i360Gov BUSINESS TECHNOLOGY NEWS ANALYSIS

i360Gov.com | SPECIAL REPORT | MAY 2010

Government Shifts Gears to Automate, Continuously Monitor Security

As complexity and culture in federal IT environments has organically flourished, so to have the risks involved in adequately securing critical resources and information. The threats now range from misguided employees to sophisticated attacks led by governments, terrorists and organized crime, each putting federal IT in the crosshairs.

This is largely why the current federal IT cybersecurity landscape is undergoing a major renovation to streamline costly security operations and help senior federal officials gain greater visibility, along with the precise information they need to improve risk-based decision-making.

The sheer technological complexity of operating systems, middleware, applications, running on massive beds of integrated circuits, hardware, software and servers that connect everything together creates the potential for seemingly limitless security breaches. Add each agency's unique people and process complexities, and the regulatory paperwork required for federal security compliance -- and it's no wonder there are so many threats chipping away at federal cybersecurity protections, said former Air Force and Department of Energy CIO, John Gilligan, who led the development of the Consensus Audit Guidelines and is President of the Gilligan Group, a Virginia-based government technology consultancy. "The complexity is so great it tends to be oversimplified. And because culturally, computing has become so individualistic, we simply didn't implement the discipline needed to fully control access," Gilligan explained.

As a result, Gilligan maintains a major shift is now under way to gain greater security automation and the lockdown of configurations, along with better product design that builds security in from the start.

Hard Truth on FISMA

As complexity and risks have grown, federal IT security mandates, especially the Federal Information Security Management Act (FISMA), have remained largely focused on testing, evaluation and the accreditation of security solutions. This created a situation in which federal organizations spent time and effort on filing paperwork and providing documentation for compliance, without gaining any further security benefits in the process. In fact, the current certification and accreditation process required by FISMA has been estimated to cost approximately $1.3 billion per year, and another $1 billion is spent for agency inspectors general to audit FISMA compliance annually. In total, the government is estimated to have spent $40 billion on FISMA compliance since its enactment in 2002.

> *"In total, the government is estimated to have spent $40 billion on FISMA compliance since its enactment in 2002."*

It's also why the White House, with OMB's guidance, issued a memo in April instructing federal departments and agencies to use an online data collection tool to file fiscal year 2010 reports by Nov. 15, as required by FISMA. This single step reverses the compliance requirements, eliminating paper filings and documentation, and further underscores the administration's efforts to drive continuous monitoring and automation into federal IT organizations.

To continuously monitor security-related information

sponsored by:

Juniper Networks

Juniper Networks delivers secure, reliable and trusted networking solutions, helping federal agencies collaborate securely and defend against cyber attacks, unauthorized access, supply chain infiltration, natural disasters or other threats to network operations and security.

from across the enterprise, "agencies need to automate security-related activities, to the extent possible, and acquire tools that correlate and analyze security-related information," the memo stated.

The memo also said federal agencies must "develop automated risk models and apply them to the vulnerabilities and threats identified by security management tools."

In addition to the electronic filing process, a team of government security specialists will quiz agencies on their security posture. The aim of the electronic and in-person questioning is to build cybersecurity profiles of each agency. According to Ron Ross, senior computer scientist at the National Institute of Standards and Technology's Computer Security Division, and chief FISMA guru, "technologies of trust are needed to build better security into solutions used by government."

Renovations to the federal IT cybersecurity landscape started in earnest last fall, following impressive results from a year-long cybersecurity pilot test conducted by the U.S. State Department, which implemented continuous monitoring and risk-based scoring to track and manage IT vulnerabilities. The State Department achieved a 90 percent drop in security risks on a key unclassified network following its pilot, which tested tools and techniques required to continuously monitor all systems and servers on the network. *(See related story in this report.)*

Effective threat detection requires continuous monitoring, and increased 'situational awareness' to learn about users across all of their identities, and to detect patterns of user behavior that are suspicious or anomalous. "What the State Department proved in it's pilot effort is that cybersecurity can be greatly improved when federal organizations move away from the old culture of compliance, to one of continuous monitoring and measurement," said Alan Paller, director of research for the SANS Institute.

A second change now taking place, in Paller's view, is a shift away from perimeter defense, as solutions such as firewalls, web filters and spam filters don't stop attackers from using email and the web to infiltrate government organizations. Instead, Paller explained, the focus is shifting toward hiring personnel and investing in tools to gain better forensics, log monitoring, deep packet analysis to understand exploits, along with configuration controls, secure coding and better security management.

Last fall, the Office of Management and Budget also launched CyberScope, a secure, data collection platform for reporting that allows research and analysis across federal agencies. CyberScope is the primary online tool to be used by federal agencies in completing fiscal 2010 FISMA requirements. And federal chief information officer Vivek Kundra formed an interagency task force to develop new metrics for information security. Meanwhile, the National Institute of Standards and Technology revised its certification and accreditation Special Publication 800-37 to increase emphasis on continuous monitoring, including a recommendation for the use of automation to obtain timely, cost-effective, and efficient monitoring results. The OMB is also working on a cybersecurity dashboard much like the one used by the State Department to further unlock the real-time monitoring value of security information currently housed in federal IT environments.

NIST's Ross maintains security must become a top priority in all IT purchasing decisions. By the fall of 2010, NIST will publish new guidelines aimed at helping federal organizations build enterprise-wide risk management strategies. "It's not just about continuous monitoring, it's really about building a step-by-step process for understanding the organization's core mission, process and information, and then deciding what protections are most necessary," he explained.

NIST will also publish systems and security engineering guidelines and a separate application security guideline, along a special new guideline on continuous monitoring. "Organizations must secure each layer, including applications, middleware, operating systems and hardware, and in the past we've not always practiced what we preached in protecting each layer," Ross explained.

The continuous monitoring guideline will focus on managing change in a dynamic environment, he said, though this element really comes in at step #6 in NIST's developing risk management framework. Ultimately, Ross said, "the federal government must stop fighting fires, and focus instead on building a long term strategy for deploying secure technologies."

NIST is working to lay the foundation, but there's still much heavy lifting to be done to complete the renovation. In the last three years, Ross said 12 pieces of legislation related to improving cybersecurity have been bouncing around in Congress, although nothing has come out yet. He added that legislation, education, training and

awareness, more secure products and more discipline in the deployment and use of technology are all required to improve cybersecurity government-wide.

To raise the level of security and improve the management of risks across the federal enterprise, "there are many reasons to consider the next iteration of FISMA," said Bob Dix, vice president of U.S. Government Affairs and Critical Infrastructure Protection, Juniper Networks. Dix pointed out that IT security discussions and efforts today are not all that new. The idea of a security configuration initiative such as the Federal Desktop Core Configuration (FDCC) was spawned out of work created by a high-level industry – government working group several years ago. Both the Consensus Audit Guidelines (CAG) and Security Content Automation Protocol (SCAP) are further important efforts that seek to improve risk management and security on an enterprise-wide basis.

FISMA isn't alone in needing renovation. Agencies struggle to comply with other regulations such as FDCC, because they must first retrofit applications and systems in their existing states, and then assess the risks associated with deviations and make sure computers work properly after the making changes, according to a recent GAO report. Officials report it's also difficult for these initiatives to remain relevant when, for example, FDCC guidance lags behind software releases.

Meanwhile, approximately a half dozen noteworthy cybersecurity bills remain under consideration by Congress. So far, the Cybersecurity Enhancement Act is the only one approved by the House of Representatives this year. Another bill, the Cybersecurity Act, has cleared the Senate. All others are still in committee. If no significant cybersecurity legislation passes before the coming election season, news reports indicate one or much such bills may serve as the foundation for actions taken in the first session of the 112th Congress, in January.

What's Needed?

Industry observers maintain that while security and compliance have been two separate disciplines, efforts under way now will likely improve both compliance and security protection. "By using automated tools and advanced analytics to more closely align both compliance and security, government organizations will address gaps and focus valuable resources on high-value projects that meet both compliance requirements and provide a significant reduction in security risk," Paller said.

According to industry observers, there's been a lack of federal leadership in leveraging its purchasing power in the security arena. Also, government could do a better job of establishing requirements in terms of security, performance and reliability. However, one of the biggest problems, according to industry research, is that as much as 80% of potentially exploitable vulnerabilities are due to poor basic security practices, including out-of-date antivirus signatures, a lack of enabled firewalls on some networks, misconfigured systems and poor password management. "Improved fundamental cyber hygiene would help reduce risks," said Dix.

Dix maintains public and private sector organizations must work together more closely to share information and further reduce risks. This is why Juniper is working with the Department of Homeland Security on the finalization of its National Cybersecurity Internet Response Plan, among other initiatives. Dix maintains sharing threat information, network anomalies and abnormalities, and bringing those capabilities together in a joint integrated capability for the nation's benefit are all important to improving federal cybersecurity. "This is part of the maturing collaboration between industry and government to improve both the preparedness and resilience of government systems to protect and defend national interests," he added.

Administration officials also hope new guidance emphasizing real-time monitoring will help federal agencies do a better job of sharing information on immediate IT security threats than they have in the past.

For now, the federal cybersecurity renovation is focused on leveraging more automation, enhancing legislation and adding continuous monitoring, as well as trying to set up better sharing of information and a more rapid evolution of guidance, Gilligan said. "The State Department's success automating monitoring, using new tools, figuring out how to score risks, and interacting with organizations to deal with cultural issues, all make great sense to me," he added.

Ultimately, while threats will change, Gilligan said the federal government has been "on a treadmill, burning calories but not getting anywhere," when it comes to improving its cybersecurity posture. Increasingly, it's clear that implementing CAG controls and increasing automation and monitoring may make all the difference.

From the Trenches

To make the transition to automated, continuous monitoring, John Streufert, Chief Information Security Officer and Deputy CIO for Information Security for the Department of State offered the following advice:

1) Begin with a small pilot.
2) Determine the algorithm to be used for each component to be scored. Begin with the raw Common Vulnerability Scoring System (CVSS) scores for vulnerability and determine how they should be transformed to be meaningfully added. Determine the parameters for other scoring components by contrasting them with vulnerability scores.
3) Establish a formal process for requesting, reviewing and approving and/or rejecting scoring exceptions.
4) Engage the owners of the underlying data so the potential impact of tool upgrades on the scoring program can be analyzed. Having scores suddenly worsen across the board will generate trouble tickets, ill will and a feeling that the scoring program is unstable.
5) Establish a team to which scoring questions can be directed. Initially, there will be many questions due to misunderstandings, issues with the underlying data and concerns about the scoring program implementation.

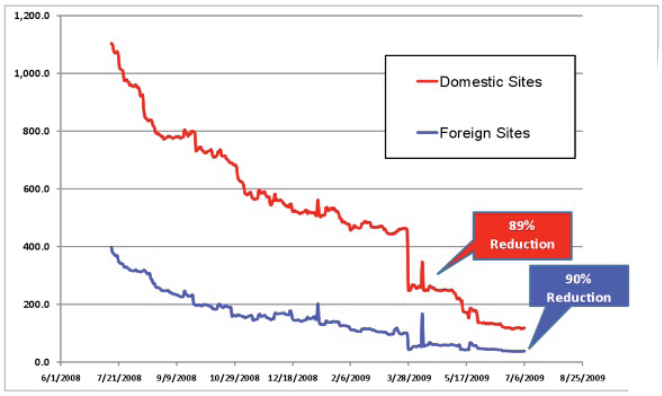
As much as possible, the pilot test's design should accommodate the addition of new scoring components and changes in calculations for components. Establishing this type of flexibility was one of the most difficult challenges at the Department of State.

State Department Slashes Security Risks Using Automated Monitoring & Measurement

When the State Department decided it's aging compliance requirements based on manual processes and annual compliance checks didn't meet the organization's need to securely implement web-based technologies and services, it launched a pilot test to see if automation and monitoring would make a difference.

The department deployed a digital security dashboard to monitor its worldwide network of 5,000 routers and 40,000 host computers that supports 285 foreign posts. Automated data collection helped the State Department implement a risk-based scoring system to reduce overall risk on a key unclassified network by 90 percent. In all, risk is now assessed 100-300 times more frequently than with traditional FISMA methods, said John Streufert, Chief Information Security Officer and Deputy CIO for Information Security for the Department of State.

Meanwhile, using the Security Content Automation Protocol (SCAP) now allows easy communication of



This graphic highlights the reduction in risks at the State Department after implementing monitoring tools.

controls to sensors, and results to the dashboard. The State Department currently scans its worldwide network at least every 36 hours to identify vulnerabilities.

In fiscal 2009, the State Department began supplementing FISMA compliance reports with a Risk

Scoring Program that scanned every computer and server connected to its network not less than every 36 hours, on eight security factors, and twice a month for safe configurations of software. The Risk Scoring Program leverages best practices such as the Consensus Audit Guidelines, which were mapped against the way the department is attacked. Now, the tools perform functions that include:

*Confirming what's connected to department networks;

*Assuring that computers, network and software are in the safest configuration of setting;

*Locating system vulnerabilities that need correction; and

*Collecting evidence for cybersecurity investigations.

Computer security officers complement the global scanning effort, supporting security regionally and locally for overseas posts as 'boots on the ground,' Streufert explained.

In a typical week, the State Department blocks 3.5 million spam e-mails, intercepts 4,500 viruses and detects over a million external probes to its primary non-classified network. Since 2008, the number of security related tickets more than doubled, while malicious code attacks increased by 47 percent. And the volatility of changes to security sensitive settings has also been problematic. Cyber attacks are evolving faster than they can be counteracted. And penetration tests showed 80% of the successful attacks used known vulnerabilities.

The new monitoring methods have allowed one critical piece of the department's information security program to move from a snapshot in time previously available under FISMA, to a program that continuously scans for weaknesses on servers and PCs; identifies weak configurations every 15 days; recalculates the most important problems daily to fix in priority order; and issues letter grades (A+ to F) monthly to senior managers tracking progress within their organizations.

Pilot testing is expected to be completed in August, when the department plans in the following eight months to fully automate security monitoring and add capabilities to its dashboard posting tool.

COST / BENEFIT ANALYSIS

On the plus side, the new system offered:

- Potential to reduce risks by 90% per year.
- Increased frequency of testing to address emerging threats.
- Added Environmental Analyses (both threat and situation) to meet emerging requirements.
- Enabled continuous accreditation.
- Spread costs over time, reducing delays.

As far as costs are concerned:

- Most cost can be covered by redirecting resources that would have been spent on one-time compliance testing;
- Communications, training and business change management critical to achieving benefit.
- Some technology for additional tools and dashboards still required.
- Time and effort required to express controls in SCAP.
- Cost reductions achieved in some areas. For example, compliance and audit costs were lowered by 62%.

i360Gov is an intelligent network of websites and e-newsletters designed to keep busy government business and technology leaders expertly informed while saving them time.

Comprised of six topic-specific news channels each functioning as its own website along with a comprehensive line-up of e-newsletters, the i360Gov network delivers daily news, analysis and perspective regarding government's largest and most important initiatives in an interactive, online environment.

i360Gov BUSINESS TECHNOLOGY NEWS ANALYSIS

i360Gov.com
i360GovHealthcare.com
i360GovBusiness.com
i360GovDefense.com
i360GovEnergy.com
i360GovIT.com
i360SLGov.com