ONLINE REPORT
SPONSORED BY:
CDW-G and Symantec

SPECIAL REPORT

INFRASTRUCTURE SECURITY

NEW CYBER THREATS DEMAND NEW CYBER SOLUTIONS

Evolve or die. That's the imperative guiding the development of cybersecurity technologies and strategies across government and industry. The ongoing evolution of the federal IT enterprise, extended in all directions by advances in networking and mobile technology, must be matched to similar advances in information and network security.

But above all, the nature of the current cybersecurity threats requires a new way of thinking. The old approach to cybersecurity, which was based on defending the perimeter, cannot hold up against the wide array of cyber threats that agencies now face.

"Threats to systems supporting critical infrastructure and federal operations are evolving and growing," according to a February 2013 report by the Government Accountability Office. "The increasing risks are demonstrated by the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, and steady advances in the sophistication and effectiveness of attack technology."

The growing threat is reflected in the fact that the number of cybersecurity incidents reported by federal agencies increased 782 percent from 2006 to 2012.

But a number of agencies are working to address these threats. The Air Force Research Laboratory, for example, recently issued a broad agency announcement (BAA) for cybersecurity research.

The lab, based in Rome, N.Y., is seeking ways to ensure that critical systems remain operational in the face of cyber threats. One area of interest is what's known as cyber agility. The goal is to make network and system architectures more dynamic, so that they are more difficult for cyberattackers to target.

Another topic of interest is system self-regeneration. The goal is to avoid the necessity of taking a system off-line if it is somehow compromised. This is especially important for mission-critical systems in the field.

"What are needed are systems that are able to dynamically recover with immunity in mission time without human intervention in response to unforeseen error and/or previously unknown cyberattacks," the BAA states.

The Department of Homeland Security is looking at a broad range of possible solutions as part of its own BAA, through which it awarded 34 contracts in October 2012. As part of this program, DHS is funding research into how cybersecurity can be strengthened at the hardware level -- what DHS officials call hardware-enabled trust.

"With cyber threats steadily increasing in sophistication, hardware can provide a game-changing foundation upon which to build tomorrow's cyber infrastructure," the BAA states. "But today's hardware still provides limited support for security, and capabilities that do exist are often not fully utilized by software. The hardware of the future also must exhibit greater resilience to function effectively under attack."

Besides the departments of Defense and Homeland Security, the other agencies involved in cybersecurity research and development are the National Science Foundation, the Energy Department and the National Institute of Standards and Technology.

Although these agencies are doing a lot of promising work, GAO is concerned about the lack of coordination. What is needed, the auditors say, is a cybersecurity research and development agenda that goes beyond the goals or needs of individual agencies.

"Although the federal strategy to address cybersecurity issues has been described in a number of documents, no integrated, overarching strategy has been developed that synthesizes these documents to provide a comprehensive description of the current strategy, including priority

actions, responsibilities for performing them, and time frames for their completion," auditors wrote in the February report.

In any case, while R&D work continues, agencies will be looking for any edge they can get in their ongoing battle against cyberattackers. One increasingly popular approach is the use of threat intelligence services, according to market research firm IDC.

Traditionally, cybersecurity measures have been developed by studying past cyberattacks and identifying the general signature of those attackers. But given the increasing evolution of security threats, the effect of such an approach is limited. Now more and more organizations are turning to firms that can provide intelligence on existing threats, "creating a shift in security posture toward being more proactive," according to IDC.

BUDGET SCRUTINY UPS ANTE FOR CYBERSECURITY PLANNING

What's the business case for improving cybersecurity? Despite the heightened awareness about the real and persistent threat to government systems, federal agencies are being asked to answer that question -- and they are not always having an easy time answering it.

It's not that agency or congressional leaders doubt the importance of cybersecurity. It's just that they want federal IT managers to do a better job of showing that they are investing their money wisely.

Ed Ferrara, a principal analyst at Forrester Research, wrote in a recent blog post that chief information security officers have often struggled to explain cybersecurity risks and impact in business terms.

Senior leaders generally will ask three questions, he writes: "1) Are we any more secure this year as compared to last year? 2) Are we spending the right amount on information security? and 3) Do we have the right people on the security team?"

Such questions are not trivial in the current budget environment, when spending across the board is getting even more scrutiny than ever. The importance of cybersecurity does not make it immune to tough questions. A key concern is prioritization.

For example, in a November 2012 report, the Government Accountability Office criticized the Agriculture Department for spending decisions related to IT security. In previous reports during the last three years, GAO auditors had identified "material weaknesses" in security and urged the department to work with its agencies to "define and accomplish a manageable number of critical objectives before proceeding to the next set of priorities," according to the report.

But when the department received sizable increases in IT funding in fiscal 2010 and 2011, IT leaders chose to spread the money across 16 individual programs, "some of which did not address the department's most critical security concerns," the auditors observed.

But the Office of Management and Budget and Congress are looking for more than a list of cybersecurity priorities to fund. They also want to see that agencies can make a good business case for their programs.

Late last year, GAO directed the State Department to improve its security-related capital planning process. The problem was something of a technical nature: When the time came to submit its recent Capital Planning and Investment Control reports on the security funding needed for its enterprise-level IT investments, the official responsible had not yet been fully trained on the submission process and so the department's Exhibit 300 documents were incomplete.

Although the problem was understandable, it was not trivial. "These project charters and risk management plans are critical not only to investments' success but also to securing the funding necessary to acquire and operate IT investments," the report states.

But these departments are hardly alone in their difficulties. In a January 2013 report, GAO auditors say they found a similar lack of business planning across government. The report traces the problem back to two documents that have guided the federal government's cybersecurity efforts: the 2000 National Plan for Information Systems Protection and the 2003 National Strategy to Secure Cyberspace.

These documents identified essential goals and activities to pursue. What they did not do, however, was make a business case for those goals and objectives based on the risks being addressed and the relative cost of mitigating them.

"Many of the private-sector experts we consulted

stated that not establishing such a value proposition makes it difficult to mobilize the resources needed to significantly improve security within the government as well as to build support in the private sector for a national commitment to cybersecurity," the report states.

For ideas on how to make this work, agencies might look to the Department of Homeland Security. DHS received kudos from its inspector general for its approach to cybersecurity-related capital planning. In particular, the IG noted that DHS officials provided component agencies with guidance on doing their own capital planning "to ensure that each investment is successfully managed, cost-effective, and supports DHS' mission and strategic goals."

AGENCIES URGED TO STRENGTHEN RISK MANAGEMENT EFFORTS

Risk management is proving to be the Achilles' heel of cybersecurity efforts at many federal agencies.

That's understandable because risk management is still a relatively new concept. For years, cybersecurity was seen primarily as a technology issue in which the technical vulnerabilities of systems and networks needed to be addressed with technology solutions.

But cybersecurity experts now say technology is not enough. Those solutions must be developed and managed in light of a broader understanding of the risks posed by various vulnerabilities -- what is the likelihood that a given vulnerability could be exploited, and what would be the impact on the organization? -- and of the resources required to mitigate those risks.

That's why the Federal Information Security Management Act requires federal agencies to develop risk management strategies as part of their cybersecurity efforts.

Unfortunately, a recent study by the Government Accountability Office found that agencies are struggling to comply. In fact, GAO notes, they are falling further behind with each passing year: In fiscal 2008, only three of the 24 agency inspectors general reported weaknesses related to assessing risk, while in fiscal 2011, 18 of the 24 IGs reported weaknesses in this area, according to the February 2013 report.

Cybersecurity, according to one expert consulted by GAO, "is not a technical problem, but an enterprisewide risk management challenge that must be tackled in a far more comprehensive manner than is generally understood both at the enterprise and government levels," according to the report.

From a systems perspective, security experts emphasize the importance of incorporating risk management into the systems development process -- not just at any point but at the beginning of that process.

This approach has two benefits. First, assessing the risks associated with a proposed system and estimating the cost of mitigating those risks will help an agency get a more accurate picture of the complete price tag for that system. Second, it is much easier to build security into a system at the start than to patch it up later in the process.

Agencies that delay or skip risk management processes are asking for trouble. Reviewing the Federal Communications Commission's Enhanced Secured Network program, GAO learned that program officials had cut corners on the agency's risk management policy because they were under pressure to get the system into the field as quickly as possible. The auditors faulted that reasoning.

"Unless FCC more effectively implements its IT security policies…unnecessary risk exists that the project may not succeed in its purpose of effectively protecting the commission's systems and information," the auditors wrote.

But risk management is not just a systems issue, according to guidelines issued by the National Institute of Standards and Technology. It also must be built into the governance processes throughout an organization, involving leadership at all levels in decisions about assessing and mitigating risks. "Risk management can be viewed as a holistic activity that is fully integrated into every aspect of the organization," the guidelines state.

In effect, risk management is about giving people the information they need to make smart strategic decisions. In a November 2011 report on cybersecurity initiatives at the State Department, the agency's IG expressed concern about the lack of leadership involvement in the risk management process.

"Because the risk management strategy had not been fully implemented at the organizational level, communication of operations at the system level is negatively affected, along with business decisions such as funding allocation, because management is not fully aware of security vulnerabilities that exist," the report states.

Finally, to be effective, risk management also must be realistic. This is especially challenging for cybersecurity professionals, wrote Andrew Rose, a principal analyst at Forrester Research, in a blog entry he posted last year after attending a vendor conference.

Cyber pros are prone to overreact to every threat, however unlikely, and to see the flaw in every solution.

"I had hoped that we all recognized that good security was not about hitting a home run," Rose wrote. "It's much more about applying the 80/20 rule over and over again, iteratively reducing the risk to the organization."

CONTINUOUS MONITORING: DON'T TAKE IT LIGHTLY

Without a doubt, the practice of continuous monitoring has the potential to dramatically improve the security of federal systems -- but only if federal IT managers commit themselves to it in a big way.

The principle of continuous monitoring is simple enough. By assessing the state of essential information security controls across the enterprise on an ongoing basis, agencies can ensure that their cyber defenses are in place and up-to-date.

Better yet, automated tools, which are widely available in commercial products, can go a long way toward simplifying the process of collecting and analyzing security data by providing security officials with near-real-time information on their security posture.

But continuous monitoring is not to be undertaken lightly, as numerous agencies have discovered. The most common problem is a lack of thoroughness. Any systems that are not routinely scanned are in essence cybersecurity blind spots.

The State Department, one of the pioneers of continuous monitoring in the federal government, has run into that problem with its groundbreaking iPost system. In 2012, State's inspector general reported that a number of essential systems -- including the department's most common database, its Unix servers and several common network components -- were not covered by iPost.

The lack of an enterprisewide continuous monitoring program "prevents the department from understanding the security state of the information system," the IG wrote. "It also prevents the department from effectively monitoring a highly dynamic network environment with changing threats, vulnerabilities, technologies, and missions/business functions."

That's not to say that every system needs to be monitored. That is a sure recipe for data overload, which would do nothing to improve security. The key is deciding which systems need to be monitored based on the impact that would result from a system breach or failure.

Security experts at the SANS Institute, a cooperative research and education organization, recommend doing some good old-fashioned investigative reporting as part of the requirements analysis. That includes conducting interviews with officials in the organization, digging up any information available on past security incidents, and reviewing old audit reports or automated assessments.

"The more thorough and accurate the requirements analysis is, the more effective the continuous monitoring effort will be," the institute's white paper states.

As with any enterprisewide initiative, continuous monitoring works best when driven from the top down within an agency. The Department of Homeland Security is a good case study. According to the department's IG, DHS has improved the overall security of its systems by holding component agencies accountable for cybersecurity.

DHS provided its agencies with a standardized monthly feed template, ensuring that their security monitoring efforts are in sync with the department's goals. The department's chief information security officer also meets monthly with component officials to discuss the continuous monitoring strategy and any issues that arise.

Officials at the Office of Personnel Management realized that they needed to take more of a top-down approach. In the past, information security efforts largely have been managed by various designated security officers scattered throughout the organization.

This decentralized structure created several problems, according to the IG. First, the CISO, having no direct "managerial leverage" over the designated security officers, could not hold them accountable for meeting the mandates of the Federal Information Security Management Act, such as conducting security control

tests on their systems. Second, the CISO had no way to ensure that the the security officers had the skills they needed to do their jobs, and in fact, according to the IG, many did not.

But those problems should soon be a thing of the past. In August 2012, the OPM director issued a memo transferring security duties from the designated security officers to a centralized team of information system security officers that reports to the agency's CIO.

The IG believes OPM is heading in the right direction. "Once this transition is fully complete, we expect to close the audit recommendations related to IT security governance and remove the material weakness," the IG concluded.

As agencies refine their continuous monitoring strategies, they should begin to realize the real benefits: the ability to put their personnel resources where they are needed most.

In a traditional environment, security experts spend a lot of time on the run responding to breaches. With continuous monitoring, however, they should be able to identify and fix vulnerabilities before they become problems, wrote James Lewis, a senior fellow and director of the Technology and Public Policy Program at the Center for Strategic and International Studies, in a whitepaper titled "Raising the Bar for Cybersecurity."

"The combination of mitigation strategies linked to continuous monitoring [frees] up IT resources and personnel to focus on higher-end challenges," he wrote.

WORKFORCE TRAINING SEEN AS KEY TO CYBER SUCCESS

The situation with the federal cybersecurity workforce is more complicated than many people might assume.

It's no secret that federal agencies often have difficulty recruiting and retaining security experts. But according to numerous reports, agencies also are running into problems with managing the staffs they have. And they are exacerbating these problems by not addressing the need for cybersecurity-related training and awareness programs among system developers and end users.

Perhaps the lack of training should not be surprising because training programs rarely fare well during tight budgets times. But in this case, the lack of training could be costly, according to the Government Accountability Office.

The ability of agencies to protect systems "is dependent on the knowledge, skills and abilities of the federal and contractor workforce that uses, implements, secures and maintains these systems," GAO wrote in a February 2013 report. That includes federal and contractor employees who use IT systems as well as system designers, developers and programmers.

The cybersecurity workforce itself, though, remains a particular concern. It's not enough to simply hire or "train up" cybersecurity workers, experts say. What is needed is a systemic approach to ensuring that an organization both understands its cyber workforce needs and has the resources available to meet them (see sidebar).

That sort of strategic thought is often sorely lacking in federal agencies. GAO notes that a study conducted in late 2011 found that only two of the eight agencies reviewed had developed cyber workforce plans, and only three had developed departmentwide training programs for their cybersecurity workforce.

Several tools are available to help agencies develop cyber workforce strategies. For example, in August 2012, the National Institute of Standards and Technology published the National Cybersecurity Workforce Framework, which provides a common vocabulary for discussing cybersecurity work and the associated knowledge, skills and abilities.

Another resource is the Federal Virtual Training Environment, available through the National Initiative for Cybersecurity Education, a joint effort of the federal government, academia and industry. FedVTE provides a library of training material, including classroom lectures.

Some experts believe that the growing complexity of cybersecurity, combined with the ongoing workforce shortages, will lead to demand for more automation.

More and more cybersecurity solutions that once required considerable expertise to deploy might soon be offered on demand in a software-as-a-service environment, noted Charles Kolodgy, research vice president for security products at IDC, a market research and consulting firm.

"As the IT infrastructure becomes more complicated, driven in part by mobile computing and cloud computing, security will need to be easier to acquire, deploy and operate," he wrote in a recent report.

Still, automation can only go so far toward securing the infrastructure. Cybersecurity workers are still an agency's most important resource.

Heidi Shey, an analyst at Forrester Research, emphasized how important it is for an organization to maintain its "security edge." Part of that is making sure that employees keep their skills up-to-date. But it's also about "encouraging new ideas to flow" and "preventing the security group from getting stale and set in their ways and habits," she wrote in a recent blog post.

"A security team and an organization that maintains their security edge will be better equipped to protect their organization and its assets through better decision-making at all levels," Shey wrote.

WORKFORCE PLANNING: ESSENTIAL INGREDIENTS

In a report released in February 2013, the Government Accountability Office identified seven leading practices that agencies ought to incorporate into their cyber workforce plans:

- Develop workforce plans that link to the agency's strategic plan.
- Identify the type and number of employees needed for an agency to achieve its mission and goals.
- Define roles, responsibilities, skills and competencies for key positions.
- Develop strategies to address recruiting needs and barriers to filling cybersecurity positions.
- Ensure that compensation incentives and flexibilities are effectively used to recruit and retain employees for key positions.
- Ensure that compensation systems are designed to help the agency compete for and retain the talent it needs to attain its goals.
- Establish a training and development program that supports the competencies the agency needs to accomplish its mission. ●

Source: Government Accountability Office

The Internet comes with infinite accessibility, infinite endpoints and infinite threats. There are breaches to worry about. People, too. We get it and can help protect your agency, inside and out. Our experts can audit, design and build a solution – supported by vendors like Symantec. It's what we call sleeping better at night.

Peace of mind available at CDWG.com/security

Symantec + CDW·G PEOPLE WHO GET IT™