

Cyber Security Mega Trends

Study of IT leaders in the U.S. federal government

Sponsored by CA

Independently conducted by Ponemon Institute LLC

Publication Date: November 18, 2009

Cyber Security Mega Trends Study

Prepared by Dr. Larry Ponemon, November 18, 2009

I. Executive Summary

What are the biggest security threats to U.S. federal organizations in terms of sensitive and confidential data, core information systems and critical infrastructure over the next few years? According to 217 senior-level IT executives located in various federal organizations, significant areas of information security risks include rapid growth in unstructured data assets, mobility of the federal workforce, cyber terrorism, outsourcing, cloud computing and much more.

The *Cyber Security Mega Trends Study* was conducted by Ponemon Institute and sponsored by CA to better understand if certain publicized IT security risks are, or should be, more or less of a concern for organizations in the federal sector. We believe the results of our study will be helpful to organizations struggling to understand how they should allocate resources to help ensure their information systems are adequately protected.

Based upon in-depth interviews with IT security experts and prior Institute research, we focus on 10 cyber security mega trends in this study. Each mega trend is believed to affect significantly an organization's security ecosystem.

- **Cloud computing** – refers to distributed computing solutions that can be owned by third-parties on data center locations outside the organization's IT infrastructure.
- **Virtualization** – refers to enabling technologies that allows end-users to access multiple secure networks from a single computer, wherein the PC or laptop essentially acts as the authenticating device.
- **Mobility** – refers to a workforce with access to information no matter where they work or travel and wherein employees can use mobile devices when they travel or work at home: laptops, smart phones, PDAs, memory sticks and more.
- **Cyber crime** – usually describes criminal activity in which the computer or network is an essential part of the illegal criminal activity. This term also is used to include attacks in which computers or botnets are used to enable illicit activity such as data theft or denial of service attacks.
- **Cyber terrorism** – is a specific form of cyber crime in which the end goal is to disrupt or harm a targeted country or region of the world. This term also is used to describe attacks that attempt to steal national secrets including information that minimizes a nation's defense or economic posture.
- **Open source** – is computer software for which the source code and certain other rights normally reserved for copyright holders are provided under a software license that is in the public domain. This permits users to change, improve the software, and redistribute software in modified or unmodified forms.
- **Data breach** – is defined as the loss or theft of information about people and households. A majority of U.S. states now require organizations to notify individuals when their information is lost or stolen.
- **Unstructured data** – is electronic information on file servers and other storage devices that are not stored in a database or other structured formats, usually resulting from workplace collaboration tools such as SharePoint.
- **Outsourcing** – usually pertains to the transfer of sensitive and confidential information to third parties for data processing or other activities. Outsourcing is done to reduce processing costs and improve operating efficiencies.
- **Web 2.0** – refers to a plethora of Internet tools that enhance information sharing and collaboration among individuals. These concepts have led to the evolution of web-based communities and hosted services, such as social networking, social messaging, wikis and blogs.

Utilizing a web-based survey, we asked respondents to answer specific questions about each one of the 10 mega trends mentioned. These questions are as follows:

- Does the given mega trend represent a significant security risk for respondents' organizations?
- Is the mega trend likely to occur and is it projected to have a severe impact on the organization?
- Are these security threats believed to be decreasing or increasing over time?
- What are the most significant consequences associated with each of these threats?
- How confident are respondents about their organization's ability to mitigate or curtail a specific security risk?

In summary, the most significant threats to confidential data, proprietary government systems, and the nation's critical infrastructure according to respondents are as follows:

- 79 percent of respondents see the rise in the use of collaboration tools as significantly increasing the storage of unstructured data sources that may contain confidential or sensitive information that is not adequately protected or secured.
- 71 percent of respondents believe that cyber terrorism is on the rise, and this trend poses a very serious threat to the protection of proprietary systems as well as our nation's critical infrastructure.
- 63 percent of respondents see the mobility of the government workforce as contributing significantly to endpoint security risks as a result of insecure mobile data-bearing devices that are susceptible to malware infections as well as insecure wireless connectivity.
- 52 percent of respondents say that Web 2.0 applications such as social networking, social messaging, blogging and wikis contribute to the leakage of confidential or sensitive information as well as susceptibility to malware and botnet attacks.

Other mega trends that appear to exacerbate security risks in the U.S. federal government according to respondents include: a continued rash of data breach incidents (40 percent), virtualization technologies (44 percent), rise in the usage of cloud computing resources and applications (39 percent), outsourcing to insecure third-parties (34 percent), and use of open source applications (18 percent).

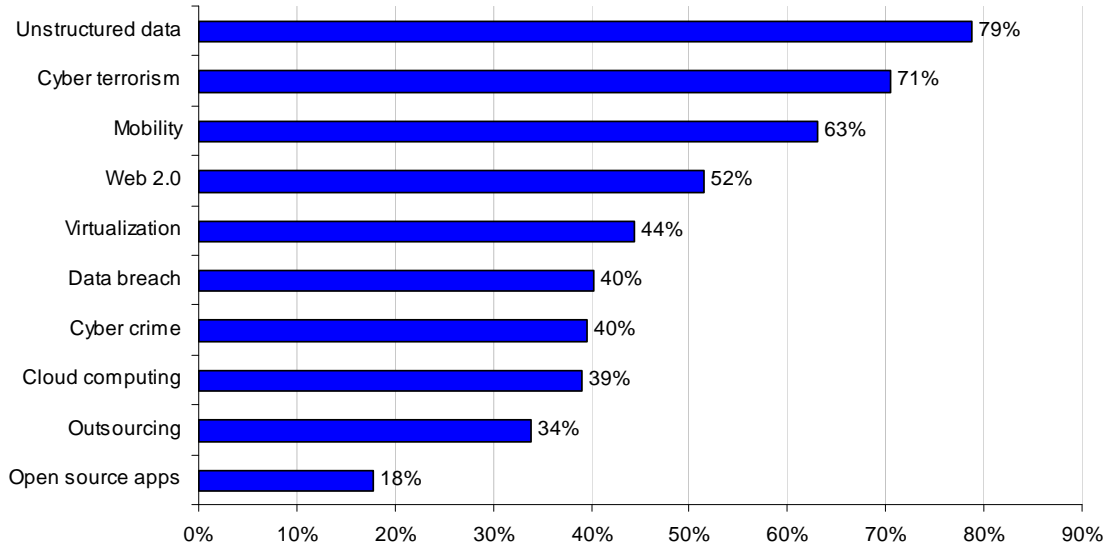
Thirty-five percent of respondents said their department's networks had been victimized by an unauthorized infiltrator one or more time over the past 12 months. Another 38 percent of respondents were unsure about possible unauthorized intrusions.

II. Findings about Mega Trends

This section provides key findings of our survey research. Please note that our findings are reported in bar chart or line graph format. The actual data utilized in each figure and referenced in the paper can be found in the percentage frequency tables attached as Appendix I to this report.

Bar Chart 1 shows the percentage frequency of respondents who report an increased security risk within their organization resulting from a given mega trend. The rise in unstructured data (79 percent), cyber terrorism (71 percent), mobility (63 percent) and Web 2.0 (52 percent) represent the mega trends considered to exacerbate information security risk the most within respondents' organizations.

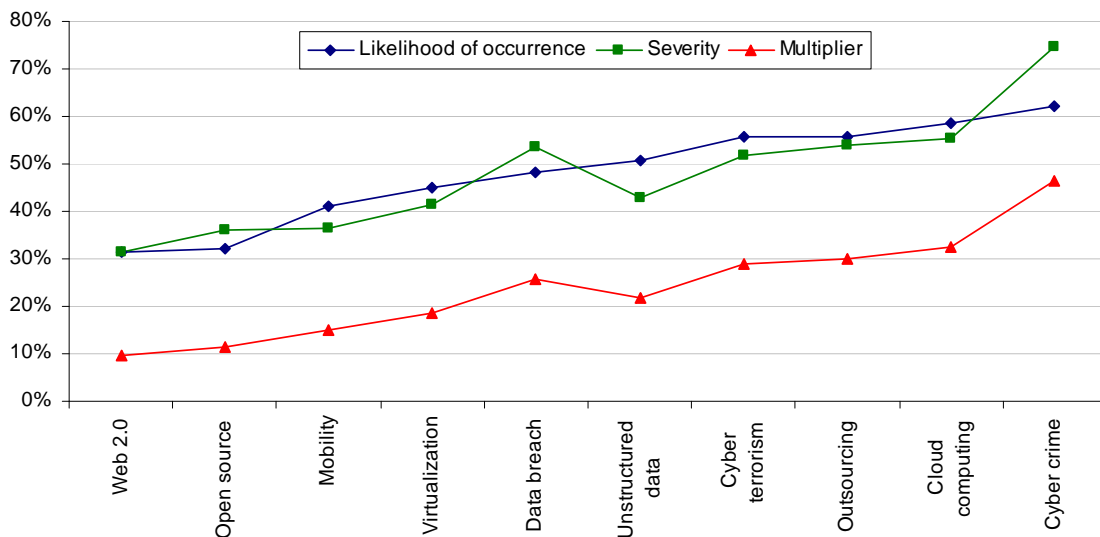
Bar Chart 1
Do you believe that each mega trend increases security risk within your organization?
 Percentage yes response.



Our survey also asked respondents to rate the likelihood that a given mega trend will cause a security incident (using a five-point scale from very high to very low) and the severity of this incident (using a five-point scale from very significant to negligible). Drawing from these two ratings, we compute a risk multiplier defined as {likelihood x severity}.

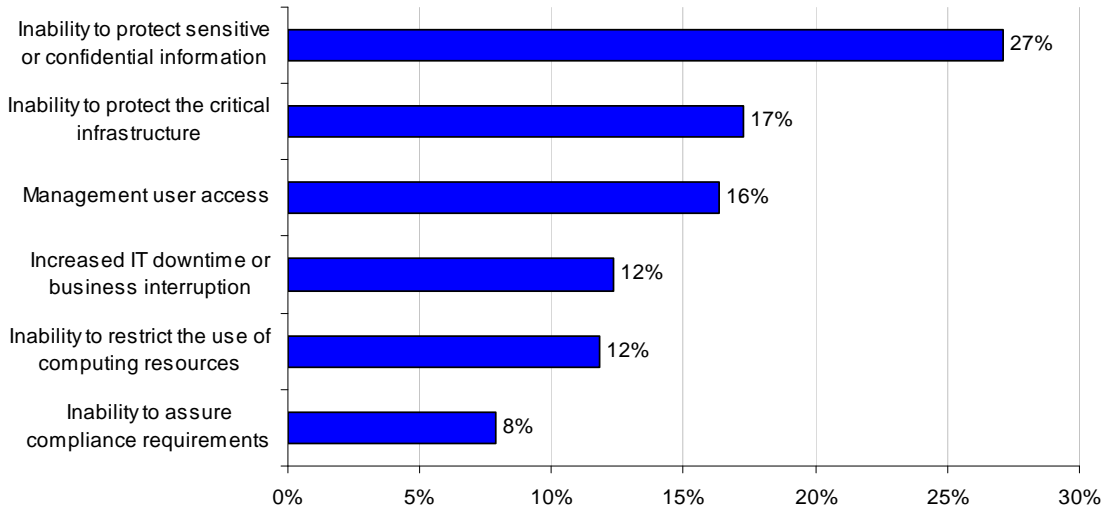
Line Graph 1 reports the likelihood of occurrence, severity, and the resulting risk multiplier. As shown, cyber crime, cloud computing, outsourcing, cyber terrorism, and unstructured data are the mega trends that generate the highest risk multipliers.

Line Graph 1
Likelihood of occurrence, severity and risk resulting from mega trends
 Percentage very high and high likelihood and percentage very significant and significant severity



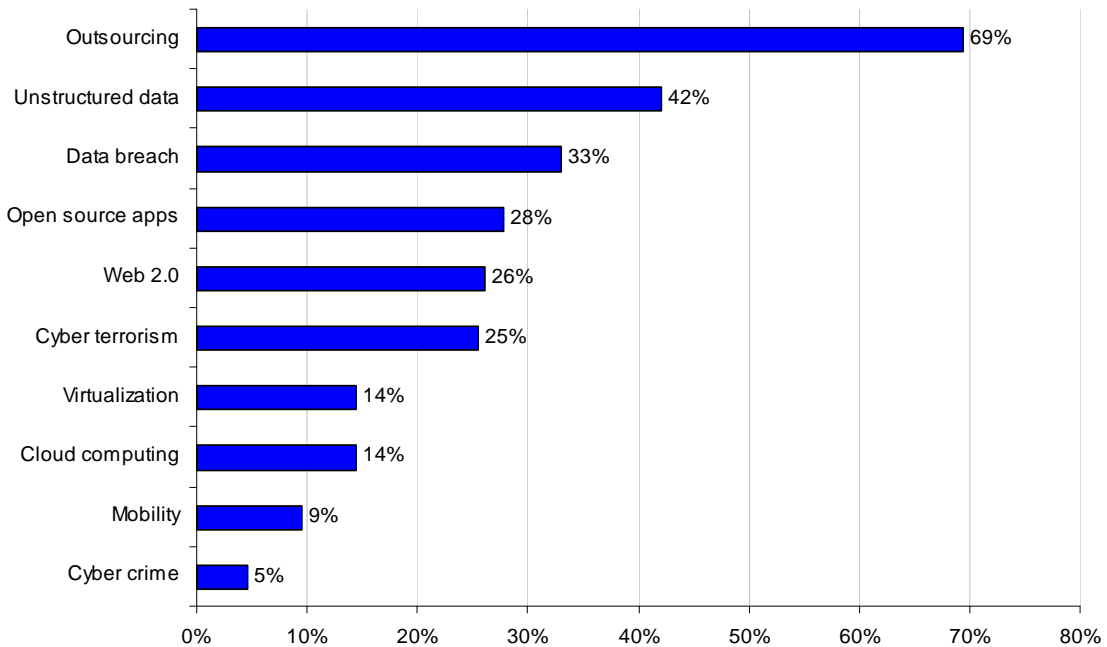
Bar Chart 2 reports a consolidated view of the most significant security threats faced by federal organizations. As can be seen, the inability to protect sensitive or confidential information is viewed as the most serious security threat, followed by the inability to protect the critical infrastructure and the management of user access to data, systems and IT infrastructure.

Bar Chart 2
What are the most significant security threats to your organization today?
 Percentages are aggregated for all mega trends.



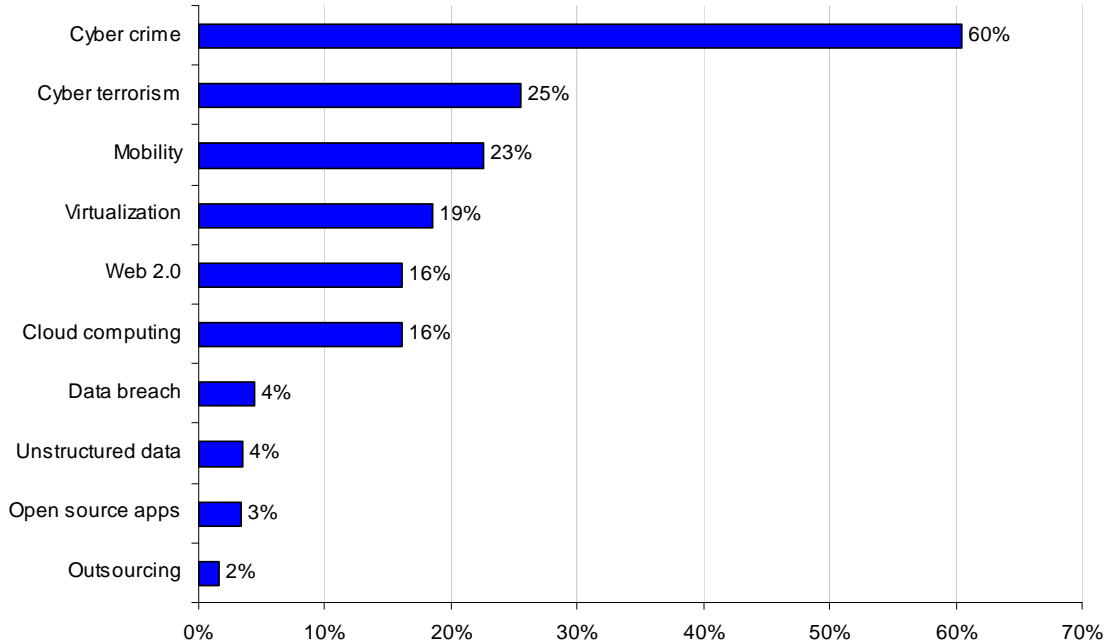
Bar Chart 3 reports that outsourcing and unstructured data are viewed as the top two root causes to the risk of insecure sensitive and confidential information among respondents.

Bar Chart 3
Inability to protect sensitive or confidential information
 What are the most significant security threats to your organization today?



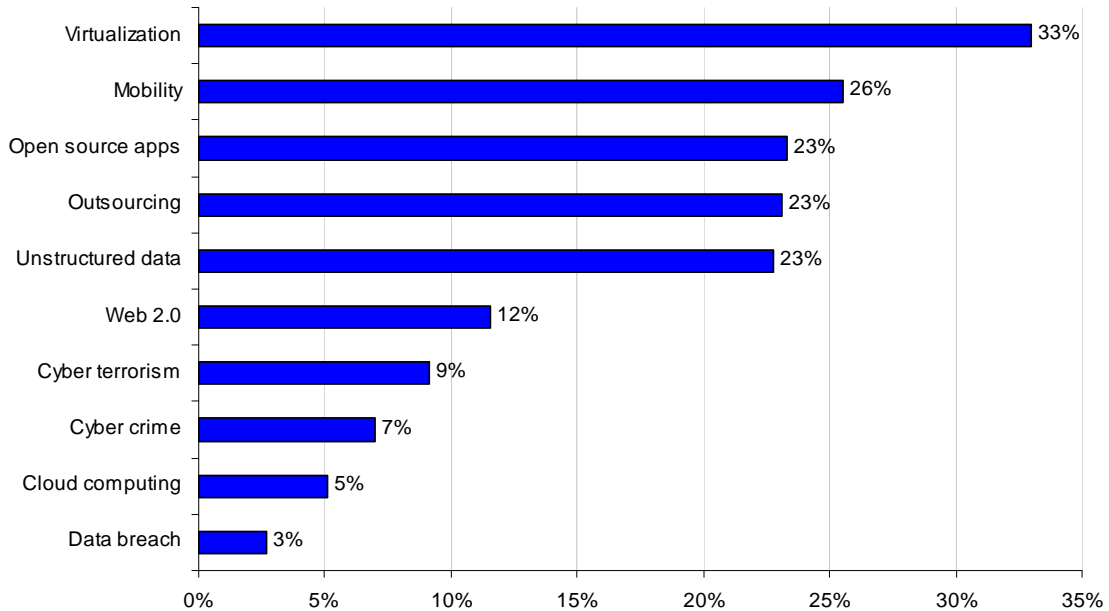
Bar Chart 4 shows cyber crime, cyber terrorism and mobility as the root causes to the risk of an insecure critical infrastructure.

Bar Chart 4
Inability to protect the critical infrastructure
 What are the most significant security threats to your organization today?



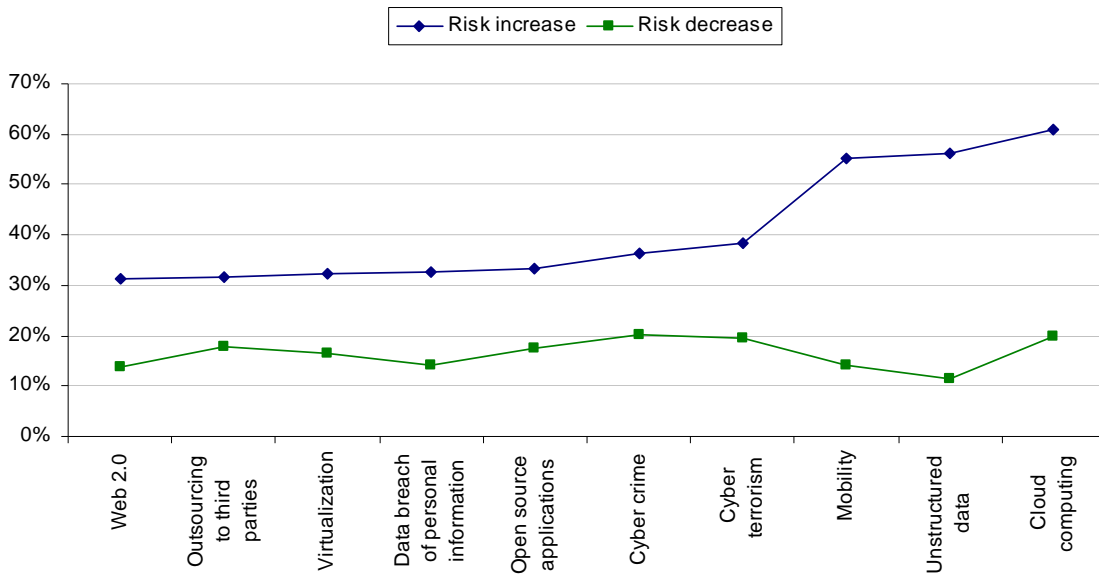
Bar Chart 5 reports virtualization and mobility as the two root causes to the risk of an organization's inability to ensure secure user access to proprietary systems, networks and data.

Bar Chart 5
Management of users' and their access to data, systems and IT infrastructure
 What are the most significant security threats to your organization today?



Line Graph 2 shows two sets of views about whether security risk associated with a given mega trend will increase or decrease within their organizations over time. As shown, 63 percent of respondents believe the security risk resulting from cloud computing will increase – as compared to only 20 percent of respondents who believe security risk from cloud computing will decrease over the next two to three years. With respect to unstructured data, 56 percent of respondents see this security risk as increasing, while only 12 percent see this risk as decreasing over time.

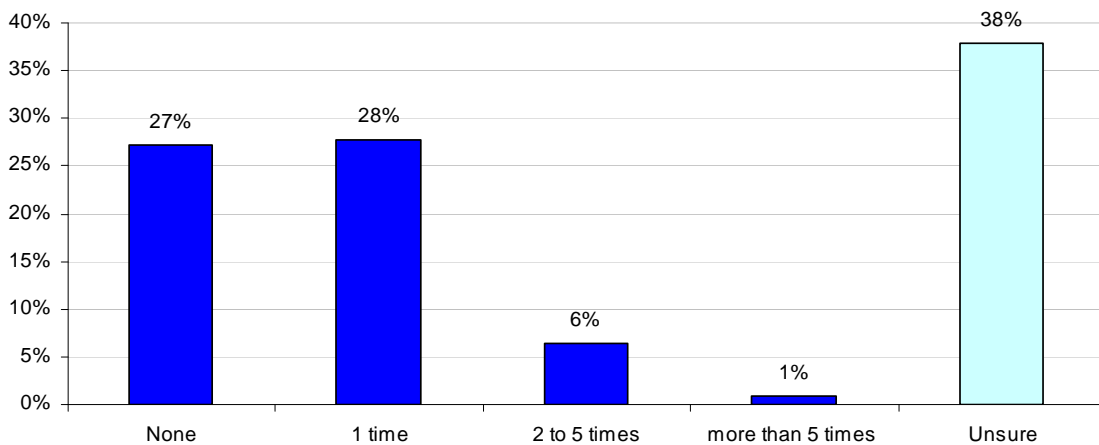
Line Graph 2
Is the mega trend's impact on risk increasing or decreasing over the next 2 to 3 years



III. Other Findings

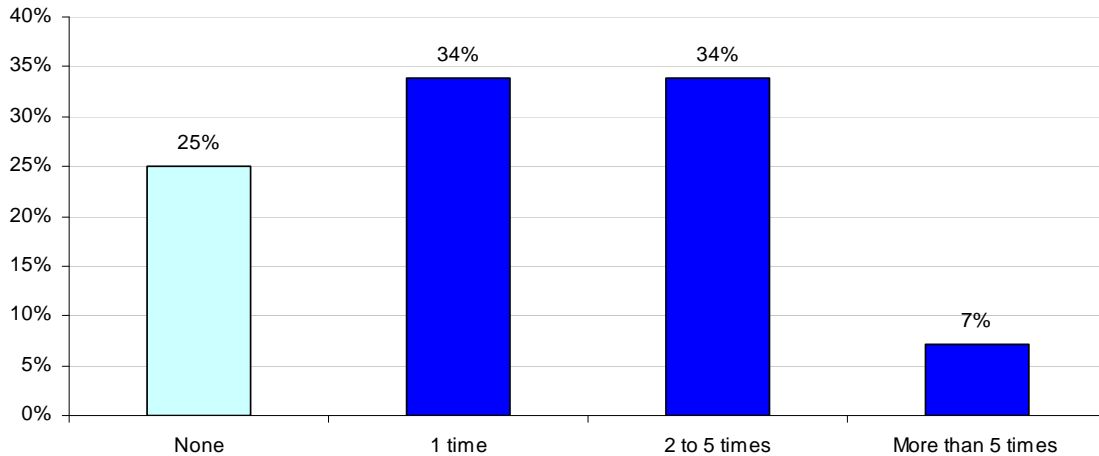
Bar Chart 6 reports the frequency of cyber attacks that infiltrated respondents' organizations over the past year. As can be seen, a majority of respondents either acknowledge one or more attacks (35 percent) or are unsure such an attack occurred (38 percent).

Bar Chart 6
How frequently has your organization experienced cyber crime that infiltrated your organization's network or enterprise system in the past 12 months?



Bar Chart 7 reports the frequency of data breach incidents occurring in respondents' organizations. As shown, more than 75 percent of respondents experienced one or more data breach incidents sometime over the past year.

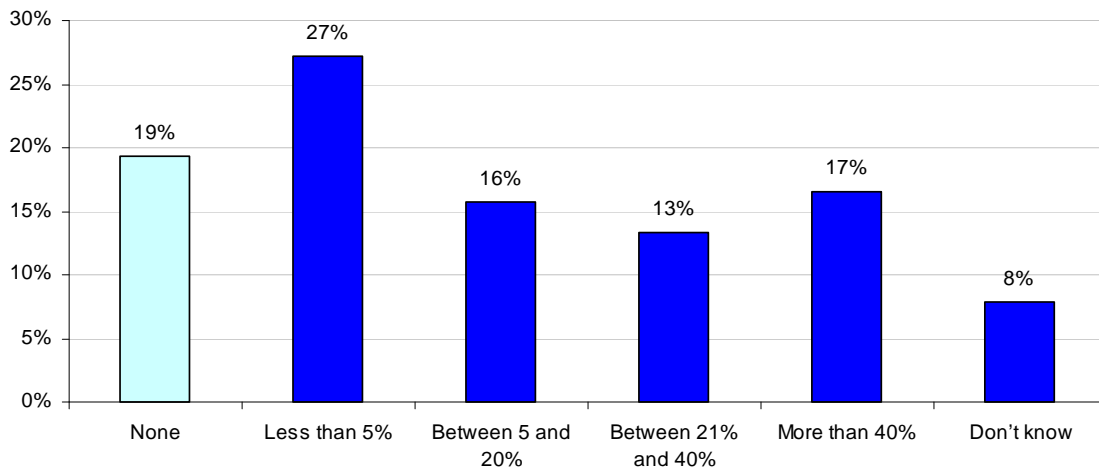
Bar Chart 7
How frequently has your organization experienced a data breach in the past 12 months?



In comparing Bar Charts 6 and 7, the frequency of a data breach occurring two or more times in a year is 41 percent. Two or more cyber crime attacks that infiltrate the organization's network is 7 percent in a year. This suggests that most data breach incidents are not due to malicious or external attacks, but rather from insider negligence, system glitches and third-party flubs. This result is supported by earlier research.¹

Bar Chart 8 reports the estimated percentage of unstructured data that resides within respondents' organizations (as a surrogate for data clutter). As shown, 38 percent of respondents say the percentage of unstructured data to total data stores exceeds 20 percent.

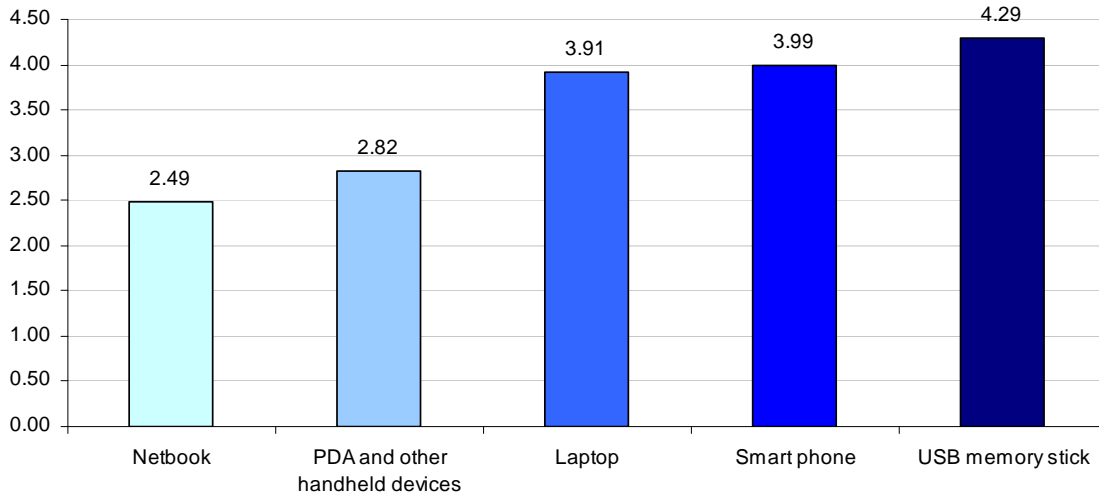
Bar Chart 8
What percentage of your organization's sensitive or confidential information resides on file servers or other storage devices in the form of unstructured data?



¹ See [Fourth Annual Cost of Data Breach](#), Ponemon Institute (January 2009).

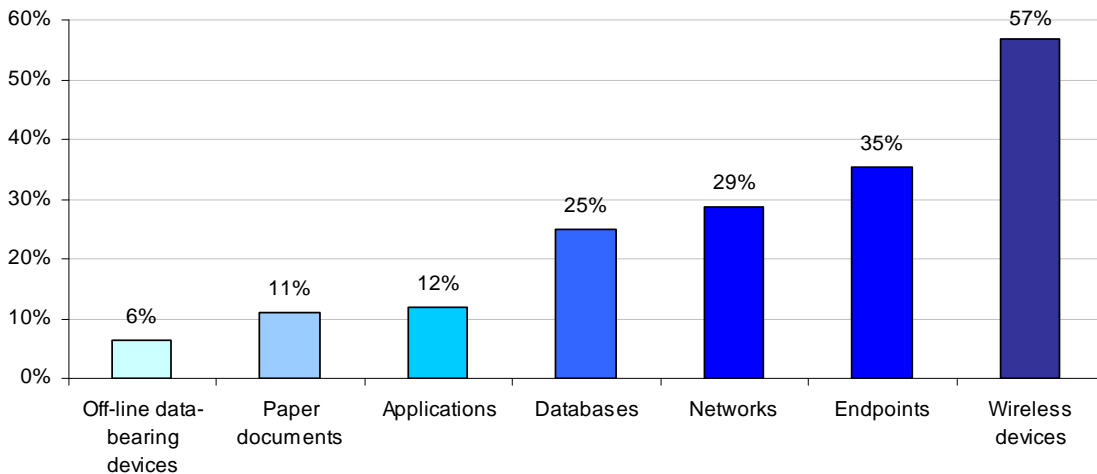
Bar Chart 9 reports the average rank order for five devices in terms of security risk to respondents' organizations. The most risky mobile device is a USB memory stick, followed by smart phones and laptops. Netbooks are the least risky, according to respondents.

Bar Chart 9
What mobile devices present the greatest security risk to you organization?
 Rank from 5 = highest risk to 1 = lowest risk.



Bar Chart 10 reports the security threat vector perceived by respondents as the most serious. As reported, wireless devices and endpoints present the most serious threats for participating organizations.

Bar Chart 10
Where are the most serious threats located?
 Top two choices

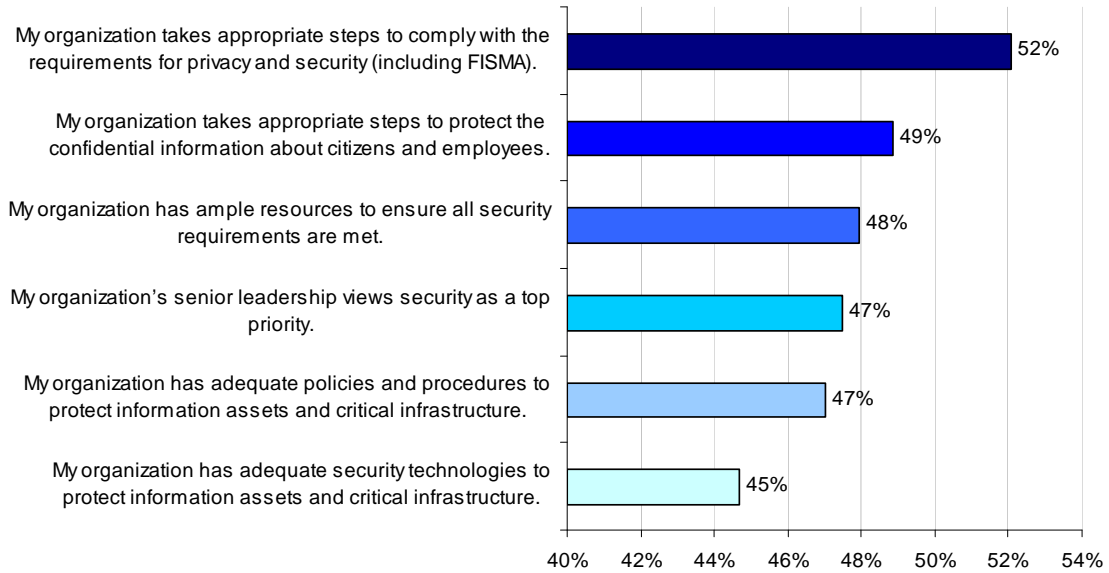


Bar Chart 11 reports respondents' views about the security ecosystem within their organizations. Six attributions or statements were used to capture each respondent's perceptions about his or her organization.

Fifty-two percent believe their organizations are taking appropriate steps to comply with FISMA. Less than half of all respondents believe their organizations are: taking appropriate steps to

protect information, have ample resources to ensure all security requirements, have the support of senior leadership, have adequate policies and procedures, and have adequate security enabling technologies.

Bar Chart 11
Six attributions about the security ecosystem within respondents' organizations
 Percentage strongly agree and agree responses (combined)



IV. Methods

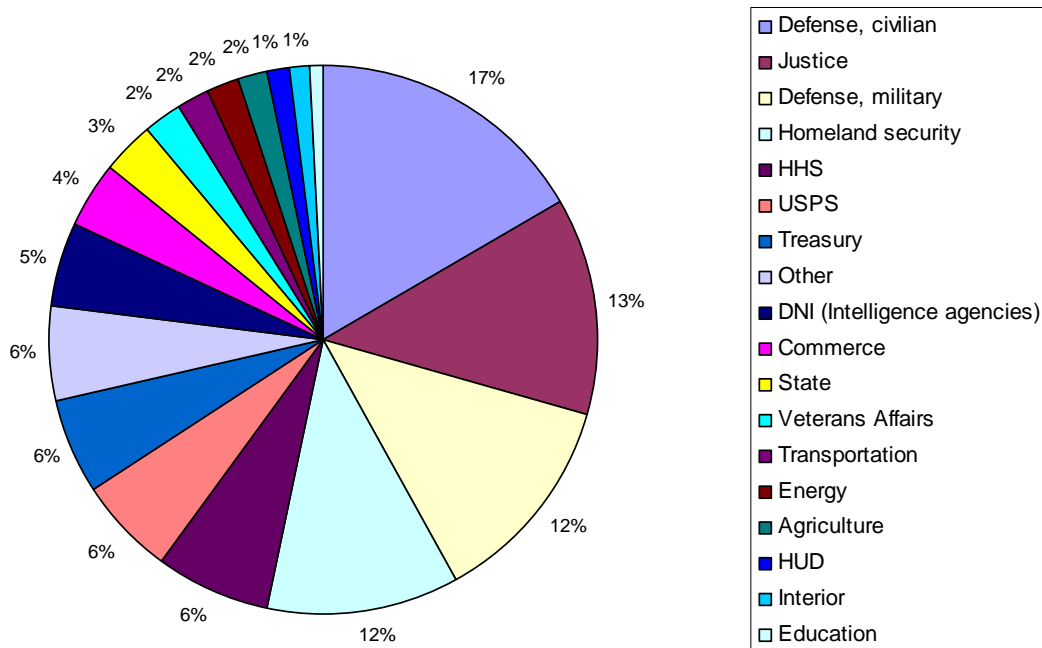
An expert panel of 4,861 adult-aged individuals who reside within the United States was used to recruit and select participants to this survey. Our expert panel was built from proprietary a list of senior-level IT and security leaders in the U.S. federal government.

Table 1 Survey response	Freq.
Sampling frame	4,861
Invitations sent	4,522
Bounce-back	893
Net responses	261
Rejections	44
Usable sample	217
Response rate	4.5%

In total, 261 respondents completed the survey. Of the returned instruments, 44 surveys failed reliability checks. A total of 217 surveys were used as our final sample, which represents a 4.5 percent net response rate.² Ninety percent of respondents completed all survey items within 26 minutes. Two versions of the instrument were used (one with additional description about the inherent security risks for each mega trend). Between-sample tests did not reveal any significant differences between these two groups and, hence, results are combined in our analysis.

Pie Chart 1 shows the U.S. federal organizations where respondents are located. As can be seen, Defense, Justice, Homeland Security, and Health & Human Services contain the largest proportion of respondents.

**Pie Chart 1
Distribution of respondents by federal department or organization**



² Three screening questions were used to the refine sample by position level and organizational size.

Table 2 reports the organizational level of respondents. As can be seen, 53 percent of respondents are at or above the director level. The average overall experience level of respondents is 16.7 years (median is 15 years).

Table 2 Respondents' organizational level	Freq.	Pct%
Executive	27	12%
Director	89	41%
Manager	52	24%
Supervisor	17	8%
Other	32	15%
Total	217	100%

Table 3 reports the respondent's reporting channel or chain of command. As shown, the majority of respondents report to either the IT leader (CIO) or a department head.

Table 3 Respondents' chain of command	Freq.	Pct%
Department or agency head	30	14%
IT leader or CIO	103	47%
CTO	42	19%
CSO/CISO	10	5%
Compliance leader	5	2%
Human resource leader	4	2%
CPO	2	1%
Other	21	10%
	217	100%

Table 4 reports the respondent organization's global headcount. The majority of respondents work in federal government organizations with more than 25,000 employees.

Table 4 Respondents' organizations headcount	Freq.	Pct%
1,001 to 5,000 people	36	17%
5,001 to 25,000 people	24	11%
25,001 to 75,000 people	63	29%
More than 75,000 people	94	43%
	217	100%

V, 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 reasonable 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 IT or IT security leaders in the federal government. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a short holdout period. 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 a truthful response.

VI. Implications for U.S. federal organizations

Federal organizations face a plethora of security threats to their data, systems and critical infrastructure. We asked senior-level IT practitioners to rate those mega trends they believe present a high or very high security risk to their organizations. Based on the inherent risks associated with each mega trend, we believe those responsible for security in the federal government should consider the following practical solutions:

- Create and enforce policies that ensure access to confidential data and IT assets is restricted to authorized parties only.
- Secure corporate endpoints to protect against data leakage and malware.
- Make sure third parties, including cloud computing vendors, who have access to your sensitive and confidential information take appropriate security precautions.
- Train employees and contractors to understand their responsibility in the protection of data and IT assets.
- Ensure mobile devices are encrypted and employees understand the organizations' policies with respect to downloading sensitive information and working remotely.
- Understand precautions that should be taken when transporting sensitive information on portable devices – especially USB memory sticks, smart phones, and laptops.

We believe the findings from this study provide government organizations with guidance on which threats are more critical than others to address. IT operations and IT security professionals identified cloud computing, outsourcing of sensitive information to third parties, external threat of organized cyber criminal syndicates, cyber terrorism, and a mobile workforce.

Appendix 1: Detailed Survey Results

The following tables summarize the partial results of a survey of 217 IT and IT security executives in the U.S. federal government. Fieldwork was completed over a four-day period ending on November 6, 2009.

I. Your role		
D1. What organizational level best describes your current position?	Freq.	Pct%
Executive	27	12%
Director	89	41%
Manager	52	24%
Supervisor	17	8%
Other	32	15%
	217	100%
D2. Where does your department report within the organization?	Freq.	Pct%
Department or agency head	30	14%
IT leader or CIO	103	47%
CTO	42	19%
CSO/CISO	10	5%
Compliance leader	5	2%
Human resource leader	4	2%
CPO	2	1%
Other	21	10%
	217	100%
	Mean	Median
D3a. Overall experience	16.7	15.0
D3b. IT or security experience	7.6	7.0
D3c. Years in current position	7.5	7.0
D4. How many network connections (nodes) do you have in your organization's IT environment?	Freq.	Pct%
Less than 50	2	1%
50 to 250	12	6%
250 to 500	23	11%
500 to 1,000	48	22%
1,000 to 2,500	73	34%
More than 2,500	59	27%
	217	100%
D5. What is the approximate size of your IT department in terms of full-time equivalent (FTE) headcount?	Freq.	Pct%
101 to 500 people	24	11%
501 to 1,000 people	36	17%
1,001 to 5,000 people	67	31%
Over 5,000 people	90	41%
	217	100%
D6. What is the headcount of your organization?	Freq.	Pct%
1,001 to 5,000 people	36	17%
5,001 to 25,000 people	24	11%
25,001 to 75,000 people	63	29%
More than 75,000 people	94	43%
	217	100%

D7. What U.S. federal government entity best describes your organization?	Freq.	Pct%
Defense, civilian	36	17%
Defense, military	27	12%
Justice	28	13%
HHS	14	6%
Homeland security	25	12%
Treasury	12	6%
State	7	3%
USPS	13	6%
DNI (Intelligence agencies)	11	5%
Commerce	8	4%
Transportation	4	2%
Veterans Affairs	5	2%
Interior	2	1%
Energy	4	2%
HUD	3	1%
Education	2	1%
Agriculture	4	2%
Other	12	6%
	217	100%

1. Cloud computing		
Q1a. How familiar are you with cloud computing?	Freq.	Pct%
Very familiar	54	25%
Familiar	111	51%
Not familiar	32	15%
No knowledge	20	9%
	217	100%
Q1b. Does your IT organization utilize cloud computing resources?	Freq.	Pct%
Yes	118	54%
No	63	29%
Unsure	36	17%
	217	100%
Q1c. If yes, do you believe that cloud computing increases security risk within your organization?	Freq.	Pct%
Yes	46	39%
No	42	36%
Unsure	30	25%
	118	100%
Q1d. If yes, what are the most significant security threats to your organization caused by cloud computing? FIRST CHOICE.	Freq.	Pct%
Inability to protect sensitive or confidential information	30	25%
Inability to restrict or limit use of computing resources or applications	21	18%
Inability to assure regulatory compliance requirements	11	9%
Increased cyber crime attacks	5	4%
Inability to protect the critical infrastructure	19	16%
Increased IT downtime or business interruption	6	5%
Management of users' and their access to cloud resources	23	19%
Other (please specify)	3	3%
	118	100%
Q1d. If yes, what are the most significant security threats to your organization caused by cloud computing? SECOND CHOICE.	Freq.	Pct%
Inability to protect sensitive or confidential information	36	31%
Inability to restrict or limit use of computing resources or applications	43	37%
Inability to assure regulatory compliance requirements	6	5%
Increased cyber crime attacks	0	0%
Inability to protect the critical infrastructure	15	13%
Increased IT downtime or business interruption	0	0%
Management of users' and their access to cloud resources	15	13%
Other (please specify)	0	0%
	115	100%
Q1e. Please rate the likelihood of occurrence that one or more of the above mentioned security threats will happen because of cloud computing sometime in the next 12 months.	Freq.	Pct%
Very high	59	27%
High	68	31%
Moderate	44	20%
Low	26	12%
Very low	20	9%
	217	100%

Q1f. Please rate the severity of the above mentioned security threats in terms of negative impact or harm to your organization's operations or mission.	Freq.	Pct%
Very significant	52	24%
Significant	67	31%
Moderate	59	27%
Insignificant	17	8%
Negligible	22	10%
	217	100%

2. Virtualization		
Q2a. How familiar are you with virtualization?	Freq.	Pct%
Very familiar	63	29%
Familiar	95	44%
Not familiar	38	18%
No knowledge	21	10%
	217	100%
Q2b. Does your IT organization utilize virtualization technologies?	Freq.	Pct%
Yes	97	45%
No	73	34%
Unsure	47	22%
	217	100%
Q2c. If yes, do you believe that virtualization increases security risk within your organization?	Freq.	Pct%
Yes	43	44%
No	35	36%
Unsure	19	20%
	97	100%
Q2d. If yes, what are the most significant security threats to your organization caused by virtualization? FIRST CHOICE.	Freq.	Pct%
Inability to protect sensitive or confidential information	14	14%
Inability to restrict or limit use of computing resources or applications	21	22%
Inability to assure regulatory compliance requirements	3	3%
Increased cyber crime attacks	3	3%
Inability to protect the critical infrastructure	18	19%
Management of users' and their access to virtualized environments and applications	32	33%
Increased IT downtime and business interruption	3	3%
Other	3	3%
	97	100%
Q2d. If yes, what are the most significant security threats to your organization caused by virtualization? SECOND CHOICE.	Freq.	Pct%
Inability to protect sensitive or confidential information	10	11%
Inability to restrict or limit use of computing resources or applications	10	11%
Inability to assure regulatory compliance requirements	8	9%
Increased cyber crime attacks	13	14%
Inability to protect the critical infrastructure	22	23%
Management of users' and their access to virtualized environments and applications	29	31%
Increased IT downtime and business interruption	2	2%
Other	0	0%
	94	100%
Q2e. Please rate the likelihood of occurrence that one or more of the above mentioned security threats will happen because of virtualization sometime in the next 12 months.	Freq.	Pct%
Very high	52	24%
High	46	21%
Moderate	32	15%
Low	33	15%
Very low	54	25%
	217	100%

Q2f. Please rate the severity of the above mentioned security threats in terms of negative impact or harm to your organization's operations or mission.	Freq.	Pct%
Very significant	44	20%
Significant	57	26%
Moderate	41	19%
Insignificant	34	16%
Negligible	41	19%
	217	100%

3. Mobility		
Q3a. Approximately, what percent of your organization's employees utilize one or more mobile devices that connect to your organization's IT platform or enterprise system (including access to email client)?	Freq.	Pct%
None	17	8%
Less than 5%	22	10%
Between 5 to 10%	21	10%
Between 10 to 20%	18	8%
Between 20 to 30%	29	13%
Between 30 to 40%	43	20%
Between 40 to 50%	23	11%
More than 50%	23	11%
Don't know	21	10%
	217	100%
Q3b. Do you believe that mobility increases security risk within your organization?	Freq.	Pct%
Yes	137	63%
No	39	18%
Unsure	41	19%
	217	100%
Q3c. If yes, what are the most significant security threats to your organization caused by mobility? FIRST CHOICE.	Freq.	Pct%
Inability to protect sensitive or confidential information.	13	9%
Inability to restrict or limit use of computing resources or applications	15	11%
Inability to assure regulatory compliance requirements	15	11%
Increased cyber crime attacks	27	20%
Inability to protect the critical infrastructure	31	23%
Management of users' and their access to the mobile environment	35	26%
Increased IT downtime and business interruption	1	1%
Other	0	0%
	137	100%
Q3c. If yes, what are the most significant security threats to your organization caused by mobility? SECOND CHOICE.	Freq.	Pct%
Inability to protect sensitive or confidential information	20	15%
Inability to restrict or limit use of computing resources or applications	24	18%
Inability to assure regulatory compliance requirements	22	16%
Increased cyber crime attacks	21	16%
Inability to protect the critical infrastructure	3	2%
Management of users' and their access to the mobile environment	27	20%
Increased IT downtime and business interruption	17	13%
Other	0	0%
	134	100%

Q3d. Please rate the likelihood of occurrence that one or more of the above mentioned security threats will happen because of mobility sometime in the next 12 months.	Freq.	Pct%
Very high	42	19%
High	47	22%
Moderate	53	24%
Low	27	12%
Very low	48	22%
	217	100%
Q3e. Please rate the severity of the above mentioned security threat in terms of negative impact or harm to your organization's operations or mission.	Freq.	Pct%
Very significant	32	15%
Significant	73	
Moderate	38	18%
Insignificant	31	14%
Negligible	43	20%
	217	100%
Q3f. What mobile devices present the greatest security risk to your organization? Please rank from 1=highest risk to 5=lowest risk.	Avg rank	Order
Laptop	2.09	3
PDA and other handheld devices	3.18	4
Smart phone	2.01	2
USB memory stick	1.71	1
Netbook	3.51	5

4. Cyber crime		
Q4a. How familiar are you with cyber crime?	Freq.	Pct%
Very familiar	51	24%
Familiar	45	21%
Not familiar	72	33%
No knowledge	49	23%
	217	100%
Q4b. Approximately, how frequently has your organization experienced cyber crime attacks that infiltrated your organization's network or enterprise system in the past 12 months?	Freq.	Pct%
None	63	29%
1 to 10 times	86	40%
11 to 50 times	25	12%
51 to 100 times	24	11%
More than 100 times	19	9%
	217	100%
Q4c. If yes, do you believe that cyber crime is an increasing security risk within your organization?	Freq.	Pct%
Yes	86	40%
No	74	34%
Unsure	57	26%
	217	100%
Q4d. If yes, what are the most significant security threats to your organization caused by cyber crime? FIRST CHOICE.	Freq.	Pct%
Inability to protect sensitive or confidential information	4	5%
Inability to restrict or limit use of computing resources or applications	6	7%
Inability to assure regulatory compliance requirements	8	9%
Inability to protect the critical infrastructure	52	60%
Management of users' and their access to confidential information	6	7%
Increased IT downtime and business interruption	6	7%
Other	4	5%
	86	100%
Q4d. If yes, what are the most significant security threats to your organization caused by cyber crime? SECOND CHOICE.	Freq.	Pct%
Inability to protect sensitive or confidential information	21	26%
Inability to restrict or limit use of computing resources or applications	12	15%
Inability to assure regulatory compliance requirements	12	15%
Inability to protect the critical infrastructure	14	17%
Management of users' and their access to confidential information	10	12%
Increased IT downtime and business interruption	8	10%
Other	5	6%
	82	100%

Q4e. Please rate the likelihood of occurrence that one or more of the above mentioned security threats will happen because of cyber crime sometime in the next 12 months.	Freq.	Pct%
Very high	74	34%
High	61	28%
Moderate	30	14%
Low	27	12%
Very low	25	12%
	217	100%
Q4f. Please rate the severity of the above mentioned security threats in terms of negative impact or harm to your organization's operations or mission.	Freq.	Pct%
Very significant	101	47%
Significant	46	21%
Moderate	31	14%
Insignificant	30	14%
Negligible	9	4%
	217	100%

5. Cyber terrorism		
Q5a. How familiar are you with cyber terrorism?	Freq.	Pct%
Very familiar	52	24%
Familiar	59	27%
Not familiar	77	35%
No knowledge	29	13%
	217	100%
Q5b. Approximately, how frequently has your organization experienced cyber crime attacks that infiltrated your organization's network or enterprise system in the past 12 months?	Freq.	Pct%
None	59	27%
1 time	60	28%
2 to 5 times	14	6%
more than 5 times	2	1%
Unsure	82	38%
	217	100%
Q5c. If yes, do you believe that cyber terrorism is an increasing security risk within your organization?	Freq.	Pct%
Yes	153	71%
No	47	22%
Unsure	17	8%
	217	100%
Q5d. If yes, what are the most significant security threats to your organization caused by cyber terrorism? FIRST CHOICE.	Freq.	Pct%
Inability to protect sensitive or confidential information	28	18%
Inability to restrict or limit use of computing resources or applications	10	7%
Inability to assure regulatory compliance requirements	8	5%
Inability to protect the critical infrastructure	39	25%
Management of users' and their access to confidential information	14	9%
Increased IT downtime and business interruption	52	34%
Other	2	1%
	153	100%
Q5d. If yes, what are the most significant security threats to your organization caused by cyber terrorism? SECOND CHOICE.	Freq.	Pct%
Inability to protect sensitive or confidential information	42	28%
Inability to restrict or limit use of computing resources or applications	3	2%
Inability to assure regulatory compliance requirements	4	3%
Inability to protect the critical infrastructure	59	39%
Management of users' and their access to confidential information	8	5%
Increased IT downtime and business interruption	33	22%
Other	2	1%
	151	100%

Q5e. Please rate the likelihood of occurrence that one or more of the above mentioned security threats will happen because of cyber terrorism sometime in the next 12 months.	Freq.	Pct%
Very high	81	37%
High	40	18%
Moderate	33	15%
Low	38	18%
Very low	25	12%
	217	100%
Q5f. Please rate the severity of the above mentioned security threats in terms of negative impact or harm to your organization's operations or mission.	Freq.	Pct%
Very significant	72	33%
Significant	31	14%
Moderate	41	19%
Insignificant	40	18%
Negligible	33	15%
	217	100%

6. Web 2.0		
Q6a. How familiar are you with Web 2.0?	Freq.	Pct%
Very familiar	71	33%
Familiar	98	45%
Not familiar	21	10%
No knowledge	27	12%
	217	100%
Q6b. Does your IT organization end-users to utilize Web 2.0?	Freq.	Pct%
Yes	130	60%
No	46	21%
Unsure	41	19%
	217	100%
Q6c. If yes, do you believe that Web 2.0 increases security risk within your organization?	Freq.	Pct%
Yes	67	52%
No	31	24%
Unsure	32	25%
	130	100%
Q6d. If yes, what are the most significant security threats to your organization caused by Web 2.0? FIRST CHOICE.	Freq.	Pct%
Inability to protect sensitive or confidential information	34	26%
Inability to restrict or limit use of computing resources or applications	21	16%
Inability to assure regulatory compliance requirements	9	7%
Increased cyber crime attacks	17	13%
Inability to protect the critical infrastructure	21	16%
Increased IT downtime or business interruption	15	12%
Management of users' and their access to cloud resources	7	5%
Other (please specify)	6	5%
	130	100%
Q6d. If yes, what are the most significant security threats to your organization caused by Web 2.0? SECOND CHOICE.	Freq.	Pct%
Inability to protect sensitive or confidential information	19	15%
Inability to restrict or limit use of computing resources or applications	33	27%
Inability to assure regulatory compliance requirements	18	15%
Increased cyber crime attacks	13	10%
Inability to protect the critical infrastructure	13	10%
Increased IT downtime or business interruption	12	10%
Management of users' and their access to cloud resources	16	13%
Other (please specify)	0	0%
	124	100%
Q6e. Please rate the likelihood of occurrence that one or more of the above mentioned security threats will happen because of Web 2.0 sometime in the next 12 months.	Freq.	Pct%
Very high	30	14%
High	38	18%
Moderate	51	24%
Low	49	23%
Very low	49	23%
	217	100%

Q6f. Please rate the severity of the above mentioned security threats in terms of negative impact or harm to your organization's operations or mission.	Freq.	Pct%
Very significant	30	14%
Significant	31	14%
Moderate	58	27%
Insignificant	53	24%
Negligible	45	21%
	217	100%

7. Outsourcing to third parties		
Q7a. Does your organization outsource any IT operation to third party organizations?	Freq.	Pct%
Yes	121	56%
No	71	33%
Unsure	25	12%
	217	100%
Q7b. If yes, how would you best describe the extent of your organization's outsourcing relationships with third parties?	Freq.	Pct%
We do not outsource any critical applications or operations	42	35%
We only outsource a few critical applications or operations	41	34%
We outsource several critical applications and operations	23	19%
We outsource most critical applications and operations	15	12%
	121	100%
Q7c. If yes, do you believe that outsourcing increases security risk within your organization?	Freq.	Pct%
Yes	41	34%
No	61	50%
Unsure	19	16%
	121	100%
Q7d. If yes, what are the most significant security threats to your organization caused by outsourcing? FIRST CHOICE.	Freq.	Pct%
Inability to protect sensitive or confidential information	84	69%
Inability to restrict or limit use of computing resources or applications	2	2%
Inability to assure regulatory compliance requirements	2	2%
Increased cyber crime attacks	2	2%
Inability to protect the critical infrastructure	2	2%
Increased IT downtime or business interruption	28	23%
Management of users' and their access to cloud resources	1	1%
Other (please specify)	0	0%
	121	100%
Q7d. If yes, what are the most significant security threats to your organization caused by outsourcing? SECOND CHOICE.	Freq.	Pct%
Inability to protect sensitive or confidential information	19	16%
Inability to restrict or limit use of computing resources or applications	28	23%
Inability to assure regulatory compliance requirements	18	15%
Increased cyber crime attacks	18	15%
Inability to protect the critical infrastructure	16	13%
Increased IT downtime or business interruption	11	9%
Management of users' and their access to cloud resources	11	9%
Other (please specify)	0	0%
	121	100%

Q7e. Please rate the likelihood of occurrence that one or more of the above mentioned security threats will happen because of outsourcing sometime in the next 12 months.	Freq.	Pct%
Very high	67	31%
High	54	25%
Moderate	45	21%
Low	22	10%
Very low	29	13%
	217	100%

Q7f. Please rate the severity of the above mentioned security threats in terms of negative impact or harm to your organization's operations or mission.	Freq.	Pct%
Very significant	63	29%
Significant	40	18%
Moderate	60	28%
Insignificant	30	14%
Negligible	24	11%
	217	100%

8. Data breach involving the loss of personal information		
Q8a. Has your organization suffered a data breach because personal information was either lost or stolen?	Freq.	Pct%
Yes	112	52%
No	83	38%
Unsure	22	10%
	217	100%
Q8b. If yes, how frequently has your organization experienced a data breach in the past 12 months?	Freq.	Pct%
None	28	25%
1 time	38	34%
2 to 5 times	38	34%
More than 5 times	8	7%
	112	100%
Q8c. If yes, how many records were either lost or stolen as a result of all the data breaches experienced in the past 12 months?	Freq.	Pct%
Don't know	47	42%
Less than 100 individual records	11	10%
101 to 1,000 individual records	24	21%
1,000 to 10,000 individual records	10	9%
10,001 to 100,000 individual records	16	14%
More than 100,000 individual records	4	4%
	112	100%
Q8d. If yes, do you believe that data breach is an increasing security risk within your organization?	Freq.	Pct%
Yes	45	40%
No	31	28%
Unsure	36	32%
	112	100%
Q8e. If yes, do you believe that data breach is an increasing security risk within your organization? FIRST CHOICE	Freq.	Pct%
Inability to protect sensitive or confidential information	37	33%
Inability to restrict or limit use of computing resources or applications	35	31%
Inability to assure regulatory compliance requirements	24	21%
Increased cyber crime attacks	3	3%
Inability to protect the critical infrastructure	5	4%
Increased IT downtime or business interruption	3	3%
Management of users' and their access to cloud resources	3	3%
Other (please specify)	2	2%
	112	100%

Q8e. If yes, do you believe that data breach is an increasing security risk within your organization? SECOND CHOICE	Freq.	Pct%
Inability to protect sensitive or confidential information	42	38%
Inability to restrict or limit use of computing resources or applications	28	25%
Inability to assure regulatory compliance requirements	34	31%
Increased cyber crime attacks	1	1%
Inability to protect the critical infrastructure	2	2%
Increased IT downtime or business interruption	2	2%
Management of users' and their access to cloud resources	1	1%
Other (please specify)	0	0%
	110	100%

Q8f. Please rate the likelihood of occurrence that one or more of the above mentioned security threats will happen because of data breach sometime in the next 12 months?	Freq.	Pct%
Very high	44	20%
High	61	28%
Moderate	66	30%
Low	27	12%
Very low	19	9%
	217	100%

Q8g. Please rate the severity of the above mentioned security threats in terms of negative impact or harm to your organization's operations or mission.	Freq.	Pct%
Very significant	55	25%
Significant	48	22%
Moderate	52	24%
Insignificant	31	14%
Negligible	31	14%
	217	100%

9. Unstructured data		
Q9a. Approximately, what percent of your organization's sensitive or confidential information resides on file servers or other storage devices in the form of unstructured data? Please provide your best estimate or gut feel.	Freq.	Pct%
None	42	19%
Only a small amount (less than 5%)	59	27%
A moderate amount (between 5 and 20%)	34	16%
A significant amount (between 21% and 40%)	29	13%
A very significant amount (more than 40%)	36	17%
Don't know	17	8%
	217	100%
Q9b. Do you believe that the collection and storage of unstructured data increases security risk within your organization?	Freq.	Pct%
Yes	171	79%
No	35	16%
Unsure	11	5%
	217	100%
Q9c. If yes, do you believe that unstructured data is an increasing security risk within your organization? FIRST CHOICE	Freq.	Pct%
Inability to protect sensitive or confidential information	72	42%
Inability to restrict or limit use of computing resources or applications	7	4%
Inability to assure regulatory compliance requirements	7	4%
Increased cyber crime attacks	6	4%
Inability to protect the critical infrastructure	6	4%
Increased IT downtime or business interruption	39	23%
Management of users' and their access to cloud resources	31	18%
Other (please specify)	3	2%
	171	100%
Q9c. If yes, do you believe that unstructured data is an increasing security risk within your organization? SECOND CHOICE	Freq.	Pct%
Inability to protect sensitive or confidential information	43	26%
Inability to restrict or limit use of computing resources or applications	7	4%
Inability to assure regulatory compliance requirements	8	5%
Increased cyber crime attacks	6	4%
Inability to protect the critical infrastructure	6	4%
Increased IT downtime or business interruption	72	43%
Management of users' and their access to cloud resources	26	15%
Other (please specify)	0	0%
	168	100%
Q9d. Please rate the likelihood of occurrence that one or more of the above mentioned security threats will happen because of the collection and storage of unstructured data sometime in the next 12 months?	Freq.	Pct%
Very high	73	34%
High	37	17%
Moderate	43	20%
Low	45	21%
Very low	19	9%
	217	100%

Q9e. Please rate the severity of the above mentioned security threats in terms of negative impact or harm to your organization's operations or mission.	Freq.	Pct%
Very significant	56	26%
Significant	54	25%
Moderate	36	17%
Insignificant	49	23%
Negligible	22	10%
	217	100%

10. Open source applications		
Q10a. Does your IT organization utilize open source applications?	Freq.	Pct%
Yes	90	41%
No	104	48%
Unsure	23	11%
	217	100%
Q10b. If yes, how would you best describe the extent of your organization's use of open source applications?	Freq.	Pct%
We do not use open source application for any critical operation	26	29%
We only use open source applications on a few critical operations	25	28%
We use open source applications for several critical operations	31	34%
We use open source applications on most critical operations	8	9%
	90	100%
Q10c. If yes, do you believe that the use of open source applications increases security risk within your organization?	Freq.	Pct%
Yes	16	18%
No	51	57%
Unsure	23	26%
	90	100%
Q10d. If yes, what are the most significant security threats to your organization caused by the use of open source applications? FIRST CHOICE.	Freq.	Pct%
Inability to protect sensitive or confidential information	25	28%
Inability to restrict or limit use of computing resources or applications	1	1%
Inability to assure regulatory compliance requirements	6	7%
Increased cyber crime attacks	3	3%
Inability to protect the critical infrastructure	3	3%
Increased IT downtime or business interruption	21	23%
Management of users' and their access to cloud resources	29	32%
Other (please specify)	2	2%
	90	100%
Q10d. If yes, what are the most significant security threats to your organization caused by the use of open source applications? SECOND CHOICE.	Freq.	Pct%
Inability to protect sensitive or confidential information	25	28%
Inability to restrict or limit use of computing resources or applications	3	3%
Inability to assure regulatory compliance requirements	13	15%
Increased cyber crime attacks	10	11%
Inability to protect the critical infrastructure	6	7%
Increased IT downtime or business interruption	21	24%
Management of users' and their access to cloud resources	11	12%
Other (please specify)	0	0%
	89	100%

Q10e. Please rate the likelihood of occurrence that one or more of the above mentioned security threats will happen because of using open source applications sometime in the next 12 months.	Freq.	Pct%
Very high	31	14%
High	39	18%
Moderate	72	33%
Low	38	18%
Very low	37	17%
	217	100%

Q10f. Please rate the severity of the above mentioned security threats in terms of negative impact or harm to your organization's operations or mission.	Freq.	Pct%
Very significant	39	18%
Significant	32	15%
Moderate	75	35%
Insignificant	35	16%
Negligible	36	17%
	217	100%

Q11. Mega trends – frequencies	Increasing risk	No change in risk
Cloud computing	132	42
Virtualization	70	111
Mobility	120	66
Cyber crime	79	94
Cyber terrorism	83	92
Web 2.0	68	119
Outsourcing to third parties	69	109
Data breach of personal information	71	115
Unstructured data	122	70
Open source applications	72	107

Q11. Mega trends – percentages	Increasing risk	No change in risk
Cloud computing	61%	19%
Unstructured data	56%	32%
Mobility	55%	30%
Cyber terrorism	38%	42%
Cyber crime	36%	43%
Open source applications	33%	49%
Data breach of personal information	33%	53%
Virtualization	32%	51%
Outsourcing to third parties	32%	50%
Web 2.0	31%	55%

Q12 Mega trends	Average Rank	Order
Cloud computing	3.5	1
Virtualization	5.0	7
Mobility	3.7	3
Cyber crime	3.8	4
Cyber terrorism	3.9	5
Web 2.0	5.3	10
Outsourcing to third parties	4.9	6
Data breach of personal information	5.2	9
Unstructured data	3.7	2
Open source applications	5.1	8

Q13. With respect to the above list of threats to privacy and data security, where are the most serious threats located (threat vectors)? Please select only two top choices.	Freq.	Total%
Wireless devices	123	57%
Endpoints	77	35%
Networks	62	29%
Applications	26	12%
Databases	54	25%
Off-line data-bearing devices	14	6%
Paper documents	24	11%
	380	

Q14. Attributions - frequencies	Strongly agree	Agree
Q14a. My organization has adequate policies and procedures to protect information assets and critical infrastructure.	45	57
Q14b. My organization has adequate security technologies to protect information assets and critical infrastructure.	48	49
Q14c. My organization takes appropriate steps to protect the confidential information about citizens and employees.	46	60
Q14d. My organization takes appropriate steps to comply with the requirements for privacy and security (including FISMA).	49	64
Q14e. My organization's senior leadership views security as a top priority.	48	55
Q14f. My company has ample resources to ensure all security requirements are met.	49	55
Q14. Attributions – percentages	Strongly agree	Agree
Q14a. My organization has adequate policies and procedures to protect information assets and critical infrastructure.	21%	26%
Q14b. My organization has adequate security technologies to protect information assets and critical infrastructure.	22%	23%
Q14c. My organization takes appropriate steps to protect the confidential information about citizens and employees.	21%	28%
Q14d. My organization takes appropriate steps to comply with the requirements for privacy and security (including FISMA).	23%	29%
Q14e. My organization's senior leadership views security as a top priority.	22%	25%
Q14f. My organization has ample resources to ensure all security requirements are met.	23%	25%

If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote from or reuse this report), please contact us by letter, phone call or e-mail:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49686 USA
1.800.887.3118
research@ponemon.org

Ponemon Institute LLC
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.