Government Business Council

DELL Software

THE HUMAN FACTOR AT THE CORE OF FEDERAL CYBERSECURITY

CYBER HYGIENE AND ORGANIZATIONAL PLANNING ARE AT LEAST AS INTEGRAL TO SECURING INFORMATION NETWORKS AS FIREWALLS AND ANTIVIRUS SOFTWARE

Cybersecurity has become a top priority across the board for the federal government in recent years. In 2012, President Obama warned that "the cyber threat to our nation is one of the most serious economic and national security challenges we face."[1] Late last year, FBI Director James Comey testified that the threat posed by cyberattacks would soon eclipse terrorism.[2] Backing up these words with action, the White House has made cybersecurity the federal government's top-listed Cross Agency Priority Goal and issued several executive orders. Moreover, the 2014 omnibus appropriations bill significantly increased spending on cybersecurity operations while general IT spending largely remained level.[3] However, despite widespread concern, a question mark remains over the current state of federal cybersecurity.

A trove of new research into this question provides greater insight. Integrating primary research from a new Government Business Council (GBC) and Dell Software survey, Government Accountability Office (GAO) reports, and the 2014 Verizon Data Breach Investigations Report offers a levelheaded assessment of federal cybersecurity. Federal employees indicate agency cybersecurity is in better shape than many give them credit for, but as threats grow and evolve, agencies will need to bolster key elements to ensure holistic cybersecurity. In particular, personnel management and cybersecurity awareness stand out as areas in need of improvement.

The Growing Cyber Threat

The last few years have witnessed a significant uptick in the number of cyber intrusions experienced by federal agencies. An April 2014 GAO report notes that federal agencies reported 64,214 information security incidents to the U.S. Computer Emergency Response Team (US-CERT) in 2013, a 104 percent increase from 2009.[4] More than 46,000 of the 2013 incidents were cybersecurity breaches, as opposed to non-cyber incidents (e.g., losing a hard copy record of sensitive information), marking a 32 percent increase from 2012.[5] On top of the worrying quantitative trend, qualitative audits offer a grimmer picture. A February 2014 report from Senator Tom Coburn's office highlights several significant cyber incidents at federal agencies indicating serious vulnerabilities, including hackers stealing sensitive information on critical infrastructure from government computers and gaining access to a database of known software vulnerabilities on government web servers.[6] Federal employees themselves recognize the prevalence of the threat, with 52 percent

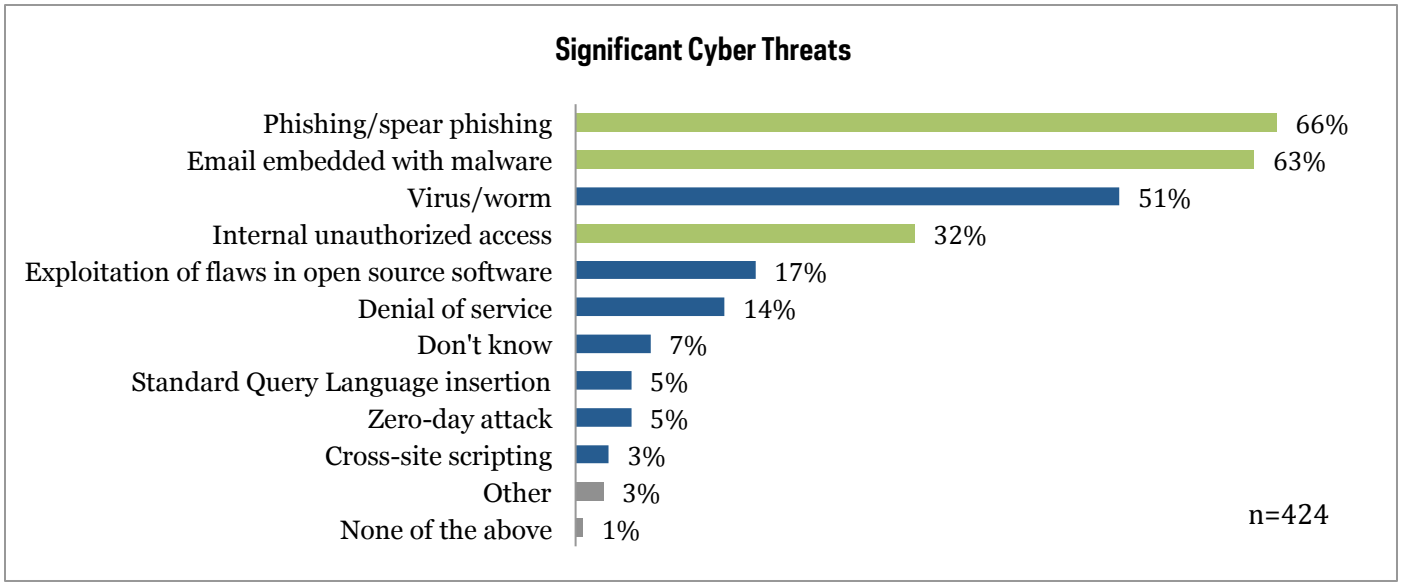
"WHETHER IT IS HACKERS DEPLOYING PHISHING ATTACKS OR EMPLOYEES MISHANDLING SENSITIVE DATA, THE TOP CYBER THREATS HAVE A COMMON DENOMINATOR— AGENCY PERSONNEL."

indicating that their agency is a target multiple times each month or more, according to the GBC-Dell survey of 424 senior federal employees with knowledge of cybersecurity.[7]

The GBC-Dell survey also offered insight into the top cyber threats federal agencies face. Respondents picked out phishing/spear phishing (66 percent) and email embedded with malware (63 percent) as top threats to federal agencies. In fact, phishing and malware have become two of the most common cyber threats across all industries. Verizon's expansive data breach report notes that these threats have risen to the top of their database for all cyber incidents analyzed in 2013. Phishing threats became the third most common incident in 2013 after ranking ninth in 2011 and 2012, while different forms of malware have consistently been among the top five.[8] Verizon also documents internal miscellaneous errors—incidents where unintentional actions compromise security—and insider misuse—unapproved or malicious use of organizational resources—as the most common categories of incidents for public sector entities. Whether it is hackers deploying phishing attacks or employees mishandling sensitive data, the top cyber threats have a common denominator—agency personnel.

Cyber Defense Assessment

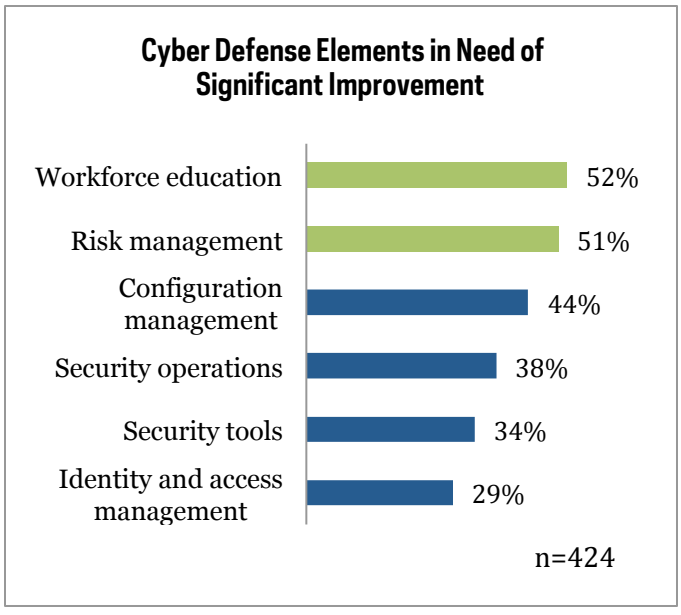
The increasing number and sophistication of cyber threats has given rise to considerable concern over the state of federal cybersecurity. GAO lists protecting federal agencies' information systems as a "high risk" area, noting that as cyber threats grow, the federal government still does not have an up-to-date, comprehensive cybersecurity strategy. Although the federal strategy has evolved in the last decade and several policy documents have been issued on sub-topics, "there is no overarching national cybersecurity strategy that synthesizes these documents or comprehensively describes the current strategy."[9] Senator Coburn's report is even more pointed. It claims "the federal government has struggled to implement a mandate to protect its own IT systems from



malicious attacks," and it "should address the immediate danger posed by the insecurity of its own critical networks."[10]

Since these reports, the federal government has taken a step toward holisitic cybersecurity with the release of the February 2014 NIST framework. This framework, resulting from Executive Order 13636, offers critical infrastructure operators a core set of activities to anticipate and mitigate against attacks on their systems. However, the lack of incentives associated with the framework may need to be addressed before the private sector adopts the standards more widely.

Despite the doubts, federal employees across defense and civilian agencies are much more confident in the government's ability to protect its information systems. The GBC-Dell survey reports that nearly two-thirds of federal employees at least somewhat familiar with cybersecurity are confident or very confident in their agency's cybersecurity.[11] This finding is corroborated by a recent Market Connections and SolarWinds survey, in which 94 percent of federal IT respondents rate their agency's cybersecurity readiness as good or excellent.[12]



"THOUGH FEDERAL EMPLOYEES ARE VERY CONFIDENT IN THE SECURITY OF THEIR AGENCY'S INFORMATION SYSTEM LAYERS, THEY ALSO INDICATE PLENTY OF ROOM FOR IMPROVEMENT IN THEIR CYBER DEFENSES."

So which is it? Is federal cybersecurity extremely vulnerable or are agencies generally secure in cyberspace? The evidence suggests the reality is somewhere in between.

The GBC-Dell survey notes that though federal employees are very confident in the security of their agency's information system layers (data, application, host, and network), they also indicate plenty of room for improvement in their cyber defenses. In particular, majorities highlight workforce education (52 percent) and risk management (51 percent) as areas that need to be improved to enhance overall federal cybersecurity.

GAO tells a similarly mixed story. It recently found that the 24 major federal agencies have established and complied with most Federal Information Security Management Act (FISMA) components, but that there is still much work to be done.[13] According to GAO analysis of cyber incidents reported in 2012, agencies took appropriate actions to contain, eradicate, and restore systems in the aftermath of the large majority of cyber incidents (between 75 and 81 percent).[14] Furthermore, Verizon reports relatively few public sector data breaches leading to data loss despite the tremendous increase in cyber incidents experienced by federal agencies.[15] Still, GAO concludes that federal cybersecurity continues to be a major challenge worthy of its "high-risk" classification because any single data loss incident could prove catastrophic for the federal government.[16]

In short, agencies are generally secure in cyberspace, but the real question now is how can they take the extra step to ensure holistic cybersecurity of their information networks in an era of ever growing threats.

Addressing The Human Factor

A close review of the top cyber threats and the most significant federal cybersecurity weaknesses revealed by the GBC-Dell survey, GAO reports, and Verizon show that personnel cyber awareness and management form the crux of the federal cybersecurity imperative. Specifically, workforce education and risk management need to be enhanced.

Because so many cyber intrusions can be attributed to human error or ignorance, assiduous cybersecurity literacy and awareness training for federal agency workforces is essential. Such training should be customized and targeted for unique agency user groups, including managers, general users, and system administrators.

Successfully managing cyber threats from a high-level requires distilling tremendous amounts of threat incident data into a coherent, strategy for mitigating risks. Specifically, effective risk management entails ensuring situational awareness and developing comprehensive continuity of operations and disaster recovery plans.[17] It is essentially a strategic management challenge.

At its core, ensuring cybersecurity is a human endeavor. Cyber hygiene and organizational planning are at least as integral to securing information networks as firewalls and antivirus software. Federal agencies should therefore look to their own personnel, as well as industry partners experienced in end-to-end solutions, to make the leap to holistic cybersecurity.

About GBC

Government Business Council (GBC), the research arm of Government Executive Media Group, is dedicated to advancing the business of government through analysis and insight. GBC partners with industry to share best practices with top government decision-makers, understanding the deep value inherent in industry's experience engaging and supporting federal agencies. Contact Zoe Grotophorst, Manager of Research & Strategic Insights, Government Business Council, at zgrotophorst@govexec.com

About Dell Software

Dell Software makes it easy to securely manage and protect applications, systems, devices and data to help organizations of all sizes fully deliver on the promise of technology. Our simple yet powerful software – combined with Dell hardware and services – provide scalable, integrated solutions to drive value and accelerate results. Whether it's Windows infrastructure, the cloud and mobile computing, or networks, databases and business intelligence, we dramatically reduce complexity and risk to unlock the power of IT.www.dell.com/software

Sources

[1] President Barack Obama, "Taking the Cyberattack Threat Seriously," Wall Street Journal, July 19, 2012.
[2] Greg Miller, "FBI director warns of cyberattacks; other security chiefs say terrorism threat has altered," November 2013.
[3] Richard Walker, "Budget Bill Boosts Cybersecurity Spending," InformationWeek, January 2014.
[4] Government Accountability Office, "Federal Agencies Need to Enhance Responses to Data Breaches," Testimony to Committee on Homeland Security and Governmental Affairs, U.S. Senate, GAO-14-487T, April 2014.
[5] Government Accountability Office, "Agencies Need to Improve Cyber Incident Response Practices," Report to Congressional Requesters, GAO-14-354, April 2014.
[6] Senator Tom Coburn, "The Federal Government's Track Record on Cybersecurity and Critical Infrastructure," February 2014.
[7] Government Business Council, *Achieving Holistic Federal Cybersecurity*, June 2014
[8] Verizon Enterprise Solutions, *2014 Data Breach Investigations Report*, April 2014
[9] Government Accountability Office, "A Better Defined and Implemented National Strategy is Needed to Address Persistent Challenges," Testimony to Committee on Commerce, Science, and Transportation and Committee on Homeland Security and Governmental Affairs, U.S. Senate, GAO-13-462T, March 2013.
[10] Senator Tom Coburn, February 2014
[11] Government Business Council, June 2014
[12] Reuters, "Internal Federal Cybersecurity Threats Nearly as Prevalent as External, SolarWinds Survey Reveals," March 2014.
[13] GAO-14-487T
[14] GAO-14-354
[15] Verizon Enterprise Solutions, April 2014
[16] GAO-14-487T
[17] Jason Andress and Steve Winterfield, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Second Edition, Syngress, 2014

Image: Flickr user Yuri Yu. Samoilov