Security in the Trenches

Comparative study of IT practitioners and executives in the U.S. federal government

Sponsored by CA

Independently conducted by Ponemon Institute LLC

Publication Date: April 14, 2010

Security in the Trenches

Comparative study of IT practitioners and executives in the U.S. federal government

Prepared by Dr. Larry Ponemon, April 14, 2010

I. Executive Summary

This research continues our examination of security threats that affect U.S. federal organizations in terms of sensitive and confidential data, core information systems and critical infrastructure. In a recent study of senior-level IT executives located in various federal organizations, we found the following areas of information security risks: rapid growth in unstructured data assets, mobility of the federal workforce, cyber terrorism, outsourcing, cloud computing and others.[1]

In this study, we examine an independent sample of 320 IT and IT security practitioners also located in various federal departments and agencies.[2] We compare these results to our earlier study of IT executives to understand if beliefs and perceptions about the state of security in government between these two groups are in agreement.

Why is it important for IT practitioners at different organizational levels to be consistent in their beliefs and perceptions about security? In short, we believe that gaps between an organization's leadership and people on the proverbial "front lines" may lead to difficulties in managing threats, misallocating resources and missing opportunities to meet mission-critical objectives. Experience shows that a lack of congruence between executives and rank-and-file staff make it difficult to execute security strategies that protect an organization from serious attack. This issue is more important than ever because our earlier research shows these attacks as increasing in scope, sophistication and severity.

Utilizing a web-based survey, we asked staff-level IT respondents (a.k.a. rank-and-file employees) to answer specific questions about their organization's security posture, the availability of certain security technologies and the areas causing the most serious risks to information resources or infrastructure. We then compared these responses to survey results collected from executive-level respondents in our earlier study. Following are the most significant findings:

- Rank-and-file employees seem to be more concerned than executives about their organization's ability to withstand cyber attacks or achieve compliance with standards such as FISMA.

- Both executive and staff-level respondents in certain entities are more concerned about their organization's ability to withstand cyber attacks or achieve compliance standards than other organizations. For example, respondents in the Department of Homeland Security, Health and Human Services, Department of Justice, and Department of Treasury are least confident about their organization's ability to respond to serious security threats. In contrast, respondents from the US Postal Service, Veterans Affairs and State Department appear to have more confidence about their organization's security posture.

- Rank-and-file employees are much more likely to see the need for privileged user management solutions than IT executives. This suggests IT executives in government may not place sufficient priority on controlling those users who have widespread access rights to the most sensitive or confidential information resources and critical infrastructure.

---

[1]The *Cyber Security Mega Trends Study* (November 2009) *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. This research involved an in-depth survey of 217 IT executives in several US federal departments and agencies.

[2]We refer to these staff-level respondents as "rank-and-file employees" because they are at or below the supervisory level, and include technicians, analysts or staff members within the IT organization.

- Rank-and-file employees are much more likely to see the need for security training and awareness activities than IT executives. This suggests senior level personnel are less aware of employee negligence, mistakes or non-compliance with policies and procedures than those who operate in the security trenches.

- The widest gaps between executives and rank-and-file employees appear to occur within organizations that require excellence in security – especially respondents in the Department of Homeland Security and Department of Defense.

- With respect to specific threat vectors, IT executives perceive a limited number of security threats and see certain risks at a lower level of intensity than rank-and-file employees. For example, executives appear to be focused on lost or stolen information assets, computers and endpoint security issues rather than systemic system attacks. On the other hand, rank-and-file employees acknowledge a wider set of issues, including database security and off-line devices.

- IT executives are consistently more positive than rank-and-file employees about the effectiveness of specific security procedures and tasks that are deployed. The widest gaps concern identity and authentication of users before granting access to information assets or IT infrastructure.

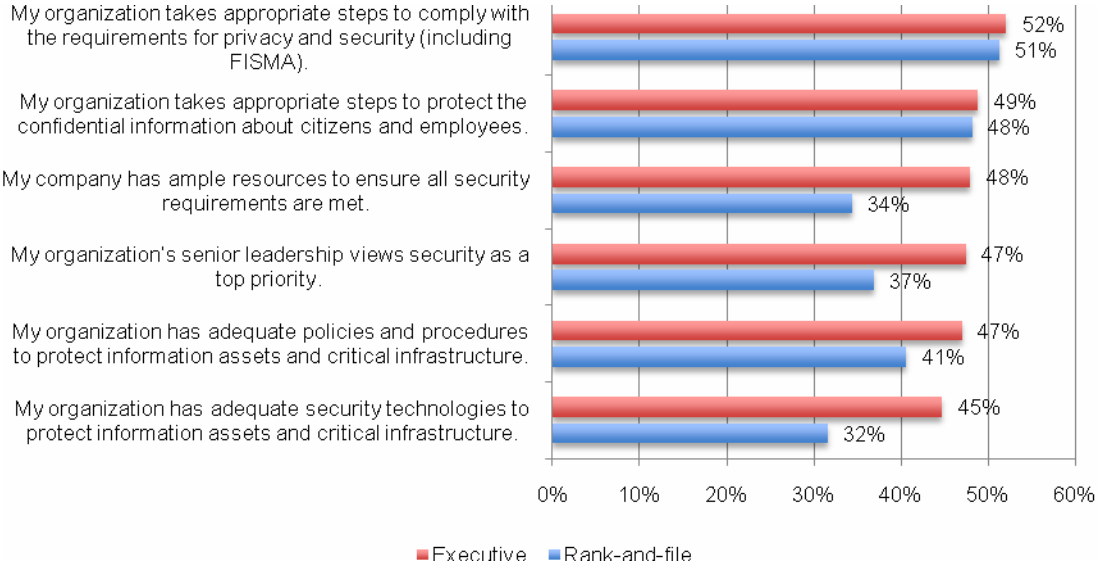
- Rank-and-file employees are much more likely than executives to see the necessity of certain enabling technologies to reduce or mitigate security risks within their organizations. The technologies with the widest difference include identity and access management systems, firewalls, database security tools, anti-virus/anti-malware tools, and others.

- Rank-and-file employees are much more likely than executives to see organizational issues as barriers and challenges that affect the management of privacy, data protection and information security requirements and objectives.

II. Key findings

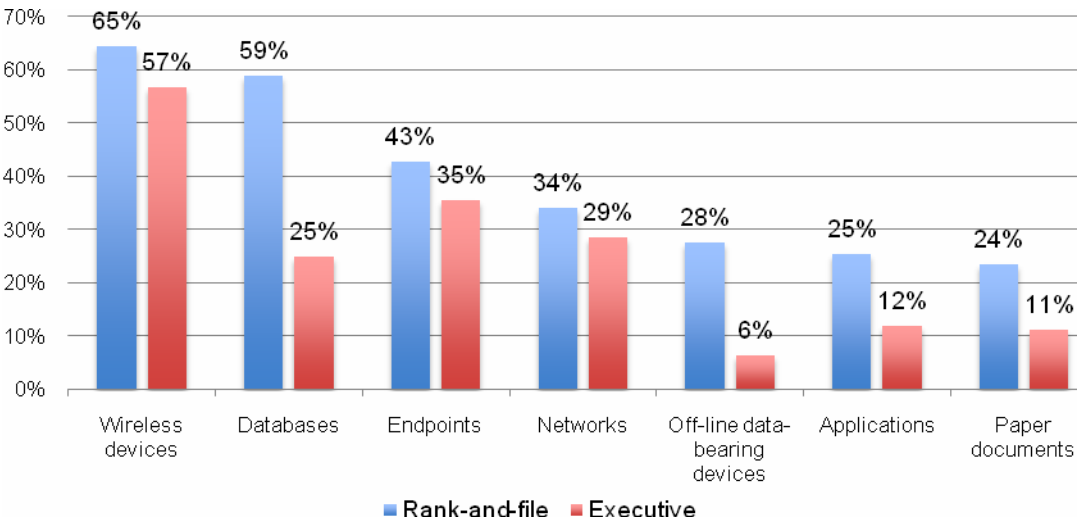
Following are six attributions used to gauge respondents' perceptions about the security posture of their department or agency. Bar Chart 1 shows rank-and-file employees are less likely than IT executives to rate each statement favorably in all cases. The biggest differences between executives and rank-and-file employees include: the availability of resources to meet security requirements (14 percent gap), the adequacy of security technologies (13 percent gap), and the support of the organization's senior leadership (10 percent gap).

Bar Chart 1
Attributions about the organization's security posture
Each bar records the strongly agree and agree response combined



Bar Chart 2 reports the most serious threat vectors confronting respondents' organizations. As can be seen, wireless devices, databases, endpoints and networks present the greatest risk.

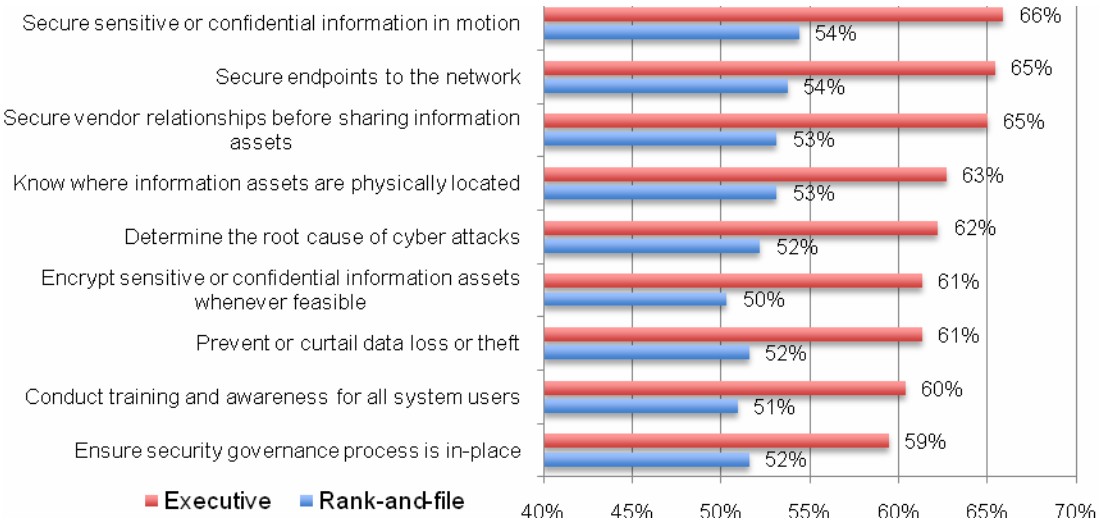
Bar Chart 2
Location of the most serious threats



The pattern of responses suggests rank-and-file employees are more likely than executives to see each of the seven possible vectors as a more serious threat to their department or agency. The biggest differences between these groups include databases (34 percent gap), off-line devices (22 percent gap), and applications (13 percent gap).

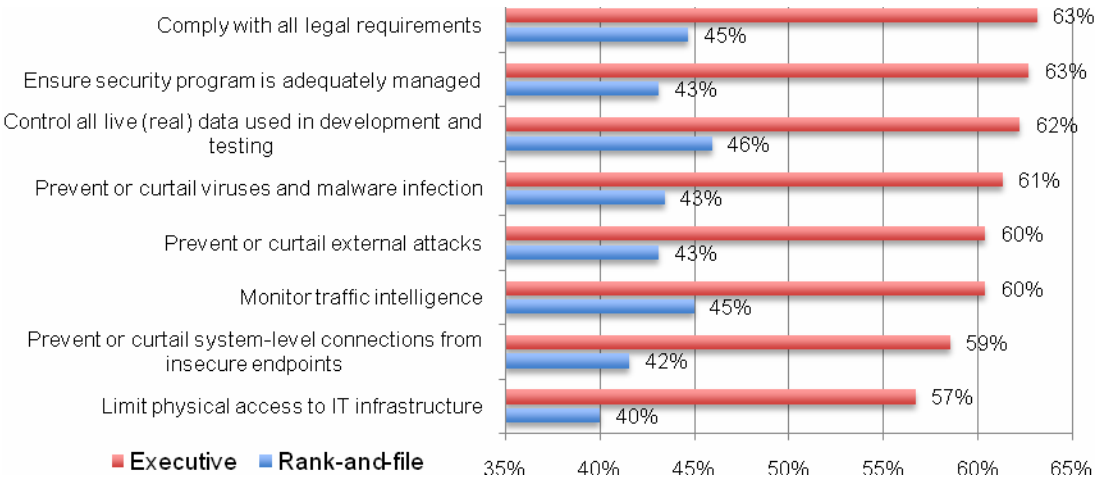
Bar Chart 3 lists nine security objectives that rank-and-file respondents feel most confident about achieving within their organization. It is clear that executives are overwhelmingly more confident about the organization's ability to achieve each of these attributes than rank-and-file employees.

Bar Chart 3
Confidence that the organization can accomplish each objective
Each bar is the combined very confident and confident response.



Bar Chart 4 lists eight security objectives that rank-and-file respondents feel least confident about achieving within their organization. It is clear that executives are overwhelmingly more confident about the organization's ability to achieve each of these attributes than rank-and-file employees.

Bar Chart 4
Confidence that the organization can accomplish each objective
Each bar is the combined very confident and confident response.



Bar Chart 5 lists seven security objectives that yield the widest differences between executives and rank-and-file employees. The most salient gaps include: the adequacy of program management (20 percent gap), hiring and retaining highly qualified personnel (19 percent gap), and securing confidential information at rest (19 percent gap).

Bar Chart 5
Seven attributes with the largest difference between executive and rank-and-file groups
Each bar is the confident response for executives minus the confident response for rank-and-file employees.

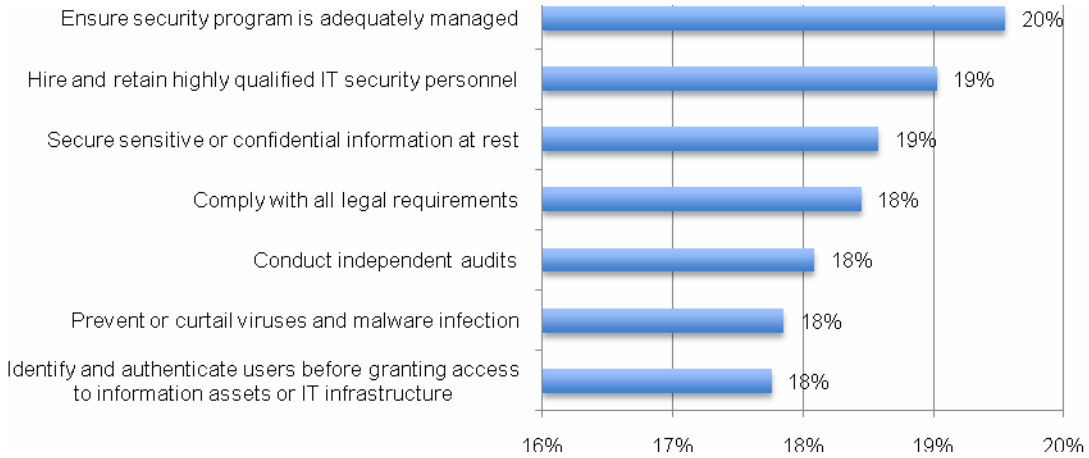


Table 1 lists 17 enabling security technologies that both executive and rank-and-file employees in US federal departments and agencies believe to be very important to achieving a security posture that is adequate for meeting their organization's mission. In general, both executives and rank-and-file respondents hold similar views, with a two exceptional differences: firewalls (26 percent gap) and database tools (20 percent gap).

Table 1
Enabling security technologies deemed very important
Difference is the rank-and-file employees' very important average rating minus executives' very important average rating.

Enabling security technologies	Rank-and-file	Executive	Difference
Firewalls	64%	38%	26%
Database scanning and monitoring	57%	37%	20%
Anti-virus & anti-malware	51%	45%	6%
Intrusion detection or prevention	46%	45%	1%
Perimeter or location surveillance	44%	40%	4%
Website sniffer or crawlers	44%	40%	4%
Virtual private network (VPN)	44%	39%	5%
Correlation or event management	42%	39%	3%
Data loss prevention (DLP)	41%	45%	-5%
Endpoint encryption solution	38%	43%	-4%
Encryption for data at rest	37%	38%	-1%
Patch management	36%	40%	-4%
Encryption for wireless communication	35%	37%	-2%
Encryption for data in motion	34%	37%	-3%
Code review	32%	37%	-5%
Web application firewalls (WAF)	29%	32%	-4%
Traffic intelligence systems	26%	33%	-8%
Average	41%	39%	2%

Table 2 lists nine identity and access management technologies that both executives and rank-and-file employees in US federal departments and agencies believe to be very important to meet security objectives. As can be seen, rank-and-file employees view these technologies as more important than executives in almost all cases (16 percent average difference).

Table 2
Identity and access management technologies deemed very important
Difference is the rank-and-file employees' very important average rating minus executives' very important average rating.

Table 2: IAM technologies	Rank-and-file	Executive	Difference
Service oriented architecture (SOA) security	66%	44%	22%
Log management	64%	45%	20%
Access governance systems	62%	43%	19%
Privileged password management	62%	31%	31%
User management and provisioning	60%	42%	18%
ID & credentialing system	58%	39%	18%
Identity federation	55%	43%	12%
Single sign-on (SSO)	48%	44%	5%
Web access management	41%	41%	0%
Average	57%	41%	16%

Bar Chart 6 lists nine identity and access management (IAM) technologies and the computed average differences between executives and rank-and-file employees. The most significant differences include: privileged password management (31 percent gap), service oriented architecture security (22 percent gap), log management (20 percent gap), and access governance systems (19 percent gap).

Bar Chart 6
Difference between executive and rank-and-file groups on IAM technologies
Each bar is the very important response for rank-and-file employees minus the very important response for executives.

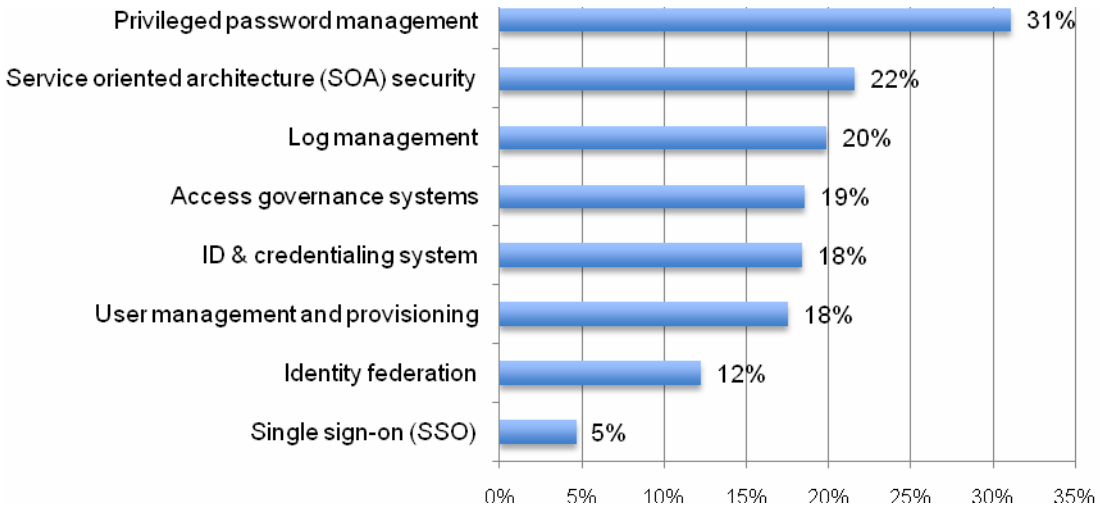


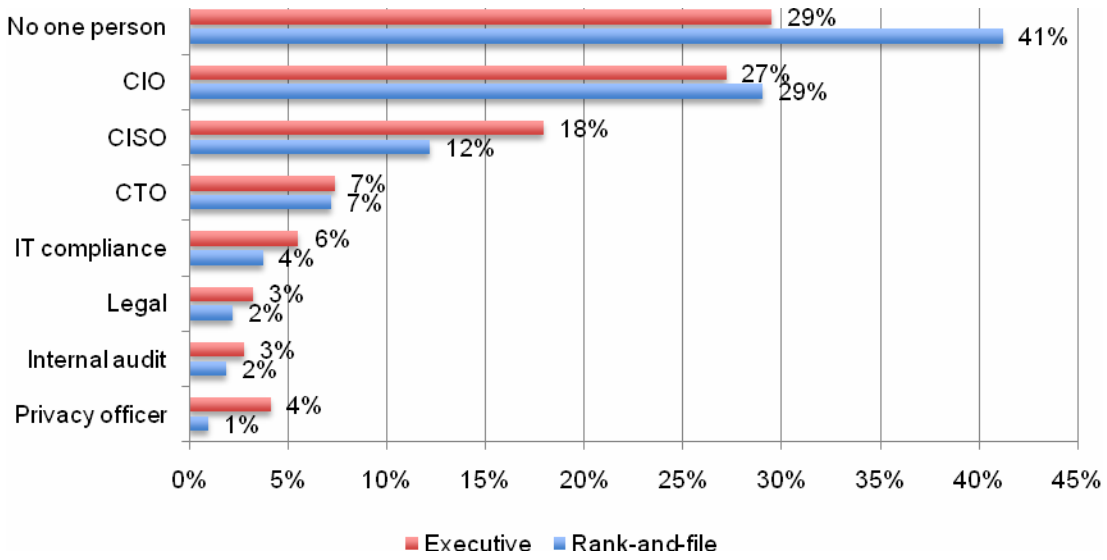
Table 3 lists 17 system control activities that both executives and rank-and-file employees in US federal departments and agencies believe to be very important to meet security objectives. As can be seen, rank-and-file employees view these technologies as more important than executives in 14 cases (9 percent average difference).

Table 3
System control activities deemed very important
Difference is the rank-and-file employees' very important average rating minus executives' very important average rating.

System control activities	Rank-and-file	Executive	Difference
Vetting and monitoring of third parties	65%	46%	19%
Training of data handlers	64%	44%	20%
Training of privacy and security experts	63%	43%	20%
Training of end users	62%	41%	21%
External audit	61%	39%	22%
Controls assessment	60%	43%	17%
Policies and procedures	59%	38%	21%
Communications	45%	43%	2%
Monitoring changes in regulations	43%	42%	1%
Background checks of privileged users	43%	39%	4%
Helpdesk activities	42%	40%	2%
Quality assurance	41%	38%	3%
Surveillance	41%	39%	2%
Certifications (such as ISO, NIST and others)	41%	42%	-1%
Redress and enforcement	40%	42%	-2%
Internal audit	38%	39%	-1%
Average	50%	41%	9%

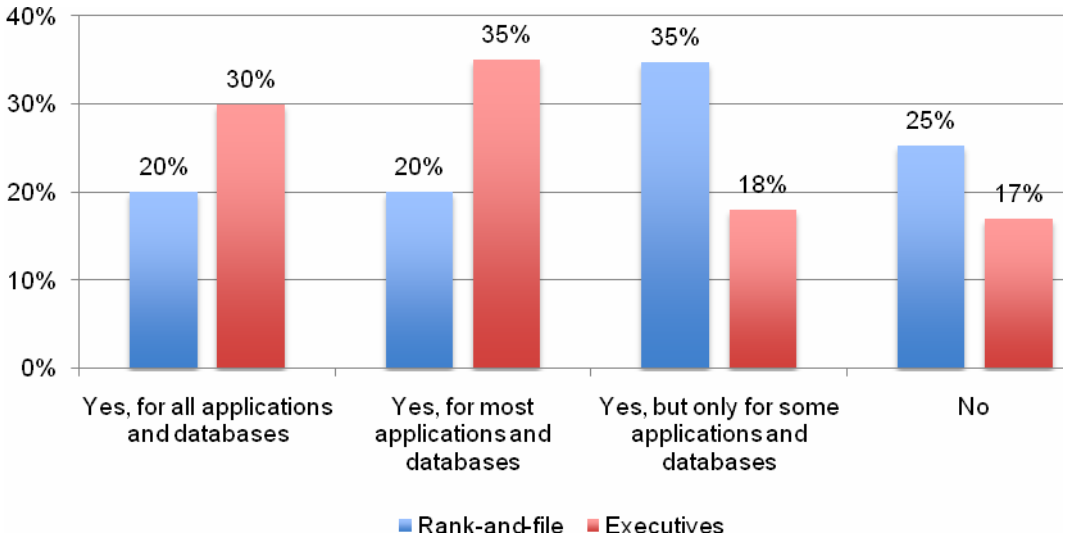
Bar Chart 7 reports the frequency of individuals who respondents believe are most responsible for meeting security objectives within their organizations. As shown, rank-and-file respondents are much less likely than executives to see "no one person" with overall responsibility for their organization's security initiatives. Also, rank-and-file respondents are more likely than executives to see the IT security leader is most likely to have overall responsibility for the organization's security initiatives.

Bar Chart 7
The individual most responsible for ensuring security requirements
Each bar is the one choice made by respondents



Bar Chart 8 provides respondents' answers to the question "To the best of your knowledge, is your organization compliant with all applicable requirements for security including FISMA?" As can be seen, rank-and-file employees are less confident than executives that their organizations are meeting all or most regulatory requirements.

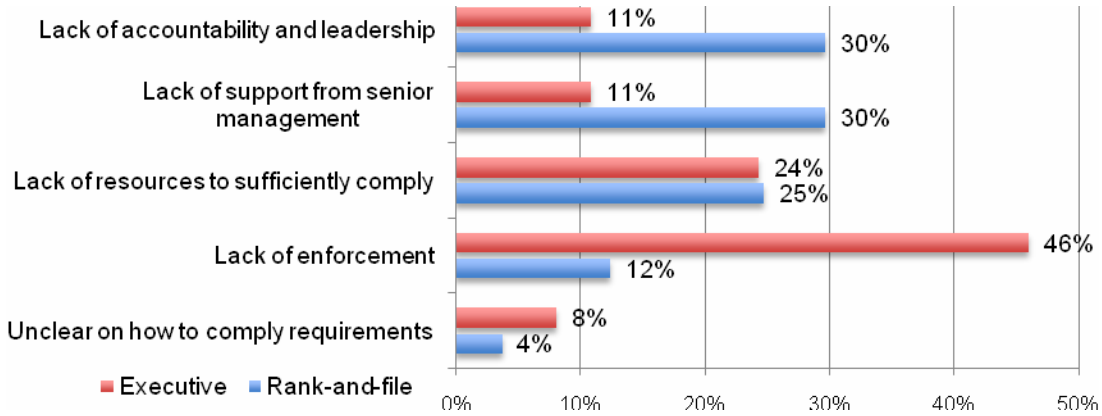
Bar Chart 8
State of compliance with all applicable regulatory requirements including FISMA
Each bar is the one choice made by respondents



Bar Chart 9 reports the reasons why respondents believe their organizations are not compliant with all or most regulatory requirements for data protection and security. As can be seen, there are significant differences between rank-and-file and executives. Specifically, rank-and-file employees are much more likely than executives to see the lack of accountability and leadership or the lack of support from senior management as primary reasons for non-compliance. In contrast, executives are much more likely than rank-and-file employees to see the lack of enforcement as a primary reason for non-compliance.

Bar Chart 9
Why organizations fail to comply with all applicable regulatory requirements

Each bar is the one choice made by respondents who said no to the question "Is your organization compliant with all applicable regulatory requirements for security including FISMA."



III. Methods

A panel of 7,067 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 IT and IT security practitioners employed by the US federal government. Table 4 reports the survey response for two independent samples. Please note that additional information about the executive panel can be found in our earlier research.[3]

Table 4: Survey response	Rank-and-file	Executives
Sampling frame	7,067	4,861
Invitations sent	6,555	4,522
Bounce-back	1,371	893
Net responses	365	261
Rejections	45	44
Usable sample	320	217
Response rate	4.53%	4.46%

In total, 365 respondents completed the survey. Of the returned instruments, 45 surveys failed reliability checks. A total of 320 surveys were used as our final sample, which represents a 4.5 percent net response rate.[4] Ninety-two percent of respondents completed all survey items within 15 minutes.

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

Pie Chart 1
Distribution of respondents by federal department or organization

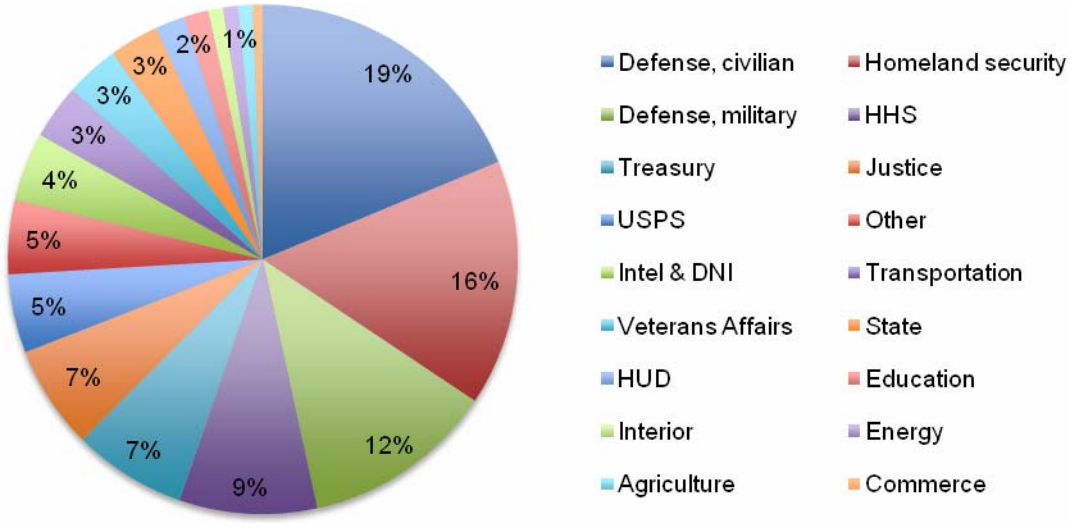


Table 5 reports the organizational level of respondents. As can be seen, 92 percent of respondents are below the supervisory level. The average overall experience level of respondents is 5.6 years (median is 6 years).

[3] Ibid, footnote 1
[4] Two screening questions were used to the refine sample by position level and organizational size.

Table 5: Respondents' organizational level	Freq.	Pct%
Supervisor	24	8%
Staff level	152	48%
Technician	116	36%
Administrative	4	1%
Other	24	8%

Table 6 reports the respondent's reporting channel or chain of command. As shown, the majority of respondents report to either the IT operations, network management or development.

Table 6: Respondents' reporting channel	Freq.	Pct%
Operations	143	45%
Network management	42	13%
Development & testing	65	20%
Security	20	6%
Quality assurance	5	2%
Compliance	7	2%
Other	38	12%

Table 7 reports the respondent organization's global headcount. The majority of respondents work in federal government organizations with more than 25,000 employees.

Table 7: Respondents' organizational headcount	Freq.	Pct%
1,001 to 5,000 people	54	17%
5,001 to 25,000 people	27	8%
25,001 to 75,000 people	97	30%
More than 75,000 people	142	44%

IV. 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 practitioners in the US 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.

V. Conclusion

In general, senior-level executives in the federal government are more confident than their staff in their organizations' ability to achieve their security objectives. The widest gaps between these two groups occur within organizations with the most pessimistic beliefs and perceptions about security. These agencies are the Department of Homeland Security, Health and Human Services and Department of Defense and these may be the most vulnerable to attacks.

As described in this study, senior executives are more likely to believe their organizations have the resources to meet security requirements, the security technologies to manage risks and the support of senior leadership. Only 37 percent of staff respondents believe their senior leadership views security as a priority.

These are important findings because they show differences between the people who are determining the priorities and direction for their agencies and those who are in the trenches and seeing the risks first-hand. Specifically, they see the need for enabling technologies, especially identity and access management technologies to safeguard data. They are also more likely than the leadership to see the importance of vetting and monitoring third parties, training data handlers, training privacy and security experts, training end users, conducting external audits and enforcing policies and procedures.

We believe these findings can assist agencies concerned about the growing privacy and data security risks to better understand the steps that should be considered to improve their security posture. The first step is to listen to those who may be closest to the risk.

Federal organizations face a plethora of security threats to their data, systems and critical infrastructure. We asked both senior and staff-level IT practitioners to provide their objective responses to a series of question about the security posture of department. What we found is there are significant differences between these two groups in terms of underlying beliefs and perceptions.

For additional information, please contact research@ponemon.org **or call 800.877.3118.**

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.

Appendix 1: Survey Response

Following are the frequencies of the aggregate responses for 320 IT and IT security practitioners employed by the US federal government for all survey questions. These are the same questions used in an earlier study of 217 IT executives in government.

D1. What organizational level best describes your current position?	Freq.	Pct%
Supervisor	24	8%
Staff level	152	48%
Technician	116	36%
Administrative	4	1%
Other	24	8%
	320	100%
D2. Where does your department report within the organization?	Freq.	Pct%
Operations	143	45%
Network management	42	13%
Development & testing	65	20%
Security	20	6%
Quality assurance	5	2%
Compliance	7	2%
Other	38	12%
Total	320	100%
Relevant experience	Mean	Median
D3a. Overall experience	5.6	6.0
D3b. IT or security experience	2.9	2.0
D3c. Years in current position	3.0	2.0
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	24	8%
250 to 500	29	9%
500 to 1,000	68	21%
1,000 to 2,500	109	34%
More than 2,500	88	28%
Total	320	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	35	11%
501 to 1,000 people	46	14%
1,001 to 5,000 people	107	33%
Over 5,000 people	132	41%
Total	320	100%
D6. What is the headcount of your organization?	Freq.	Pct%
1,001 to 5,000 people	54	17%
5,001 to 25,000 people	27	8%
25,001 to 75,000 people	97	30%
More than 75,000 people	142	44%
Total	320	100%

D7. What U.S. federal government entity best describes your organization?	Freq.	Pct%
Defense, civilian	60	19%
Defense, military	39	12%
Justice	21	7%
HHS	28	9%
Homeland security	50	16%
Treasury	23	7%
State	10	3%
USPS	16	5%
DNI (Intelligence agencies)	14	4%
Commerce	2	1%
Transportation	11	3%
Veterans Affairs	11	3%
Interior	3	1%
Energy	3	1%
HUD	6	2%
Education	5	2%
Agriculture	3	1%
Other	15	5%
Total	320	100%

Q1. 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	140	65%
Endpoints	93	43%
Networks	74	34%
Applications	55	25%
Databases	128	59%
Off-line data-bearing devices	60	28%
Paper documents	51	24%
Total	601	

Attributions 1 = Strongly agree, 2 = Agree	1	2
Q2a. My organization has adequate policies and procedures to protect information assets and critical infrastructure.	20%	20%
Q2b. My organization has adequate security technologies to protect information assets and critical infrastructure.	12%	20%
Q2c. My organization takes appropriate steps to protect the confidential information about citizens and employees.	29%	19%
Q2d. My organization takes appropriate steps to comply with the requirements for privacy and security (including FISMA).	20%	31%
Q2e. My organization's senior leadership views security as a top priority.	25%	12%
Q2f. My company has ample resources to ensure all security requirements are met.	11%	23%

How confidential are you that your organization can accomplish the following security 25 objectives? 1 = Very confident, 2 = Confident	1	2
Determine the root cause of cyber attacks	25%	27%
Know where information assets are physically located	22%	32%
Secure sensitive or confidential information at rest	19%	27%
Secure sensitive or confidential information in motion	23%	32%
Secure endpoints to the network	24%	29%
Identify and authenticate users before granting access to information assets or IT infrastructure	21%	28%
Secure vendor relationships before sharing information assets	22%	31%
Prevent or curtail data loss or theft.	19%	32%
Prevent or curtail external attacks	19%	24%
Limit physical access to IT infrastructure	14%	26%
Ensure security governance process is in-place	30%	21%
Prevent or curtail system downtime and business interruption	14%	32%
Prevent or curtail system-level connections from insecure endpoints	16%	25%
Comply with all legal requirements	20%	25%
Achieve compliance with leading self-regulatory frameworks including ISO, NIST and others.	16%	31%
Prevent or curtail viruses and malware infection	17%	27%
Perform patches to software promptly	18%	31%
Control all live (real) data used in development and testing	17%	29%
Enforce security policies	23%	27%
Hire and retain highly qualified IT security personnel	18%	29%
Conduct training and awareness for all system users	18%	33%
Conduct independent audits	16%	32%
Ensure security program is adequately managed	16%	27%
Monitor traffic intelligence	16%	29%
Encrypt sensitive or confidential information assets whenever feasible	22%	29%

Enabling security technologies. Yes = security feature exists.	Yes	Very important
Anti-virus & anti-malware	87%	51%
Code review	80%	32%
Correlation or event management	73%	42%
Data loss prevention (DLP)	75%	41%
Database scanning and monitoring	83%	57%
Encryption for data at rest	79%	37%
Encryption for data in motion	83%	34%
Encryption for wireless communication	78%	35%
Endpoint encryption solution	85%	38%
Firewalls	98%	64%
Intrusion detection or prevention	83%	46%
Patch management	78%	36%
Perimeter or location surveillance	80%	44%
Traffic intelligence systems	69%	26%
Virtual private network (VPN)	78%	44%
Web application firewalls (WAF)	87%	29%
Website sniffer or crawlers	57%	44%

Identity & access management technologies. Yes = security feature exists.	Yes	Very important
Access governance systems	76%	62%
ID & credentialing system	79%	58%
Identity federation	37%	55%
Log management	79%	64%
Privileged password management	79%	62%
Service oriented architecture (SOA) security	85%	66%
Single sign-on (SSO)	50%	48%
User management and provisioning	82%	60%
Web access management	80%	41%

System control activities. Yes = security feature exists.	Yes	Very important
Background checks of employees (especially those who are privileged users)	63%	43%
Certifications (such as ISO, NIST and others)	60%	41%
Communications	62%	45%
Controls assessment	55%	60%
External audit	83%	61%
Helpdesk activities	61%	42%
Internal audit	63%	38%
Monitoring changes in regulatory requirements	64%	43%
Policies and procedures	88%	59%
Quality assurance	60%	41%
Redress and enforcement	61%	40%
Surveillance	61%	41%
Training of data handlers	85%	64%
Training of end users	86%	62%
Training of privacy and security experts	86%	63%
Vetting and monitoring of third parties	86%	65%

Q6. Who in your organization is most responsible for ensuring security requirements are met? Please select one response.	Freq.	Pct%
No one person	132	41%
CIO	93	29%
CTO	23	7%
IT security leader (CISO)	39	12%
Privacy officer or leader (CPO)	3	1%
IT compliance	12	4%
Internal audit	6	2%
Legal	7	2%
Other (please specify)	5	2%
Total	320	100%

Q7a. To the best of your knowledge, is your organization compliant with all applicable regulatory requirements for security (including FISMA)?	Freq.	Pct%
Yes, for all applications and databases throughout the enterprise	64	20%
Yes, for most applications and databases throughout the enterprise	64	20%
Yes, but only for some applications and databases throughout the enterprise	111	35%
No	81	25%
Total	320	100%

Q7b. If you said No (Q7a), why is your organization not compliant with these requirements? Please check the top two reasons only.	Freq.	Pct%
Lack of enforcement	10	12%
Lack of resources to sufficiently comply	20	25%
Lack of support from senior management	24	30%
Lack of accountability and leadership	24	30%
Unclear on how to comply requirements	3	4%
Other	0	0%
Total	81	100%

Q8. Please select the value security compliance activities provides your organization. Check all that applies.	Freq.	Pct%
Organization's control over information assets	91	28%
Improves our organization's ability to protect critical infrastructure.	144	45%
Improves our organization's reputation or "good name"	32	10%
Improves our organization's relationship with key partners.	23	7%
Heightens awareness among leaders within our organization.	18	6%
Helps secure more funding for IT security.	7	2%
Other	5	2%
Total	320	100%

Q9. What is the purpose of FISMA security compliance requirements? Please choose the statements you believe to be true about compliance.	Freq.	Pct%
Not necessary.	41	13%
Only "CYA."	108	34%
Necessary to achieve consistent security practices across the enterprise.	52	16%
Necessary to obtain buy-in from leadership.	35	11%
Necessary to secure security budget and funding.	39	12%
Necessary to prioritize security requirements.	23	7%
Essential to achieving an effective security posture.	22	7%
Total	320	100%