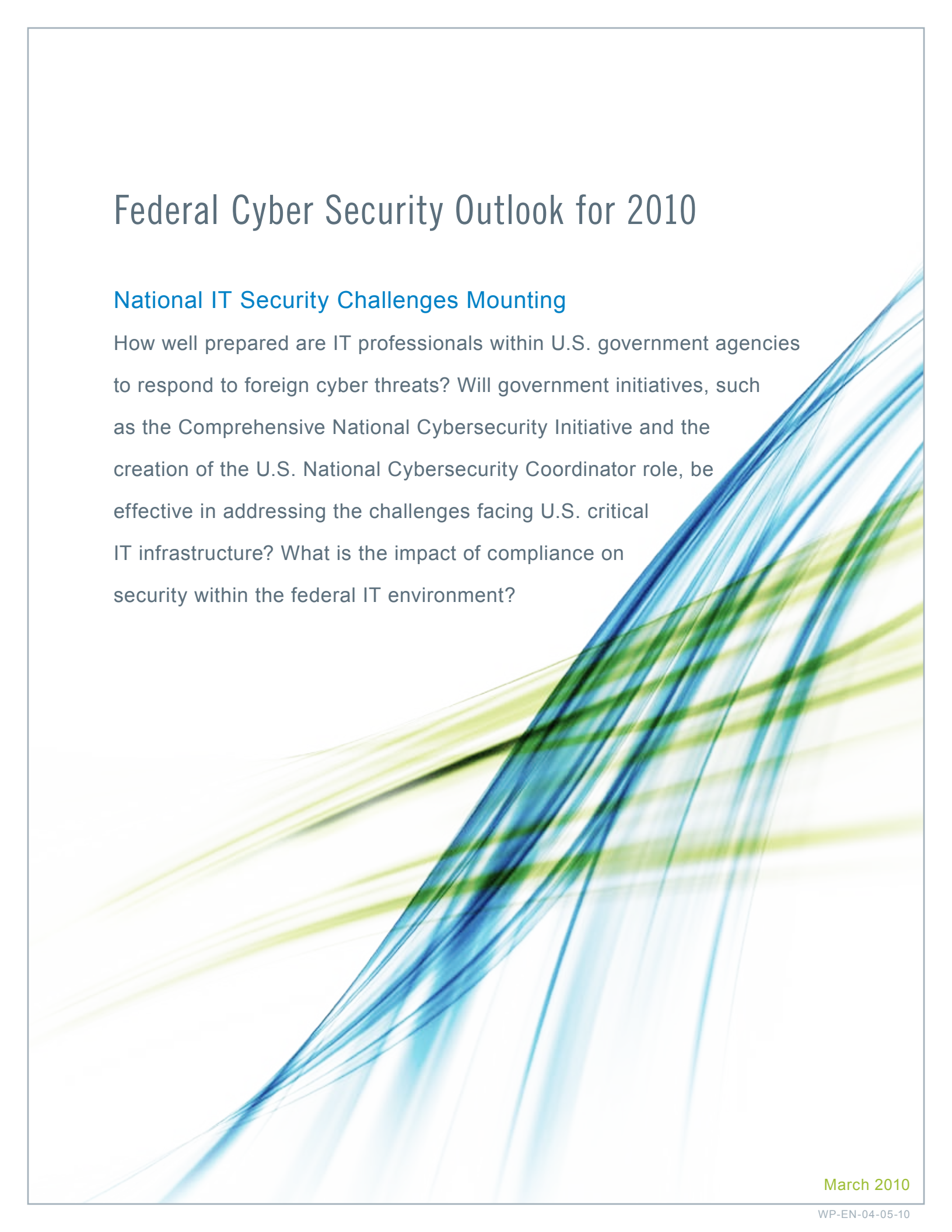
Federal Cyber Security Outlook for 2010

National IT Security Challenges Mounting

How well prepared are IT professionals within U.S. government agencies to respond to foreign cyber threats? Will government initiatives, such as the Comprehensive National Cybersecurity Initiative and the creation of the U.S. National Cybersecurity Coordinator role, be effective in addressing the challenges facing U.S. critical IT infrastructure? What is the impact of compliance on security within the federal IT environment?



March 2010

WP-EN-04-05-10

Executive Summary:

How well prepared are IT professionals within U.S. government agencies to respond to foreign cyber threats? Will government initiatives, such as the Comprehensive National Cybersecurity Initiative and the creation of the U.S. National Cybersecurity Coordinator role, be effective in addressing the challenges facing U.S. critical IT infrastructure? What is the impact of compliance on security within the federal IT environment?

Commissioned by Lumension, Clarus Research Group set about to answer these and other important questions facing federal IT in Lumension's "**Federal Cyber Security Outlook for 2010: National IT Security Challenges Mounting**" study. Clarus Research Group interviewed over 200 federal IT decision-makers and influencers about endpoint operations, IT security and compliance issues.

The survey identifies the top security risks facing federal IT in the coming year as the growing volume and sophistication of cyber attacks and the potential loss of sensitive data due to mounting insider risk. Also, the survey found that there is an advanced persistent threat targeting critical U.S. IT infrastructure. However, current government initiatives, such as the Comprehensive National Cybersecurity Initiative, may not be enough to overcome the challenges facing federal IT professionals in addressing these new risks and challenges.

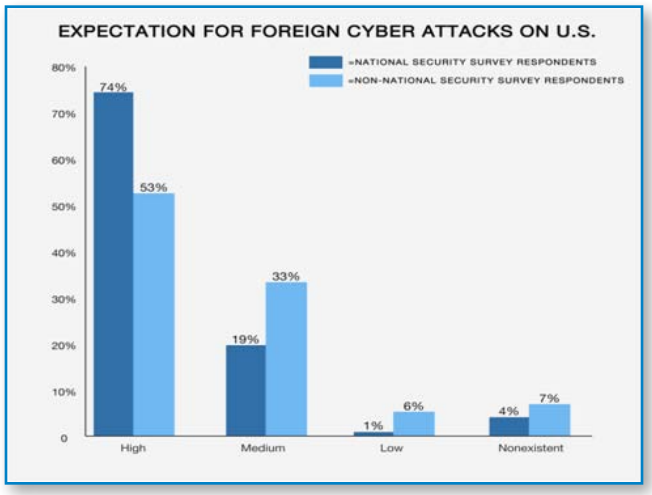
While the majority of respondents feel more confident in their level of IT security today versus a year ago, this is mainly due to improved IT security technology, stronger collaboration between IT operations and security, and a focus on meeting compliance requirements. However, increasing audit burdens and a lack of resources are identified as major challenges in meeting compliance requirements.

While the challenges, threats and risks facing federal IT professionals in their task to secure America's critical IT infrastructure are daunting, these professionals are making progress in meeting these challenges head on. To be successful in the long run, a stronger focus and empowerment of current federal initiatives will be required.

Continued »

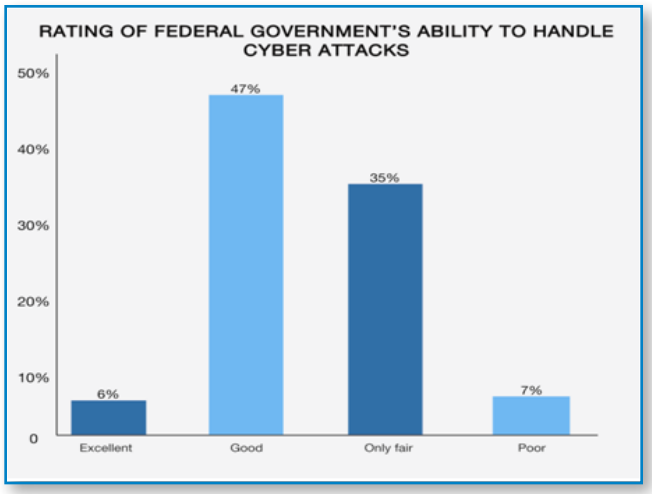
The State of National Security

What is the expectation for foreign cyber attacks on critical U.S. IT infrastructure?



Nearly three-quarters of survey respondents (74 percent) who work in national defense and security departments or agencies say the possibility is "high" for a cyber attack by a foreign nation in the next year. Additionally, a third of these respondents say they have already experienced such a cyber attack within the last year.

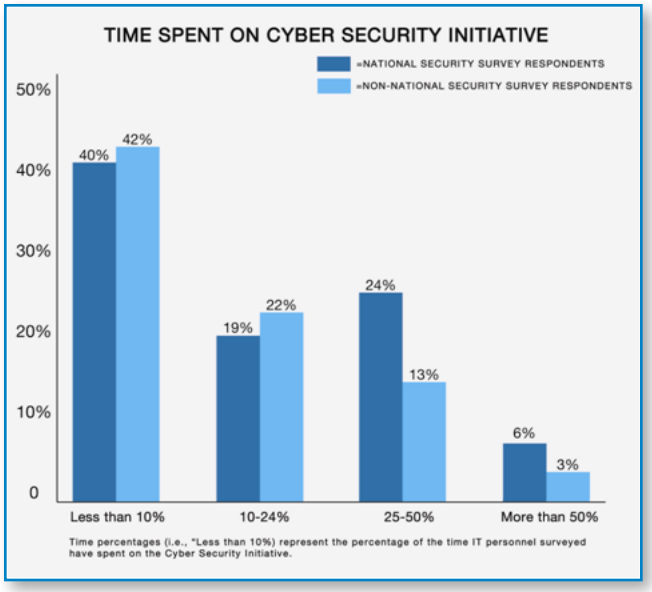
What is the perception of the federal government's ability to handle cyber attacks?



While the majority of respondents rate the government's ability to handle cyber attacks as "good" or "excellent," a significant percentage of IT professionals rated the federal government's ability to handle cyber attacks as "fair" to "poor."

Continued »

How much time is spent working on tasks related to the Comprehensive National Cyber Security Initiative?



Overall, respondents indicate having spent less than 10 percent of their time over the past year working on the Comprehensive National Cybersecurity Initiative.

What type of changes are federal IT pros expecting in terms of cyber security policies with the appointment of the new U.S. National Cybersecurity Coordinator?

More than half of those surveyed expect only minor policy changes as a result of the recently created U.S. National Cybersecurity Coordinator position. Only a small percentage (6 percent) of respondents rate the federal government's overall ability to prevent or handle possible threats from cyber attacks on critical IT infrastructure in the U.S. as "excellent".

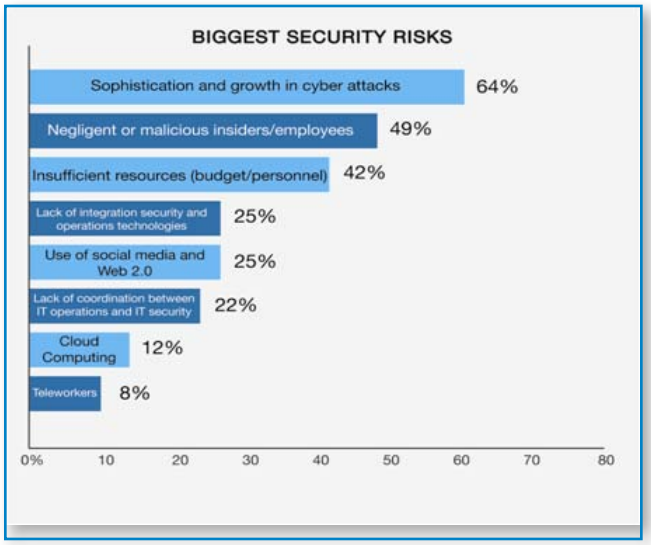
Summary of the State of National Security

An advanced persistent threat to critical U.S. IT infrastructure clearly exits today with an overwhelming majority of IT operations and IT security professionals saying the threat of cyber attacks from foreign nations on critical U.S. technology infrastructure over the next year is "high". In addition, a third of national security IT professionals indicate such attacks have already occurred in the last year. With only a small fraction of respondents indicating the ability of the federal government to handle cyber attacks as "excellent," there exists a large potential for improvement of IT security capabilities and processes.

A key question raised is whether the Comprehensive National Cybersecurity Initiative and the U.S. National Cybersecurity Coordinator are enough to address the growing risk to critical U.S. infrastructure. Most of respondents indicated that they expect only minor policy changes as a result of the initiatives, with little time allocated to tasks related to these efforts.

The State of Federal IT Risk

What are the biggest security risks facing IT professionals in the next year?

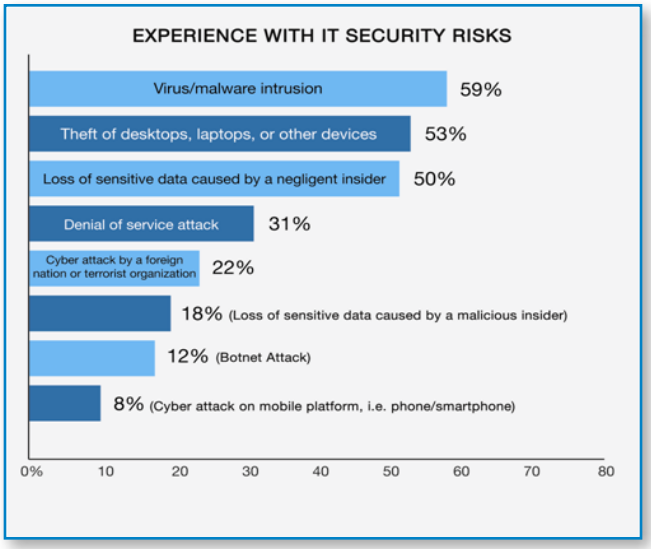


According to federal IT professionals surveyed, the biggest security risks facing their agencies during the next year include the sophistication and volume of cyber attacks on critical IT infrastructure (64 percent), followed by insider risk both accidental and malicious (49 percent). These risks are exacerbated by insufficient resources (i.e. budget and personnel).

National security personnel are much more likely to see negligent or malicious insiders/employees as a security risk than non-national security personnel.

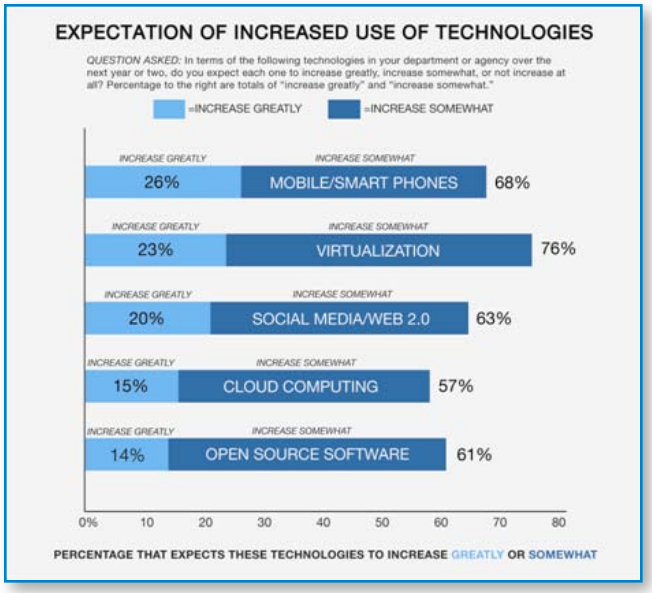
A lack of coordination between IT security and operations and a lack of integration of technologies across the two functional areas are also factors in IT risk. Integration of technologies rated much higher among national security agency respondents than non-national security respondents. Other IT risk drivers include increasing use of social media and Web 2.0 technologies. Interestingly, social media/Web 2.0 is viewed as more of a security risk by non-national security agency respondents than those in national security agencies.

What security incidents happened in your agency or department in the last year?



Malware intrusions, theft of desktops, laptops, or other devices, and loss of sensitive data caused by a negligent insider are the most typical IT security incidents seen across the federal landscape. Interestingly, IT operations personnel reported equally (58 percent) that both virus/malware intrusion and loss of sensitive data by a negligent insider were the most common IT security incidents seen in the last year. Further, 22 percent of total survey respondents indicated they have experienced a cyber attack by a foreign nation or terrorist organization.

What technologies are expected to grow in the coming year within the federal IT environment?



Survey respondents expect virtualization and mobile/smart phone platforms to experience the greatest overall increases. Overall, virtualization, use of Web 2.0 social media applications and mobile smart phone platforms are expected to see the greatest expansion. More than 50 percent of survey respondents said they expect all of the technologies tested to increase either greatly or somewhat. Virtualization scored highest (76 percent) followed by social media/Web 2.0. While cloud computing is much talked about, it scored lowest (57 percent) overall, but was still over 50 percent. Interestingly, cloud computing is expected to increase the most by national security respondents and IT operations personnel.

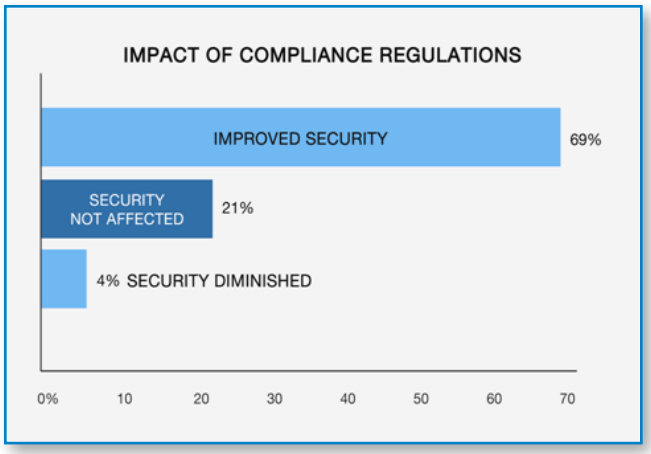
Summary of the State of Federal IT Risk

Federal IT professionals must deal with mounting risk coming from malware and virus intrusions that are both increasing in number and sophistication. Another challenging dimension is added when having to manage the insider risk and the associated loss of potentially sensitive information as a result of negligence or outright maliciousness. These challenges are made even more difficult for federal IT personnel due to lack of coordination across IT operations and security functions, as well as a lack of technology integration between the two areas. This challenge will mount as the endpoint environment is clearly becoming more distributed and virtual, mobile and social.

Continued »

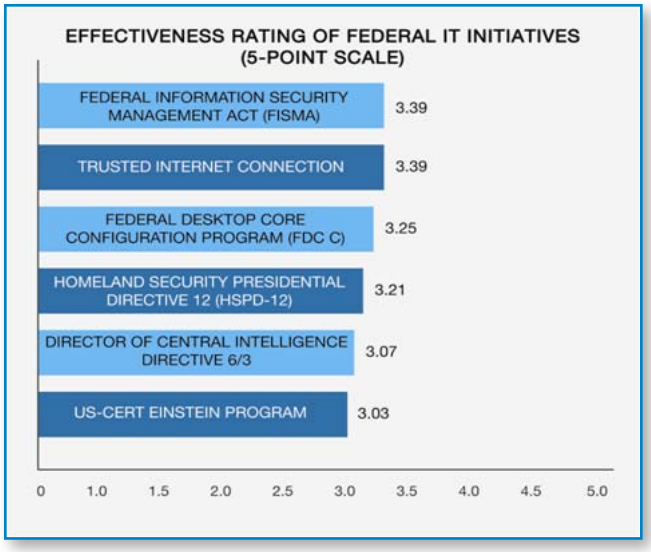
The Impact of Compliance

How have compliance regulations affected your organization's security position?



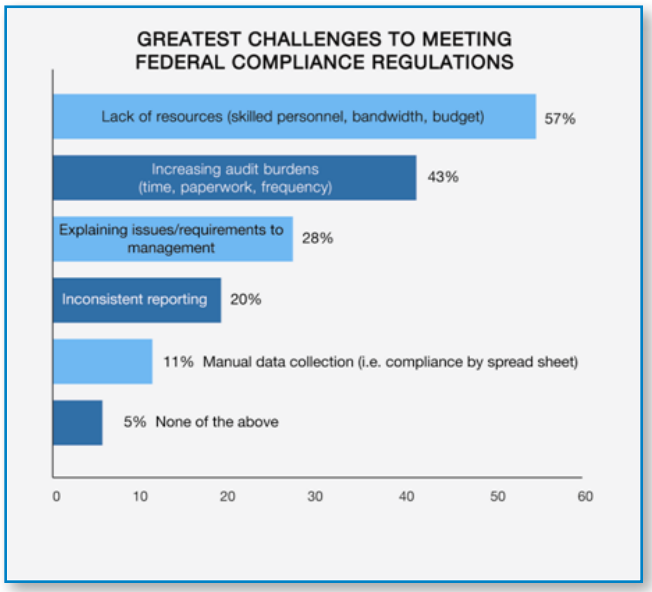
In regards to IT security, the majority of respondents indicated that the overall state of their IT security has improved due to compliance initiatives and audits.

What is the effectiveness of each of the following initiatives in terms of the POSITIVE impact it has had in your organization's IT security?



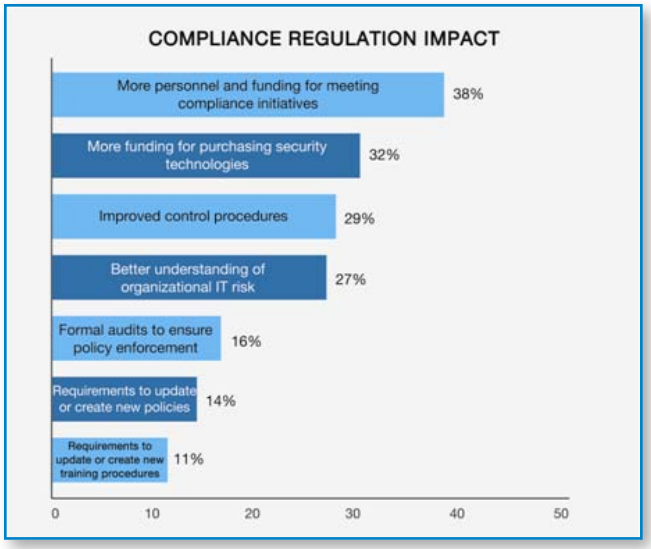
An overwhelming majority rated the effectiveness of federal IT initiatives as generally average (between 3.03 and 3.39 on a 5-point scale, with 5 being most effective), with no clear cut winner in terms of a specific initiative having greatest impact. Of the initiatives measured, the Federal Information Security Management Act (FISMA) and Trusted Internet Connection (TIC) rated on top in terms of effectiveness. US-CERT Einstein Program rated on the bottom.

What are the greatest challenges facing federal IT professionals in meeting compliance regulations?



The greatest challenge in meeting federal compliance regulations for federal IT professionals is the lack of resources (i.e. skilled personnel, bandwidth, and budget) (57 percent). This is especially true of personnel in operations, C-level and general IT roles. The second greatest challenge according to compliance and risk personnel is increasing audit burdens (time, paperwork and frequency), capturing 43 percent.

What compliance regulations have the most impact to your organization's IT security function?



In general, compliance has proved valuable in garnering more resources and personnel for organizations to meet compliance initiatives and purchase new IT security technologies. Additional benefits include improved control procedures and a better understanding of overall organizational IT risk.

While compliance regulations have enabled organizations to secure more funding for personnel and technology purchases, this could be having an unintended consequence in adding to IT security challenges through the lack of integration and the complexity of current technologies.

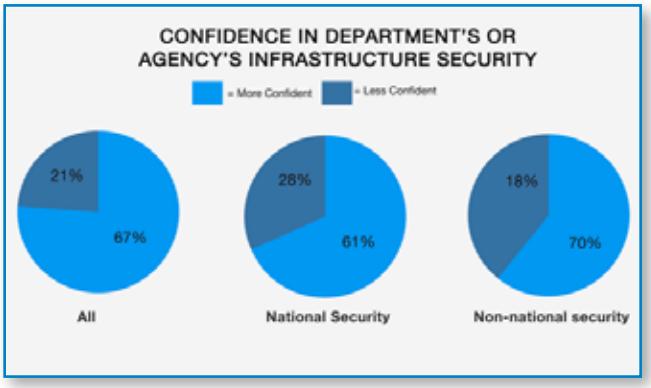
Summary of the Impact of Compliance

In general, compliance seems to be having a positive impact to the general state of federal IT security in terms of enabling organizations to garner additional resources or personnel to meet compliance initiatives, and in acquiring new technologies to address rising IT security risk. However, no single federal compliance initiative really stands out in its ability to affect IT security, and as more compliance initiatives are added, the growing audit burden is placing a strain on federal IT resources and driving a lack of integration between technologies.

Continued »

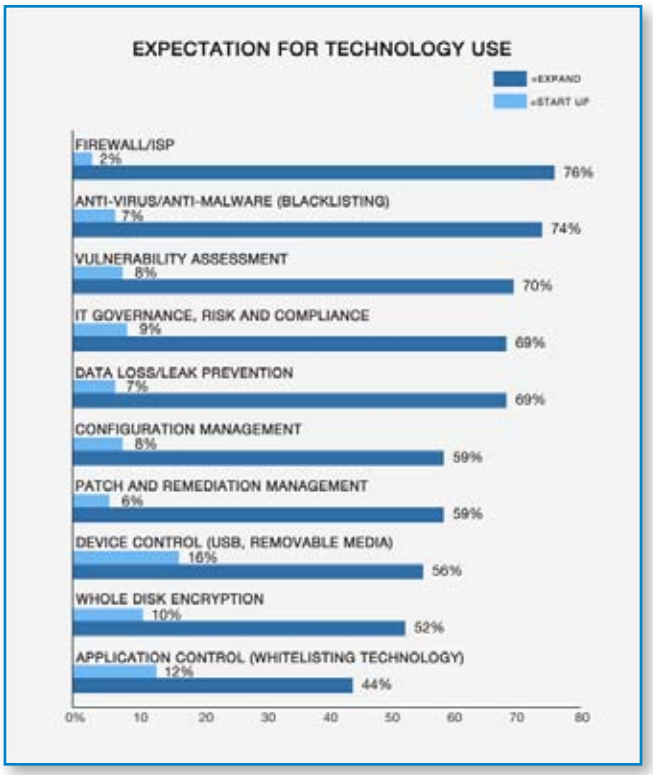
Some Additional Insights

Overall, do you feel more confident or less confident in the security of the IT infrastructure in your department or agency than you did a year ago?



Overall, most of the respondents surveyed feel more confident in their department's IT security posture than they did a year ago, indicating improvement across the board. However, among national security IT professionals, 28 percent felt less confident in their agencies IT security posture. This may be due to a deeper understanding of the threats that exist. A majority of respondents indicate the reason they feel more secure is due to improved IT security technology.

Of the following IT security technologies, which ones do you expect to start using or expand its usage in the coming year?



During the next year we can expect to see expanded usage of core IT security technology, such as firewalls, anti-virus, vulnerability assessment and patch management.

Newer and emerging IT security technology will also see increased start up within federal IT environments. These technologies include application whitelisting device control and whole disk encryption.

Continued »

Conclusion

Federal IT decision-makers believe there is now a growing and persistent cyber threat to sensitive information and critical IT infrastructure from a foreign nation and terrorist organizations.

While progress is being made with the creation of the Comprehensive National Cybersecurity Initiative and the appointment of the new U.S. National Cybersecurity Coordinator, many respondents remain skeptical that this will be enough to overcome the new threats and risks.

Personnel from both civilian and defense agencies and across the IT spectrum--operations, security, C-level leadership and everyone in between--are looking for ways to meet the growing challenges buffeting federal IT infrastructure in the modern technology era.

These roles will need to find better ways to collaborate amongst themselves and with private sector colleagues. They will need to deploy new and innovative IT security technologies like application whitelisting to stay ahead of the game, look to reduce technology complexity through integration, and shift from an absolute focus on meeting compliance with ad-hoc monitoring to greater focus on security and continuous monitoring of the IT risk environment.

About Lumension Security, Inc.

Lumension Security, Inc., a global leader in operational endpoint management and security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets. Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, and Compliance and Risk Management offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year. Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Virginia, Utah, Florida, Texas, Luxembourg, the United Kingdom, Germany, Ireland, Spain, France, Australia, and Singapore. Lumension: IT Secured. Success Optimized.™ More information can be found at www.lumension.com.

Lumension®
IT Secured. Success Optimized.™

Global Headquarters
8660 East Hartford Drive, Suite 300
Scottsdale, AZ 85255 USA
phone: +1.888.725.7828
fax: +1.480.970.6323