CYBERSECURITY IN THE FEDERAL GOVERNMENT

Managing the Ongoing Challenge of Insider Threats

A WHITE PAPER PRESENTED BY:
solarwinds

May 2015
CYBERSECURITY IN THE FEDERAL GOVERNMENT

Managing the Ongoing Challenge of Insider Threats

"Interestingly, we have positioned ourselves relatively strongly against external threats, but it is the accidental or malicious insider threat that has caused us more problems. People do what they want to do and there are many people (particularly younger) who view security as interference and also have some skills to successfully work around security protocols."

— DIRECTOR OF OPERATIONS, DCMA

EXECUTIVE SUMMARY

Every day we see stories in the news about external cyber threats—in late 2014, for example, unclassified networks at the White House and State Department were hacked. This constant focus on malicious attacks from outsiders has prompted increased investment in preventing such breaches. Yet those managing cybersecurity in federal agencies know that day in and day out, it is the people on the inside that pose the greatest threat to cybersecurity, and these insider threats continue to prove more challenging to manage.

In January 2014, SolarWinds commissioned Market Connections, Inc. to conduct a survey to learn about the primary cybersecurity threats facing federal agencies, the degree of cybersecurity readiness within agencies and top cybersecurity obstacles agencies face. That study revealed that whether through human error or malicious intent, people are a highly unpredictable and significantly damaging threat to an agency’s cybersecurity defense.

In December 2014, SolarWinds commissioned a follow-up survey among 200 federal government IT decision-makers and influencers to identify challenges IT professionals face to prevent insider and external IT security threats; gauge confidence levels of combating insider and external IT security threats; and measure changes in concern and investment of resources in addressing threats.
Sources of Security Threats

Insiders are the biggest security threat agencies face, and the threat is increasing. More than half (53%) of respondents believe careless/untrained insiders are the top source of security threats within federal agencies—a 26% increase (from 42%) in the SolarWinds cybersecurity survey just one year ago. Nearly one-quarter (23%) find malicious insiders the biggest security threat, which also increased, from 17%, in the previous survey.

Respondents also cite the general hacking community (46%), foreign governments (38%) and hacktivists (30%) as primary security threats, and 69% of agencies have increased investments in addressing external threats (23% indicating the increase is significant). External threats are constant, and investment helps reduce an agency’s vulnerability to them. However, it is also critical for agencies to invest in mitigating insider threats.

More than one-third (38%) of respondents believe that malicious external and malicious internal threats are the most damaging breach sources. One-quarter (26%) believe malicious internal threats are most damaging. However, not all internal security breaches are malicious; in fact, many are unintentional. Yet even unintentional breaches can cause serious damage. More than one-third (35%) believe accidental insider threats are as damaging as malicious insider threats, and more than one in five (22%) believe accidental insider threats are more damaging than malicious internal threats.

Where is data most at risk? Almost half of respondents indicate data on employee or contractor personal computers (47%) and removable storage media (42%) is most at risk.

Challenges Overcoming Cybersecurity Threats

While agencies have a clear understanding of the major threat sources, they face numerous challenges in addressing them.

The Discrepancy Between Threats and Resources

While it is not surprising that budget constraints top the list of significant obstacles to maintaining or improving agency IT security (29%), this number has actually decreased from 40% last year.

Federal agencies’ concern regarding internal and external threats has increased in the last two years, but the investment in resources lags slightly. For example, 53% say the concern about accidental insider threats has increased, yet only 44% say investment to address those threats has increased.
Respondents indicate both higher concern and greater investment into preventing malicious external threats than insider threats—whether malicious or accidental—despite the recognition that careless/untrained insiders are the greater source of security threats (53%).

Perhaps it is also because external threats are more visible. However, agencies need to know what is going on internally as well—with visibility comes understanding and the ability to quickly mitigate threats. Agencies need to have the tools in place to identify where the threats exist, as well as appropriate resources—budget, time and knowledge—to keep employees and contractors up-to-date on security policies and protocols.

“This discrepancy between threats and resources points to a lack of understanding or a perception issue—agencies perceive that external threats are more prevalent or a greater risk, when in fact internal threats post the biggest potential threats, but don’t get the same resources to address as external ones do,” said Joel Dolisy, CIO, SolarWinds.

**Educating the Workforce**

Untrained personnel are a key reason for increased insider threats—almost half of federal IT and IT security pros (46%) see insufficient security training for government employees or contractors as an obstacle to preventing accidental insider threats. The majority have supplemental policies to the Security Technical Implementation Guide (STIG) from National Institute of Standards and Technology (NIST) and the Federal Information Security Management Act (FISMA) that already apply. The research revealed more than half (56%) of agencies also provide supplemental policies during onboarding. Three quarters (76%) of respondents say they receive frequent email reminders and tips regarding security. However, there appears to be a lack of enforcement and infrequent updates to internal security policies and procedures.

The majority of respondents (56%) are only somewhat confident that their organization’s security policies can address accidental or careless insider threats, and 14% are not at all confident.

**Insider Threat Detection Challenges**

Increased use of mobile technology is noted as the top obstacle for preventing insider threats—the majority of respondents (56%) cite the use of mobile technology as an obstacle for preventing accidental threats and 44% say it is an obstacle for preventing malicious threats. One-third of respondents believe their agency data is most at risk on government-owned mobile devices and 29% are concerned about employee- or contractor-owned mobile devices.
“The concern regarding mobile devices is likely to increase as more agencies implement bring-your-own-device (BYOD) programs. This shift in technology at work will likely contribute to the increased risk from insiders.” —JOEL DOLISY, CIO SOLARWINDS

Inadequate monitoring of user authentication activity and failures are the second biggest obstacle to insider threat prevention at 39% for accidental threats and 41% for malicious threats. And inadequate automation of IT asset management is the third largest obstacle at 39% for accidental threats and 38% for malicious threats. These obstacles indicate agencies are doing a lot of work manually and, given the size of the networks, this makes insider threats caused by human error hard to manage.

HOW AGENCIES CAN ADDRESS INSIDER THREATS

Despite the many challenges and obstacles to managing insider threats, the solution is simple: know the devices on the network, who is using them and when. Agencies need to know the who, what, where and when of every network operation—desktop, mobile and virtual.

Visibility is an agency’s essential tool to combat insider threats.

For example, when a federal IT program has a complete and current picture of what is on the network, they can monitor network traffic, replace obsolete items and know whether things are approved—with the ability to answer, “Was this here last time I checked?” As one high-ranking DOD official remarked: “It’s hard to secure a network if you don’t even know what’s on it.”

Prevention tools help agencies answer these who, what, when and where questions. For insider threats, respondents indicated identity and access management tools (malicious 46%, accidental 39%); internal threat detection/intelligence (malicious 44%, accidental 36%); and intrusion detection and prevention tools (malicious 43%, accidental 32%) as the most important. However, IT asset management, configuration management and threat detection can also provide valuable safeguards against internal threats.

Training delivery is also important, but requires constant investment while the security landscape continues to change rapidly. But to prevent insider breaches—especially accidental ones—internal users must be vigilant. And to be vigilant, they need to know how to behave. This is hard for many organizations to accept—only eight percent see lack of training personnel as a high-level IT security obstacle. Yet insider threats remain an issue, indicating a significant disconnect between
realization of the problem and understanding of how to address it. It is key for leadership to buy in to the need for training to prevent the continued growth of insider breaches.

The very tools used to prevent threats can also help develop useful training—by providing real-world examples that deliver impact, users better understand the consequences and will be more likely to change their behavior. For example, a monitoring tool will identify risky behaviors, such as a single user being authenticated to five different computers simultaneously, which indicates the possibility of multiple people sharing an account (username/password). Training could focus on the risks of practices like this.

Log monitoring can also inform training by detecting activity that may slip under the radar, like software installs, outbound web traffic to suspicious sites and critical file changes—all of which can be used as examples to educate users on how to detect suspicious emails, unauthorized applications and the damage that can be caused. Vulnerability assessment results can be used to train users on the importance of patching, even though that task is perceived as an inconvenience.

Agencies can also stay on top of training requirements by evolving their policies and procedures regularly. The first step is to develop success metrics and ensure that users are learning and understand what they can do—users don’t need to become cybersecurity experts, but they do need to be on the lookout for basic attacks.

CONCLUSIONS

The growing investment in external threat detection and prevention certainly detects and thwarts many damaging security breaches, but alone cannot fully secure an agency’s data. Internal threats will continue to exist as long as agencies continue to employ people, so agencies need to make at least an equal investment in addressing insider threats. The good news is that many existing tools can provide insight into user behaviors that cause issues, such as identity and access management, IT asset management, configuration management tools and threat detection tools. Agencies are already using many of these tools for their daily IT operations, and the tools can also add visibility into the security posture of agency IT infrastructures.

Ensuring that the workforce is educated about the risks and appropriate behaviors is also a critical step. By using the tools that provide the necessary visibility of potential problems, agencies can address user behaviors and build a constant awareness of what is on the network, thus protecting the agency and its data.
ABOUT THE STUDY
The SolarWinds Federal IT Security Survey identified challenges IT professionals face in preventing insider and external IT security threats; gauged confidence levels of combating insider and external IT security threats; and measured changes in concern and investment of resources to address those threats. The blind online study surveyed 200 IT decision-makers and influencers, of which 54% were federal, civilian or independent government agencies; 39% were defense; and 8% were other agencies. Half are on a team that makes decisions regarding IT security and/or IT operations and management solutions; 43% evaluate and/or recommend firms offering IT security and/or IT operations and management solutions; 41% develop technical requirements for IT security and/or IT operations and management solutions; 40% manage or implement IT security and/or IT operations and management solutions; 17% make the final decision on IT security and/or IT operations and management solutions. One-third were the IT manager/director, 32% IT/IS staff, 10% security/IA staff, 7% CIO/CTO, and 7% security/IA director or manager.

ABOUT SOLARWINDS
SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide from Fortune 500 enterprises to nearly every civilian agency, DOD branch and intelligence agencies. In all market areas, the SolarWinds approach is consistent—focusing exclusively on IT professionals and striving to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use and maintain, while providing the power to address any IT management problem on any scale. Each solution is rooted in the company’s deep connection to their user base, which interacts in an online community, thwack, to solve problems, share technology and best practices, and directly participate in the product development process.

SolarWinds provides IT management and monitoring solutions to numerous common public sector IT challenges including continuous monitoring, cybersecurity, network operations, compliance, data center consolidation, cloud computing, mobile workforce and devices, and scaling to the enterprise. SolarWinds software is available on the U.S. General Services Administration (GSA) Schedule, Department of Defense ESI and numerous other contract vehicles. For more information and fully functional free trials visit: www.solarwinds.com/federal.

ABOUT MARKET CONNECTIONS, INC.
Market Connections 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; healthcare; and education. For more information visit: www.marketconnectionsinc.com.