RSA®CONFERENCE2012
FEBRUARY 27 – MARCH 2 | SAN FRANCISCO

Ponemon
INSTITUTE

Future State of IT Security

A Survey of IT Security Executives

In Partnership with RSA® Conference

Independently conducted by Ponemon Institute LLC

Publication Date: February 2012

Future State of IT Security

A Survey of IT Security Executives

February 2012

Part 1. Introduction

We are pleased to present the findings of the *Future State of IT Security* conducted by Ponemon Institute in partnership with RSA® Conference. In this report, we examine the main drivers or antecedents that are shaping the future state of security. The trends include the affect of disruptive technologies on organizations such as mobile devices, social media, IT virtualization, cloud computing resources and use of collaboration/document sharing technologies. Other drivers include cyber crime, government and regulations, human factors, resource constraints and organizational culture and governance.

To predict the future state of IT security, we surveyed 614 senior-level individuals with deep expertise and knowledge about their organization's IT security function. Sixty-seven percent of these respondents hold positions at the supervisor level or higher in their organization. Sixty-five percent report directly to the Chief Information Officer (CIO) or Chief Information Security Officer (CISO). On average, respondents have 11 years of relevant experience.

We asked these experts to evaluate the current state of IT security in their organizations, the negative affect certain factors or mega trends are having on their organizations' security posture and if these factors or mega trends will improve or worsen over the next 12 to 24 months. Based on the findings, we attempt to provide a prediction about the future state of IT security in the next one to two years in order to allocate the right amount of available resources (people and technologies) to achieve the most fortified security posture possible.

The following is a summary of the key findings:

Respondents' negative perceptions about the current state of IT security in their organizations are clouding the future state of IT security. Specifically the majority of respondents agree with the following:

- Senior leadership does not view IT security as a strategic priority.
- Policies and procedures are in place to protect information assets and critical infrastructure but the necessary security technologies to support these procedures are often not available.
- More resources are needed to invest in security technologies and hire experienced security practitioners.
- A cyber attack affecting the critical infrastructure of an organization in their industry is imminent or very likely.

Based on their perceptions, the majority of IT security experts surveyed do not believe that their organization's IT security posture will improve and predict that the following security issues are likely to get worse over the next 12 to 24 months. These include:

- The use of mobility and social media tools in the workplace will put their organizations at risk.
- Cyber crimes are growing in sophistication and stealth and target organizations' intellectual property and finances.
- Advanced persistent threats or government-sponsored cyber attacks and cyber terrorism will target their organizations.
- To deal with the growing complexity of IT security and threats to their organization, there is a dearth of skilled and knowledgeable security practitioners.
- Government, regulatory actions and future mandates on protecting the critical infrastructure will put a strain on budgets.
- Growth of unstructured data assets leaves valuable information assets vulnerable to attack.

Not all is negative. Certain areas of IT security are expected to improve over the next 12 to 24 months**:**

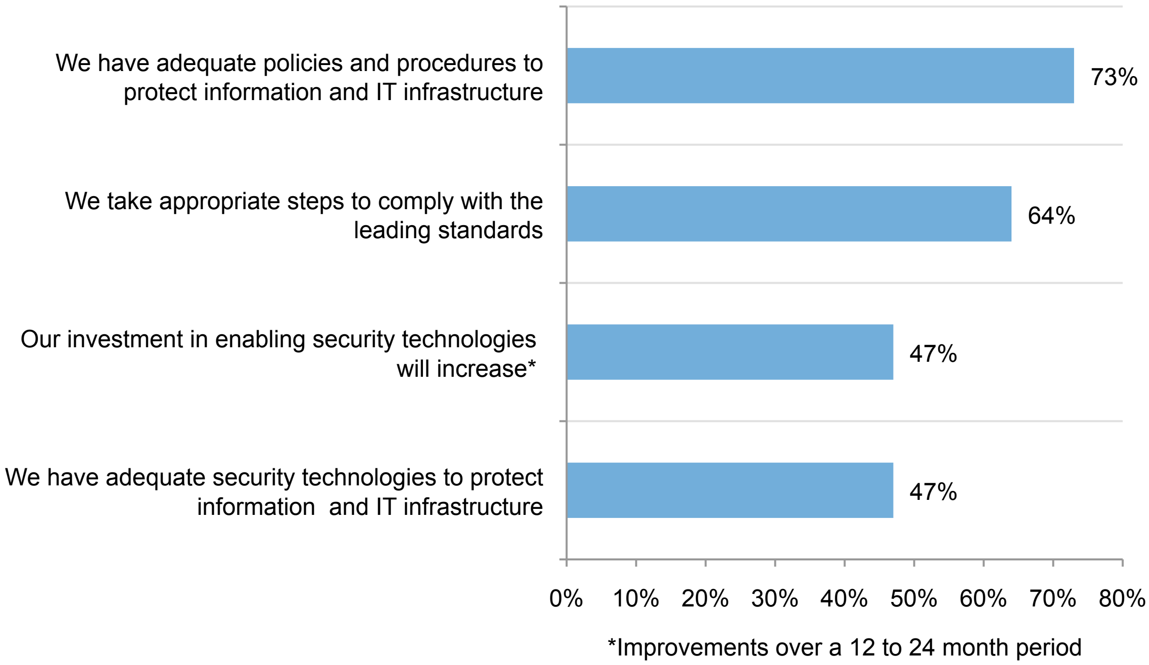
- Companies' use of cloud computing will become more secure.
- Expect improvements in managing the risk of criminal insiders, including malicious privileged users, as well as employees who are negligent.
- Mobile workforce will become less of a security risk.
- Risks from the integration of partners into internal networks and applications will be better managed.

Part 2. Key Findings

Respondents have the following perceptions about their organization's current security posture, which we believe influences their predictions about the future state of IT security.

Policies and procedures are in place to protect information assets and critical infrastructure but many organizations lack the necessary security technologies. As shown in Bar Chart 1, the majority of respondents (73 percent) say they have policies and procedures to protect information and IT infrastructure and 64 percent say they are taking appropriate steps to comply with the leading standards for privacy and IT security. However, less than half of respondents (47 percent) say they have adequate security technologies and resources. Forty-seven percent predict that their investment in enabling security technologies will increase.

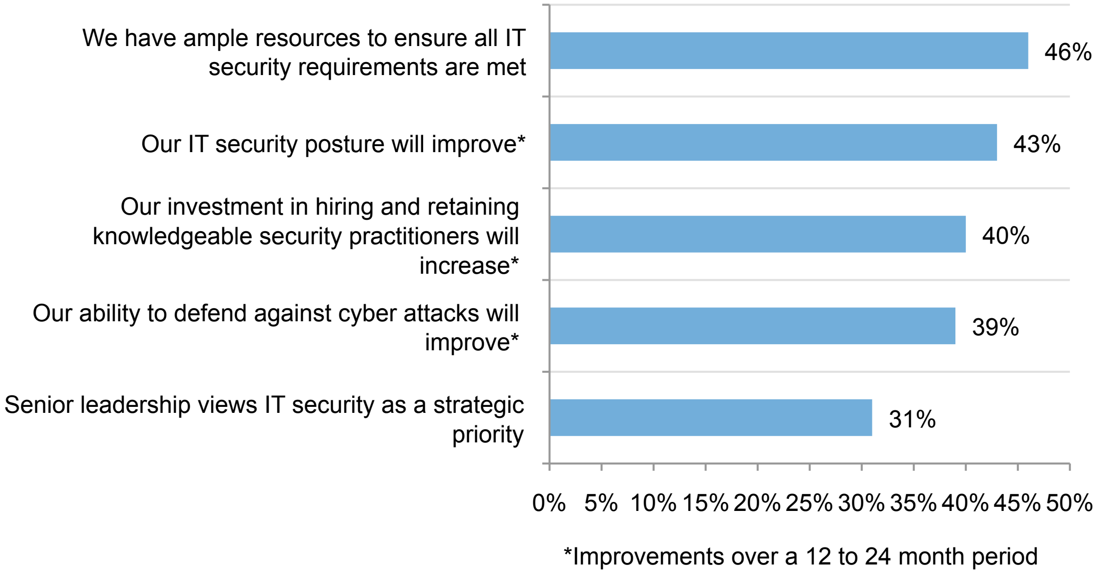
Bar Chart 1. The current state of IT security
Each bar reflects strongly agree & agree responses



Senior leadership is not making IT security a strategic priority thus dampening the optimism of respondents. Only 31 percent of security professionals surveyed believe their senior leadership views IT security strategy a priority in their organizations, according to Bar Chart 2. This perception may be influencing respondents' concern about their ability to improve their organizations' security posture.

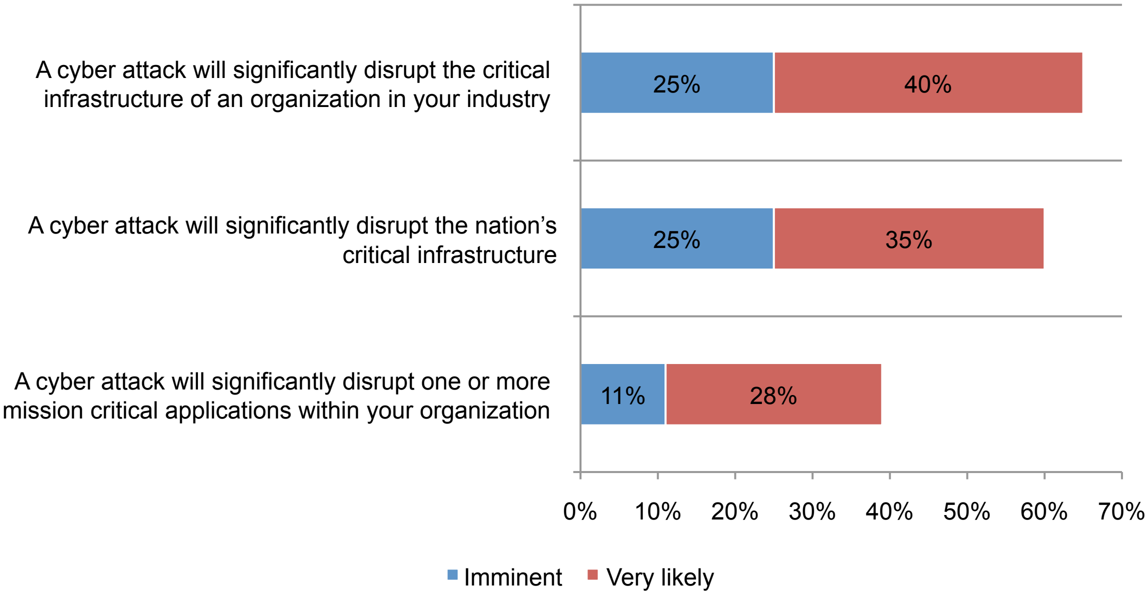
Less than half (46 percent) say they have ample resources to meet security requirements and only 43 percent say their organization's IT security posture will improve over the next 12 to 24 months. Forty percent say they will be able to increase their investment in hiring and retaining knowledgeable and experienced security practitioners. Only 39 percent are confident in their organization's ability to defend against cyber attacks.

Bar Chart 2. The current state of IT security (continued)
Each bar reflects strongly agree & agree responses combined



A cyber attack on the public and private sector is imminent or very likely. As shown in Bar Chart 3, 25 percent say that a cyber attack that will significantly disrupt the critical infrastructure of an organization in their industry is imminent and 40 percent say it is very likely. They are similarly concerned that a cyber attack will soon significantly disrupt the nation's critical infrastructure. Thirty-nine percent say a cyber attack that will significantly disrupt one or more mission critical applications within an organization is imminent or very likely.

Bar Chart 3. The likelihood of a cyber attack
Only imminent and very likely ratings are shown



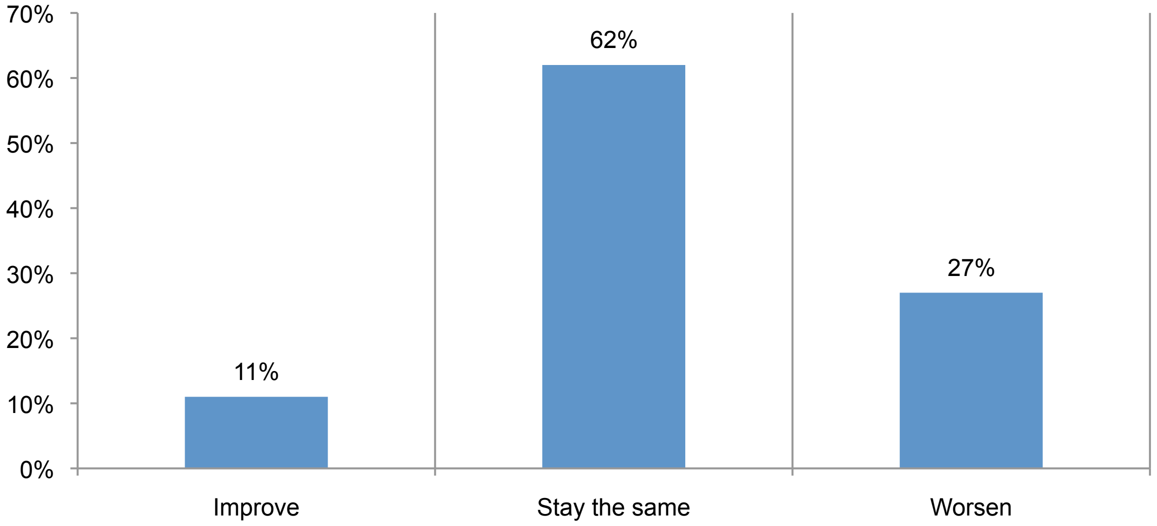
Predicting the Future State of IT

In the survey, we identified six security mega trends and a series of scenarios related to those megatrends. Security mega trends were rated according to their importance: disruptive technologies, cyber crime, government and regulations, human factors, resource constraints and organizational factors.

We then asked the IT security practitioners surveyed to rate whether the affect of the scenarios within each mega trend has a very significant, significant, no significance or no impact on their organization's current security posture. They were then asked if they expect the scenario to worsen, stay the same or improve.

By design, we did not ask respondents to provide additional information to support their rankings. The audited results of their responses are presented in the Appendix. Overall, the majority of respondents (62 percent) expect the state of IT security will stay the same over the next 12 to 24 months, as shown in Bar Chart 4.

Bar Chart 4. The future state of IT security over the next 12 to 24 months

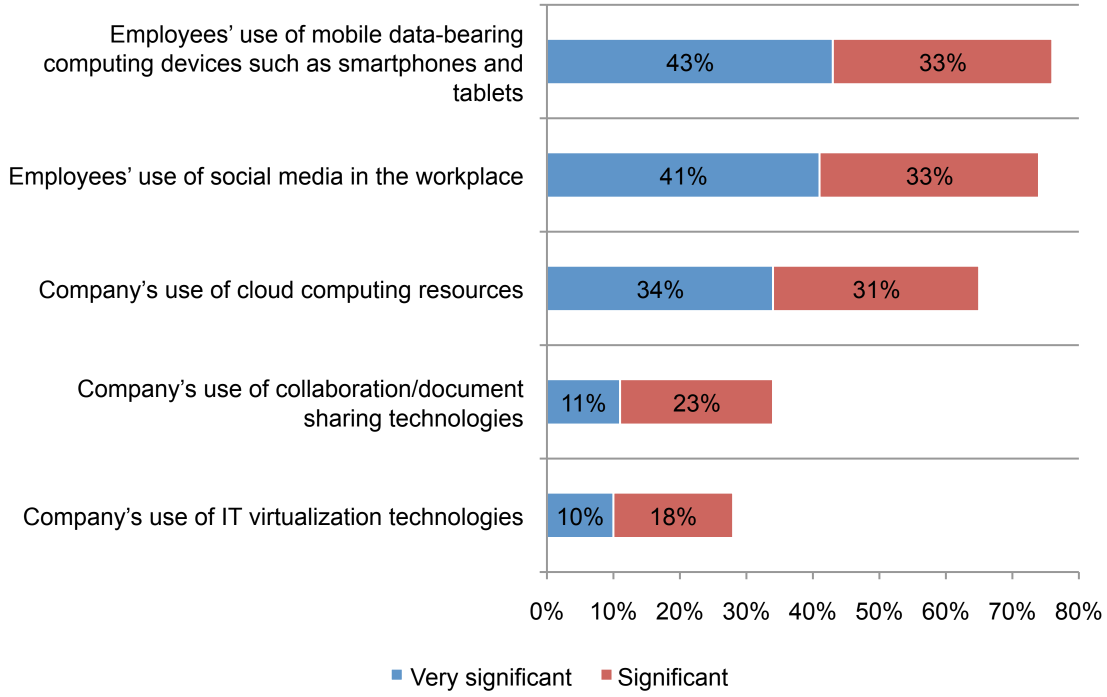


Mega Trend 1: Disruptive technologies. We identified disruptive technologies as mobility, social media, cloud computing, collaboration/document sharing technologies and IT virtualization technologies. Bar Chart 5 summarizes what disruptive technologies respondents believe are having a very significant or significant negative affect on their organization. Bar Chart 6 summarizes whether respondents expect the risk to improve or worsen.

Mobile data-bearing devices and social media are proving to have the most negative affect on the security posture of an organization. Possible explanations include the difficulty in protecting the security of their infrastructure when mobile devices are connected to the network, the ease in which mobile devices and social media tools can affect the security of valuable information assets and the lack of enforceable policies and procedures.

According to Bar Chart 5, 76 percent of respondents say mobile data-bearing computing devices such as smartphones and tables present a very significant or significant risk and more than half (56 percent) says it will get worse over the next 12 to 24 months (Bar Chart 6). Seventy-five percent say social media tools used in the workplace present a very significant or significant risk and 59 percent says it will get worse.

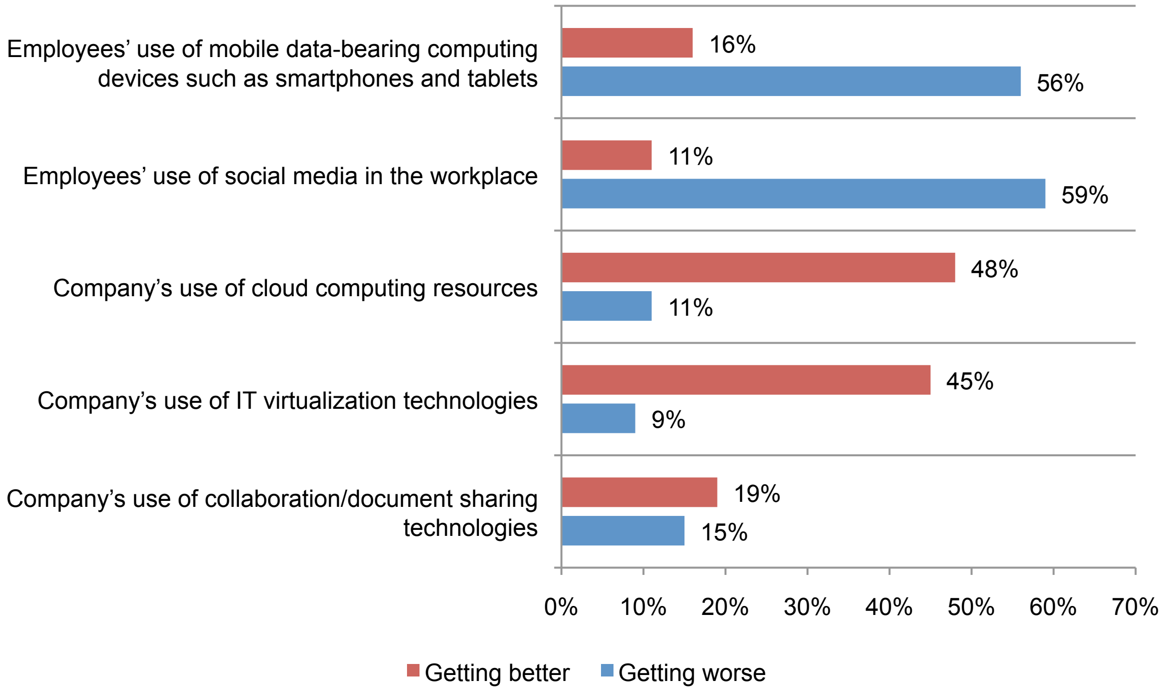
Bar Chart 5. Risk of disruptive technologies affect on an organization's security posture



A company's use of cloud computing resources, according to 65 percent of respondents is having a very significant or significant impact on the current state of their organization's security posture. However, as shown in Bar Chart 6, almost half (48 percent) say it will get better. This could possibly result from a better vetting of cloud service providers and assurances of strict data protection practices in place.

Collaboration/document sharing and IT virtualization technologies are not considered to create as significant a risk to their organizations. According to Bar Chart 5, 34 percent say their organization's use of this technology is having a negative affect on their organizations and 28 percent of respondents say the company's use of IT virtualization technologies is having a negative affect. According to Bar Chart 6, only 9 percent say the company's use of IT virtualization technologies will get worse and 15 percent say the use of collaboration/document sharing technologies will get worse.

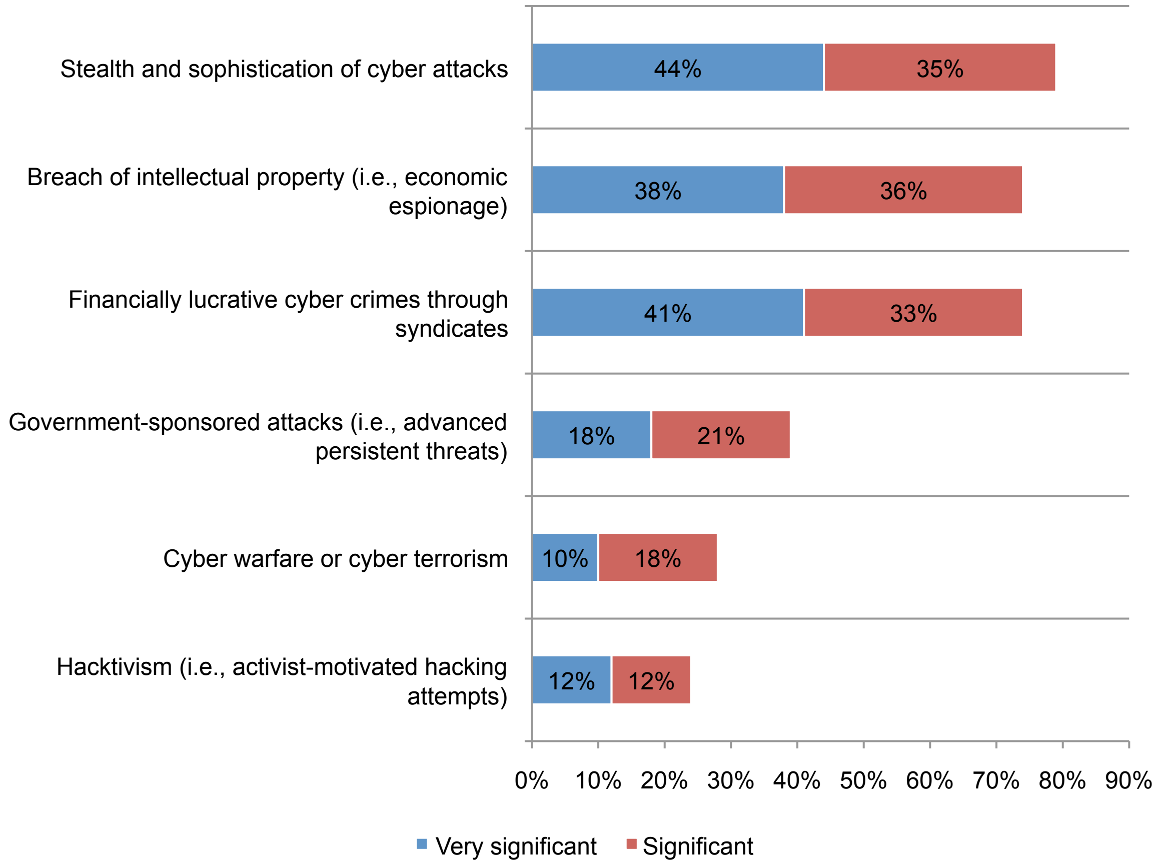
Bar Chart 6. The future state of disruptive technologies risk



Mega Trend 2: Cybercrime. In the survey, we listed scenarios involving different types and attributes of cyber crime. These include: concerns that cyber attacks are becoming more stealthy and sophisticated, cyber crimes involving intellectual property, financially lucrative cyber crimes that are committed through syndicates, government-sponsored attacks, cyber warfare or terrorism and hactivism or activist-motivated hacking attempts. We asked respondents to indicate if they believe the risk is very significant, significant, not significant or of no impact.

As discussed previously, the IT security practitioners surveyed are very much concerned about their organization's ability to defend against a cyber attack. Bar Chart 7 summarizes the responses to the various types of cyber attacks that are having a very significant or significant negative affect on their organization. Bar Chart 8 summarizes whether respondents expect the risk is expected to improve or worsen. (We did not include the response "expected to stay the same").

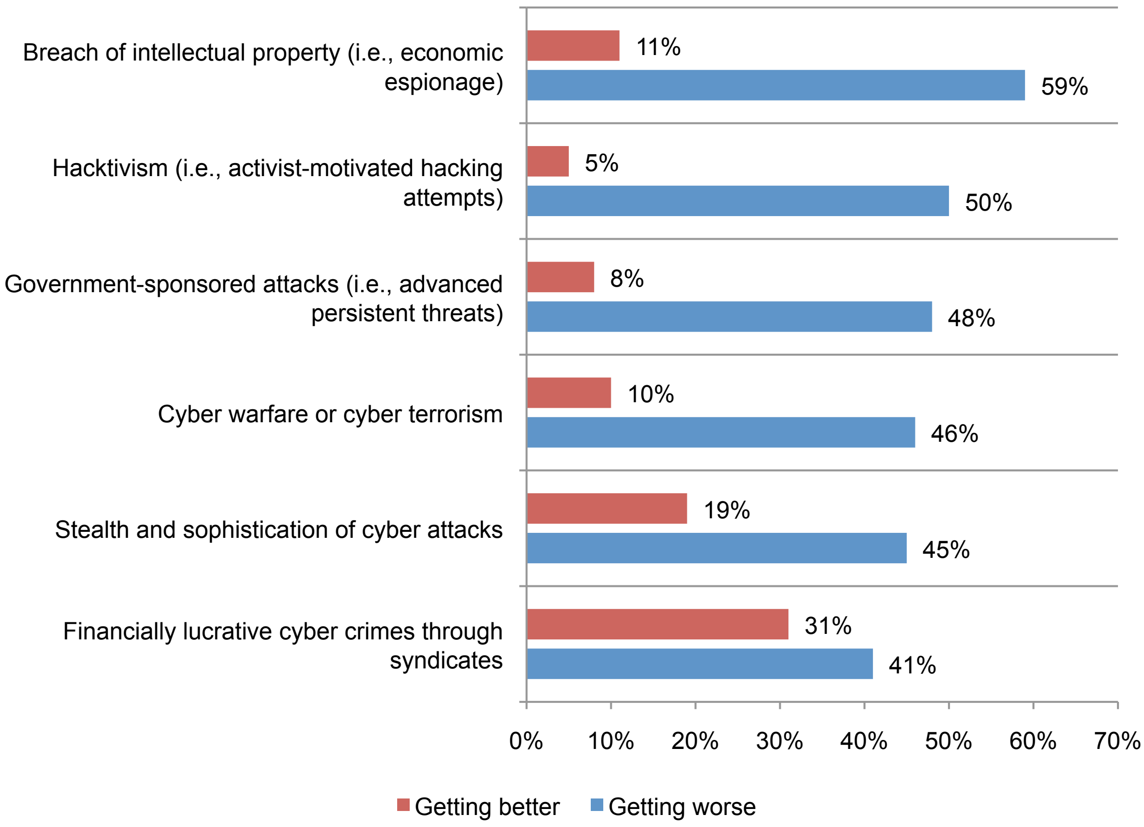
Bar Chart 7. Risk of a cyber crime on an organization's security posture



As shown in Bar Chart 7, stealth and sophistication, economic espionage and cyber crimes through syndicates are having the most significant negative affect on the security posture of organizations (79 percent, 74 percent and 74 percent, respectively)**.** Currently, 39 percent say advanced persistent threats or government-sponsored attacks are having a very significant or significant followed by 28 percent who say cyber warfare is a major concern or hacktivism (24 percent).

The types of cyber crime expected to worsen the most over the next 12 to 24 months are breach of intellectual property (59 percent), hactivism (50 percent) and government-sponsored attacks (48 percent).

Bar Chart 8. The future state of cyber crime risk

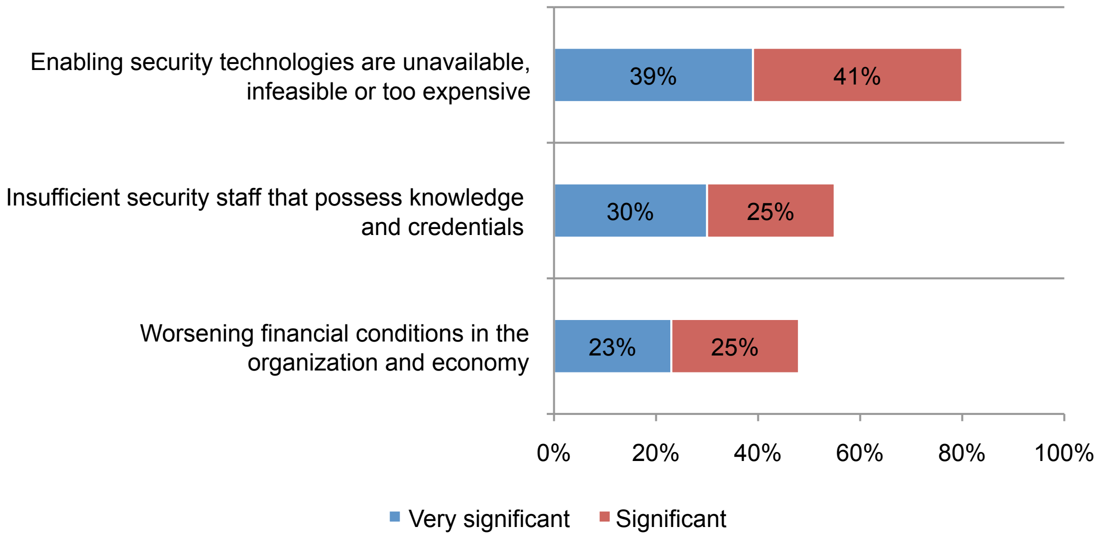


Mega Trend 3: Resource constraints. The majority of respondents believe that their senior leadership is not making IT security the strategic priority it deserves to be. Consequently, they are concerned about having the ability to invest in skilled personnel and technologies in order to achieve their security mission.

In the survey, we listed scenarios that affect organizations ability to have the necessary resources. These include: security technologies are unavailable, infeasible or too expensive, security staff who have knowledge and credentials are difficult to find and the worsening economy. We asked respondents to indicate if they believe the risk is very significant, significant, not significant or of no impact.

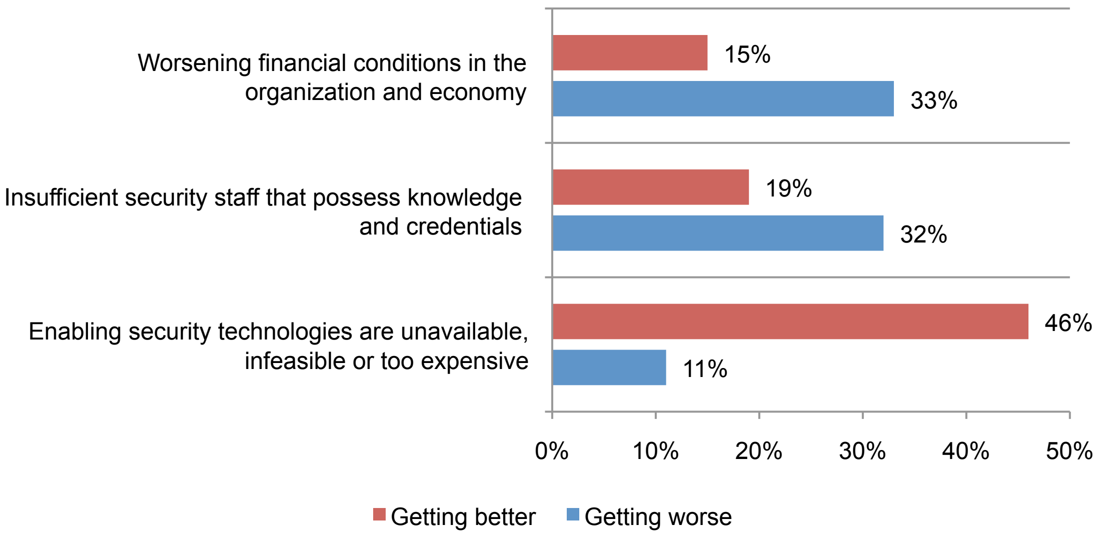
According to Bar Chart 9, 80 percent say the technology issue is a very significant or significant risk followed by 55 percent who say the lack of skilled staff is leaving a gap in their organization's security posture. Almost half are concerned about the economy.

Bar Chart 9. The risk of limited resources on an organization's security posture



As shown in Bar Chart 10, the most promising change with respect to resources involves the availability of security technologies. Forty-six percent expect the situation to improve over the next 12 to 24 months. Almost one-third, expect the situation with staffing to improve and only 15 percent say the economy will get better.

Bar Chart 10. The future state of resource constraint risk

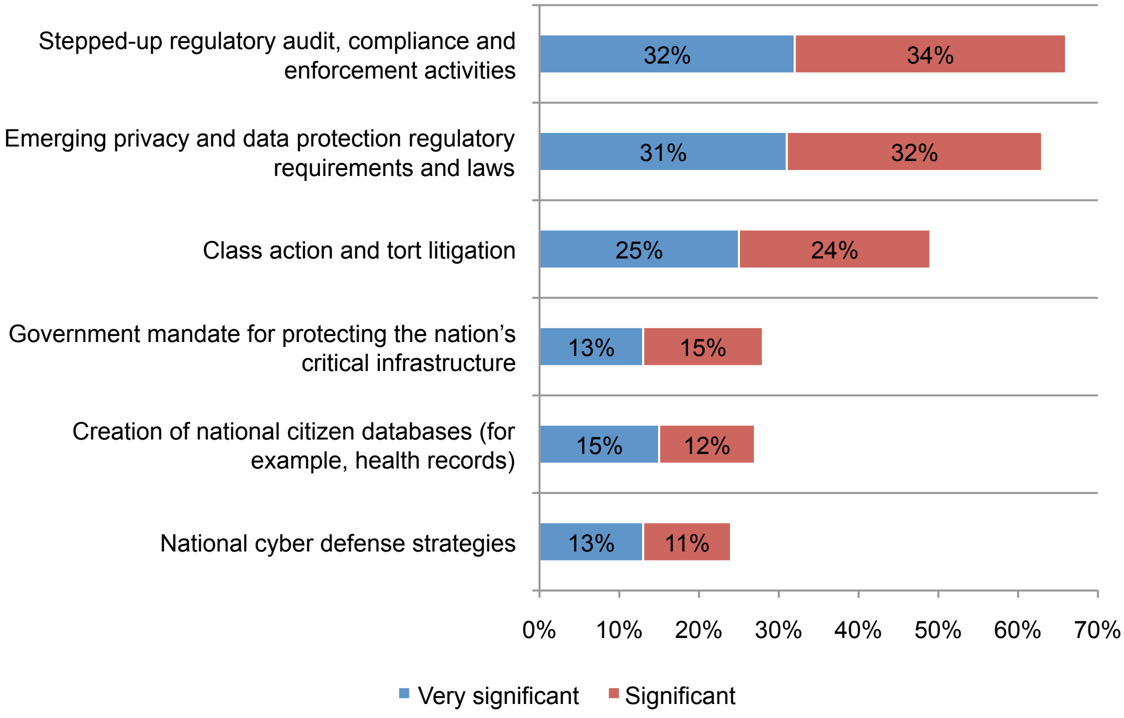


Mega Trend 4: Government and regulations. The need to comply with a plethora of data security and privacy regulations can affect an organization's security for better or worse. Regulations can focus an organization's attention on the need to increase investments in people, processes and technologies.

However, audits, uncertainty about emerging privacy and data protection laws, class action and tort litigation, government mandates on the protection of the nation's critical infrastructure can put a strain on resources. We also believe that government's creation of national citizen databases and cyber defense strategies can have a negative impact on an organization's security posture.

In the survey, we listed various government and regulatory scenarios that affect organizations. These include: stepped-up regulatory audit, compliance and enforcement activities, new privacy and data protection regulations, class action and tort litigation, government mandates for protecting CNI, creation of national citizen data bases and national cyber defense strategies. We asked respondents to indicate if they believe the impact is very significant, significant, not significant or of no impact. Their responses are shown in Bar Chart 11.

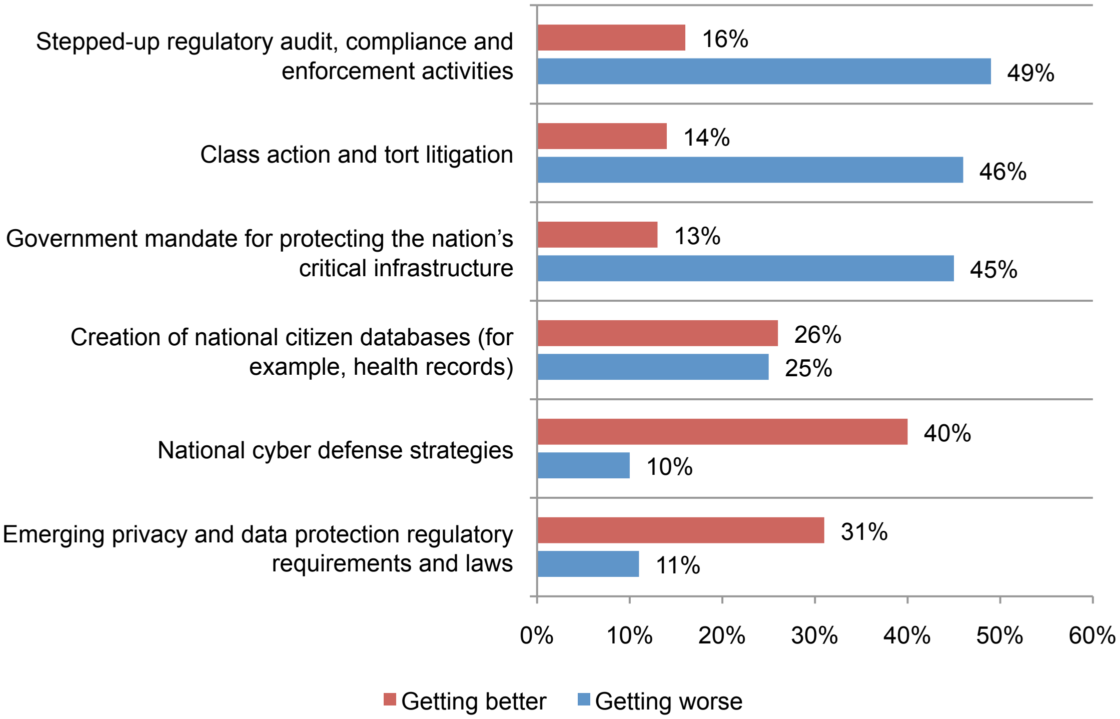
Bar Chart 11. The affect of government, regulatory & legal activities on an organization



In general, the current regulatory and legal environment is having a very significant and significant affect on the security posture of organizations. Sixty-six percent say audit, compliance and enforcement activities are increasing and 63 percent say new privacy and data protection regulatory requirements and laws are affecting their organizations. Of less impact are class action and tort litigation and government mandates for protecting the nation's CNI (49 percent and 28 percent, respectively). National citizen databases and national cyber defense strategies are having a minimal impact.

Bar Chart 12 describes the changes anticipated. Respondents believe the current regulatory and legal environment will get worse. While national cyber defense strategies and emerging privacy and data protection regulatory requirements and laws will get better.

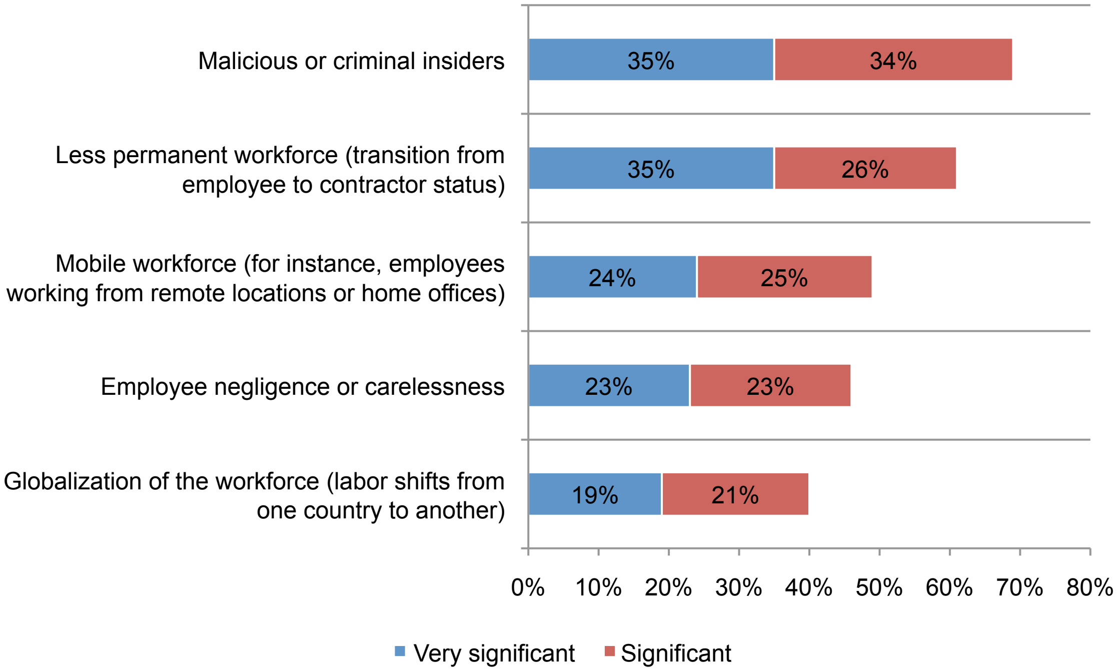
Bar Chart 12. The future state of government, regulatory & legal activities



Mega Trend 5: Human factor. The most serious risks to the security of sensitive and confidential information are employees, contractors and malicious outsiders. In the survey, we listed various human factor risks that affect organizations. These include: malicious or criminal insiders, less permanent workforce, mobile workforce, employee negligence and globalization of the workforce. We asked respondents to indicate if they believe the impact is very significant, significant, not significant or of no impact. Their responses are shown in Bar Chart 13.

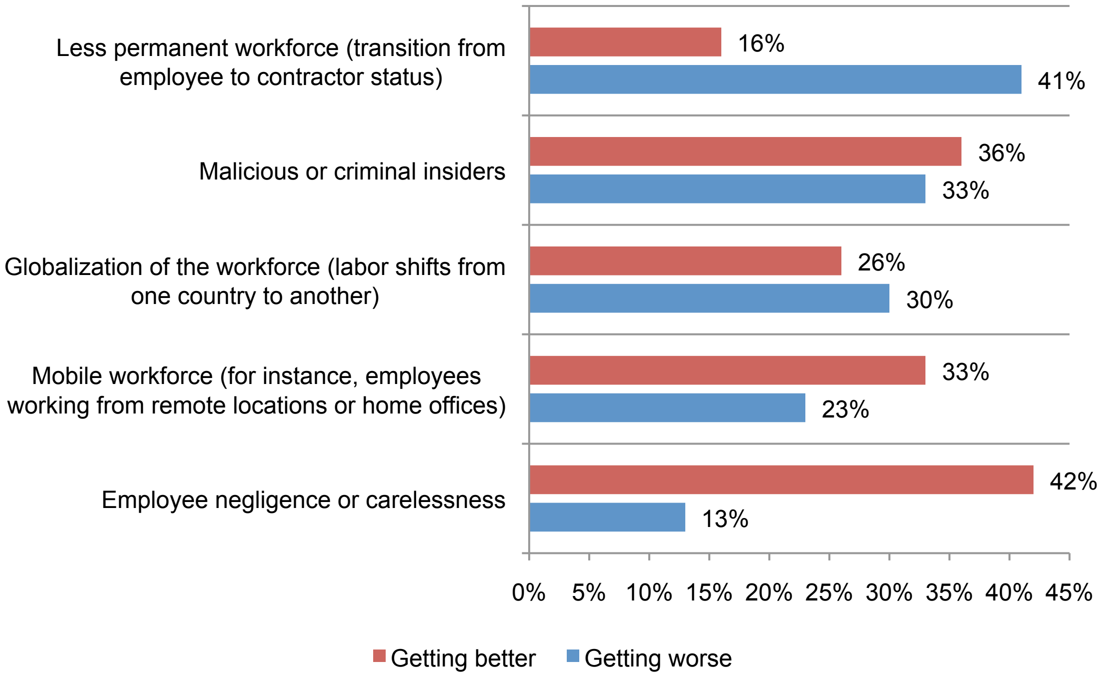
With respect to the human factor risk, the greatest negative impact on an organization's security posture is the malicious or criminal insider (69 percent of respondents) followed by a less permanent workforce (61 percent). Less than half believe it is the mobile workforce, employee negligence and globalization of the workforce.

Bar Chart 13. Human factor impact on an organization's security posture



Bar Chart 14 summarizes whether respondents expect the human factor risk to improve or worsen. (We did not include the response "expected to stay the same"). The risks of malicious or criminal insider followed by employee negligence are the risks most expected to improve. The transitional workforce is the human factor risk most expected to get worse.

Bar Chart 14. The future state of human factor risk



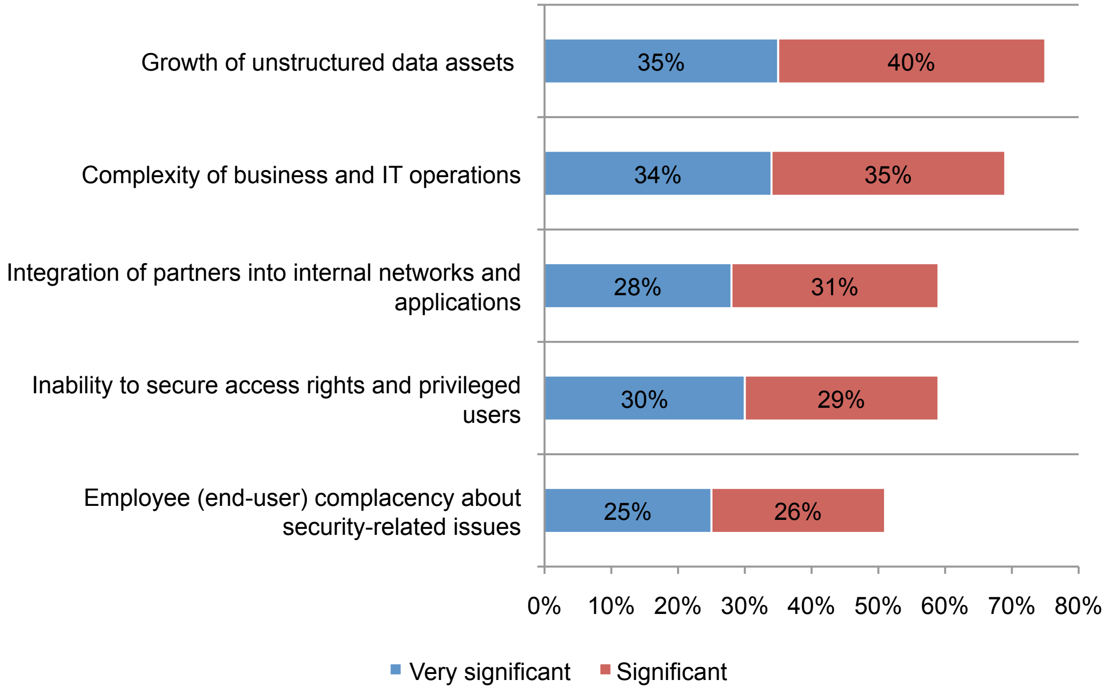
Mega Trend 6: Organizational factors. These factors focus on how certain practices can make it more difficult to protect data and infrastructure. In the survey, we listed various organizational factors that can influence the security posture.

These include growth of unstructured data assets, complexity of business and IT operations, integration of partners into internal networks and applications, inability to secure access rights and privileged users, employee (end-user) complacency about security-related issues. We asked respondents to indicate if they believe the impact is very significant, significant, not significant or of no impact. Their responses are shown in Bar Chart 11.

As shown in Bar Chart 15, 75 percent say the growth of unstructured data assets presents a very significant or significant risk to the organization. Often residing outside of traditional databases and data structures, a typical business or government organization stores many thousands of files containing sensitive non-financial data in shared folders on file servers and NAS devices. Examples of this unstructured data include electronic spreadsheets, PowerPoint and Word documents, audio files, videos, blueprints, software source code, instant messages, Web pages and so forth.

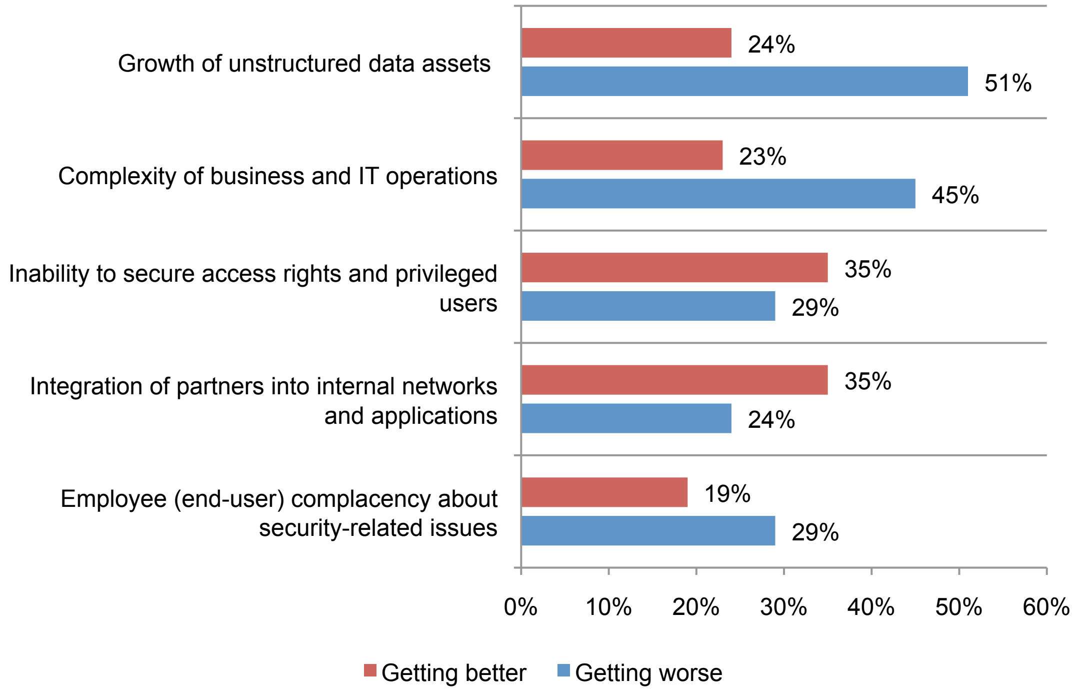
Sixty-nine percent believe it is complexity of business and IT operations that affect the organization's security posture. The majority of respondents believe that the remaining factors pose a very significant and significant risk.

Bar Chart 15. Organizational risk to an organization's security posture



Bar Chart 16 summarizes the factors believed to get better or get worse. Growth of unstructured data assets and complexity of business and IT operations are expected to get worse by 51 percent and 45 percent of respondents, respectively. The ability to secure access rights and privileged users and integration of partners into internal networks and applications are expected to get better.

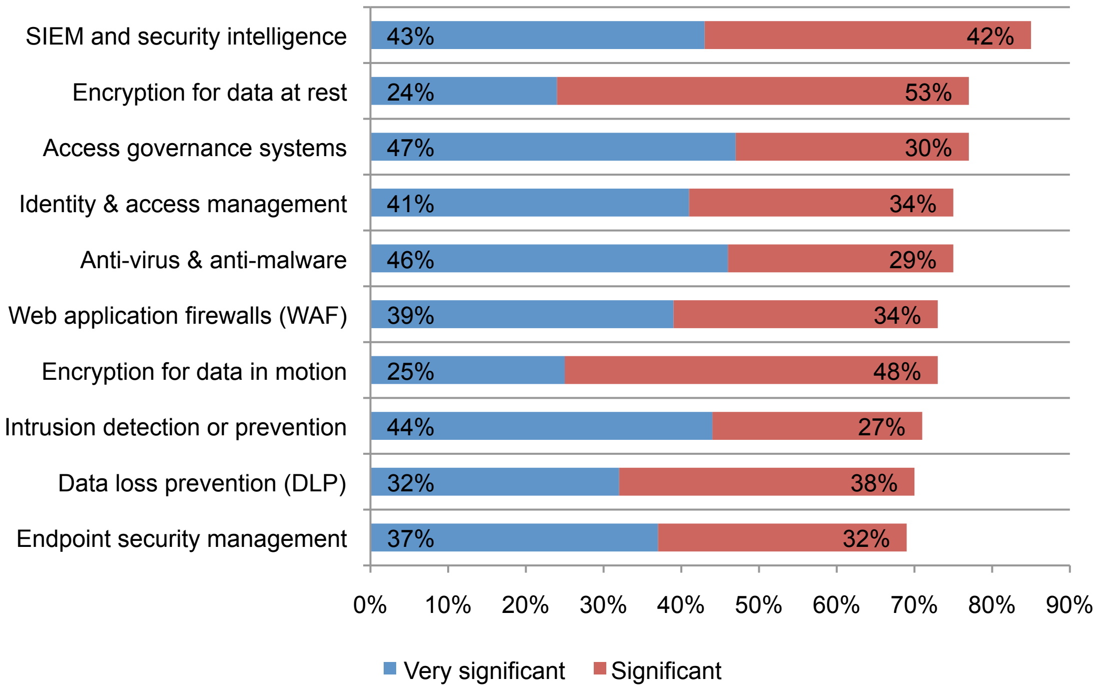
Bar Chart 16. The future state of organizational risk



Technologies to maintain or improve an organization's security posture. Respondents were asked to rank enabling technologies according to the value they provide to their organizations' security posture. The top 10 technologies are shown in Bar Chart 17.

We believe the ranking of these technologies is related to the most serious risks identified to worsen over the next 12 to 24 months. Specifically, they include SIEM and security intelligence, encryption for data at rest, access governance systems, identity & access management, anti-virus & anti-malware, web application firewalls, encryption for data in motion, intrusion detection or prevention, data loss prevention and endpoint security management.

Bar Chart 17. Technologies that are most important to combating mega trend security risks



Part 3. Conclusion & Implications

The purpose of this research is to help organizations better understand how they should plan for the security risks over the next 12 to 24 months. As we discussed, the research was designed to have respondents rate various risks and whether they will get worse, stay the same or get better. We did not ask them to provide their rationale for their predictions.

The most serious risks that exist today and are expected to worsen are associated with the use of mobile devices and social media tools in the workplace. Cyber crimes are expected to grow in stealth and sophistication and, as indicated by respondents, time is running out to address this risk. The increase in organizations' unstructured data assets is also a problem that will get worse and needs to become a priority for IT security and business units. Unfortunately, to help IT security address these problems there is a lack of skilled and knowledgeable security practitioners. This suggests the need for a more aggressive approach to training and educating future security practitioners.

On a more positive note, IT security practitioners believe the use of cloud computing will become more secure. Perhaps due to improvements and availability of technologies, organization will be better able to manage the risk of criminal insiders, especially malicious privileged users, as well as employees who are well-meaning but negligent.

In conclusion, understanding the future state of a dynamic security risk environment will hopefully help organizations to better allocate scarce resources. As a result they will be in a better position to achieve a more effective and efficient security posture.

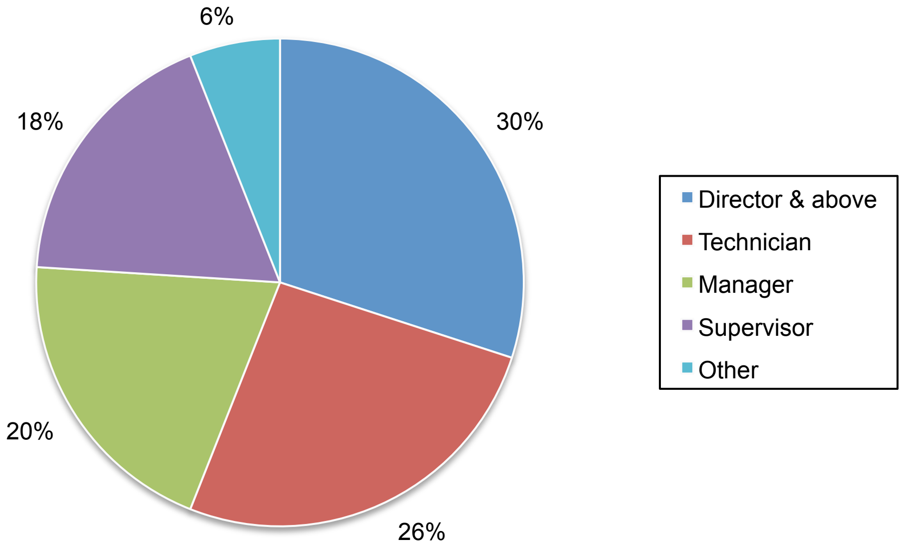
Part 4. Methods

Our sample frame consists of 20,552 individuals drawn at random from a larger proprietary database of IT practitioners – all with bona fide credentials in security and or data protection. As shown in Table 1, 671 respondents completed the survey. Of the returned instruments, 57 surveys were rejected for reliability concerns. This resulted in a final sample of 614 surveys or a three percent response rate.

Table 1. Sample response	**Freq.**	**Pct%**
Sample frame (IT & IT security practitioners)	20,552	100.0%
Survey returns	671	3.3%
Rejected surveys	57	0.3%
Final sample	614	3.0%

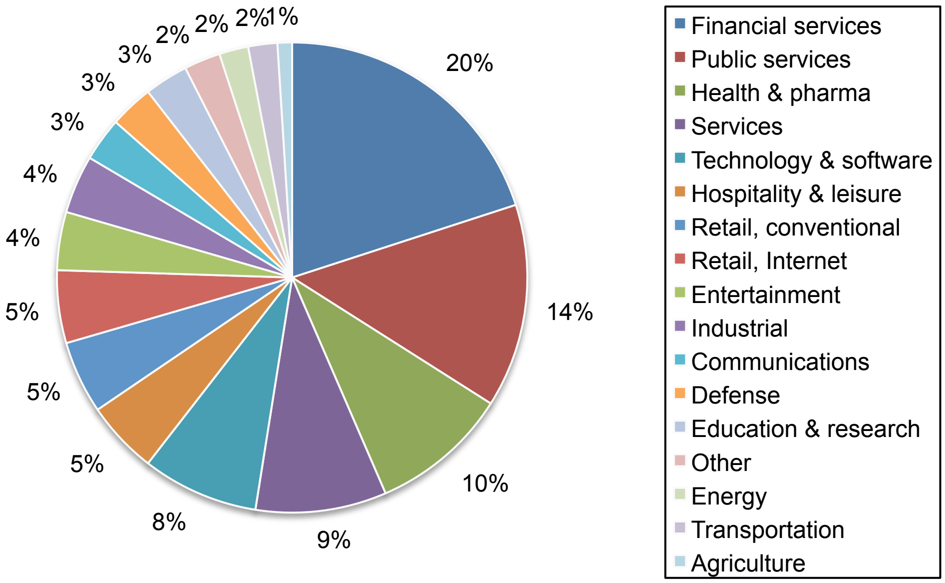
Pie Chart 1 reports the respondents' position level. Fifty-two percent of the respondents are directors and technicians, 20 percent are managers and 18 percent are supervisors. The approximate experience level of respondents is 11.46 years.

Pie Chart 1. Distribution of respondents according to position level



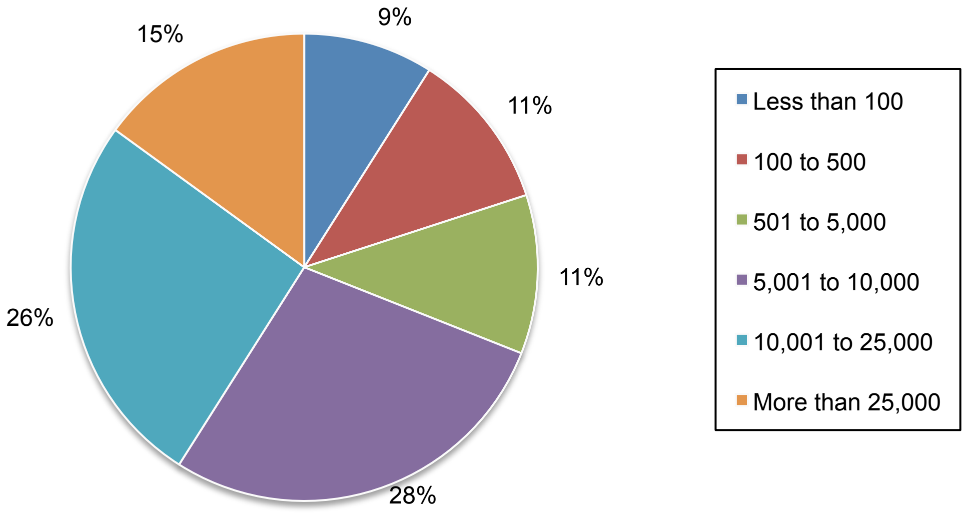
Pie Chart 2 reports the respondents' organizations primary industry segments. As shown, 20 percent of respondents are located in financial services, which includes banking, investment management, insurance, brokerage, payments and credit cards. Another 14 percent are located in the public services segment.

Pie Chart 2. Distribution of respondents according to industry segment



According to Pie Chart 3, the majority of respondents (69 percent) are located in larger-sized organizations with a global headcount of more than 5,000 employees.

Pie Chart 3. Worldwide headcount of respondents' organizations



Part 5. Limitations

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

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of IT and IT security practitioners, which resulted 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 survey.

- Sampling-frame bias: The accuracy of survey results is dependent upon the degree to which our sampling frames are representative of individuals who are senior-level IT or IT security practitioners within the sample frame selected.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from respondents. While certain checks and balances were incorporated into our survey evaluation process including sanity checks, there is always the possibility that some respondents did not provide truthful responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured over a four-week period ending in January 2012.

Part 1. Attributions about your organization. Following are nine (9) attributions about your organization's security posture. Please rate each statement using the scale provided below each item to express your opinion.	Strongly agree	Agree	Combined
Q1a. My organization has adequate policies and procedures to protect information assets and critical infrastructure.	45%	28%	73%
Q1b. My organization has adequate security technologies to protect information assets and IT infrastructure.	26%	21%	47%
Q1c. My organization takes appropriate steps to comply with the leading standards for privacy and IT security	30%	34%	64%
Q1d. My organization's senior leadership views IT security as a strategic priority.	13%	18%	31%
Q1e. My organization has ample resources to ensure all IT security requirements are met.	24%	22%	46%
Q1f. My organization's IT security posture will improve over the next 12 to 24 months.	23%	20%	43%
Q1g. My organization's ability to defend against cyber attacks will improve over the next 12 to 24 months.	21%	18%	39%
Q1h. My organization's investment in enabling security technologies will increase over the next 12 to 24 months.	23%	24%	47%
Q1i. My organization's investment in hiring and retaining knowledgeable and experienced security practitioners will increase over the next 12 to 24 months.	21%	19%	40%

Part 2. Mega trends

	Current state		Future state	
Q2 Disruptive technologies	Very significant	Significant	Getting worse	Getting better
Employees' use of mobile data-bearing computing devices such as smartphones and tablets	43%	33%	56%	16%
Employees' use of social media in the workplace	41%	33%	59%	11%
Company's use of IT virtualization technologies	10%	18%	9%	45%
Company's use of cloud computing resources	34%	31%	11%	48%
Company's use of collaboration/document sharing technologies	11%	23%	15%	19%

	Current state		Future state	
Q3. Cyber crime	Very significant	Significant	Getting worse	Getting better
Stealth and sophistication of cyber attacks	44%	35%	45%	19%
Financially lucrative cyber crimes through syndicates	41%	33%	41%	31%
Hacktivism (i.e., activist-motivated hacking attempts)	12%	12%	50%	5%
Breach of intellectual property (i.e., economic espionage)	38%	36%	59%	11%
Government-sponsored attacks (i.e., advanced persistent threats)	18%	21%	48%	8%
Cyber warfare or cyber terrorism	10%	18%	46%	10%

	Current state		Future state	
Q4. Government and regulations	Very significant	Significant	Getting worse	Getting better
Emerging privacy and data protection regulatory requirements and laws	31%	32%	11%	31%
Government mandate for protecting the nation's critical infrastructure	13%	15%	45%	13%
Stepped-up regulatory audit, compliance and enforcement activities	32%	34%	49%	16%
Creation of national citizen databases (for example, health records)	15%	12%	25%	26%
National cyber defense strategies	13%	11%	10%	40%
Class action and tort litigation	25%	24%	46%	14%

	Current state		Future state	
Q5. Human factors	Very significant	Significant	Getting worse	Getting better
Mobile workforce (for instance, employees working from remote locations or home offices)	24%	25%	23%	33%
Less permanent workforce (transition from employee to contractor status)	35%	26%	41%	16%
Employee negligence or carelessness	23%	23%	13%	42%
Malicious or criminal insiders	35%	34%	33%	36%
Globalization of the workforce (labor shifts from one country to another)	19%	21%	30%	26%

	Current state		Future state	
Q6. Resource constraints	Very significant	Significant	Getting worse	Getting better
Enabling security technologies are unavailable, infeasible or too expensive	39%	41%	11%	46%
Insufficient security staff that possess knowledge and credentials	30%	25%	32%	19%
Worsening financial conditions in the organization and economy	23%	25%	33%	15%

	Current state		Future state	
Q7. Organizational factors	Very significant	Significant	Getting worse	Getting better
Complexity of business and IT operations	34%	35%	45%	23%
Growth of unstructured data assets	35%	40%	51%	24%
Employee (end-user) complacency about security-related issues	25%	26%	29%	19%
Integration of partners into internal networks and applications	28%	31%	24%	35%
Inability to secure access rights and privileged users	30%	29%	29%	35%

Q8a. The following table summarizes the six mega trend categories listed above. Please allocate all 100 points according to each category to denote its impact on your organization's overall state of IT security today. The sum of all points must be 100.

Six mega trend categories	Allocate all 100 points	Priority rank
Disruptive technologies	24	1
Cyber crime	13	5
Government and regulations	11	6
Human factors	17	3
Resource constraints	21	2
Organizational factors	14	4
Total points	100	

Q8b. Please allocate points to each mega trend category to denote its impact on your organization's overall state of IT security in the next 12 to 24 months. Remember the sum of all points must be 100.

Six mega trend categories	Allocate all 100 points	Priority rank
Disruptive technologies	21	1
Cyber crime	20	2
Government and regulations	15	4
Human factors	13	5
Resource constraints	19	3
Organizational factors	12	6
Total points	100	

Part 3. Other questions.

Q9. Following are security technologies that may be deployed by your organization. Please rate the relative impact that each technology has (or will have) on maintaining or improving the state IT security within your organization **over the next 12 to 24 months**. Your best guess is welcome.	Impact on maintaining or improving the organization's security posture			
Enabling security technologies	Very significant	Significant	Not significant	No impact
Access governance systems	47%	30%	16%	7%
Anti-virus & anti-malware	46%	29%	17%	8%
Automated policy generation	11%	24%	34%	31%
Configuration & log management	29%	22%	41%	8%
Data loss prevention (DLP)	32%	38%	17%	13%
Database scanning and monitoring	28%	22%	41%	9%
Device anti-theft solutions	24%	22%	45%	9%
Encryption for data at rest	24%	53%	16%	7%
Encryption for data in motion	25%	48%	20%	7%
Endpoint security management	37%	32%	24%	7%
ID & credentialing system	13%	21%	31%	35%
Identity & access management	41%	34%	13%	12%
Intrusion detection or prevention	44%	27%	25%	4%
Next generation firewalls (NGFW)	24%	34%	24%	18%
Perimeter or location surveillance	25%	21%	36%	18%
SIEM and security intelligence	43%	42%	11%	4%
Tokenization tools	38%	21%	24%	17%
URL or content filtering	22%	27%	31%	20%
Virtual private network (VPN)	29%	31%	31%	9%
Web application firewalls (WAF)	39%	34%	21%	6%

Q10. Who in your organization is most responsible for ensuring information security requirements are met? Please select one response.	Pct%
No one person	39%
CIO	27%
CTO	9%
IT security leader (CISO)	20%
Compliance	3%
Internal audit	0%
Legal	2%
Other (please specify)	0%
Total	100%

Q11. To the best of your knowledge, is your organization compliant with all applicable requirements including regulations for IT security?	Pct%
Yes, for all applications and databases throughout the enterprise	25%
Yes, for most applications and databases	34%
Yes, but only for some applications and databases	23%
No	18%
Unsure	100%

Q12. Following are three scenarios about cyber attacks that may significantly impact your organization. Please rate each scenario using the five-point likelihood scale provided below. Imminent, very likely, likely, not likely & unsure.	Imminent	Very likely	Likely	Combined
Q12a. A cyber attack will significantly disrupt the nation's critical infrastructure	25%	35%	17%	77%
Q12b. A cyber attack will significantly disrupt the critical infrastructure of an organization in your industry	25%	40%	13%	78%
Q12c. A cyber attack will significant disrupt one or more mission critical applications with your organization	11%	28%	11%	50%

Q13. In your opinion, please choose the one statement that best describes your belief about the future state of IT security in the next 12 to 24 years. Your best guess is welcome.	Pct%
My organization's security posture will improve over the next 12 to 24 months	11%
My organization's security posture will stay at about the same level over the next 12 to 24 months	62%
My organization's security posture will decline over the next 12 to 24 months	27%
Total	100%

Part 4. Organizational characteristics

D1. What organizational level best describes your current position?	Pct%
Senior Executive	1%
Vice President	2%
Director	26%
Manager	20%
Supervisor	18%
Technician	26%
Associate/Staff	2%
Consultant	3%
Other (please specify)	2%
Total	100%

D2. Check the **Primary Person** you or your supervisor reports to within your organization.	Pct%
Business owner	7%
CEO/President	2%
Chief Financial Officer	2%
Chief Information Officer	52%
Compliance Officer	3%
Chief Privacy Officer	1%
Director of Internal Audit	1%
General Counsel	3%
Chief Technology Officer	9%
Human Resources VP	1%
CSO or CISO	13%
Chief Risk Officer	6%
Other (please specify)	0%
Total	100%

D3. Check the country or U.S. region where your company's **primary** headquarters is located.	Pct%
US Northeast	13%
US Mid-Atlantic	12%
US Midwest	9%
US Southeast	9%
US Southwest	8%
US Pacific/west	12%
Canada	11%
Europe	9%
Middle east & Africa	3%
Asia-Pacific	8%
Latin America	6%
Total	100%

D4. Experience	Mean	Median
D4a. Total years of relevant experience	10.46	11.0
D4b. Total years in IT and/or IT security field	9.34	9.5
D4c. Total years in present position	5.03	5.0

D5. What industry best describes your organization's industry concentration or focus?	Pct%
Agriculture	1%
Communications	3%
Defense	3%
Education & research	3%
Energy	2%
Entertainment	4%
Financial services	20%
Health & pharmaceutical	10%
Hospitality & leisure	5%
Industrial	4%
Public services	14%
Retail, conventional	5%
Retail, Internet	5%
Services	9%
Technology & software	8%
Transportation	2%
Other (please specify)	2%
Total	100%

D6. What is the worldwide headcount of your organization?	Pct%
Less than 100	9%
100 to 500	11%
501 to 5,000	11%
5,001 to 10,000	28%
10,001 to 25,000	26%
More than 25,000	15%
Total	100%

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.