Market Connections®
Research you can act on.

SEPTEMBER 2016

CYBERSECURITY IN THE FEDERAL GOVERNMENT

How Agencies Can Manage the Increasing Threats from Outside

For the last three years, SolarWinds has kept a pulse on where and how cybersecurity threats most impact federal agencies. The study looks at what respondents perceive as the biggest threats their agencies face, the consequences of breaches, where respondents feel their agencies are vulnerable, and the challenges they face in securing their agencies against cyber threats.

PRESENTED BY
solarwinds

PREPARED BY
Market Connections, Inc.
11350 Random Hills Road, Suite 800
Fairfax, VA 22030
TEL 703.378.2025
www.marketconnectionsinc.com

SHARE THIS STUDY

Executive Summary

In the world of technology, issues and priorities can change quickly. Cybersecurity is an area where that truism is clear. In the first and second years of the SolarWinds cybersecurity study (2014/15), internal threats — whether accidental or malicious — emerged as the most pressing cyber threat in federal agencies. In this third year of the research, a clear trend is emerging: agencies feel positive about how they have addressed the challenges of unintended internal threats, but are feeling increasingly vulnerable to outside threats.

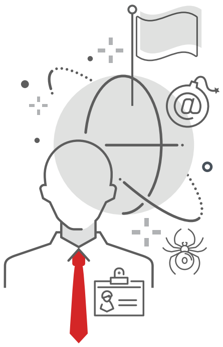
The data shows that overall, agencies feel they have put solid procedures, processes and tools in place to manage insider threats — particularly accidental breaches caused by lack of training and procedures (which emerged as a top threat in the 2014 study). Now agencies are turning their attention toward external threats from a host of sources, including foreign governments, hacktivists and terrorists.

The Biggest Threats and Consequences

The foreign government hack of the Office of Personnel Management shook federal agencies—and the public—to the core. While external hacks had happened in other agencies, the degree of this breach was staggering. This is perhaps a factor in why, according to the survey, foreign governments now rival careless or untrained insiders as the biggest threat to IT security: nearly half (48%) of respondents said foreign governments are the top IT security threat, tying with careless or untrained insiders. This is a significant increase from 2015 and 2014, where 38% and 34% of respondents, respectively, listed it as the primary threat.

TOP IT SECURITY THREATS

Changes over the last three years



	2014	2015	2016
FOREIGN GOVERNMENTS	34%	38%	**48%**
CARELESS/UNTRAINED INSIDERS	42%	53%	**48%**
GENERAL HACKING COMMUNITY	47%	46%	**46%**

At the same time the threat from foreign governments is increasing, agencies report the impact of careless and untrained insiders is lessening. At 48%, the numbers dropped this year from 2015 results, when 53% of respondents saw insiders as the biggest threat. However, this years’ result is still higher than 2014 (42%).

Other external threats have also seen increases over the last two years. While threats from the general hacking community have remained steady at 46%, the threat from hacktivists has been steadily rising over the last three years: 38% of respondents see hacktivists as a threat, versus 30% from 2015 and 26% from 2014. While not as dramatic, the threat from terrorists is also rising — 24% this year over 18% in 2015 and 21% in 2014.

Top Consequences

All breaches, whether insider or external, have serious consequences for agency operations. Imagine if FEMA was not able to respond to a hurricane, or DoD operations were impacted while deploying resources to address a national security threat or the Social Security Administration could not disburse benefits to retirees. The consequences could be catastrophic, ranging from private information landing in the hands of criminals to an inability to respond to an act of war.

BREACHES: TOP CONSEQUENCES

44% Theft of Personally Identifiable Information (PII)

40% Service Outages

39% Service Degradation

SURPRISINGLY FINANCIAL FRAUD, OFTEN A RESULT OF PII, WAS ONLY **8%**

For two-thirds (66%) of respondents, a breach results in more than one consequence. Forty-four percent of respondents list theft of Personally Identifiable Information (PII) as the top consequence. Interestingly, only 8% of respondents cited financial fraud as a consequence, which seems low considering that PII theft often results in fraud. Perhaps the reason PII rated as the number one consequence is because the OPM breach is still top of mind, while the fall out of that breach (and the likely fraud that will result) is still largely unknown.

Other top consequences include service outages (40%), service degradation (39%), misuse of systems (36%) and agency data theft (25%). While these consequences may not seem as impactful as the loss of PII, service outages could mean thousands of veterans don't receive timely medical care or law enforcement agencies are unable to share time-sensitive information.

Are Agencies More or Less Vulnerable?

When asked to compare their agency's IT security attack vulnerability with last year, more than half (55%) feel there has been no change in their agency's vulnerability. However, 28% feel less vulnerable today while 17% feel more vulnerable.

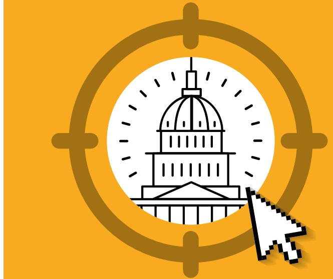
Respondents say the increased sophistication of threats (44%) has made their agencies more vulnerable than a year ago. It is not surprising that there are significant differences between Defense (37%) and Civilian (50%) in this regard — defense agencies have been guarding against sophisticated threats for some time, whereas this is a newer problem for civilian agencies.

The other top two factors leading to agency feelings of vulnerability include an increased volume of attacks (26%) and end user policy violations (24%). Interestingly, only one in ten respondents said the use or increased use of public cloud makes their agency more vulnerable to security threats, possibly indicating that agencies feel providers can meet security challenges.

While there are areas in which agencies feel vulnerable, there are also areas in which they feel an increased sense of security.

Respondents give the increased use of Smart Cards for dual-factor authentication the most credit for making agencies less vulnerable to IT security attacks than a year ago (38%). This is significantly more so for Civilian at 49% versus Defense at 26%.

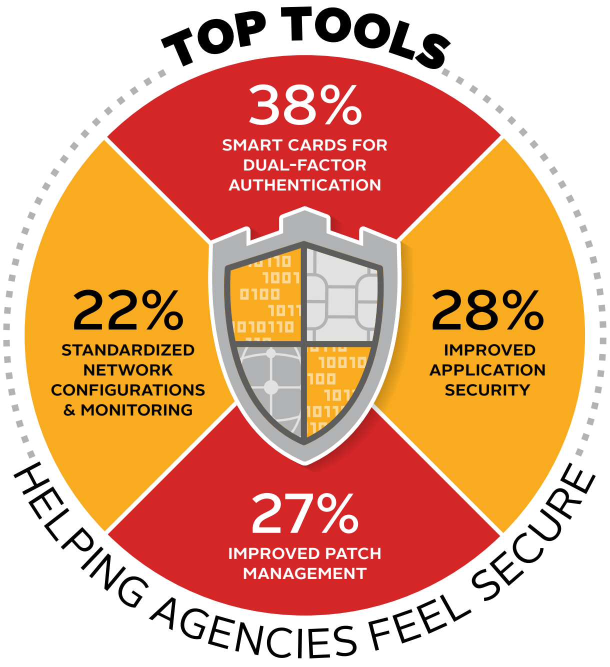
AGENCY VULNERABILITY



44% Increased sophistication of threats

26% Increased volume of attacks

24% End user policy violations



In addition, improved application security (28%), improved patch management (27%) and standardized network configurations and monitoring (22%) are also top factors in the increased sense of security agencies feel. This makes sense, as the tools give agencies the visibility into the networks they need to understand what is happening and address issues quickly when they arise.

Ability to Detect Threats

When the foreign government attacked OPM, the hackers stole credentials that allowed access to the network, then planted malware and created a backdoor for exfiltration[1]. Once the malware was detected and an anti-malware tool was deployed, it took a full week to evict the hackers. Have agency-wide response times tightened since that breach?

More than one-third of respondents believe that the time to detect security events has decreased since 2015, while the number of IT security incidents has increased (38%). However, it still takes 39% of agencies a few days or more to detect misuse/abuse of credentials (with another 14% unsure how long it takes) and 26% take a few days or more to detect malware (with another 11% unsure how long it takes). Agencies are doing best with detection of rogue devices, with 39% able to detect them within minutes. But this still means it takes days (or longer) for nearly two-thirds of agencies to detect these breaches.

Other types of security events can also increase agency vulnerability. For example, less than half of agencies (20%) can detect Cross-Site Scripting of web applications and only 38% are able to detect inappropriate Internet access within minutes, leaving agencies open to attack. In addition, internal configuration issues can open up vulnerabilities to external threats (for example, changing a secure configuration can open a door for an external attack).

The good news is that agencies feel that response times are getting faster — 38% said the time to respond has decreased since 2014.

Challenges Agencies Face

Despite the importance cybersecurity initiatives play, almost one-third (29%) of agencies still face budget constraints when addressing challenges. However, this number has decreased from 40% in the 2014 study. Behind budget constraints, the greatest obstacles to improving IT security are complexity of internal environments (16%) followed by competing priorities and other initiatives (14%) and inadequate collaboration with other internal teams (12%).

IT Consolidation & Modernization Security Challenges

INCOMPLETE TRANSITIONS
48%

COMPLEX MANAGEMENT TOOLS
46%

LACK OF FAMILIARITY WITH NEW SYSTEMS
44%

Almost half of respondents say that IT consolidation and modernization efforts have actually resulted in an increase in IT security challenges because transitions are incomplete

[1] Lyngaas, Sean. “Exclusive: The OPM breach details you haven’t seen.” FCW, Aug 21, 2015

(48%), enterprise management tools are too complex (46%), and there is a lack of familiarity with new systems (44%).

While consolidation and modernization can increase security challenges (especially when the transitions are incomplete), Mav Turner, SolarWinds Senior Director of Product Strategy, says, "It's still important to do it because once those transitions are complete, they allow for significantly more secure environments as well as more efficient operations." The 20% of respondents who indicate that modernization and consolidation could decrease security challenges cite replacing legacy software (55%) and equipment (52%) and simplified administration and management (42%) as key security benefits of modernization.

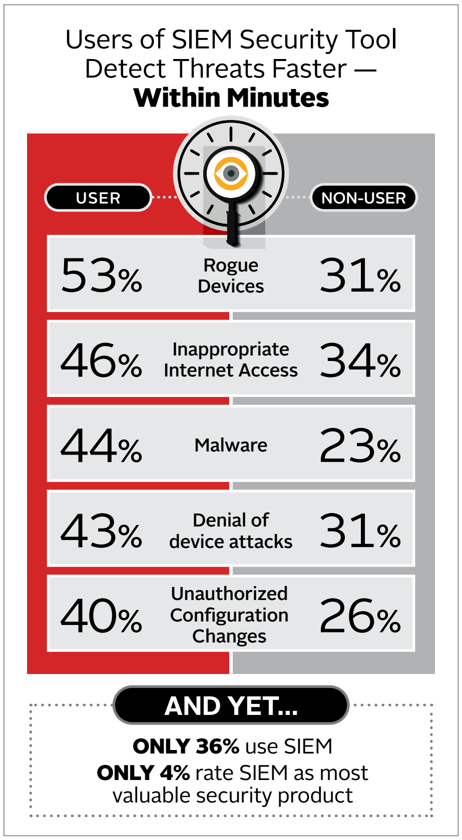
How Agencies Can Address the Threats

The majority of respondents either see their investment in security tools increasing (51%) in 2016 or staying the same (33%) as it was in 2015. Turner says that however much budget is allocated to security tools, it is important to ensure the investment is in the right security tools.

The good news is that the same key tools can be used to address any threat — whether that from foreign governments or careless insiders. Agencies first need to know what is on the network: who, what, where, and when. They need to be able to answer the question: "was this here last time I checked?" IT Operations Management tools, which can also be used by security teams, provide insight into what is currently on the network, what has changed, network traffic information, and more.

> "Attackers look for the most vulnerable entry points. SIEM, configuration management and patch management are a dynamic trio that strengthen an agency's ability to see where vulnerable entry points are and remediate those issues before damage is done. They can also be used to identify and respond to active attacks."
>
> **MAV TURNER**
> *Senior Director of Product Strategy, SolarWinds*

The Unsung Security Workhorses: SIEM, Configuration and Patch Management



Users of SIEM Security Tool Detect Threats Faster — **Within Minutes**

USER		NON-USER
53%	Rogue Devices	31%
46%	Inappropriate Internet Access	34%
44%	Malware	23%
43%	Denial of device attacks	31%
40%	Unauthorized Configuration Changes	26%

AND YET...

ONLY 36% use SIEM
ONLY 4% rate SIEM as most valuable security product

Turner says that while Smart Cards are important, there are other security tools that are critical. Security Information and Event Management (SIEM) is an extremely effective tool for detecting threats quickly, yet it is also the most underutilized with only 36% of respondents using it and only 4% rating it as the most valuable security product.

Turner suggests agencies rethink their use of SIEM. He says SIEM tools can look at a complex combination of activities, and without it, agencies can't address more sophisticated attacks that other tools miss. SIEM tools that can do real-time, in-memory correlation and automate immediate corrective actions can reduce time to detect and remediate more threats, and do so in a matter of seconds.

The data supports this: SIEM users detect phishing attacks in their agency within minutes significantly more (29%) than those who do not use SIEM (18%). In fact, those who currently use SIEM software are significantly more able to detect, within minutes, the most common security threats: rogue devices (53% vs. 31%), malware (44% vs. 23%) and unauthorized configuration changes (40% vs. 26%).

Configuration and patch management are also valuable security tools, and almost two-thirds (62%) of respondents use them. Of those who do use them, 20% say implementing configuration management tools have made them less vulnerable and 27% credit patch management with making them more secure. While these numbers may seem low, it is possible that those who have implemented basic configuration and patch management tools simply take them (and their security benefits) for granted.

Conclusions

The increasing sophistication of cyber threats, coupled with the challenges of consolidation and modernization, make securing our government's infrastructure more challenging. Fortunately, says Turner, using IT operations and security management tools such as SIEM, configuration management and patch management offers protections that can give agencies confidence that their networks and systems are more secure.

The reality is, the nature and sophistication of cyber threats will continue to evolve. As the last three years of data show, the origination of the most serious threats continues to change and shift. What remains constant is how agencies can address those threats.

When agencies put the right tools in place, they are in a position to understand who is attacking them—internal or external actors—and how they are doing it. That information allows them to respond quickly to minimize the threat and have confidence that their agency is secure.

About the Study

The annual SolarWinds cybersecurity study is in its third year. The study looks at what respondents perceive as the biggest threats their agencies face, the consequences of breaches, where respondents feel their agencies are vulnerable, and the challenges they face in securing their agencies against cyber threats. The 2016 blind, online survey of 200 federal IT decision makers included IT decision makers from federal, civilian or independent government agencies (50%); defense (43%); federal judiciary (2%); intelligence (2%); and federal legislature (2%). More than half (54%) are on a team that makes decisions regarding IT security and/or IT operations and management solutions; 50% manage or implement IT security and/or IT operations and management solutions; 46% evaluate and/or recommend firms offering IT security and/or IT operations and management solutions; 45% develop technical requirements for IT security and/or IT operations and management solutions; and 20% make the final decision on IT security and/or IT operations and management solutions. One third (36%) are an IT manager/director; 27% are IT/IS staff; 8% are security/IA staff; 6% are security/IA director or manager; 4% are the CIO/CTO; 2% are the CSO/CISO; and 16% stated their position as "other" (Director of Operations, Management Analyst, Program Manager). Nearly one-third (30%) have more than 20 years' experience in IT security.

ABOUT SOLARWINDS

SolarWinds provides IT management and monitoring solutions to numerous common public sector IT challenges including continuous monitoring, cybersecurity, network operations, compliance, IT consolidation, data center operations, cloud computing, mobile workforce and devices, DevOps, and scaling to the enterprise. SolarWinds software is available through numerous channel partners and systems integrators worldwide as well as the U.S. General Services Administration (GSA®) Schedule, Department of Defense ESI, United Nations Global Marketplace (UNGM), Crown Commercial Service (CCS), United Nations Atlas.

For more information and fully functional free trials visit:
www.solarwinds.com/federal or
www.solarwinds.com/nationalgovernment

ABOUT MARKET CONNECTIONS, INC.

Market Connections, Inc. delivers actionable intelligence and insights that enable improved business performance and positioning for leading businesses, trade associations and the public sector. The custom market research firm is a sought-after authority on preferences, perceptions and trends among the public sector and the contractors who serve them, offering deep domain expertise in information technology and telecommunications, health care and education.

For more information visit: www.marketconnectionsinc.com.

TO DOWNLOAD THE REPORT

www.solarwinds.com/assets/surveys/cybersecurity-slide-deck.aspx

SHARE THIS STUDY