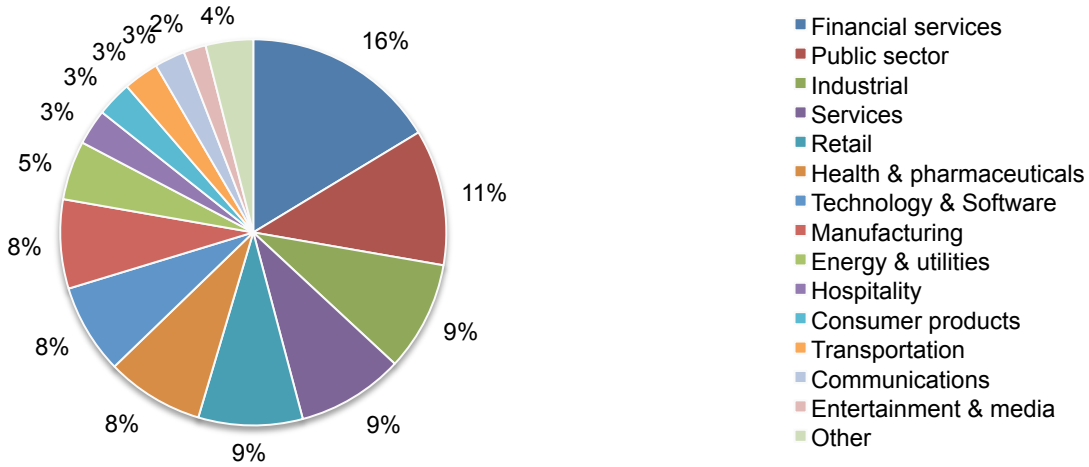
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, 57 percent of respondents are at or above the supervisory levels.

Pie Chart 1. Current position within the organization
Consolidated view



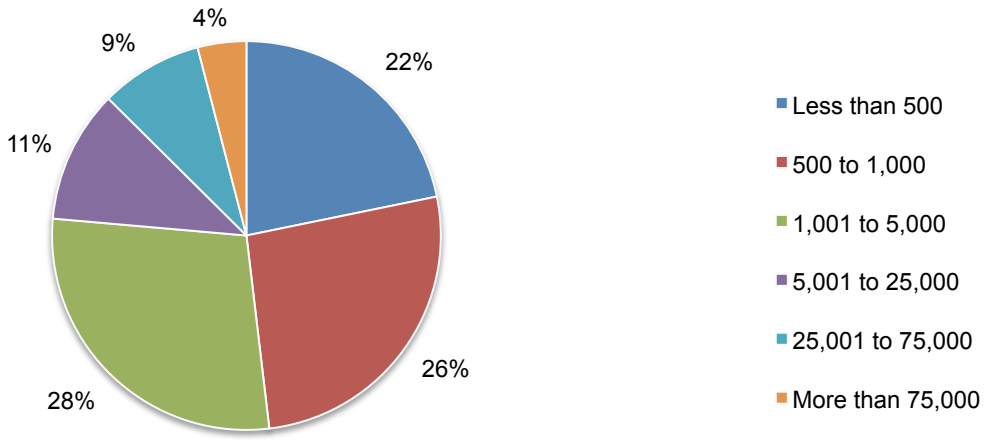
Pie Chart 2 reports the industry classification of respondents' organizations. This chart identifies financial services (16 percent) as the largest segment, followed by public sector (11 percent), and industrial, services and retail, each at 9 percent.

Pie Chart 2. Primary industry classification
Consolidated view



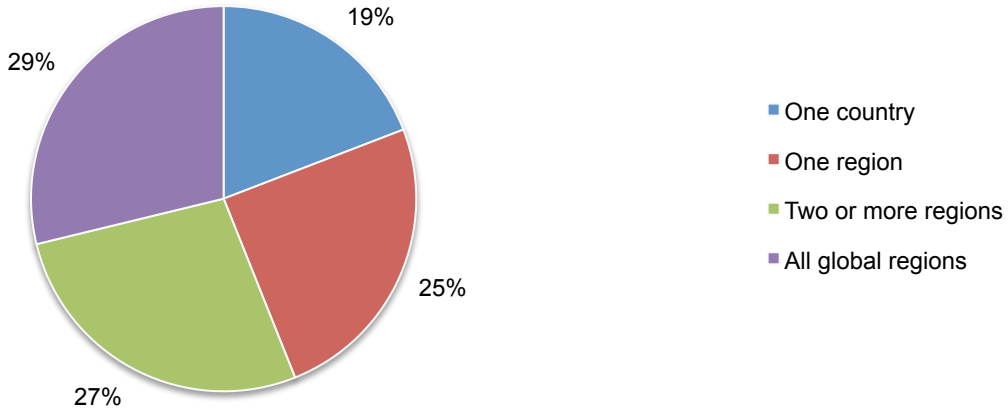
As shown in Pie Chart 3, 52 percent of respondents are from organizations with a global headcount of 1,000 or more employees.

Pie Chart 3. The full-time headcount of the global organization
Consolidated view



According to Pie Chart 4, more than half (56 percent) of respondents are from organizations with a global presence in more than two regions.

Pie Chart 4. The organization's geographic footprint
Consolidated view



Part 5. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the consolidated frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in April 2014.

Sample response	Total
Sampling frame	63,120
Total returns	2,586
Rejections and screened surveys	286
Final sample	2,300
Response rate	3.6%

S1a. Are you involved in the following activities in your organization? Please check all that apply.	Total
Mobile strategy	62%
Cloud services strategy	57%
None of the above (stop)	0%
Total	119%

S1b. Are you involved in document or file level security practices?	Total
Yes	100%
No (stop)	0%
Total	100%

Attributions: Please rate the following statements using the scale provided below each item.	
Q2. The use of personally-owned mobile devices (BYOD) in the workplace makes it difficult to place invasive controls on these devices.	Total
Strongly agree	35%
Agree	23%
Unsure	25%
Disagree	12%
Strongly disagree	5%
Total	100%

Q3. My organization's security strategy is focused on protecting information rather than securing the IT stack.	Total
Strongly agree	33%
Agree	34%
Unsure	19%
Disagree	11%
Strongly disagree	4%
Total	100%

Q4. Document security can help to protect the confidentiality, integrity, authenticity, access, availability and utility of information as one layered defense.	Total
Strongly agree	37%
Agree	35%
Unsure	18%
Disagree	8%
Strongly disagree	1%
Total	100%

Q5a. Does your organization believe that restrictive, preventative security controls are not effective?	Total
Yes	60%
No	40%
Total	100%

Q5b. If yes, why? Please select all that apply	Total
They reduce employees' productivity	40%
They are not effective in keeping documents secure because of the new types of mobile devices	66%
They are not effective in keeping documents secure because of the new types of cloud services	55%
None of the above	24%
Total	186%

Q6. In your opinion, what are the most important steps to ensuring document security? Please rank the following list from 1 = most important to 4 = least important. If possible, please try to avoid ties.	Total
Document security technologies	1.86
Employee training and awareness	2.35
Enforcement of document security policies	3.26
Safe destruction of documents	3.21

Q7a. Does your organization's security strategy incorporate individual accountability or a people-centric approach to managing risk?	Total
Yes	66%
No	26%
Unsure	8%
Total	100%

Q7b. If yes, how is this accomplished? Please select the top two choices.	Total
Training and awareness programs	69%
Performance evaluations	63%
Workplace monitoring	57%
Rewards and incentives	10%
Other (please specify)	1%
Total	200%

Q8a. Has the increased use of cloud services affected the IT function's influence on strategy and technology investments within your organization?	Total
Yes	71%
No	23%
Unsure	5%
Total	100%

Q8b. If yes, how has it changed IT's influence? Please select only one choice.	Total
Increased IT's role and influence in determining strategy and investments	8%
Decreased IT's role and influence in determining strategy and investments	34%
Increased the lines of business role and influence	57%
Other (please specify)	1%
Total	100%

Respondent and Organizational Characteristics

D1. What organizational level best describes your current position?	Total
Executive/VP	3%
Director	15%
Manager	21%
Supervisor	18%
Technician	37%
Staff/associate	5%
Other (please specify)	2%
Total	100%

D2. What best describes your organization's primary industry focus? Please choose only one.	Total
Agriculture & food service	1%
Communications	3%
Consumer products	3%
Defense & aerospace	0%
Education & research	1%
Energy & utilities	5%
Entertainment & media	2%
Financial services	16%
Health & pharmaceuticals	8%
Hospitality	3%
Industrial	9%
Logistics	1%
Manufacturing	8%
Public sector	11%
Retail	9%
Services	9%
Technology & Software	8%
Transportation	3%
Other (please specify)	1%
Total	100%

D3. What is the worldwide headcount of your organization?	Total
Less than 500	22%
500 to 1,000	26%
1,001 to 5,000	28%
5,001 to 25,000	11%
25,001 to 75,000	9%
More than 75,000	4%
Total	100%

D4. What best describes your organization's geographic footprint?	Total
One country	19%
One region	25%
Two or more regions	27%
All global regions	29%
Total	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling our toll free line at 1.800.887.3118.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances 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.

As a member of the **Council of American Survey Research Organizations (CASRO)**, 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.