Ponemon INSTITUTE

State of Cybersecurity in Local, State & Federal Government

Sponsored by Hewlett Packard Enterprise

Independently conducted by Ponemon Institute LLC

Publication Date: October 2015

The State of Cybersecurity in Local, State and Federal Government

Ponemon Institute, October 2015

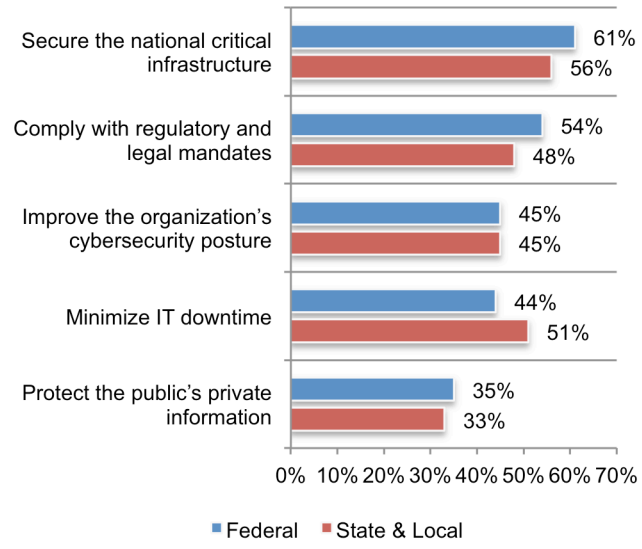
Part 1. Introduction

The State of Cybersecurity in Local, State and Federal Government sponsored by Hewlett Packard Enterprise was conducted by Ponemon Institute to understand the challenges IT and IT security practitioners face in keeping the various government agencies secure from cyber attacks and threats. Similar to the private sector, government is the target of cybercriminals and nation state attackers. The recent Office of Personal Management (OPM) data breach resulted in the theft of millions of federal workers' personal data and is one example.

According to the findings in this research, cybersecurity breaches that compromise the organization's networks or enterprise systems are happening an average of almost every two months at the federal level and about every three months at the state level. We surveyed 443 IT and IT security practitioners in the federal government and 402 IT and IT security practitioners in state and local government who are familiar with their organization's[1] ability to defend against cybersecurity attacks and have responsibility in directing cybersecurity activities.

As shown in Figure 1, 61 percent of federal respondents and 56 percent of state and local respondents believe their main responsibility is to protect the national critical infrastructure from cyber threats and attacks. However, only 45 percent of both groups of respondents say a priority is to improve the cybersecurity posture in their organizations.

Figure 1. The top 5 cybersecurity objectives in government



The following findings illustrate the current state of cybersecurity in government.

- Cybersecurity practices are not clearly defined, according to 52 percent of federal respondents and 71 percent of state and local respondents.
- The majority of respondents rate their effectiveness in preventing and detecting cyber attacks as low.
- Both groups of respondents cite a lack of skilled personnel and frustration with organizational politics as a deterrent to achieving a strong cybersecurity posture.
- Overly restrictive requirements or mandates and bureaucracy stifle organizations ability to use technologies and personnel in new ways to minimize cyber threats.

[1] In the context of this research, organization refers to the working unit where the respondent exercises their role or function. For instance, an organization is a government agency, department, enterprise or public university.

- Sharing threat intelligence is considered important but organizations have yet to make it effective in predicting malicious IP activities.

- Eighty-six percent of respondents in state and local government and 73 percent of federal respondents believe the responsibility for managing cybersecurity risk in their organizations is the most stressful job they have.

Part 2. Key findings

In this section, we provide an analysis of the key findings. The complete research findings are presented in the appendix of this report. We have organized the report according to the following topics:

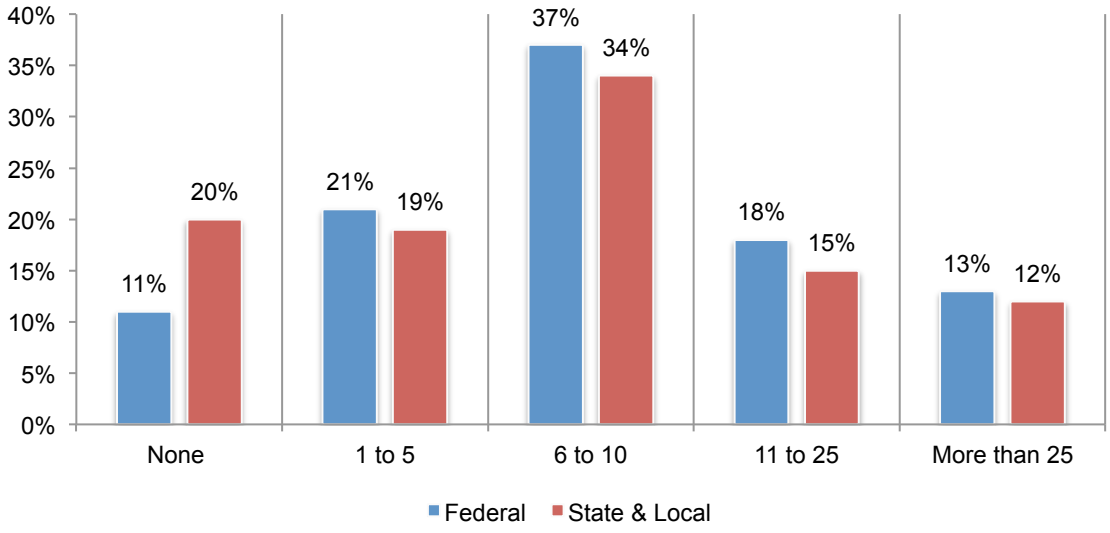
- The cybersecurity posture of government organizations
- Threat intelligence sharing is ineffective
- Necessity drives security innovation

The cybersecurity posture of government organizations

Data breaches happen about every two to three months. Without the necessary resources, dealing with a serious data breach that occurs with regular frequency is straining the resiliency of organizations' IT security capabilities. In the context of this study, we define a data breach as an attack that compromises the organization's networks or enterprise systems. The attack or compromise can be internal (i.e., malicious insider), external (i.e., hacker) or both.

According to the findings in Figure 2, in the past 24 months federal agencies had a material data breach about every 9 weeks (an average of 10.5 in two years). Eighteen percent of respondents believe some were nation state attacks. State and local agencies had such an incident a little less than every 12 weeks (an average of 9.4 in two years) and 11 percent of respondents believe some were nation state attacks.

Figure 2. How many material security breaches did your organization experience in the past 24 months? Extrapolated value = 10.5 (federal) and 9.4 (state & local)

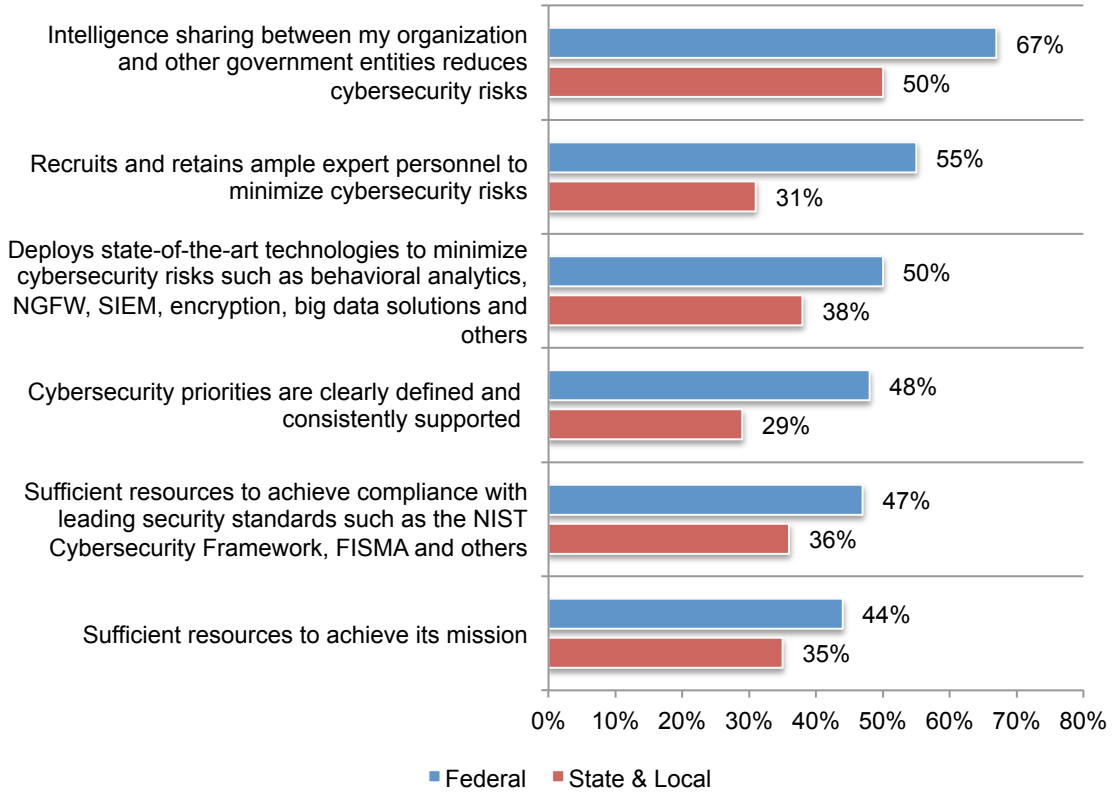


Federal organizations have a stronger cybersecurity posture than state and local organizations. Figure 3 shows six attributes about an organization's cybersecurity posture. According to the findings, federal respondents are much more positive about their ability to deal with cyber attacks. The biggest difference between the two groups is the ability to recruit and retain ample expert personnel to minimize cybersecurity risks (55 percent of federal vs. 31 percent of state and local respondents).

At the federal level, cybersecurity priorities are more clearly defined and consistently supported throughout their organization (48 percent of federal respondents vs. 29 percent of state and local respondents). The majority of federal organizations have state-of-the-art technologies to minimize cybersecurity risks such as behavioral analytics, next generation firewall, SIEM, encryption, big data solutions and others (50 percent of respondents vs. 38 percent of respondents).

Sixty-seven percent of federal respondents say intelligence sharing between their organization and other government entities reduces cybersecurity risks and 50 percent of state and local organizations believe threat intelligence sharing is important.

Figure 3. Perceptions about the state of cybersecurity in government
Strongly agree and agree response combined

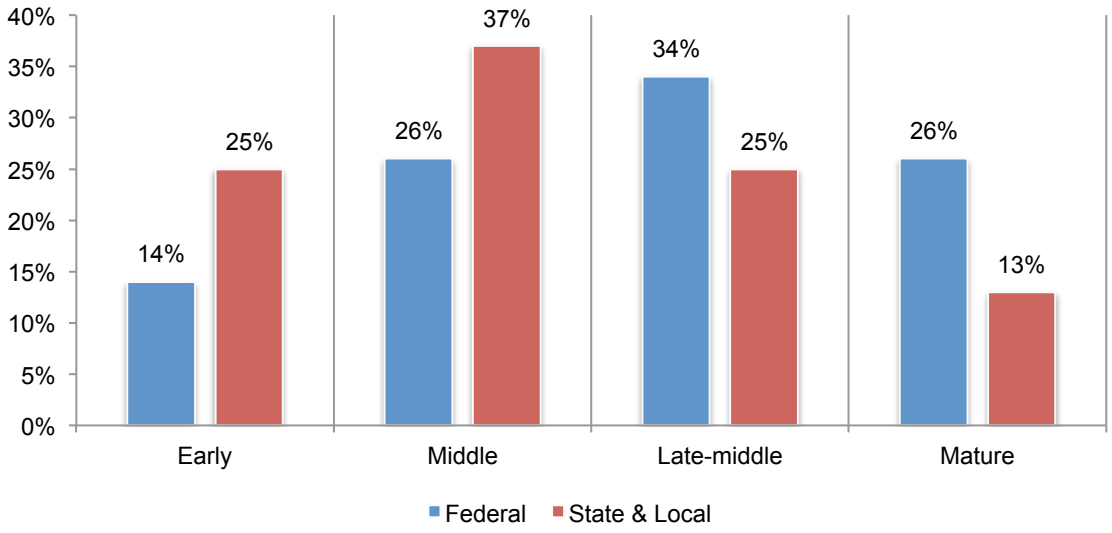


The cybersecurity program in state and local governments lacks maturity. In the context of this survey, we define an organizations cybersecurity program according to the following four progressive stages of maturity from early to fully mature:

- Early stage means most mission-critical program activities are planned, but not yet initiated
- Middle stage means most mission-critical program activities are initiated or partially deployed
- Late-middle stage – most mission-critical program activities are partially or fully deployed
- Mature stage – most mission-critical program activities are fully deployed

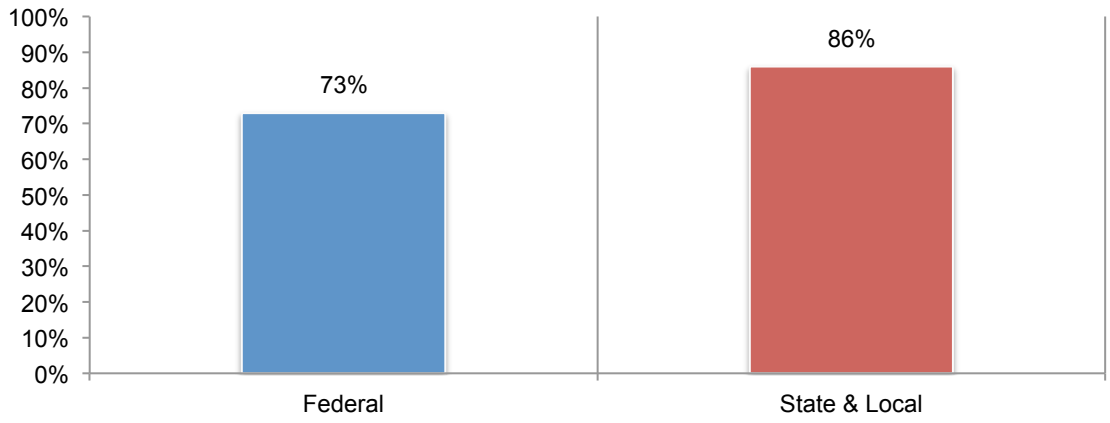
In many cases, the federal government has a more mature cybersecurity posture than state and local governments. In fact, 60 percent of respondents describe the maturity level of their organization's cybersecurity program or activities as late-middle (34 percent of respondents) or mature (26 percent of respondents). In contrast, only 38 percent of state and local respondents say their agencies have achieved that level of maturity in their cybersecurity initiatives.

Figure 4. What best describes the maturity level of your organization's cybersecurity program or activities today?



As shown in Figure 5, almost every IT practitioner in this study considers his or her job as stressful due to a dearth of in-house expertise, lack of clearly defined cyber security priorities and not having the necessary technologies.

Figure 5. Managing cybersecurity risk in my organization is one of the most stressful jobs



The research reveals four areas where the federal government is outpacing state and local agencies. They are presented in order of the most significant difference to the least significant difference (based on a reported rating of 7+ on a scale of 1 = very low to 10 = very high). As shown in Figure 6, the most significant difference is in the ability to recover from a cyber attack.

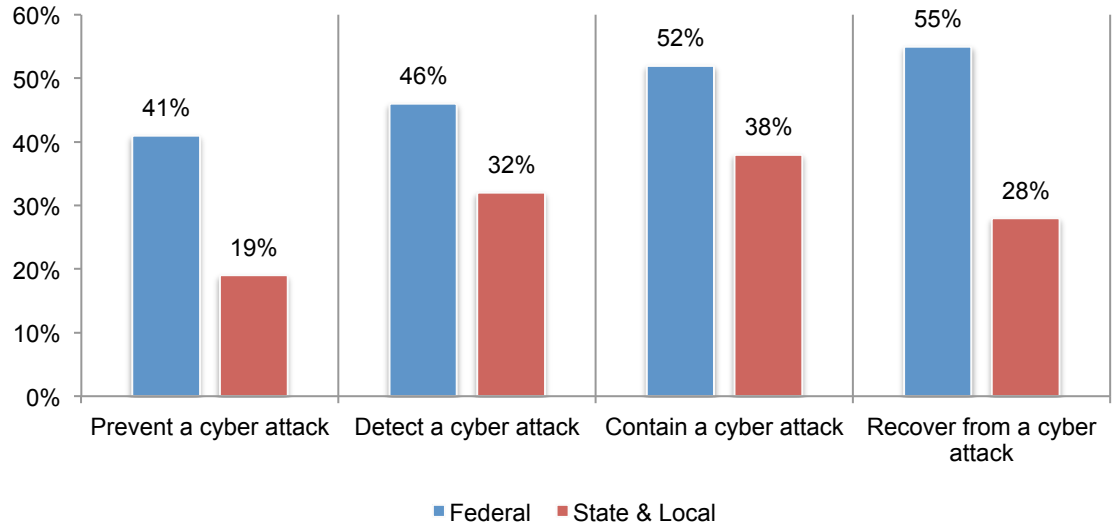
1. **Ability to recover**. Fifty-five percent of federal respondents rate their ability to recover from a cyber attack as very high. In contrast, only 28 percent of state and local respondents say their ability is very high.

2. **Ability to prevent**. Forty-one percent of federal respondents rate their ability to prevent a cyber attack as very high. In contrast, only 19 percent of state and local respondents rate their ability as very high.

3. **Ability to quickly detect**. Forty-six percent of federal respondents rate their ability to quickly detect a cyber attack as very high and 32 percent of state and local agencies are confident they would detect an attack.

4. **Ability to contain.** Fifty-two percent of federal respondents say they rate their organization's ability to contain a cyber attack as very high and 38 percent of respondents are very confident in being able to contain an attack.

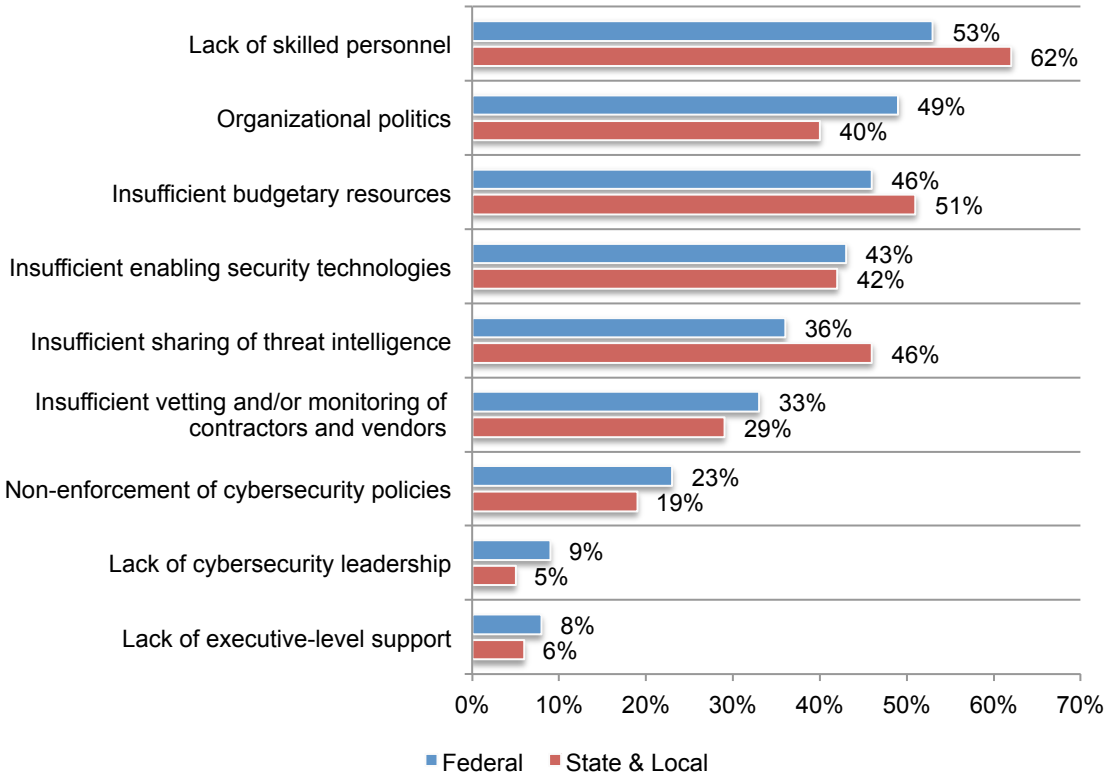
Figure 6. How organizations rate their ability to prevent, detect, contain and recover from a cyber attack
7+ on a scale of 1 = low to 10 = high



A lack of skilled personnel is a challenge at the local, state and federal organizations. However, the challenge is more severe at the state and local level (62 percent say this is a major challenge) as shown in Figure 7. At the federal level, 53 percent of respondents say not having the necessary expertise is a disadvantage.

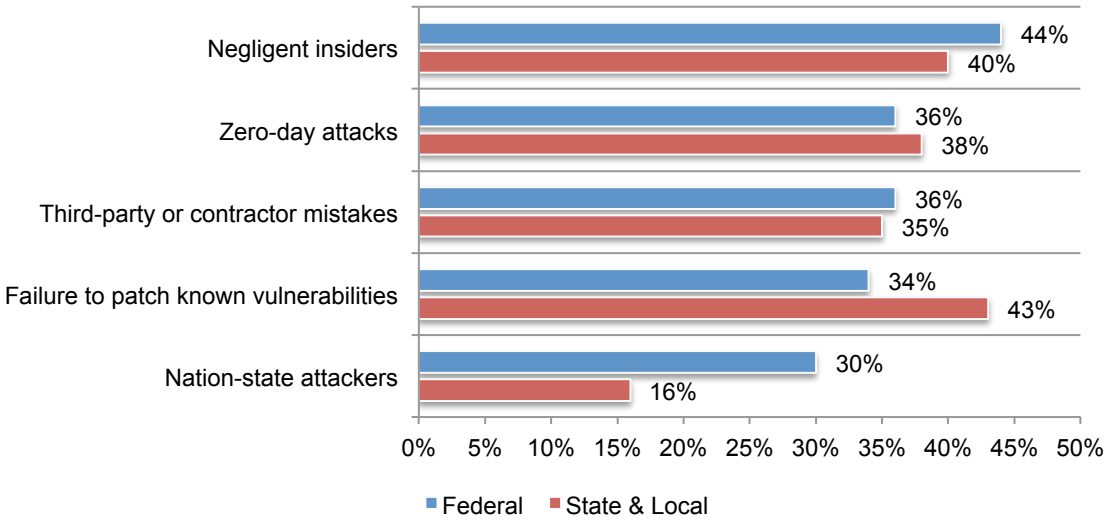
Both groups see lack of budgetary resources as an issue. State and local respondents say they are not as involved as they should be in the sharing of threat intelligence. Federal respondents say it is dealing with organizational politics that keeps them from achieving a strong cybersecurity posture within their organizations.

Figure 7. What are the main challenges to achieving a strong cybersecurity posture within your organization?
Three responses permitted



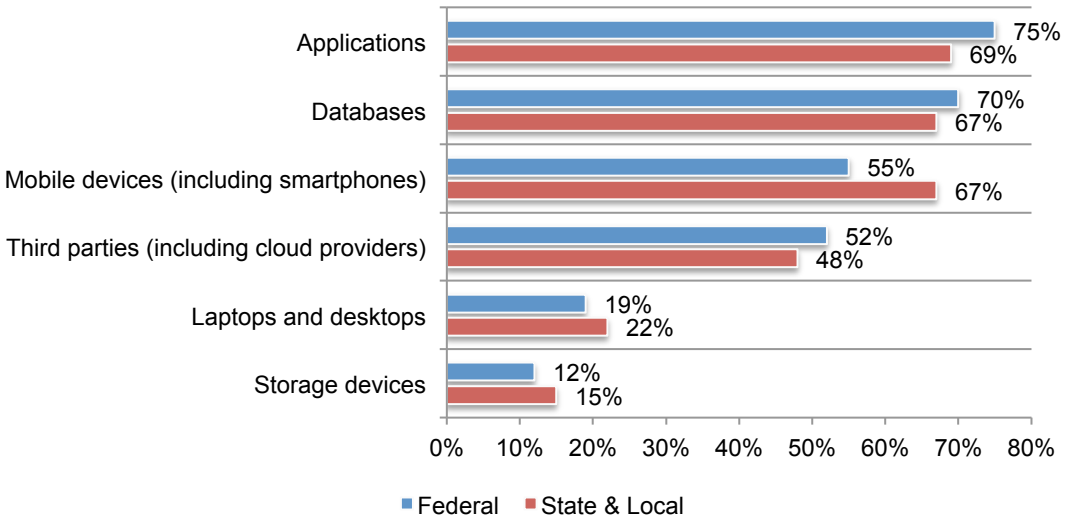
Top security threats differ between federal and state and local organizations. According to Figure 8, the primary security threat facing federal organizations is the negligent insider followed by the zero-day attacks and third party or contractor mistakes. State and local agencies say it is the failure to patch known vulnerabilities, negligent insiders and zero-day attacks. Federal respondents are far more concerned about nation-state attackers (30 percent) versus state and local respondents (16 percent).

Figure 8. What are the top 5 security threats that affect your organization?
Four responses permitted



Information assets are most at risk at the application layer. Databases, mobile devices and cloud providers are also considered prime targets for cyber attacks. Respondents are least concerned about laptops and desktops and storage devices.

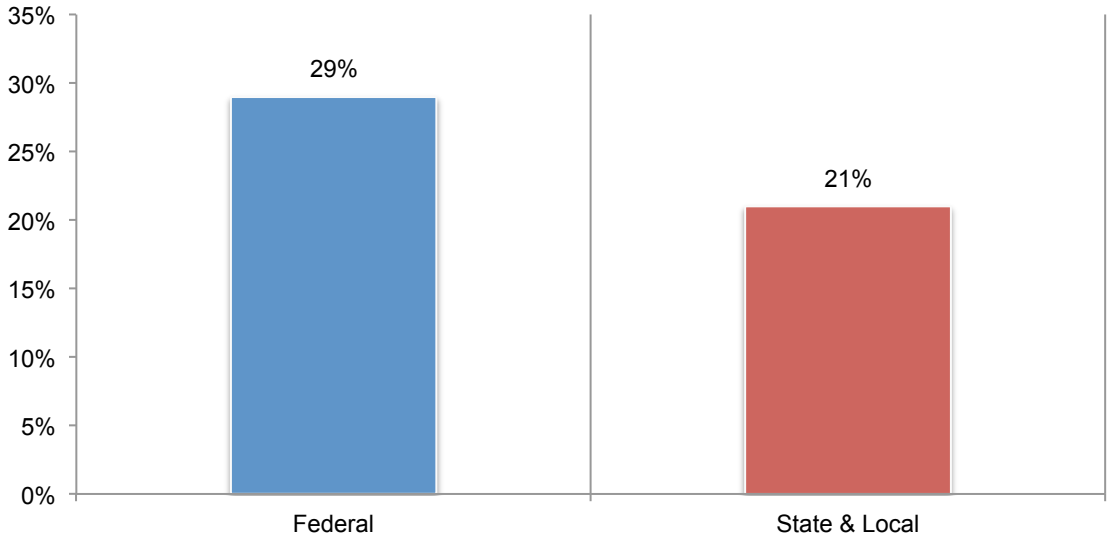
Figure 9. In your organization, where are your information assets most susceptible to loss, theft, misuse or other security compromise?
Three responses permitted



Threat intelligence sharing is ineffective

The collection and use of actionable intelligence to predict malicious IP activities is considered essential but at this time ineffective. While almost every federal, state and local respondent says gathering and using threat intelligence is essential to a strong cybersecurity posture, they report their organizations are not able to collect and use it effectively. As revealed in Figure 10, only 29 percent of federal respondents and 21 percent of state and local respondents say collection and use of actionable intelligence from such sources as vendor-supplied threat feeds is effective.

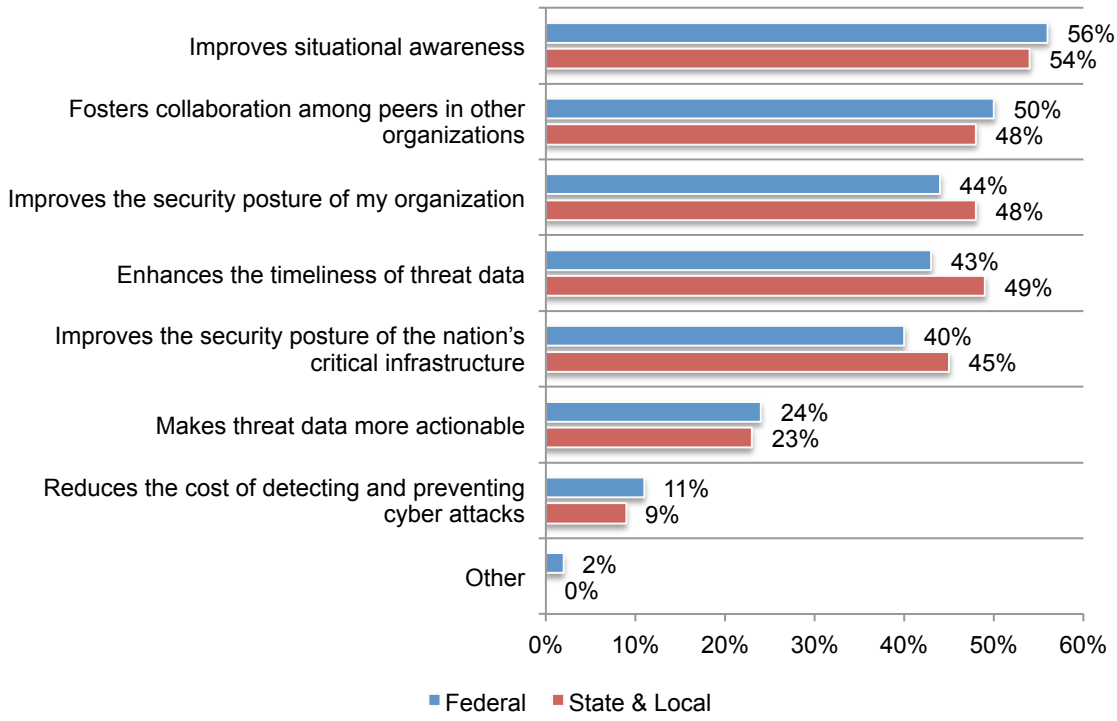
Figure 10. How effective is your organization's collection and use of actionable intelligence from various sources to predict malicious IP activities?
7 + on a scale of 1 = low effectiveness to 10 = high effectiveness



Improving situational awareness is the main reason many organizations participate in an initiative or program for exchanging threat intelligence. Seventy-two percent of federal respondents and 55 percent of state and local respondents say they exchange threat intelligence with peers, government entities and/or commercial companies.

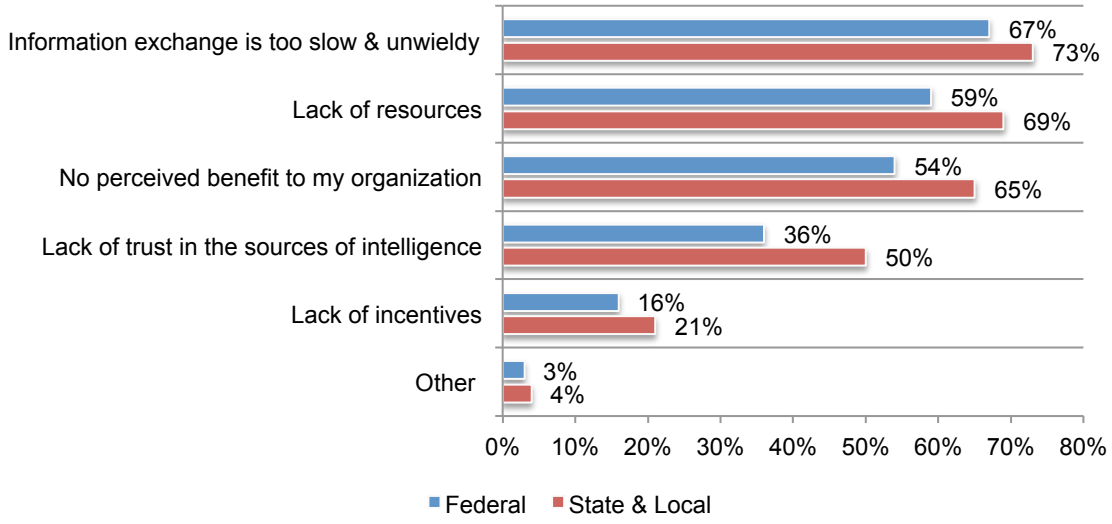
Besides benefiting from situational awareness, respondents say it fosters collaboration among peers in other organization and improves their security posture. While federal respondents believe their top priority is to protect the critical national infrastructure, only 40 percent say a main reason for exchanging threat intelligence is to improve the security posture of the nation's critical infrastructure.

Figure 11. What are the main reasons your organization participates in an initiative or program for exchanging threat intelligence with peers, government entities and/or commercial companies?
More than one response permitted



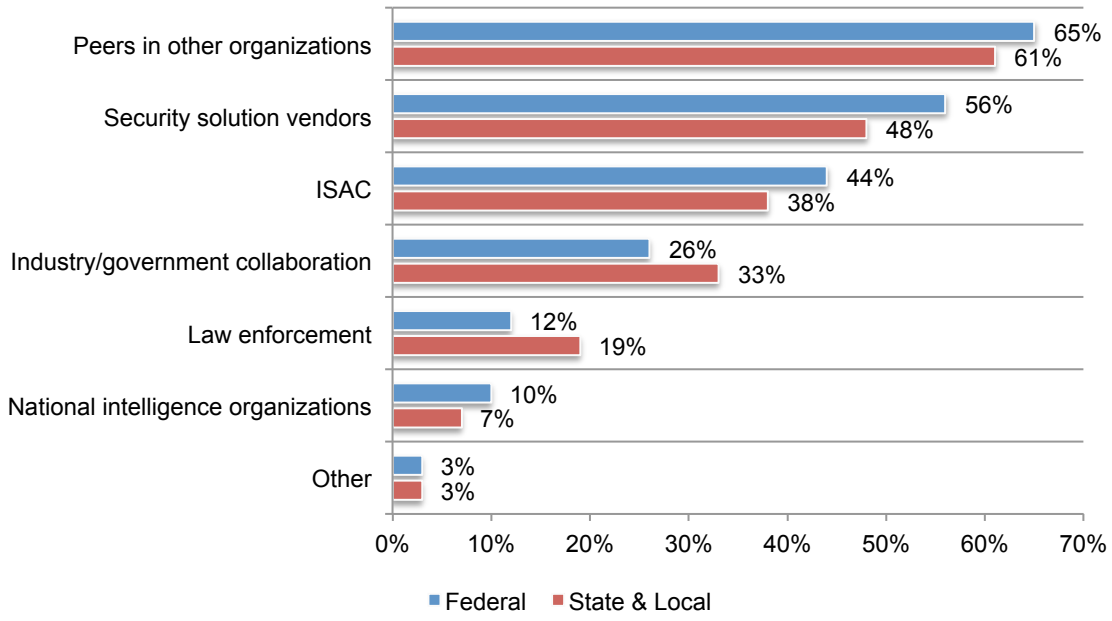
If they do not share intelligence, as shown in Figure 12, it is because information exchange is too slow and unwieldy, they lack the resources and there is no perceived benefit.

Figure 12. What are the main reasons for not participating in exchanging threat intelligence?
More than one response permitted



Federal, state and local agencies choose to share intelligence with the private sector—not government. Threat intelligence is mainly exchanged through a government exchange and respondents say it is only somewhat effective or not effective (57 percent of federal respondents and 70 percent of state and local respondents). As shown in Figure 13, when asked how they mainly share intelligence, it is with peers in other organizations, security solution vendors and ISAC. Very few say it is with law enforcement and national intelligence organizations.

Figure 13. What organizations do you share threat intelligence with?
More than one response permitted

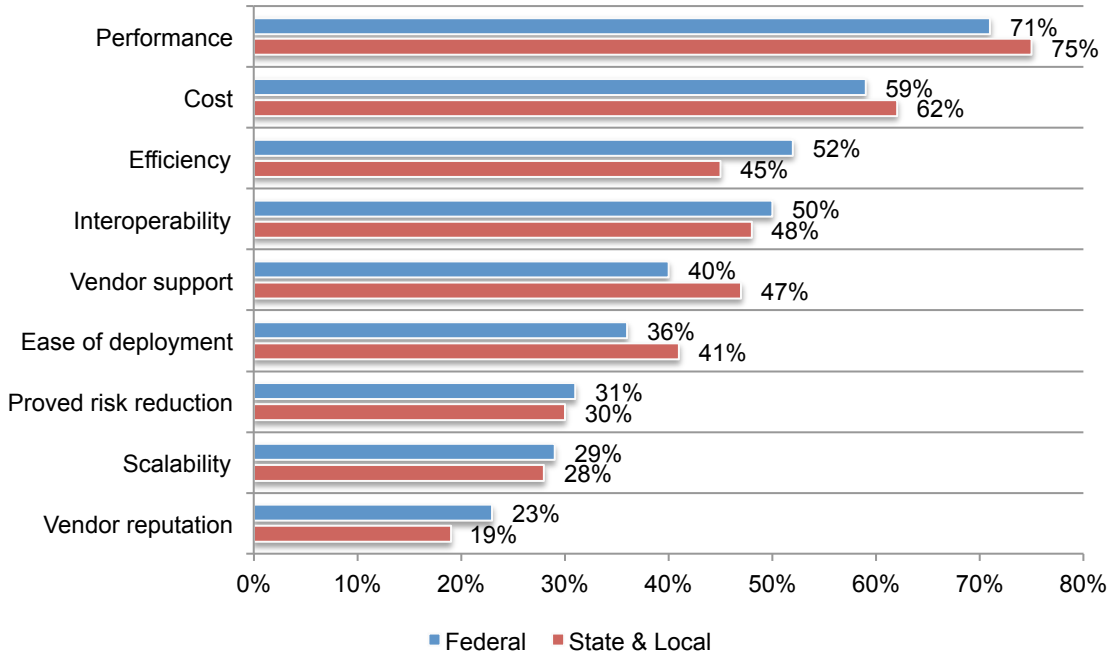


Necessity drives security innovation

Performance and cost are the factors used to determine the viability of a particular security technology. Federal respondents value efficiency and state and local government respondents say vendor support is key, as shown in Figure 14.

The top technologies deployed at all levels of governments are anti-virus/anti-malware, identity & access management and intrusion & detection management solutions. Despite the advantages of big data analytics for prevention and detection of cyber attacks, only 16 percent of federal and 8 percent of state and local respondents say their organizations are using it.

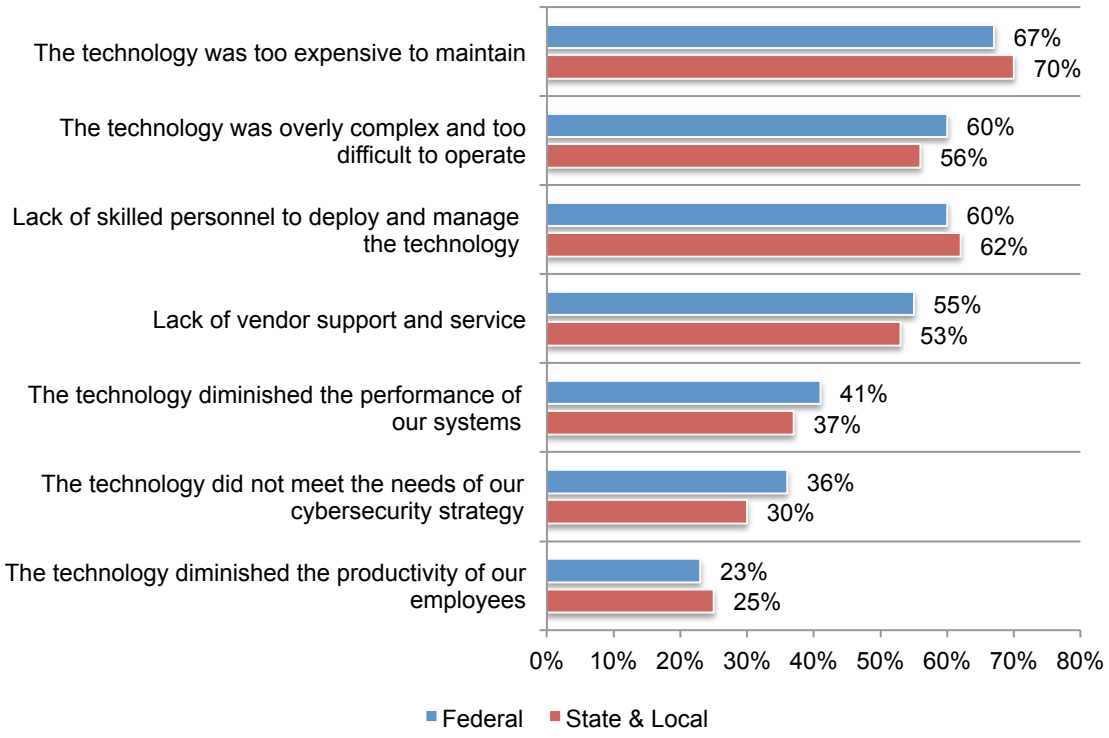
Figure 14. What factors are most important when determining the viability of security technologies?
Four responses permitted



Most respondents at all levels of government are either very satisfied or satisfied with the enabling technologies currently used (62 percent of federal respondents and 61 percent of state and local respondents).

Those respondents in the minority who are not satisfied say it is because of the expense in maintaining the technology, the complexity and difficulty in operating the technology and the lack of skilled personnel to deploy and manage the technology.

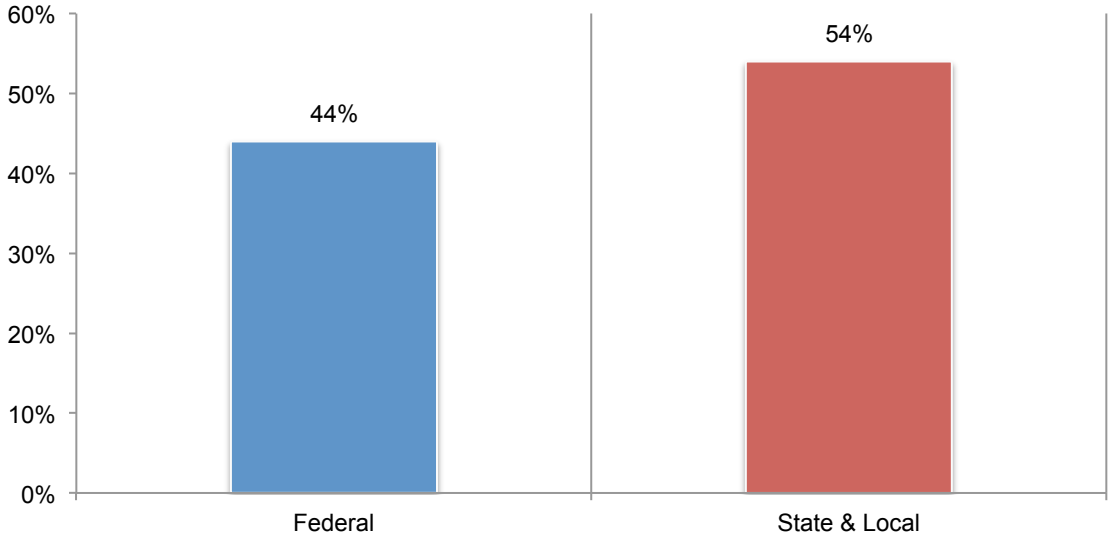
Figure 15. Reasons for not being satisfied with enabling security technologies used by your organization
More than one response permitted



Necessity is the mother of invention and security innovation. In this study, we define security innovation as the use of enabling technologies and personnel in new ways to create a more secure and efficient organization and to improve alignment between security initiatives and organizational mission.

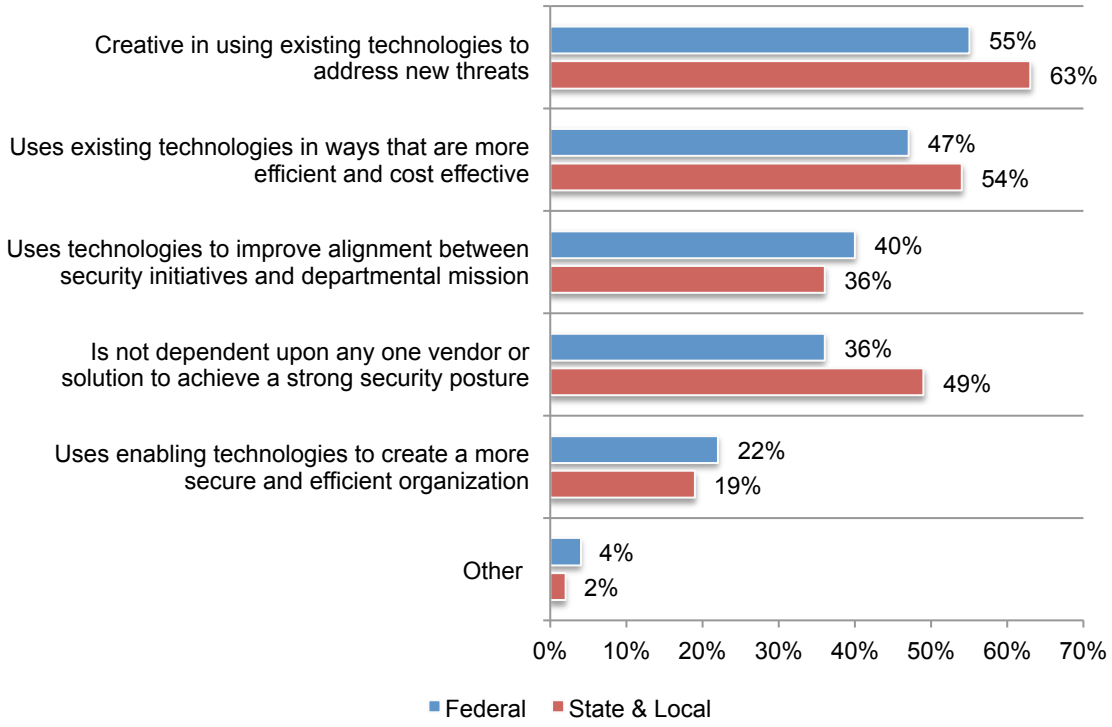
Based on the definition provided in the survey, state and local government respondents are more positive about their ability to innovate.

Figure 16. What is your organization's level of security innovation today?
7 + on a scale of 1 = low innovation to 10 = high level of innovation



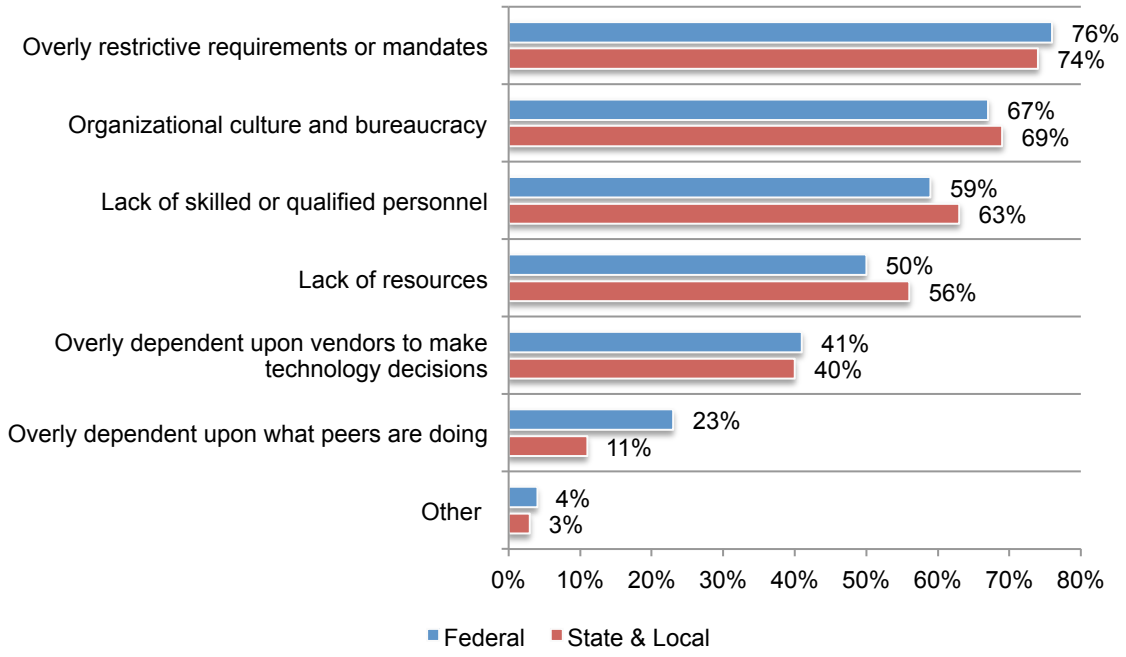
According to respondents who rate their organization's ability to innovate as high, it is mainly because they are creative in using existing technologies to address new threats and they are able to use existing technologies that are more efficient and cost effective. Almost half of state and local respondents (49 percent) say they are innovative because they are not dependent upon any one vendor or solution to achieve a strong security posture.

Figure 17. Why do you think your organization is innovative?
More than one response permitted



While all respondents believe security Innovation is important, those who are not able to innovate say it is because of the overly restrictive requirements or mandates, organizational culture and bureaucracy and lack of skilled or qualified personnel. The biggest difference between the two groups is overly dependent on what peers are doing (23 percent of federal vs. 11 percent of state and local respondents). State and local respondents are also more likely to blame a lack of resources on their inability to be innovative.

Figure 18. Reasons why organizations are not innovative
More than one response permitted



Part 4. Methods

A sampling frame composed of 25,540 IT and IT security practitioners located in federal, state and local governments and who are familiar with their organization's ability to defend against cybersecurity attacks and have some involvement in cybersecurity activities were selected for participation in this survey. As shown in Table 1, 938 respondents completed the survey. Screening removed 93 surveys. The final sample was composed of 443 federal government respondents and 402 state and local government respondents.

Table 1. Sample response	Federal	State & Local	Combined
Total sampling frame	12,990	12,550	25,540
Total returns	496	442	938
Rejected or screened surveys	53	40	93
Final sample	443	402	845
Response rate	3.4%	3.2%	3.3%

Table 2 reports the current position or organizational level of respondents. As shown, more than half of Federal respondents (58 percent) and state and local respondents (61 percent) reported their position as supervisory or above.

Table 2. Current position or organizational level	Federal	State & Local	Combined
Director	17%	15%	16%
Manager	23%	26%	24%
Supervisor	18%	20%	19%
Technician	25%	27%	26%
Staff/associate	16%	12%	14%
Other	1%	0%	1%
Total	100%	100%	100%

As shown in Table 3, 70 percent of federal respondents and 73 percent of state and local respondents indicated civil servant as their current status.

Table 3. Current status	Federal	State & Local	Combined
Civil servant	70%	73%	71%
Political appointee	16%	9%	13%
Contractor	14%	18%	16%
Total	100%	100%	100%

As shown in Table 4, 40 percent of federal respondents are from organizations with a total headcount of more than 1,000 employees. Seventy-five percent of state and local respondents are from organizations with less than 1,000 employees.

Table 4. Total organizational headcount	Federal	State & Local	Combined
Less than 100	6%	16%	11%
100 to 500	21%	33%	27%
501 to 1,000	33%	26%	30%
1,001 to 5,000	23%	18%	21%
5,001 to 25,000	10%	6%	8%
25,001 to 75,000	4%	1%	3%
More than 75,000	3%	0%	2%
Total	100%	100%	100%

As shown in Table 5, 61 percent of federal respondents are located in the Mid-Atlantic region followed by 12 percent in the Northeast. Twenty percent of state and local respondents are located in the Northeast followed by 19 percent in the Mid-Atlantic and 18 percent in the Pacific-West.

Table 5. U.S. region of the organization	Federal	State & Local	Combined
Northeast	12%	20%	16%
Mid-Atlantic	61%	19%	41%
Midwest	8%	17%	12%
Southeast	6%	13%	9%
Southwest	3%	13%	8%
Pacific-West	8%	18%	13%
Other	2%	0%	1%
Total	100%	100%	100%

Part 5. Caveats

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

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

Sampling frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners in federal, state and local governments. 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 specified time period.

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

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in July 2015.

Survey response	Federal	State & Local	Combined
Total sampling frame	12990	12550	25540
Total returns	496	442	938
Rejected or screened surveys	53	40	93
Final sample	443	402	845
Response rate	3.4%	3.2%	3.3%
Sample weights	52.4%	47.6%	100.0%

Part 1. Screening questions			
S1. What best describes your organization?	Federal	State & Local	Combined
U.S. federal department or agency	100%	0%	100%
U.S. state government	0%	48%	48%
U.S. local or municipal government	0%	43%	43%
Public educational institution	0%	9%	9%
None of the above (stop)	0%	0%	0%
Total	100%	100%	200%

S2. What best describes your role in the cybersecurity function within your organization?	Federal	State & Local	Combined
High level of involvement	40%	42%	41%
Moderate level of involvement	45%	47%	46%
Low level of involvement	15%	11%	13%
Not involved (stop)	0%	0%	0%
Total	100%	100%	100%

S3. How familiar are you with your organization's cyber defenses?	Federal	State & Local	Combined
Very familiar	44%	50%	47%
Familiar	47%	44%	46%
Not familiar	9%	6%	8%
No knowledge (stop)	0%	0%	0%
Total	100%	100%	100%

S4. What best describes your decision-making responsibilities for deploying cybersecurity solutions?	Federal	State & Local	Combined
Primary decision-making responsibility	25%	23%	24%
Some decision-making responsibility	42%	42%	42%
Influencer, not a decision maker	33%	35%	34%
None of the above (stop)	0%	0%	0%
Total	100%	100%	100%

Part 2. Attributions: Please rate each one of the following statements using the scale provided below each item. Strongly agree and agree responses combined.	Federal	State & Local	Combined
Q1a. My organization has sufficient resources to achieve its mission.	44%	35%	40%
Q1b. My organization has sufficient resources to achieve compliance with leading security standards such as the NIST Cybersecurity Framework, FISMA and others.	47%	36%	42%
Q1c. My organization deploys state-of-the-art technologies to minimize cybersecurity risks such as behavioral analytics, NGFW, SIEM, encryption, big data solutions and others.	50%	38%	44%
Q1d. My organization recruits and retains ample expert personnel to minimize cybersecurity risks.	55%	31%	44%
Q1e. Cybersecurity priorities are clearly defined and consistently supported throughout my organization..	48%	29%	39%
Q1f. Intelligence sharing between my organization and other government entities reduces cybersecurity risks.	67%	50%	59%
Q1g. Managing cybersecurity risk in my organization is one of the most stressful jobs.	73%	86%	79%

Part 3. Background Questions

Q2. Using the following 10-point scale, please rate your organization's ability to **prevent** a cyber attack from 1 = low to 10 = high.	Federal	State & Local	Combined
1 or 2	12%	30%	21%
3 or 4	34%	35%	34%
5 or 6	13%	16%	14%
7 or 8	20%	11%	16%
9 or 10	21%	8%	15%
Total	100%	100%	100%
Extrapolated value	5.58	4.14	4.89

Q3. Using the following 10-point scale, please rate your organization's ability to quickly **detect** a cyber attack from 1 = low to 10 = high.	Federal	State & Local	Combined
1 or 2	8%	13%	10%
3 or 4	25%	29%	27%
5 or 6	21%	26%	23%
7 or 8	25%	16%	21%
9 or 10	21%	16%	19%
Total	100%	100%	100%
Extrapolated value	6.02	5.36	5.71

Q4. Using the following 10-point scale, please rate your organization's ability to **contain** a cyber attack from 1 = low to 10 = high.	Federal	State & Local	Combined
1 or 2	10%	15%	12%
3 or 4	16%	27%	21%
5 or 6	22%	20%	21%
7 or 8	26%	20%	23%
9 or 10	26%	18%	22%
Total	100%	100%	100%
Extrapolated value	6.34	5.48	5.93

Q5. Using the following 10-point scale, please rate your organization's ability to fully **recover** from a cyber attack from 1 = low to 10 = high.	Federal	State & Local	Combined
1 or 2	10%	14%	12%
3 or 4	14%	31%	22%
5 or 6	21%	27%	24%
7 or 8	32%	16%	24%
9 or 10	23%	12%	18%
Total	100%	100%	100%
Extrapolated value	6.38	5.12	5.78

Q6. What best describes the maturity level of your organization's cybersecurity program or activities today?	Federal	State & Local	Combined
Early	14%	25%	19%
Middle	26%	37%	31%
Late-middle	34%	25%	30%
Mature	26%	13%	20%
Total	100%	100%	100%

Q7. What are the top cybersecurity objectives within your organization? Check only the top three choices.	Federal	State & Local	Combined
Prevent cyber attacks	23%	25%	24%
Detect cyber attacks	27%	29%	28%
Minimize IT downtime	44%	51%	47%
Comply with regulatory and legal mandates	54%	48%	51%
Secure the national critical infrastructure	61%	56%	59%
Improve the organization's cybersecurity posture	45%	45%	45%
Protect the public's private information	35%	33%	34%
Share cybersecurity intelligence	11%	13%	12%
Other (please specify)	0%	0%	0%
Total	300%	300%	300%

Q8. What are the main challenges to achieving a strong cybersecurity posture within your organization? Check only the top three choices.	Federal	State & Local	Combined
Lack of executive-level support	8%	6%	7%
Lack of skilled personnel	53%	62%	57%
Insufficient budgetary resources	46%	51%	48%
Lack of cybersecurity leadership	9%	5%	7%
Insufficient enabling security technologies	43%	42%	43%
Insufficient sharing of threat intelligence	36%	46%	41%
Organizational politics	49%	40%	45%
Non-enforcement of cybersecurity policies	23%	19%	21%
Insufficient vetting and/or monitoring of contractors and vendors	33%	29%	31%
Other (please specify)	0%	0%	0%
Total	300%	300%	300%

Q9. What are the top security threats that affect your organization? Check only the top four choices.	Federal	State & Local	Combined
Advanced persistent threats	21%	20%	21%
Zero-day attacks	36%	38%	37%
Identity theft/fraud	9%	11%	10%
Credential theft	10%	11%	10%
Negligent insiders	44%	40%	42%
System glitches	23%	31%	27%
Malicious insiders	19%	16%	18%
Web-based attacks	29%	30%	29%
Insecure web applications	13%	11%	12%
Insecure endpoints	28%	35%	31%
Insecure network gateways	10%	6%	8%
Third-party or contractor mistakes	36%	35%	36%
Denial of service attacks	25%	23%	24%
Failure to patch known vulnerabilities	34%	43%	38%
Electronic agents such malware, botnets and others	15%	16%	15%
Nation-state attackers	30%	16%	23%
Phishing	18%	18%	18%
Other (please specify)	0%	0%	0%
Total	400%	400%	400%

Q10. In your organization, where is data (information assets) most susceptible to loss, theft, misuse or other security compromise? Please select the top three choices.	Federal	State & Local	Combined
Applications	75%	69%	72%
Databases	70%	67%	69%
Storage devices	12%	15%	13%
Servers	3%	2%	3%
Laptops and desktops	19%	22%	20%
Data capture devices	2%	1%	2%
Mobile devices (including smartphones)	55%	67%	61%
Third parties (including cloud providers)	52%	48%	50%
Backup media	8%	6%	7%
Paper documents	4%	3%	4%
Other (please specify)	0%	0%	0%
Total	300%	300%	300%

Q11a. How many material security breaches did your organization experience in the past 24 months?	Federal	State & Local	Combined
None (skip to Q11)	11%	20%	15%
1 to 5	21%	19%	20%
6 to 10	37%	34%	36%
11 to 25	18%	15%	17%
More than 25	13%	12%	13%
Total	100%	100%	100%
Extrapolated value	10.5	9.4	9.9

Q11b. Were any of these security breaches the result of nation-state attackers?	Federal	State & Local	Combined
Yes	18%	11%	15%
No	42%	59%	50%
Unsure	40%	30%	35%
Total	100%	100%	100%

Q12. How effective is your organization's collection and use of actionable intelligence from various sources (such as vendor-supplied threat feeds) to predict malicious IP activities? Please use the following scale from 1 = low effectiveness to 10 = high effectiveness.	Federal	State & Local	Combined
1 or 2	12%	22%	17%
3 or 4	24%	34%	29%
5 or 6	35%	23%	29%
7 or 8	17%	13%	15%
9 or 10	12%	8%	10%
Total	100%	100%	100%
Extrapolated value	5.36	4.52	4.96

Q13. Do you believe gathering and using threat intelligence is essential to a strong security posture?	Federal	State & Local	Combined
Yes	87%	90%	88%
No	13%	10%	12%
Total	100%	100%	100%

Q14a. Does your organization participate in an initiative or program for exchanging threat intelligence with peers, government entities and/or commercial companies?	Federal	State & Local	Combined
Yes	72%	55%	64%
No	28%	45%	36%
Total	100%	100%	100%

Q14b. If yes, what are the main reasons?	Federal	State & Local	Combined
Improves the security posture of my organization	44%	48%	46%
Improves the security posture of the nation's critical infrastructure	40%	45%	42%
Reduces the cost of detecting and preventing cyber attacks	11%	9%	10%
Improves situational awareness	56%	54%	55%
Fosters collaboration among peers in other organizations	50%	48%	49%
Enhances the timeliness of threat data	43%	49%	46%
Makes threat data more actionable	24%	23%	24%
Other (please specify)	2%	0%	1%
Total	270%	276%	273%

Q14c. If no, what are the main reasons?	Federal	State & Local	Combined
Lack of resources	59%	69%	64%
Lack of incentives	16%	21%	18%
No perceived benefit to my organization	54%	65%	59%
Information exchange is too slow & unwieldy	67%	73%	70%
Lack of trust in the sources of intelligence	36%	50%	43%
Other (please specify)	3%	4%	3%
Total	235%	282%	257%

Q14d. If yes, how does your organization exchange threat intelligence? Please select all that apply.	Federal	State & Local	Combined
Through a government exchange	92%	91%	92%
Through a vendor threat exchange service	57%	49%	53%
Informal peer-to-peer exchange of information	35%	36%	35%
Other (please specify)	2%	3%	2%
Total	186%	179%	183%

Q14e. Please select all the organizations with which you share threat intelligence.	Federal	State & Local	Combined
ISAC	44%	38%	41%
Industry/government collaboration	26%	33%	29%
Peers in other organizations	65%	61%	63%
Security solution vendors	56%	48%	52%
Law enforcement	12%	19%	15%
National intelligence organizations	10%	7%	9%
Other (please specify)	3%	3%	3%
Total	216%	209%	213%

Q14f. How effective is the collaboration between your organization and other entities in the sharing of threat intelligence?	Federal	State & Local	Combined
Very effective	18%	12%	15%
Effective	25%	18%	22%
Somewhat effective	30%	30%	30%
Not effective	27%	40%	33%
Total	100%	100%	100%

Part 4. Technology investments

Q15. What factors are most important when determining the viability of security technologies? Please select the top four choices.	Federal	State & Local	Combined
Cost	59%	62%	60%
Performance	71%	75%	73%
Efficiency	52%	45%	49%
Proved risk reduction	31%	30%	31%
Vendor support	40%	47%	43%
Vendor reputation	23%	19%	21%
Interoperability	50%	48%	49%
Scalability	29%	28%	29%
Redundancy	8%	3%	6%
Ease of deployment	36%	41%	38%
Other (please specify)	1%	2%	1%
Total	400%	400%	400%

Q16. Please select all the technologies that are presently deployed within your organization.	Federal	State & Local	Combined
Anti-virus / anti-malware	99%	96%	98%
Identity & access management	89%	76%	83%
Intrusion & detection management	89%	85%	87%
Virtual private network (VPN)	67%	53%	60%
Configuration & log management	65%	63%	64%
Encryption for data in motion	55%	47%	51%
Encryption for data at rest	54%	47%	51%
Database scanning & monitoring	53%	44%	49%
URL or content filtering	53%	52%	53%
Web application firewalls (WAF)	53%	46%	50%
Key management tools	51%	44%	48%
Sandboxing or isolation tools	49%	39%	44%
Endpoint security solutions	48%	45%	47%
SIEM and security intelligence	45%	41%	43%
Perimeter or location surveillance	44%	45%	44%
Data loss prevention (DLP)	40%	36%	38%
Next generation firewalls (NGFW)	39%	29%	34%
Forensic tools	33%	30%	32%
Mobile device management	30%	24%	27%
Big data analytics for cyber	16%	8%	12%
Automated policy generation	11%	8%	10%
Device anti-theft solutions	9%	6%	8%

Q17a. What best describes your level of satisfaction with the enabling security technologies used by your organization?	Federal	State & Local	Combined
Very satisfied	23%	25%	24%
Satisfied	39%	36%	38%
Not satisfied	38%	39%	38%
Total	100%	100%	100%

Q17b. If not satisfied, why? Please select all that apply.	Federal	State & Local	Combined
Lack of skilled personnel to deploy and manage the technology	60%	62%	61%
The technology did not meet the needs of our cybersecurity strategy	36%	30%	33%
The technology was overly complex and too difficult to operate	60%	56%	58%
Lack of vendor support and service	55%	53%	54%
The technology was too expensive to maintain	67%	70%	68%
The technology diminished the productivity of our employees	23%	25%	24%
The technology diminished the performance of our systems	41%	37%	39%
Total	342%	333%	338%

Part 5. Security Innovation

Q18a. Based on the above definition, please rate your organization's level of security innovation today using the following 10-point scale.	Federal	State & Local	Combined
1 or 2	21%	18%	20%
3 or 4	20%	13%	17%
5 or 6	15%	15%	15%
7 or 8	21%	27%	24%
9 or 10	23%	27%	25%
Total	100%	100%	100%
Extrapolated value	5.60	6.14	5.86

Q18b. [For risk score at or above 6] If your organization is innovative, why?	Federal	State & Local	Combined
Uses enabling technologies to create a more secure and efficient organization	22%	19%	21%
Uses technologies to improve alignment between security initiatives and departmental mission	40%	36%	38%
Creative in using existing technologies to address new threats	55%	63%	59%
Uses existing technologies in ways that are more efficient and cost effective	47%	54%	50%
Is not dependent upon any one vendor or solution to achieve a strong security posture	36%	49%	42%
Other (please specify)	4%	2%	3%
Total	204%	223%	213%

Q18c. [For risk score at or below 5] If your organization is not innovative, why?	Federal	State & Local	Combined
Lack of resources	50%	56%	53%
Organizational culture and bureaucracy	67%	69%	68%
Overly dependent upon vendors to make technology decisions	41%	40%	41%
Overly dependent upon what peers are doing	23%	11%	17%
Overly restrictive requirements or mandates	76%	74%	75%
Lack of skilled or qualified personnel	59%	63%	61%
Other (please specify)	4%	3%	4%
Total	320%	316%	318%

Q19. In your opinion, what is the relative importance of security innovation to achieving a strong security posture? Please use the following scale.	Federal	State & Local	Combined
Essential	11%	13%	12%
Very important	27%	33%	30%
Important	34%	30%	32%
Not important	20%	18%	19%
Irrelevant	8%	6%	7%
Total	100%	100%	100%

Part 6. Your role and organization

D1. What organizational level best describes your current position level?	Federal	State & Local	Combined
Director	17%	15%	16%
Manager	23%	26%	24%
Supervisor	18%	20%	19%
Technician	25%	27%	26%
Staff/associate	16%	12%	14%
Other (please specify)	1%	0%	1%
Total	100%	100%	100%

D2. What best describes your current status?	Federal	State & Local	Combined
Civil servant	70%	73%	71%
Political appointee	16%	9%	13%
Contractor	14%	18%	16%
Total	100%	100%	100%

D3. What U.S. region best defines the location of your organization?	Federal	State & Local	Combined
Northeast	12%	20%	16%
Mid-Atlantic	61%	19%	41%
Midwest	8%	17%	12%
Southeast	6%	13%	9%
Southwest	3%	13%	8%
Pacific-West	8%	18%	13%
Other (please specify)	2%	0%	1%
Total	100%	100%	100%

D4. What is the total headcount of your organization?	Federal	State & Local	Combined
Less than 100	6%	16%	11%
100 to 500	21%	33%	27%
501 to 1,000	33%	26%	30%
1,001 to 5,000	23%	18%	21%
5,001 to 25,000	10%	6%	8%
25,001 to 75,000	4%	1%	3%
More than 75,000	3%	0%	2%
Total	100%	100%	100%

Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

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.