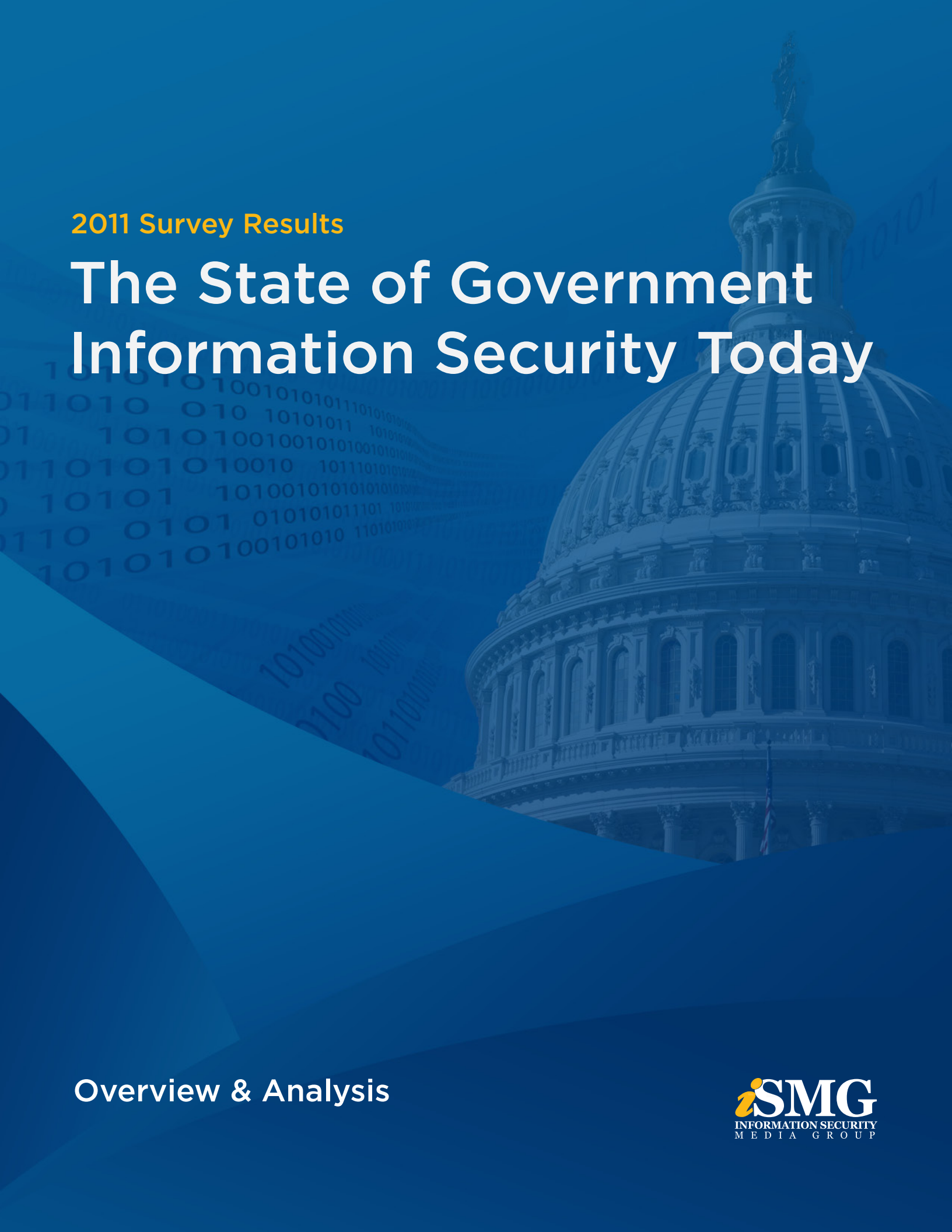


2011 Survey Results

The State of Government Information Security Today

Overview & Analysis

ISMG
INFORMATION SECURITY
MEDIA GROUP

Introduction

Eric Chabrow

Weeks after the 2008 presidential election, the bipartisan Commission on Cybersecurity for the 44th Presidency issued a report detailing the steps the new administration should take to meet the challenges government faces in securing IT. Within a month of his inauguration, President Obama asked Melissa Hathaway to conduct a governmentwide IT security review. By late May 2009, in a White House address, Obama issued the administration's Cyberspace Policy Review. That was significant because it made cybersecurity a national security priority.

But the healthcare debate, deteriorating economy and two wars distracted the administration from swiftly implementing changes to the government's approach to IT security. Indeed, it took the administration more than a half-year to name its cybersecurity coordinator, Howard Schmidt, who took office in January 2010. Congress for two years debated but never enacted significant cybersecurity reform legislation.

There had been some progress on cybersecurity: the military stood up its cyber command in 2010, agencies began to move to the continuous monitoring of their IT systems, the government developed the National Cyber Incident Response Plan to coordinate cyber defense with the private sector and the departments of Homeland Security and Defense agreed to collaborate to safeguard government IT.

Still, the pace of change to many felt slow, and questions were raised whether the administration provided the leadership needed to take government IT security to the next level.

Away from Washington, many states, counties, municipalities, tribes and quasi-governmental regional authorities faced a problem not as pronounced in the federal government: getting money to pay for IT security. In addition, finding skilled IT security personnel remained a top challenge for all levels of government, placing government IT systems at risk.

To fully appreciate the environment in which government IT security practitioners work, GovInfoSecurity.com conducted the State of Government Information Security 2011 survey in early 2011. This is the executive summary of the survey results.

Eric Chabrow
Executive Editor
GovInfoSecurity.com

Table of Contents

What is the Survey About?

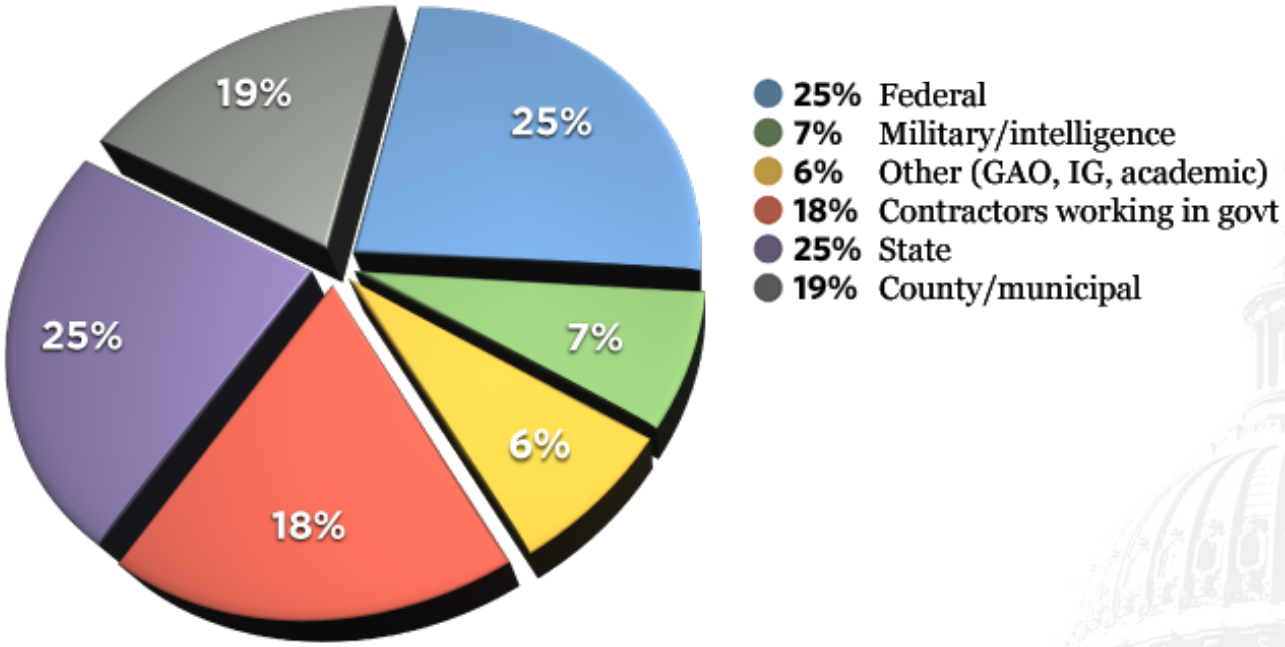
President Obama declared cybersecurity a national security priority in May 2009, in effect, making the IT experts working in and for governments at all levels the frontline troops defending local, state and federal information assets.

The purpose of this survey is to gauge the attitudes of government IT security practitioners on the current state of government IT security, expose barriers they must clear to do their jobs effectively, identify services and technology they need to safeguard IT and determine the comfort level they have with cloud computing, a platform many see as being a dominant one in the years to come.

This survey is not about the routine work many of these professionals perform daily, such as how often they patch or manage servers, laptops, mobile devices and Internet connections. We wanted to find out what they thought about IT security leadership, vulnerabilities, regulations, budget challenges, skills and cloud computing.

This survey was developed by the editorial staff of Information Security Media Group with the help of members of GovInfoSecurity.com Board of Advisers, which includes some of the most prominent experts in government IT security. The survey was fielded online from mid-January to early February 2011, and 205 IT and IT security professionals responded.

Who took the survey?



Hot Topics

The survey unveils seven hot topics on the mind of government IT security practitioners.

1. Leadership: Federal government's commitment to cybersecurity questioned

IT security practitioners at all levels of government – federal, state and local – look to Washington to provide direction on cybersecurity.

2. Vulnerabilities: Self assessment

Risks to IT systems come from everywhere, but those emanating from within the organization are among the greatest threats.

3. Rules: Initiatives aimed to make IT safe

Government IT security pros question the effectiveness of the Federal Information Security Management Act and the Einstein intrusion detection and Trusted Internet Connection initiatives.

4. Personnel: Skills shortage threatens systems

Government salaries that cannot meet those offered by the private sector only exacerbate the shortage of highly qualified IT security experts.

5. Beyond Washington: Laws, regulations, guidance

State and local IT security practitioners look to Washington, and organizations such as the National Institute of Standards and Technology, to provide guidance to safeguard their IT systems.

6. Buck Stops Here: Budget challenges

Spending priorities are changing as technologies such as cloud computing and mobility become more pervasive.

7. Cloud Computing: High anxieties

The benefits are clear, yet government IT security practitioners remain hesitant about moving forward with cloud computing because of concerns about security and regulatory compliance.

We'll dive into each of these hot topics with survey results and analysis in the following pages.

Sponsor's Analysis

CSC on Leadership and Cybersecurity

By Sam Visner, Vice President and cyber lead executive


Sam Visner

On the subject of leadership and the government's commitment to cybersecurity, I believe that having meaningful and helpful legislation in place will bring clarity. I think there are a couple of key decisions that are needed for this to happen: Who is going to be in charge of cybersecurity and what's going to be the government's responsibility, particularly in the messy domain in which the government and the private sector have common interests?

There has been a lot of give take and a little pushing and shoving about the extent to which Congress should exercise authority and the administration believes that this is more about policy and less about operational responsibility. The debate continues and the scope of the Government's efforts, particularly in regard to critical infrastructure, is not fully defined, but I believe we will see progress and it will come later in the year. Once this is done, I believe agencies, from the federal to the local levels, will have a more positive view of government's commitment to cybersecurity.

A burning issue to address: Congress needs to decide how government intends to approach the private sector, and, perhaps more importantly, the private sector needs to decide what it needs from government. There are two strains at the higher level – one is that the private sector is not going to do a good job on its own in cybersecurity, so they not only must have standards but should be told specifically what to do. Another viewpoint says that the private sector will do a good job if given the right standards, but they should be given some latitude in how they do their job, and that incentives regarding the protection of critical infrastructure have an important role to play. I believe Congress is beginning to move in this more collaborative direction, but there is a ways to go to bring this discussion to a close.

When talking about the greatest threats and vulnerabilities, I think that it is the advanced persistent threat, a class of weapons-grade threats, which ranked surprisingly low in the survey. Those capable of employing such threats appear well-resourced, have experienced people, and are patient. I consider them the most sophisticated and dangerous; over a long period of time they can apply more resources and refine capabilities. This is a really serious problem,

Finally, one area really caught my attention: cloud computing. Not because "cloud" is the buzzword of the day. No, I was struck

by a couple of things.

First, according to the survey results, nearly two-thirds of government agencies are implementing, planning to implement or conducing a cloud initiative. While that alone is not surprising, the fact is less than 20 percent are confident that sensitive data can be secured in the cloud. So, what this says to me is that while agencies are adopting the cloud solution, they are not sure it is secure. Further, even if the information was in a private cloud, or an internal cloud, more than half still say they are not confident that data is secure.

> ***"Congress needs to decide how government intends to approach the private sector, and, perhaps more importantly, the private sector needs to decide what it needs from government."***

Second, the data provides powerful insights regarding the factors holding agencies back from moving to the cloud while securing sensitive data. It's clear that the issue of security keeps many agencies from taking the ball over the goal line. Specific concerns include enforcing agency security policies, preventing data loss, and mixing data with other users. It is interesting that the concern given the least emphasis is compliance with the Homeland Security/Presidential Directive 12 (HSPD-12). This says to me that agencies may be less concerned with compliance than they are with the possibility or likelihood of data loss.

What many IT practitioners don't realize is that cloud service providers often place as much emphasis on security as government agencies. We need to move to a situation in which security concerns are not a barrier to embracing cloud computing at government agencies, especially since there is a middle ground.

A compromise exists between moving all workloads to the cloud and keeping all workloads in traditional datacenters. In fact, it may be the best solution. Agencies looking to move towards the cloud need to analyze each of their workloads individually. By having a plan and smartly implementing cloud services into their IT environments, agencies can get all of the benefits that cloud computing offers while addressing security requirements.

The "Enterprise of the Future" concept that we're seeing spread across the private sector can and should make government departments and agencies more secure, effective and efficient.

Other Resources

VIDEO

Interview with Sam Visner from RSA Conference 2011

WHITE PAPER

THE SECURITY STACK: A Model for Understanding The Cybersecurity We Need

WEBINAR

Fulfilling the Cybersecurity Agenda

Sponsor's Analysis

SafeNet on CyberSecurity and Cloud Computing Challenges within Government.

In 2011, government information security practitioners face increased scrutiny on both performance and budget. Constraints due to slashed budgets, potential governmental shutdowns and a consistent barrage of new threats on sensitive networks, has many concerned for the risks faced by their organization. In this survey, conducted by GovInfoSecurity.com, the current attitudes towards IT security leadership, vulnerabilities, regulations, budget challenges, skills and emerging technologies such as cloud computing are examined. The respondents provided perspective from across all corners of the federal community including academic, state and local, civilian government, defense and intelligence, and the contractor community.

Study Overview

When asked about leadership, the majority of the respondents felt that not enough emphasis was being placed on cybersecurity; however, the results are very split on who should solve the problem. There was not a strong consensus on which part of the government should drive IT security governance for the civilian agencies. This is a critical issue especially with a third of respondents indicating that their agencies had been involved in a breach within the past 12 months. Additionally, there is significant concern about the pool of IT security specialists available to the federal workforce, which contributed to below average self assessment results in our findings.

Protecting sensitive data continues to be a major concern for federal organizations. Accidental exposures of data connected to "poorly trained / careless users" or deliberate exfiltration "insider employees / contractors" were high on the list of vulnerabilities reported. Organizations need to secure classified information, citizen personal information, and intellectual property throughout its lifecycle, as it is created, shared, stored, and accessed. They need to ensure that protection follows data wherever it goes, from the data center to the endpoint and into virtualized settings, including cloud computing environments. This is aligned well with the top spending trends identified in the study, which include cloud computing, identity and access management, and encryption.

A Move to the Cloud

> ***"Without the right security in place, the move to cloud computing has risk."***

Cloud computing raises some pretty vexing questions when it comes to security. Some challenges are shared by most federal agencies. Today, issues of risk, information/data privacy, and compliance are the chief inhibitors to most federal agencies' adoption of cloud services. In fact, the study results cite significant concerns about security in both public and private clouds. Enforcing security policy, data loss prevention, and multi-tenant environments were the top three participant reservations about cloud computing. Therefore, delivering cloud solutions that meet federal tenants' mission requirements and enable cross-domain/agency information sharing is an invaluable asset. Understanding how to effectively safeguard data in the cloud, federal agencies can begin to fully maximize the potential of cloud offerings to enhance the efficiency of government operations, improve performance, and provide better service to the American people.

Conclusion

An evolved cybersecurity strategy has direct implications on the potential of transformative technologies like the cloud and can only be realized when security is efficiently, persistently, and effectively employed to safeguard sensitive data. There are already solutions in the market that enable the protection of data throughout it's lifecycle, prevent data leakage, facilitate secure data sharing and implement access controls. All key tenants of an evolved cyber security strategy. Additionally, SafeNet's sophisticated data-centric security solutions enable federal agencies and organizations to gain the agility they need to leverage cloud environments most effectively, without making any compromises in security, privacy, or compliance. For more information on SafeNet, please visit us at http://www.safenet-inc.com/solutions/industry/government/.

About SafeNet

Founded in 1983, SafeNet is a global leader in information security. SafeNet protects its customers' most valuable assets, including identities, transactions, communications, data, and software licensing, throughout the data lifecycle. More than 25,000 customers across both commercial enterprises and government agencies, and in over 100 countries, trust their information security needs to SafeNet.

Survey Results

1. LEADERSHIP

Federal government's commitment to cybersecurity questioned

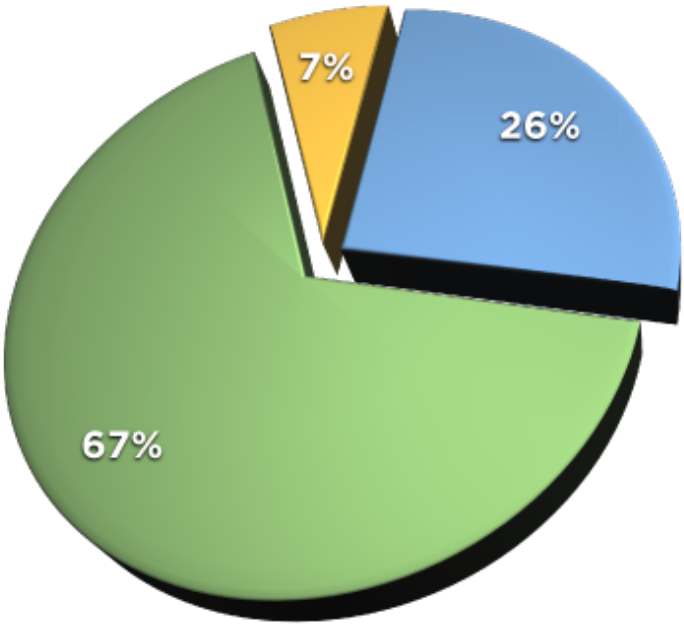
A perception exists among federal, state and local government IT security practitioners that the federal government hasn't provided adequate leadership to make IT systems secure over the past two years. Only one-quarter of our respondents see IT being more secure since the beginning of 2009.

Why did such a lower percentage of government IT security practitioners respond that way? Look at some recent history.

In January 2011, GovInfoSecurity.com published an article that carried the headline: Giving Obama a D in Cybersecurity. A group called the National Security Cyberspace Institute assessed the first two years of the Obama presidency, and issued the D because it took the president more than a half-year to name a cybersecurity coordinator. The rest of the report card wasn't as awful; it contained a smattering of B's and C's. Melissa Hathaway, who led the White House cyberspace review in 2009, vetted the report card for us, and reported back: "I thought the report card was well researched and thoughtful."

Also in January, the Commission on Cybersecurity for the 44th Presidency issued its final report that the administration had addressed many of its recommendations made in December 2008, but noted that the economy and two wars have distracted the president and his top aides from doing more. Commission Co-Chairman Harry Raduege, a retired Air Force general who ran the Defense Information Systems Agency, says this White House has done more than any other administration in addressing the nation's cybersecurity challenges, yet its work has not been sufficient.

Has the federal government placed enough emphasis on cybersecurity?



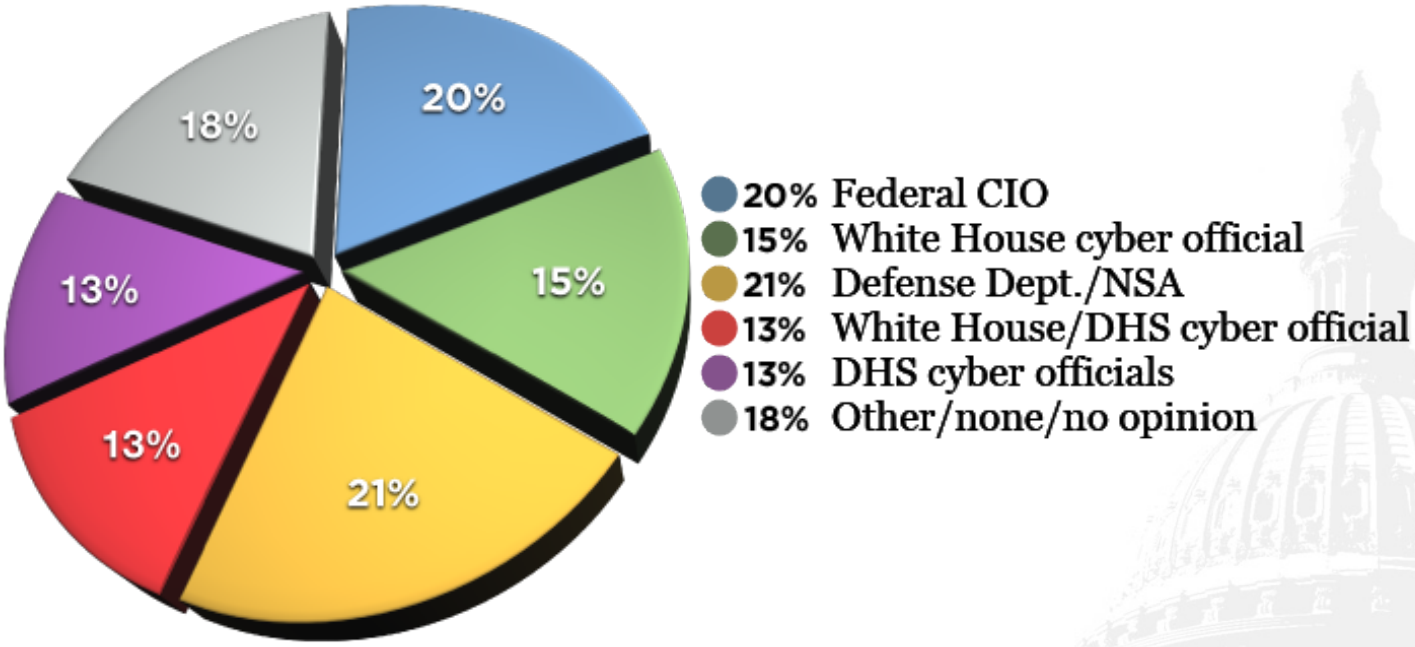
26% Yes
67% No
7% No opinion

Washington was abuzz last year on who should lead IT security in the federal government.

Bills were introduced – though never enacted – to create a White House Office of Cyberspace, with its director confirmed by the Senate. Some lawmakers such as Sen. Susan Collins sought more authority for Department of Homeland Security. A few even saw an increased role for the National Security Agency. But granting the NSA authority over civilian agency IT gives civil libertarians and privacy advocates the jitters.

Our survey takers' responses shown in the chart below reflect the lack of consensus found on Capitol Hill.

IT Security governance for civilian federal government agencies should be led by:

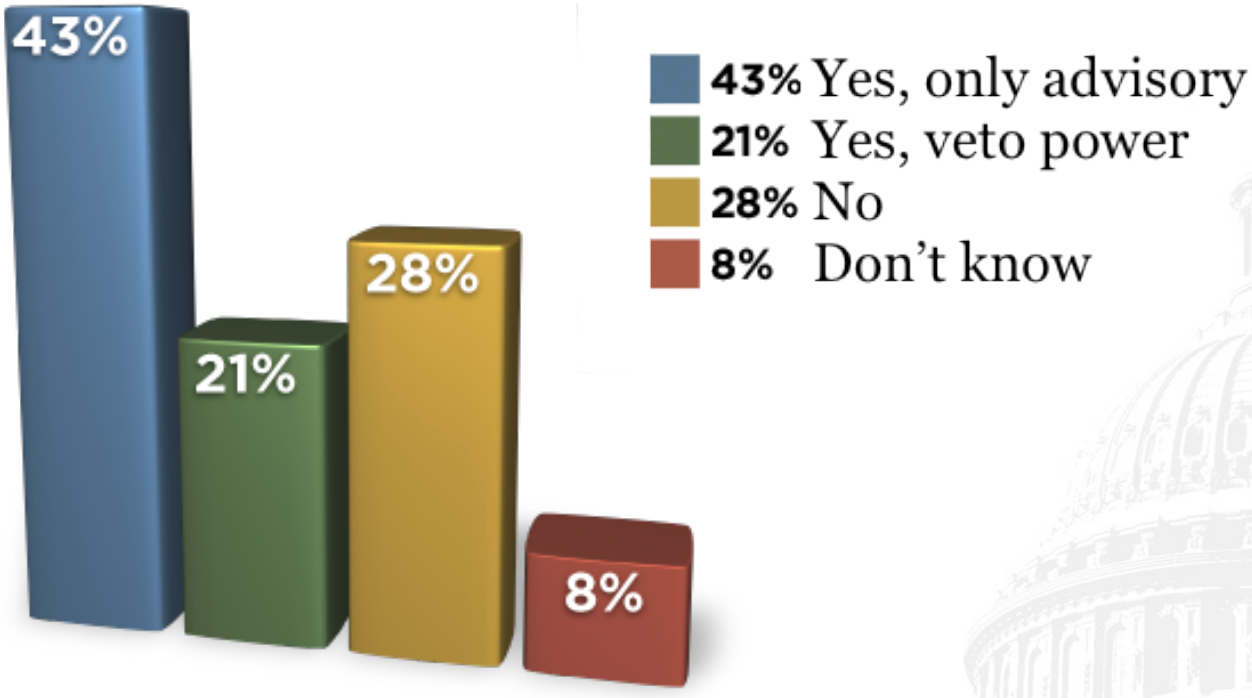


As you look at the chart below, disregard the words “White House.” Substitute “DHS” or some other agency, if you will. The point of this question – Should a cybersecurity director have budgeting authority? – is telling. More than half feel he or she should.

That suggests that those IT security practitioners in the trenches seek leadership; they want someone to make the hard decisions on the direction government IT security is heading.

The attitudes government IT security practitioners have toward leadership translate into a feeling that federal IT systems are not as secure as they should be, with only one-quarter of respondents seeing government information getting more secure over the past two years.

Should a White House cybersecurity director have budgeting authority?



Proof: Continuous Monitoring Does Work

by Eric Chabrow

At the urging of John Streufert, the State Department deputy chief information officer for security, I took a closer look at the written testimony presented by Alan Paller, research director of the SANS Institute, at a hearing last June of the Senate Committee on Homeland Security and Governmental Affairs on continuous monitoring.

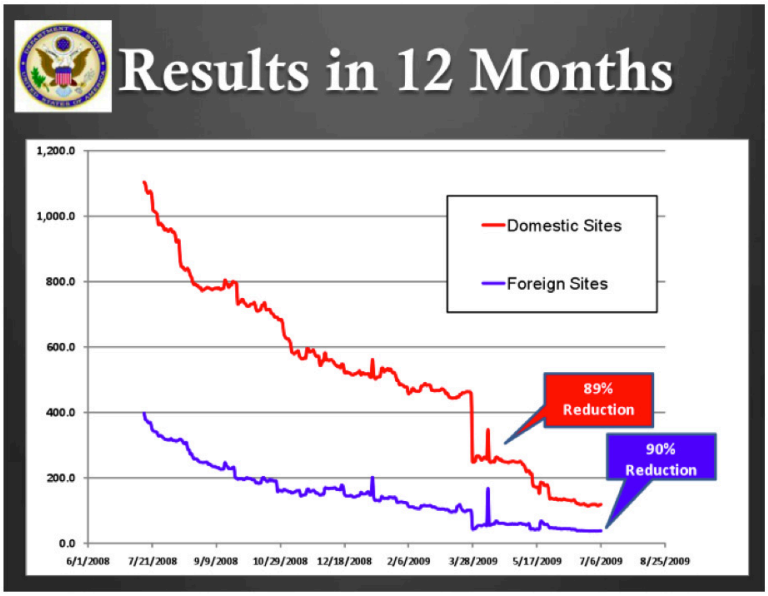
A major point Paller made was that the State Department reduced reliably measured risk by over 85 percent in less than a year by the continuous monitoring of its IT systems as compared with the traditional paper-process reporting requirements under the Federal Information Security Management Act of 2002. Said Paller:

> "Look closely at the chart, and you will see what continuous monitoring means – the updated data comes in daily or every couple of days – not quarterly or annually. Had State used the longer time periods favored by the other agencies, many more State Department computers and networks would have been open to attack, for far longer periods."

What are some real results of continuous monitoring? Paller, in his testimony, referenced Operation Aurora, the computer attack first disclosed by Google early last year:

> "State can tell, within a day, which systems have and have not been patched. When State's CISO learned of the critical problem posed by the Aurora vulnerability, he didn't have to send an e-mail. He raised the vulnerability's risk factor (the value used to weight it in the overall risk score). Every office saw immediately that their security score had fallen and their bosses also saw the fall. Within six days, 90 percent of all vulnerable systems in all embassies and in all State Department offices around the world had been patched and were safe from attacks.

That's six days, not weeks or months. No e-mails had to be sent; the scoring risk system did all the work. A clear example of why daily continuous monitoring is so important: it causes rapid risk reduction with low overhead."



Few other agencies have replicated what State has done, blaming the high costs of complying with FISMA as tying up their funds, Paller said. Indeed, the State Department estimated it spent $133 million over six years to certify and accredit 150 of its major IT systems, producing 95,000 pages of documentation.

But Paller said it's not just antiquated FISMA rules that interfere with a move to continuous monitoring, but the business interest of some government contractors:

> "The contractors that charge federal agencies hundreds of millions of dollars for writing the out-of-date reports are fighting to stop the move to continuous, daily monitoring, even though they and their firms can continue to be employed to enable and manage the new way of doing business. Their rear-guard actions are being supported by federal officials who appear to be uncomfortable with change or afraid of taking responsibility for active risk reduction."

That's a point made to me by Jerry Davis, then deputy CIO for security at the National Aeronautics and Space Administration, which is following State's leading and moving to continuous monitoring. I asked Davis in an interview about the reaction at NASA after he issued a memo in May announcing the continuous monitoring initative:

> "I think it started off with a little bit of concern internally throughout the IT community because we had, in a sense, more or less been caught up in the old way of doing things and this is a change, and as you know at most organizations change is very, very difficult to impart on an organization. So, we have been working through a lot of change in management's activities and really getting around and out and about to the constituency that we service internal to NASA and the folks that are actually going to be helping us move forward with this move toward automated continuous monitoring.

Where was this concern coming from? Answered Davis:

> "It's really the folks in the middle ... because there is uncertainty as you move away from this third-party activity that we had been doing. It takes a lot of manpower. It takes somebody to prepare to package it, to make sure that the certification, accreditation packages, the system security packages, all of those things are updated and when you talk about going to continuous monitoring where that's not such a big focus, I think some folks don't understand.

Despite the high cost to document FISMA compliance, employing automated tools to continuous monitor critical IT systems requires significant investments, too, that must be properly managed. I've been exchanging e-mails on this topic with Streufert, and here's what he wrote:

> "In place of the unacceptably wasteful spending for snapshots of process and compliance, the State Department redirected its FISMA energies 18 months ago – wherever we possibly could – toward a different


John Streufert
Deputy CIO, State Department

outcome. We were in search of strategies that would offer a higher return on investment for time and money we spent on security, just as our CIO asked us to do.

> "For us, this meant setting a long-term goal of merging our cyber policy and operational security groups into a single integrated team. Numerically, we went from 60 writers of three-ring certification and accreditation reports, to a total workforce of 4,135 technicians with significant security responsibilities working on continuous monitoring. The key seemed to be letter grades A to F-minus that everyone including top executives could relate to.

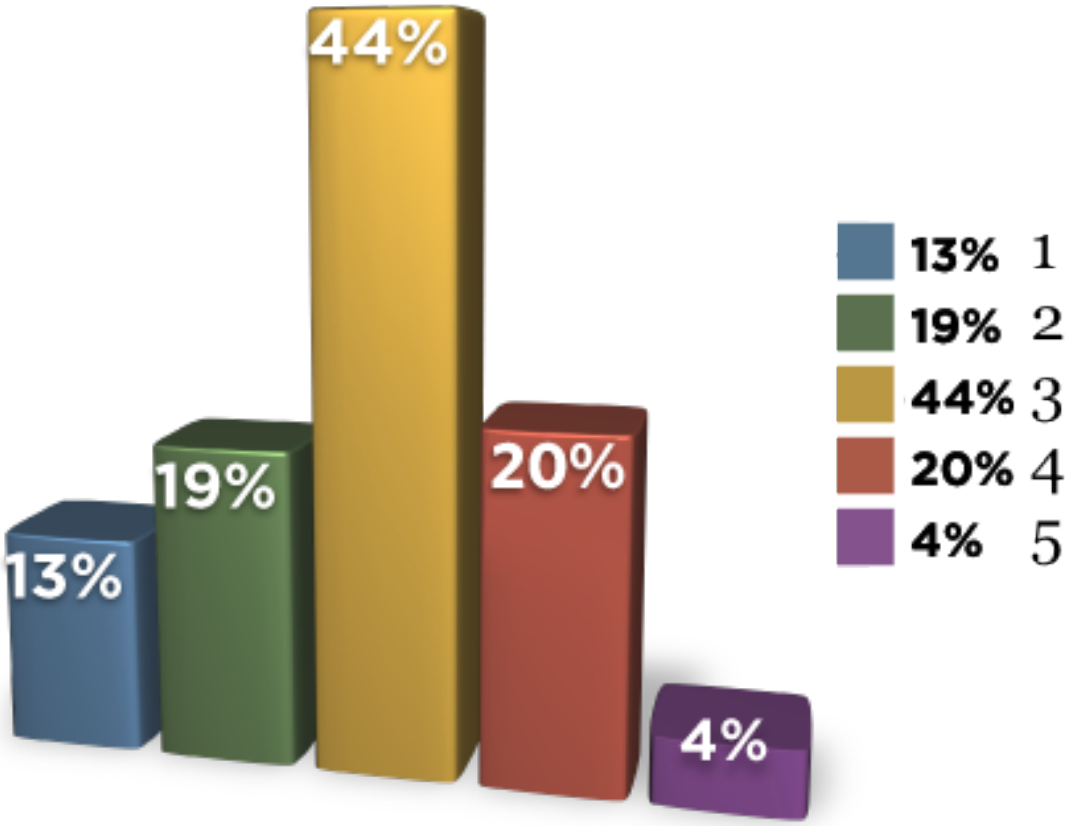
> "Why shift emphasis? Our adversaries have far more people. In doing so, not only did our work force applied to defensive cybersecurity dramatically increase, we can now focus the time and attention of all the information assurance professionals we have on the most damaging potential risks first through risk scoring. That is the power of a well-crafted cybersecurity dashboard, good metrics, personal accountability and the ability to focus on where you are being attacked."

http://blogs.govinfosecurity.com/posts.php?postID=591

Have federal government IT systems been more or less secure over the past two years?

On a scale of 1 to 5, with 1 being Less Secure and 5 being More Secure

Their view turns marginally more optimistic when looking ahead to the next two years.



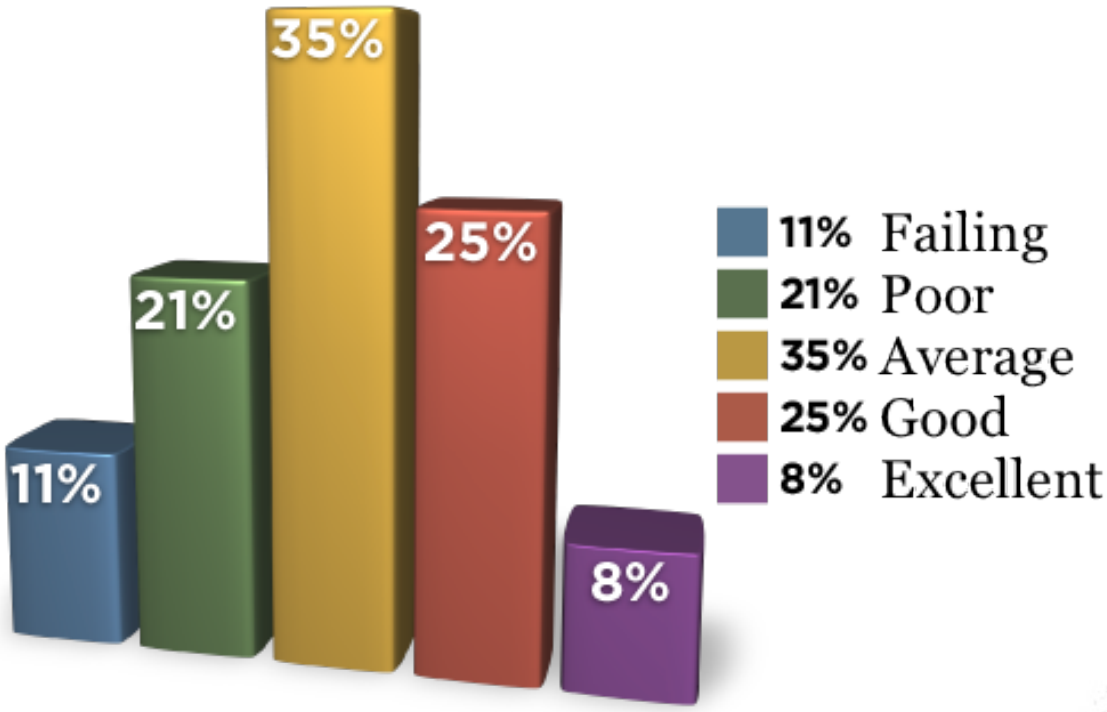
2. VULNERABILITIES

Self assessment

As seen in this chart, there is no consensus by government IT security practitioners on their view of the ability of their organizations to counter threats.

Dig deeper into the results, and you'll find that managers – at 66 percent – have a more optimistic estimation than do staffers – at 30 percent – on their agencies ability to safeguard IT. And state IT security pros have a dimmer view than those working at the federal level on their agencies' abilities to thwart cyberthreats.

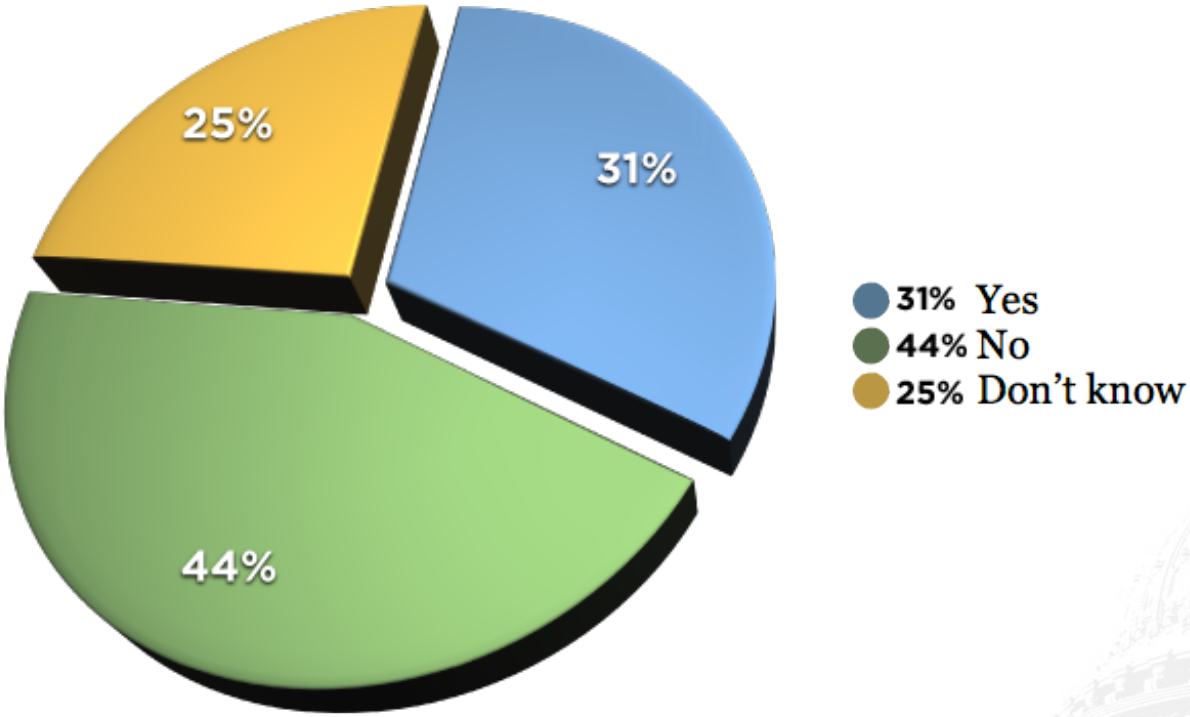
Rate your agency's ability to counter threats.



Just about one-third of our respondents say their agencies experienced a significant breach this past year. And that one-quarter of respondents don't know if their agencies experienced a breach is alarming. Some suggest "don't know" could be the same as "yes."

Federal respondents, by nearly a 2-to-1 margin, say their agencies experienced more breaches than with those working for state and local governments. That shouldn't be surprising; WikiLeaks, after all, was a federal breach.

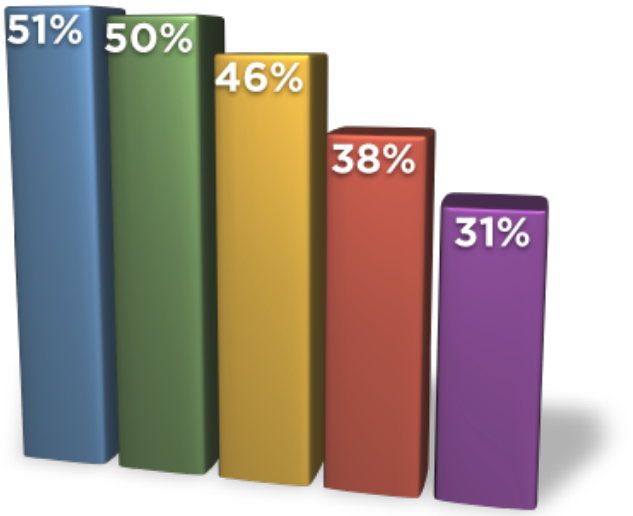
Has your agency experienced a breach involving the disclosure, modification or loss of data in the past 12 months?



Look at the charts below, and the first thing that comes to mind is WikiLeaks.

The Greatest Threats

The What

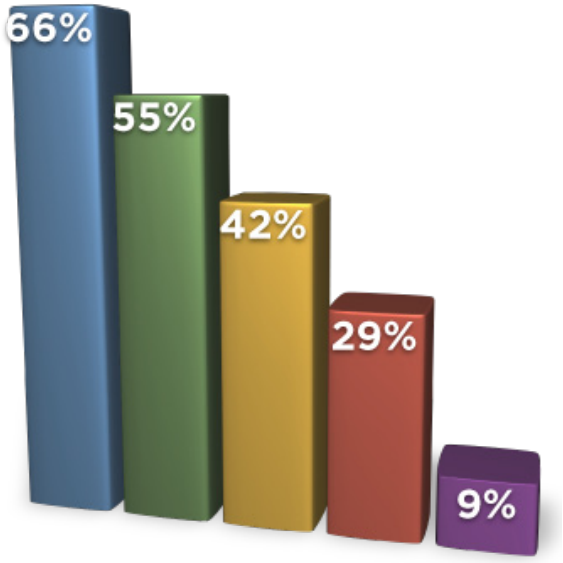


51% - Insider threat
50% - Poor practices
46% - Exploitable software vulnerabilities
38% - Configuration errors
31% - Malware

The disclosure of more than a quarter-million sensitive and classified diplomatic cables came, allegedly, from a low-ranking military enlistee who, despite his security clearance, accessed and retrieved – many would say stole – information to which he was not entitled.

The enemy is within. And, if not the enemy, the vulnerability is clearly from within the agencies. Poor practices, poor training, careless users – the non-malicious threat – is of equal concern, if not more so, than those who intentionally would do harm. "Individuals may do something accidently, not intentionally; however, the consequence would be the same if it were intentional," says Multistate Information

The Who



66% - Poorly trained/careless users
55% - Insider employees
42% - Insider contractors
29% - Foreign nations
9% - Terrorists

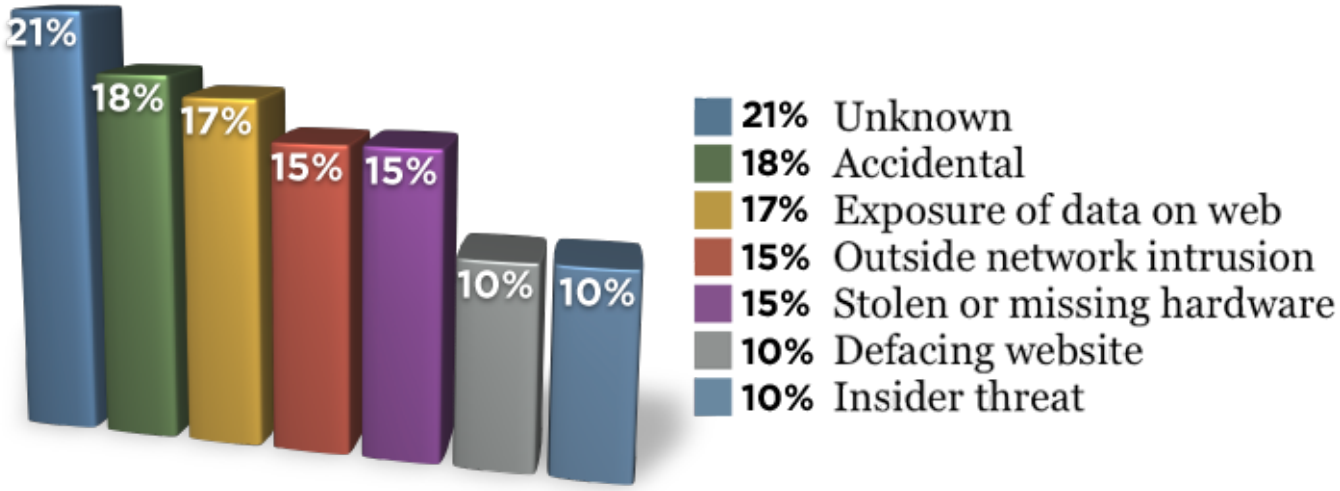
Sharing and Analysis Center founder Will Pelgrin, Center for Internet Security CEO and former New York State CISO. Still, those intentionally wanting to cause damage remain a big concern. "You're always worried about insider threats in terms of either espionage or compromising capabilities, and cyber is no different," says Deputy Defense Secretary William Lynn, the DoD's point man on IT security.

Government IT security practitioners don't get to pick their enemy; danger lurks everywhere.

The types of breaches shown below confirm what the previous charts suggest. Threats originate from all over.

If your organization experienced a breach in the past twelve months, what type?

(Multiple answers allowed)

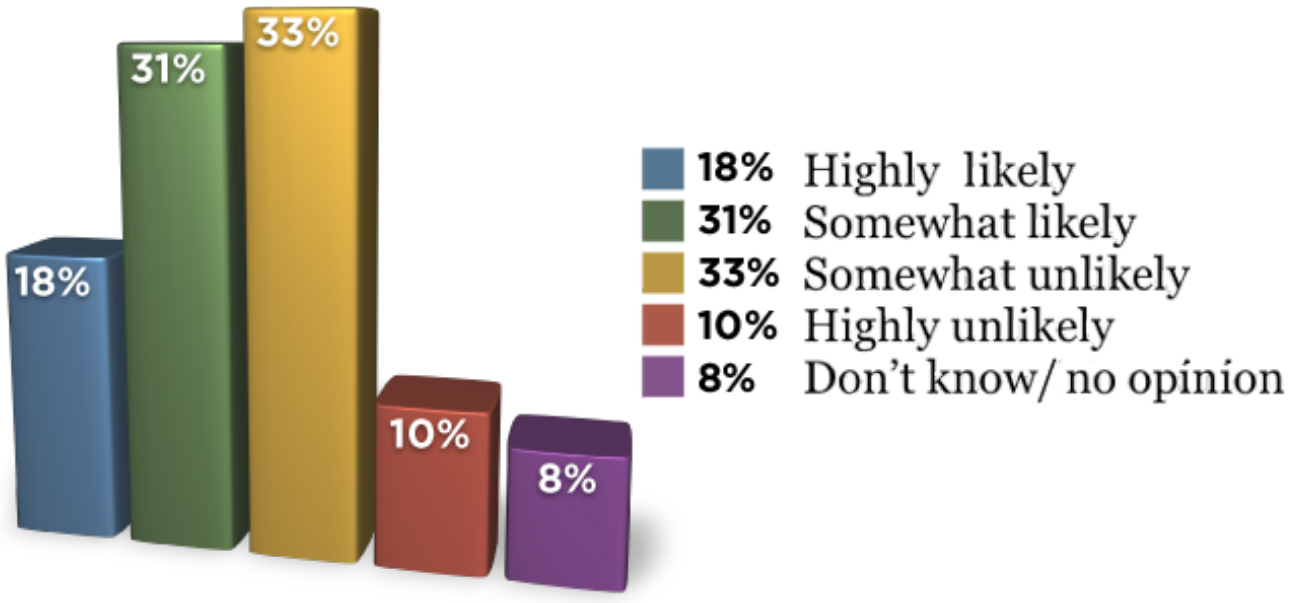


That 1 in 5 respondents say some of the breaches their organizations experienced were unknown suggests that not all breaches can be clearly identified. And a single breach could fall into multiple categories. Exposure of data on the web could be accidental.

What is clear here is that no one type of breach dominates, and that requires the IT security practitioner to defend against all types.

Cleary, our respondents see threats continuing, with about half expecting a breach in the next 12 months.

What's the likelihood of your agency being breached in the next 12 months?



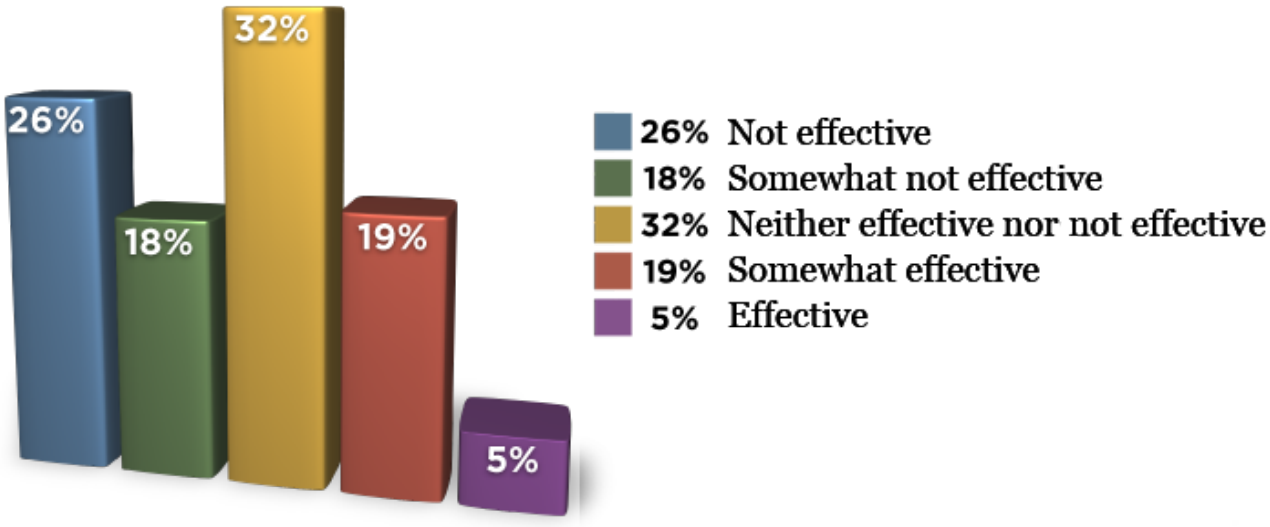
It's becoming part of the culture, and that means IT security practitioners must not only keep up their guard, but figure out how to respond once a breach occurs.

3. RULES

Initiatives aimed to make IT safe

How effective is the Federal Information Security Management Act in securing your agency's IT systems?

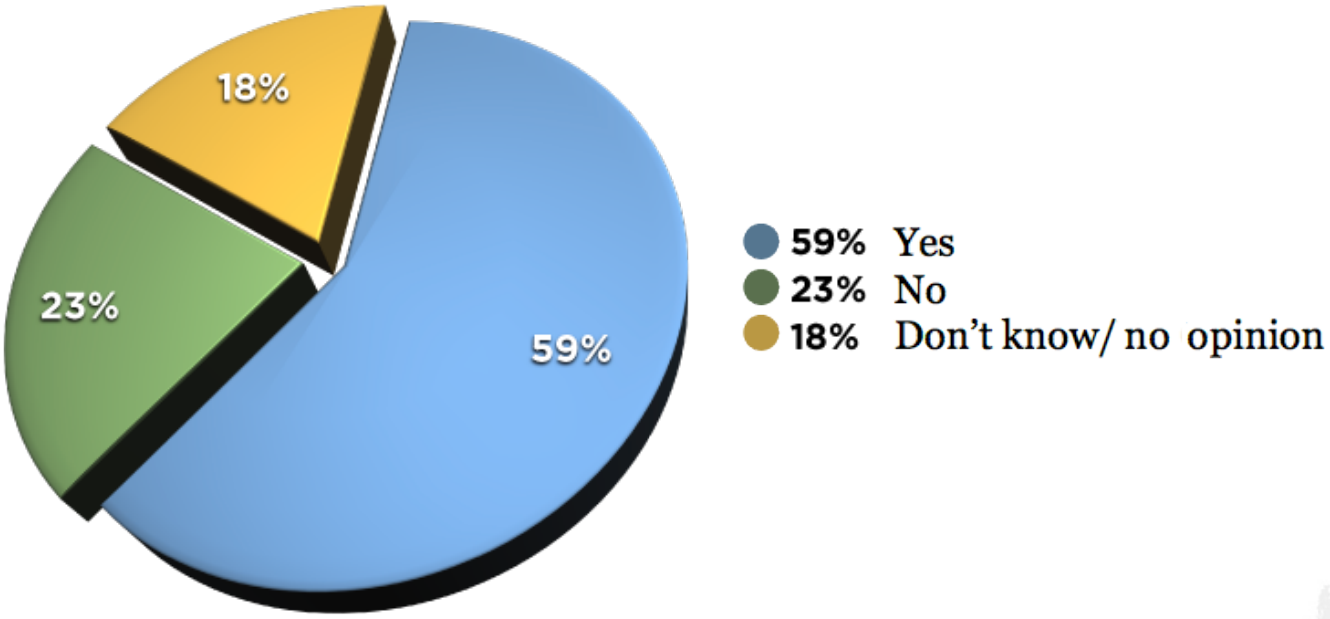
Asked of those working at federal agencies.



A plurality of government IT security practitioners – 45 percent – does not find the check-box approach to IT security spelled out in the Federal Information Security Management Act of 2002 as being effective in securing government IT. But the government is moving away from paper compliance toward continuous monitoring, and overwhelmingly, IT security professionals in government believe that will improve their ability to safeguard government data.

Will continuous monitoring make your agency's systems and networks safer than existing FISMA requirements?

Asked only of those working at federal agencies



The Department of State was an early adopter of continuous monitoring, and Deputy Chief Information Officer John Streufert says it works better than the old FISMA approach.

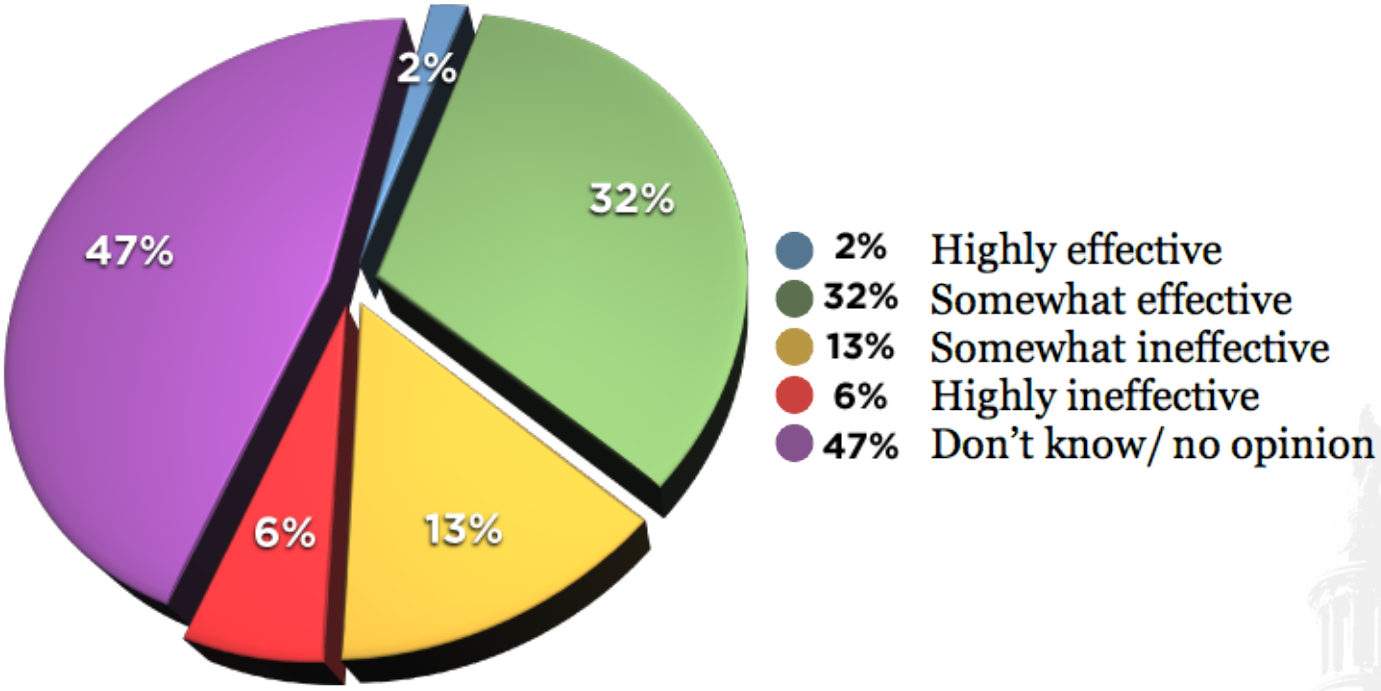
"For us, this meant setting a long-term goal of merging our cyber policy and operational security groups into a single integrated team," Streufert says. "Numerically, we went from 60 writers of three-ring certification and accreditation reports, to a total workforce of 4,135 technicians with significant security responsibilities working on continuous monitoring. The key seemed to be letter grades A to F-minus everyone including top executives could relate to.

"Why shift emphasis? Our adversaries have far more people. In doing so, not only did our workforce applied to defensive cybersecurity dramatically increase, we can now focus the time and attention of all the information assurance professionals we have on the most damaging potential risks first through risk scoring. That is the power of a well-crafted cybersecurity dashboard, good metrics, personal accountability and the ability to focus on where you are being attacked."

Administered by the Department of Homeland Security, the aim of Einstein 1 is to collect traffic flow information entering government systems from the Internet for threat analysis, Einstein 2 is to detect vulnerabilities and Einstein 3 is to prevent vulnerabilities.

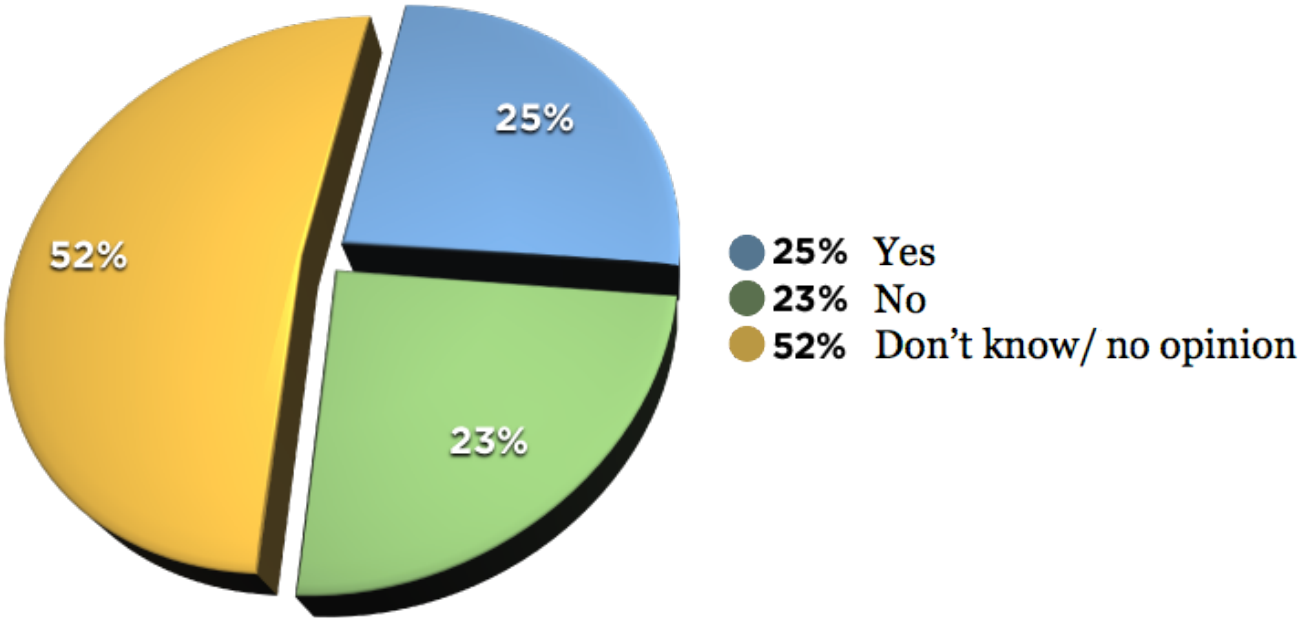
How effective is the Einstein 1 program in collecting data about vulnerabilities?

Asked of those working at federal agencies.



Our respondents give the Einstein initiatives mixed grades. DHS Inspector General Richard Skinner, in testimony before Congress last year, suggested the department needs to do a better job educating agencies on Einstein. He said DHS hasn't provided sufficient training on the Einstein program. "Some agencies indicated that they received compact disk, portable document format brochures and handbooks about the Einstein program, while other agencies received nothing," he said.

Will the Einstein 2 detection system make government IT more secure?



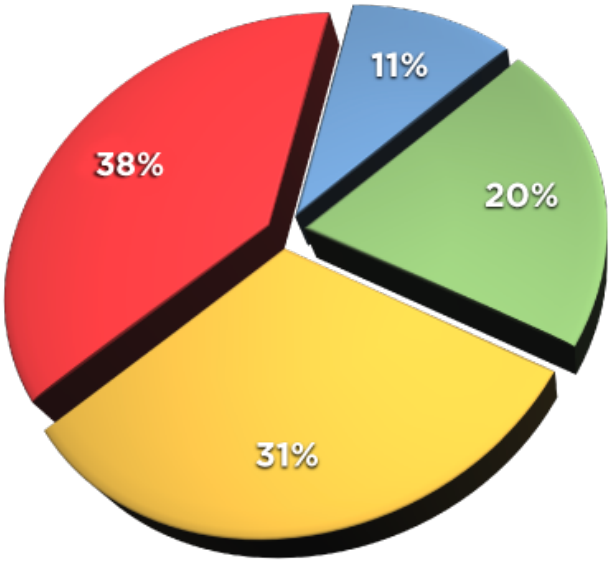
Though government IT security practitioners may have their doubts, or no opinion, about the effectiveness of the Einstein initiatives, the Obama administration believes in them. The third phase of Einstein is intrusion prevention, and the Department of Homeland Security seeks $233.6 million to expedite the deployment of Einstein 3 to prevent and detect intrusions on computer systems and to upgrade the National Cybersecurity Protection System, building an intrusion detection capability and analysis capabilities to protect federal networks.

Einstein 2 is a federal program, but had been tested in Michigan. "What Einstein has taught us is that even if you think you're good, there are always opportunities to get a lot better, and I think Einstein has taken us up a couple of notches because it's really providing us with a vision into a whole other level of threats that current processes in our current systems aren't capable," says Ken Theis, who served as Michigan's CIO when the state tested Einstein.

The goal of the Trusted Internet Connection is to reduce the number of gateways between federal networks and the Internet from 8,000 four years ago to fewer than 100. Fewer access points simplifies monitoring of traffic moving between the government and the Internet.

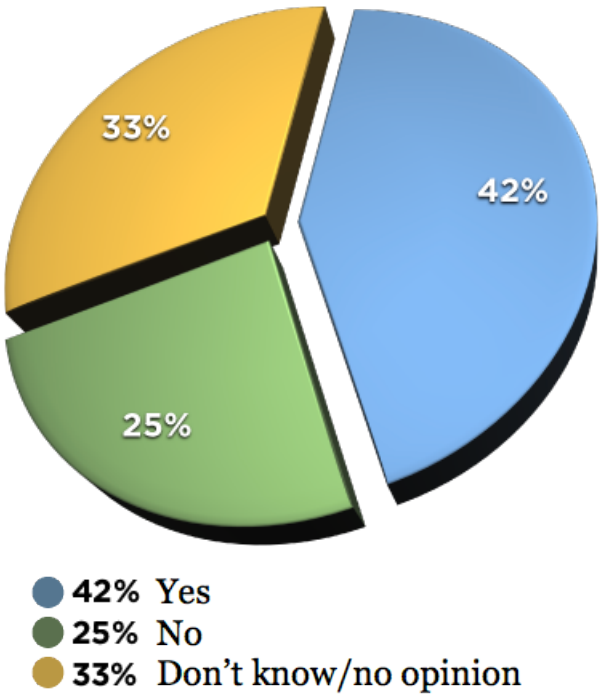
More than two-thirds of respondents familiar with their agencies TIC initiatives say it has been or will be implemented by year's end.

When will your agency implement the Trusted Internet Connection?



And, by nearly a 2-to-1 margin, those having an opinion of TIC see it making IT systems more secure than those who do not.

Will TIC make IT systems more secure?



4. PERSONNEL

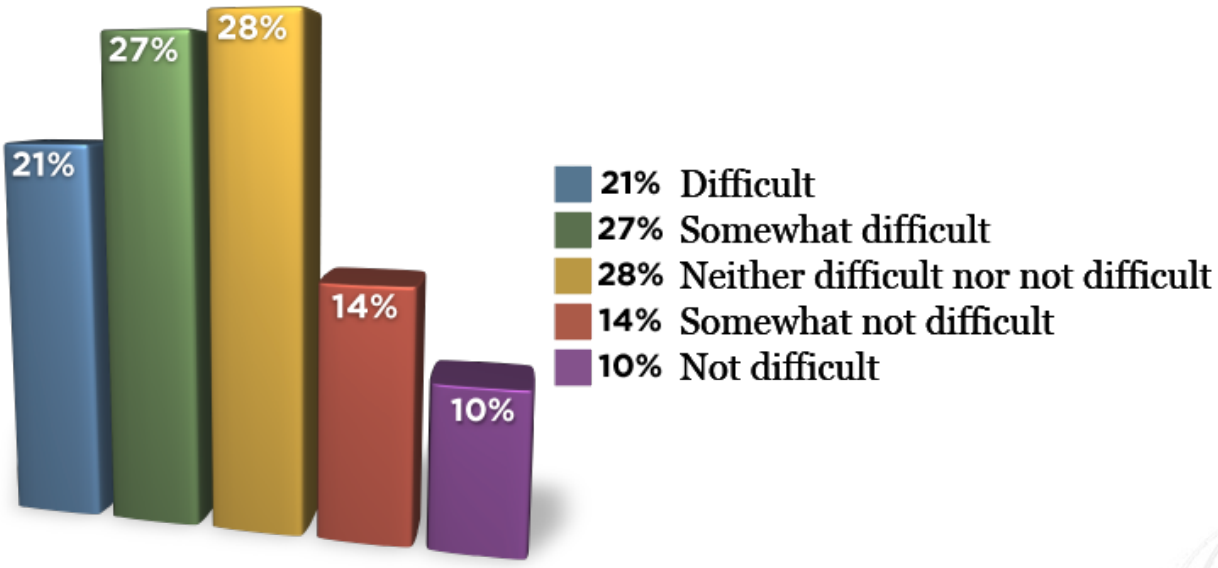
Skills shortage threaten systems

Finding qualified IT security specialists is one of the biggest challenges facing governments at all levels. It's a two-edged sword. First, there are just not enough IT security experts – especially with highly valued technical skills. Second, government salaries cannot match those offered by the private sector.

How difficult is it to find a qualified IT security professional to hire?

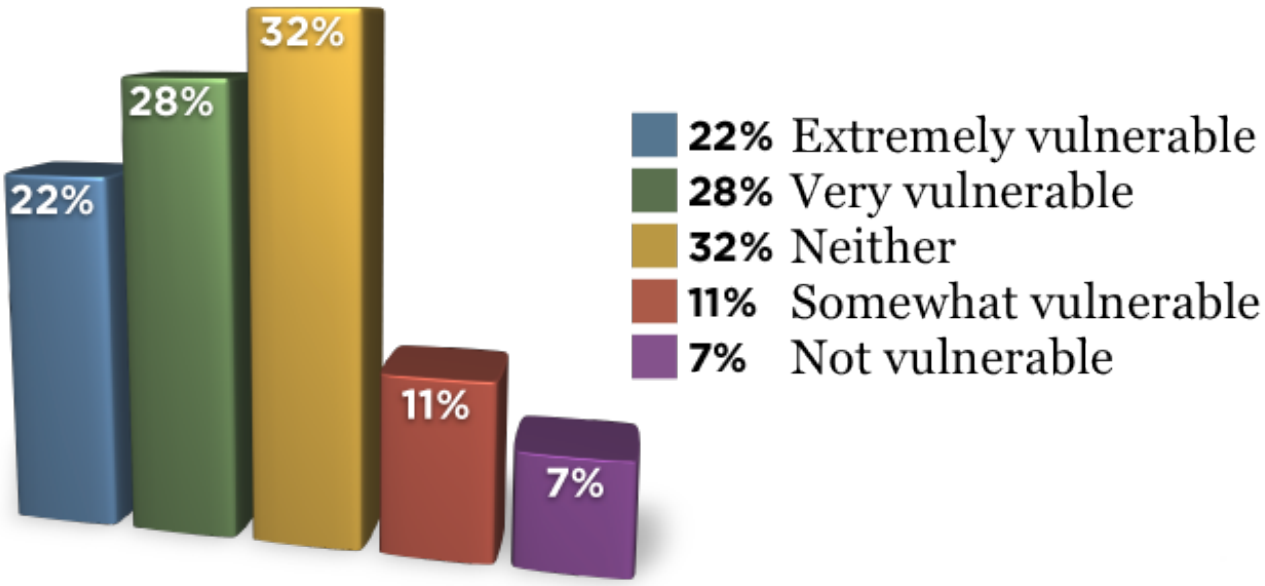
Nearly half of all respondents say it's difficult for their government organizations to find qualified IT security experts to hire. It's tougher for states, though. The fact that states and cities must balance their budget is the situation there.

The 10-percentage point differential between federal and state, county and local governments could be attributed to a greater availability of IT security professionals living in or near Washington, D.C., where many of the federal IT security operations are based. By a 44 percent-to-34-percent margin, state IT security practitioners said it was more difficult to recruit IT security experts than did their federal counterparts.



The consequence of the skills shortage is that government IT systems are more vulnerable. That's how half our respondents see it.

How vulnerable are government IT systems because of a shortage of qualified IT security professionals?



"If we don't have human capital in place, the other stuff is not going to work," says Bank of America CISO Patrick Gorman, former associate director of the Office of National Intelligence. "It is the most critical piece of cybersecurity."

The frustration for federal, state and local CISOs is that there isn't much they can do about it. The number of experts with the key skills just aren't there to hire.

If the personnel are not there, what can organizations do? Look to technology. Says Former FBI CIO Zal Azmi, a CACI senior vice president: "We are providing a technical solution that will eliminate the need for a lot of cyber professionals because we just don't have enough of them."

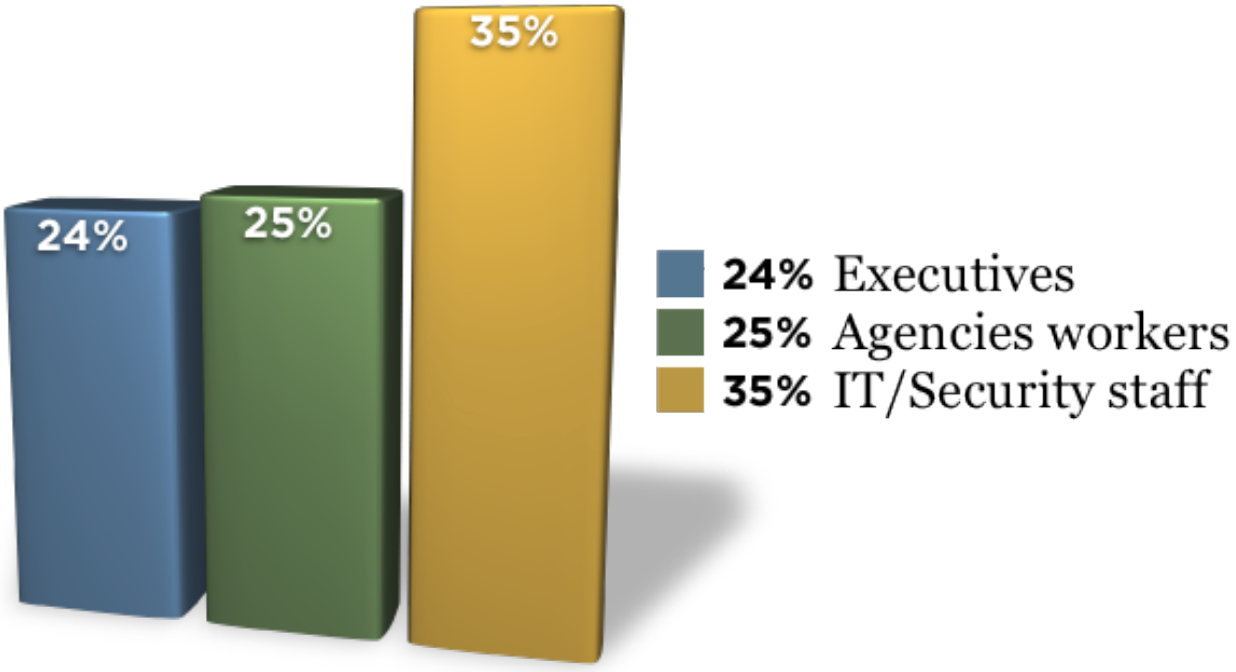
That's a theme picked up by McAfee Chief Technology Officer/Public Sector Phyllis Schneck. "Just as your body defends against thousands of colds every year and you maybe only get one, that's what these systems are designed to do: push off the enemy and push off malicious traffic," she says.

Still, we're years away from having technology replace humans in IT security.

Clearly, our respondents place more emphasis on security and awareness training for their technical staffs than for other agencies employees and managers.

How do you grade the effectiveness of your agency's security/awareness training for the following individuals?

Respondents answering good or excellent.



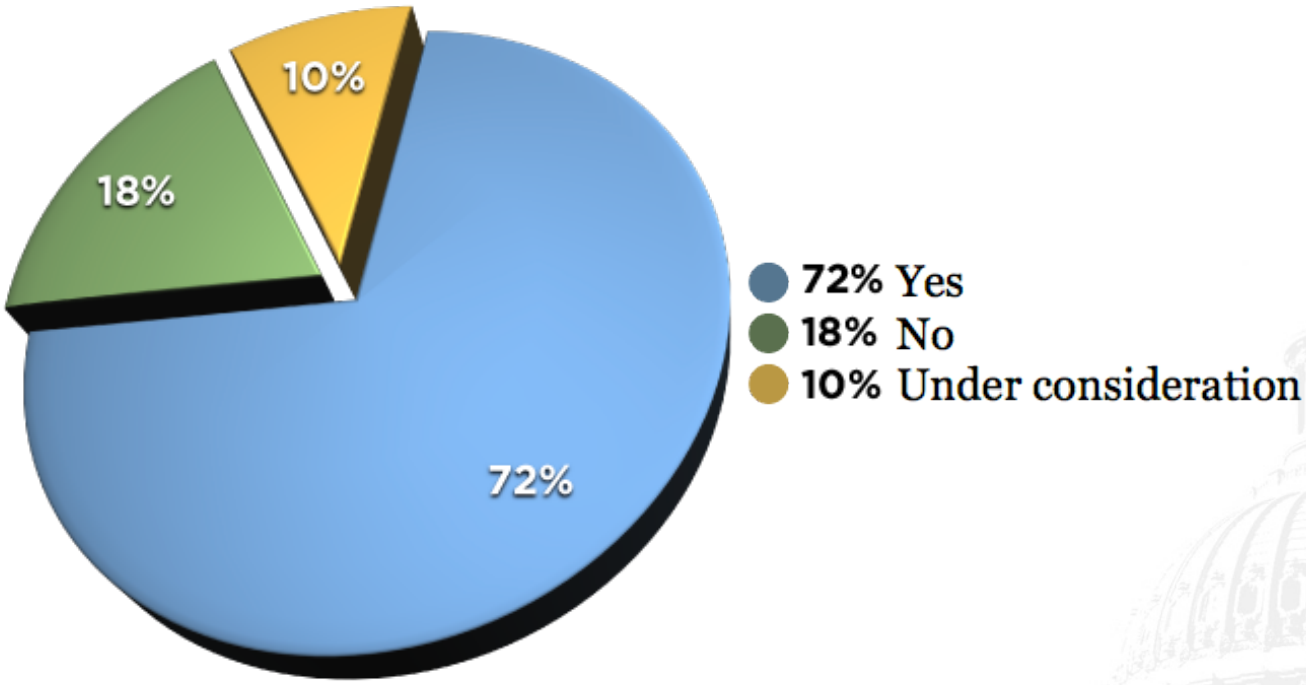
Defense Deputy CIO Rob Carey, who served as Navy CIO until last summer, says the Navy works hard to educate its senior executives and flag officers. "They don't have to be IT experts by any stretch, but every person who engages in the network to do their job becomes a cyberspace warrior because you present an opportunity for both being a defender and being a vulnerability at the same time."

5. BEYOND WASHINGTON

Laws, regulations, guidance

Federal agencies have laws such as the E-Government Act and FISMA, as well as guidance from the National Institute of Standards and Technology, to govern IT security. That's not necessarily the case in many states. More than one-quarter of our local and state respondents say their government IT organizations do not have laws or regulations that govern IT security.

Has your local and/or state government enacted laws and/or adopted regulations that govern information security?



An overwhelming number of our local and state respondents say their governments and agencies adhere to guidance published by the National Institute of Standards and Technology.

Minnesota, for instance, has a law that governs state IT security, yet its tactical plan that lays out core milestones is modeled on NIST guidance. “We think that is pretty important in our environment because we think the FISMA requirements, which are primarily directed at federal agencies, ultimately will be brought down to the state level,” says state CISO Chris Buse. “By centering our program around the NIST model, by trying to follow the NIST guidelines, we think that we will be in a better position to ultimately demonstrate compliance with the FISMA requirements if that ever comes down to the state level. And, we also like the NIST documents and the NIST framework. I think the research that is put into NIST documents and the publications is simply outstanding. It is really good literature, and NIST is well funded.”

What’s puzzling, though, is that three-quarters of our respondents believe NIST guidance should be mandatory, yet only 43 percent say they closely adhere to it.

75% believe NIST guidance should be mandatory vs. 11% that do not.

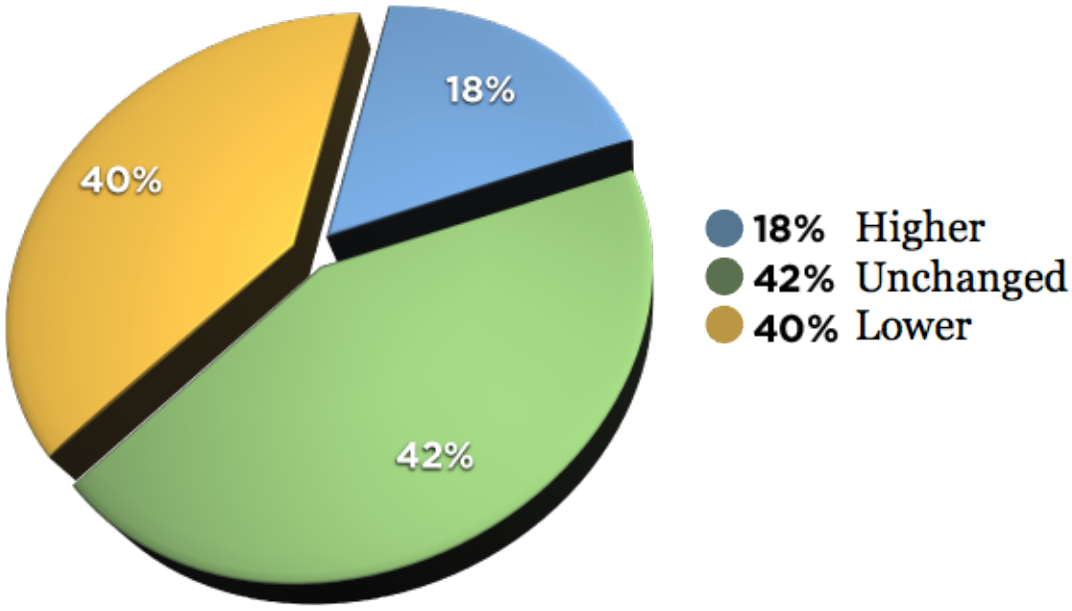
43% closely adhere to IT security standards established by NIST vs 29% that do not.

6. THE BUCK STOPS HERE

Budget challenges

Like nearly everything else, success often depends on how much money you have, or at least how you allot your financial resources. Sixty percent of our respondents say their agencies should have at least as much money to spend on IT security in the coming years as they had in the past year. If that happens, then IT security, for many, will be in much better shape than other government programs.

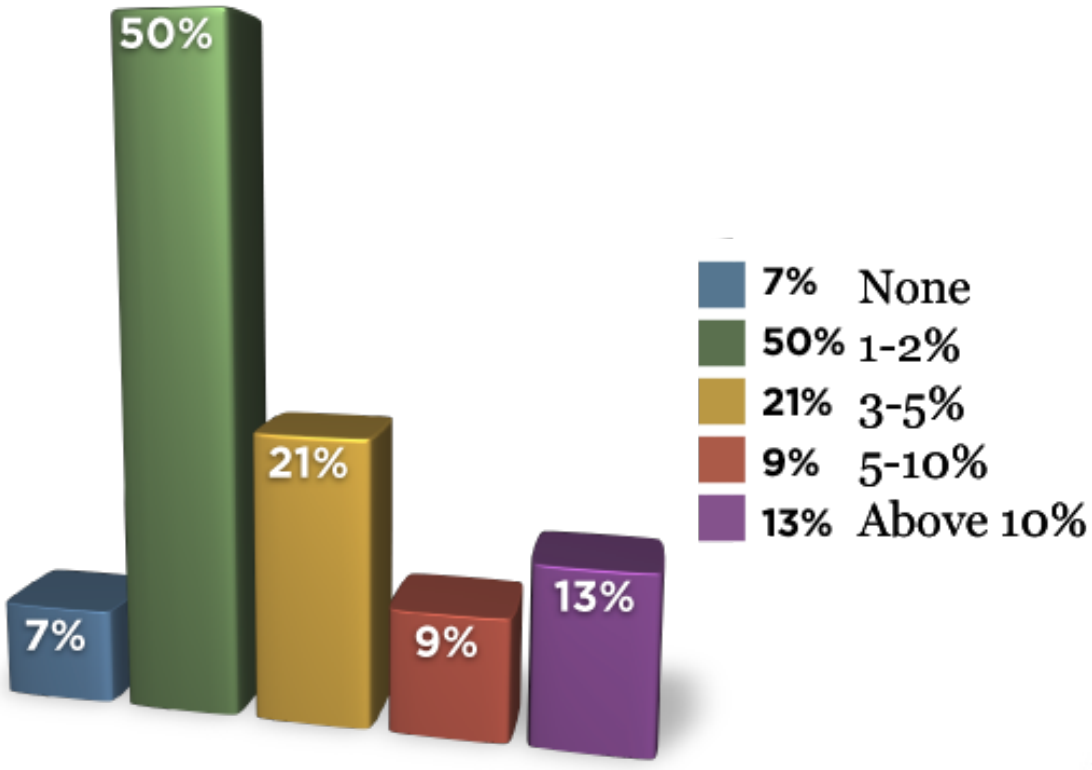
How is your agency's information security budget changing from 2011 to 2012?



More than half our respondents say their agencies' IT security budgets represent no more than 2 percent of the overall IT budget. In 2010, Gartner estimated that, on average, private-sector businesses allotted 5 percent of their IT budgets to security. Among government agencies, our respondents report, fewer than one-quarter in 2010 designated 5 percent or more of their IT spend to security.

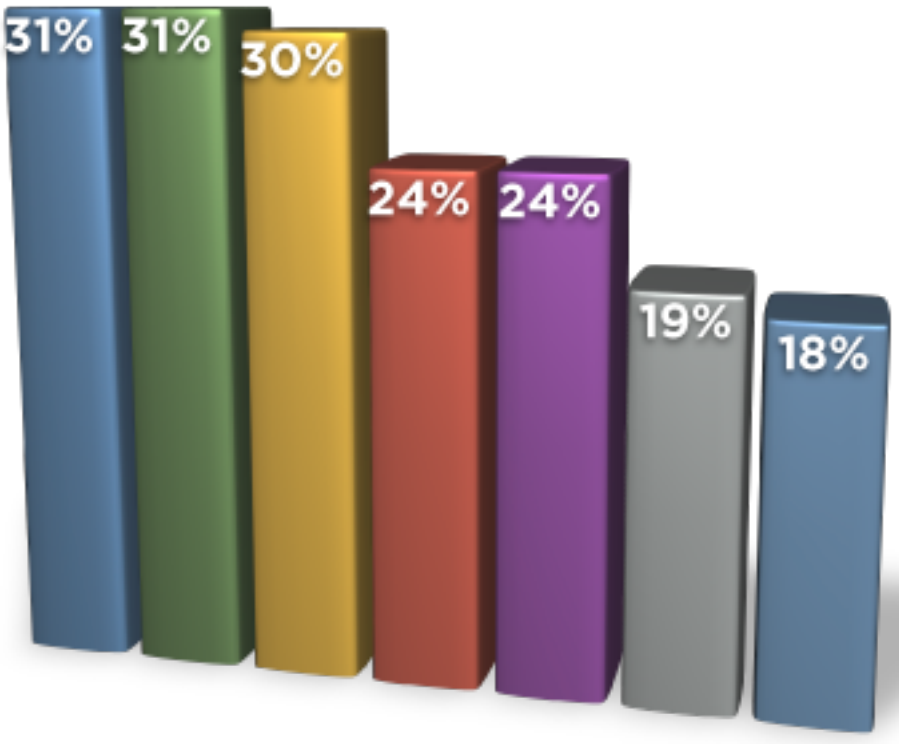
But percentages can be tricky. An analyst at the National Association of State Chief Information Security Offiers points out that one state's allotment of the overall IT budget rose to 2 percent from 1 percent. Was the state spending more on IT security? Not necessarily. Data center consolidation significantly reduced that state's IT spending, so the same amount of money allotted for security represented a bigger slice of a smaller IT pie.

What percentage of the IT budget goes to security?



New technologies are needed as new threats surface as well as new challenges – such as mobility – are addressed. And, as we've seen, there's a demand for IT skills, and even with a skills shortage, governments will be hiring.

Spending Priorities

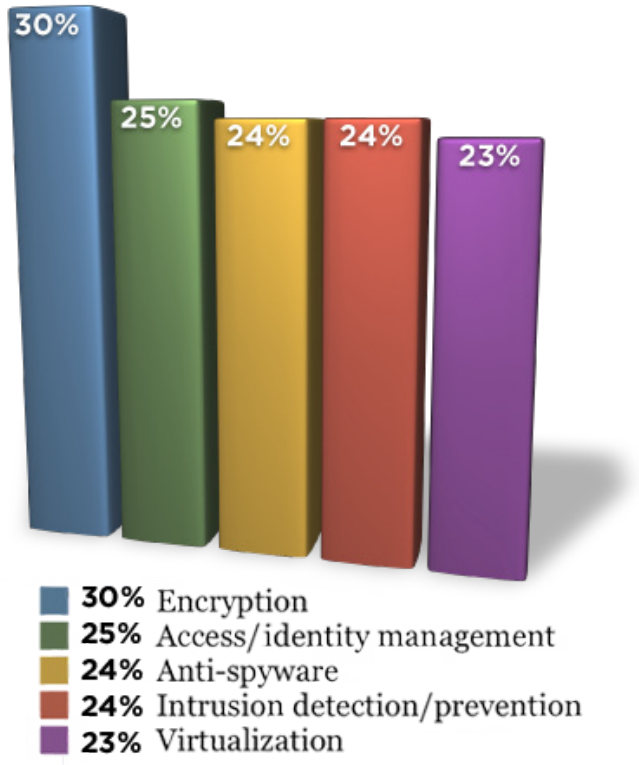


- **31%** New technologies
- **31%** Staffing
- **30%** Contractors/third-party service providers
- **24%** New services
- **24%** Risk management
- **19%** FISMA/regulatory compliance improvements
- **18%** IT security awareness

In the survey, we asked respondents to list their security priorities for the past year and the coming year. Encryption and access management remained top priorities. Done properly, most IT security experts agree they help prevent data loss and secure systems.

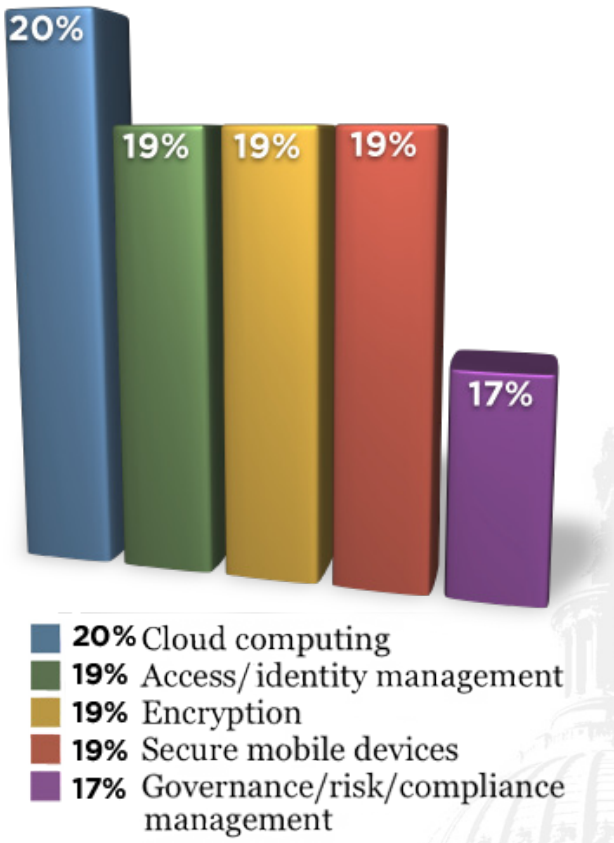
Security Priorities

Past Year



For the coming year, cloud computing and mobility join the top five. These two technologies are being lobbied by two different constituencies CISOs serve. Their bosses, whether in government or the private sector, are drawn to cloud computing because of its potential to save money, an attractive characteristic in these tough economic times. Agencies workers want to use their mobile devices on the job.

Coming Year

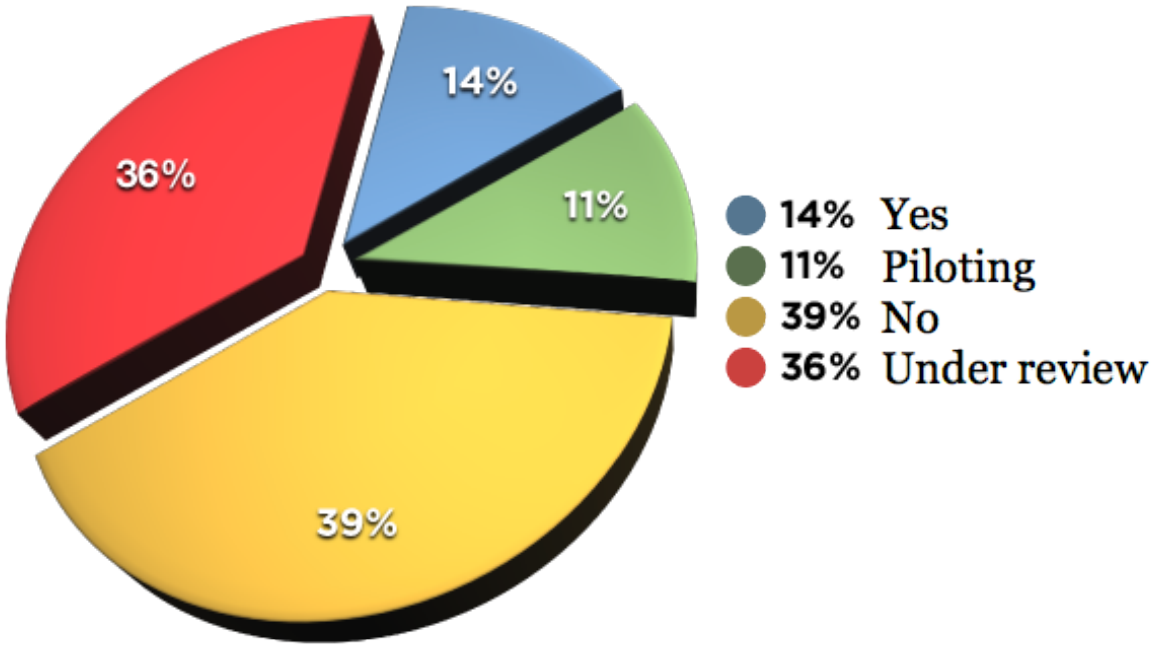


7. CLOUD COMPUTING

High Anxieties

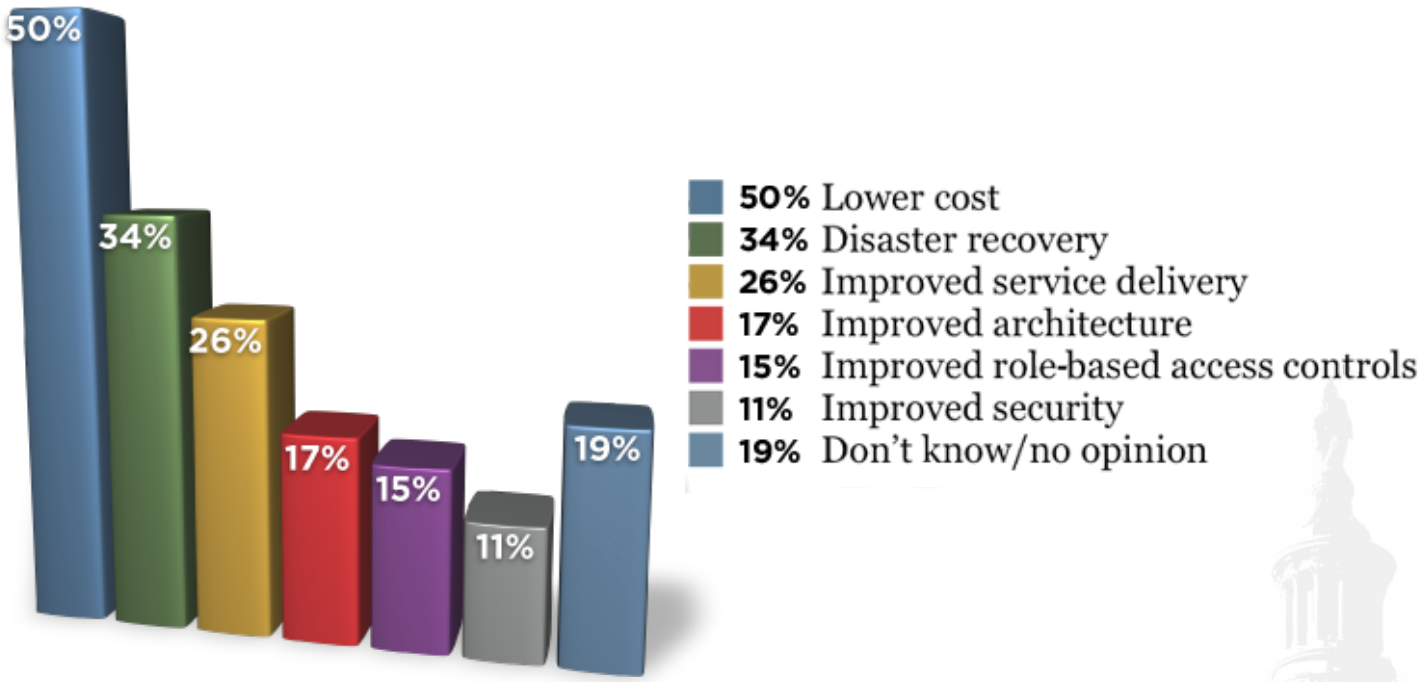
Cloud computing holds a lot of promise for government IT security practitioners, but so far most of their agencies have yet to try it. Only one-quarter have initiated or piloted a significant cloud computing initiative, while nearly 2 of 5 respondents say their agencies haven't tried cloud computing.

Has your agency implemented significant cloud computing initiatives?



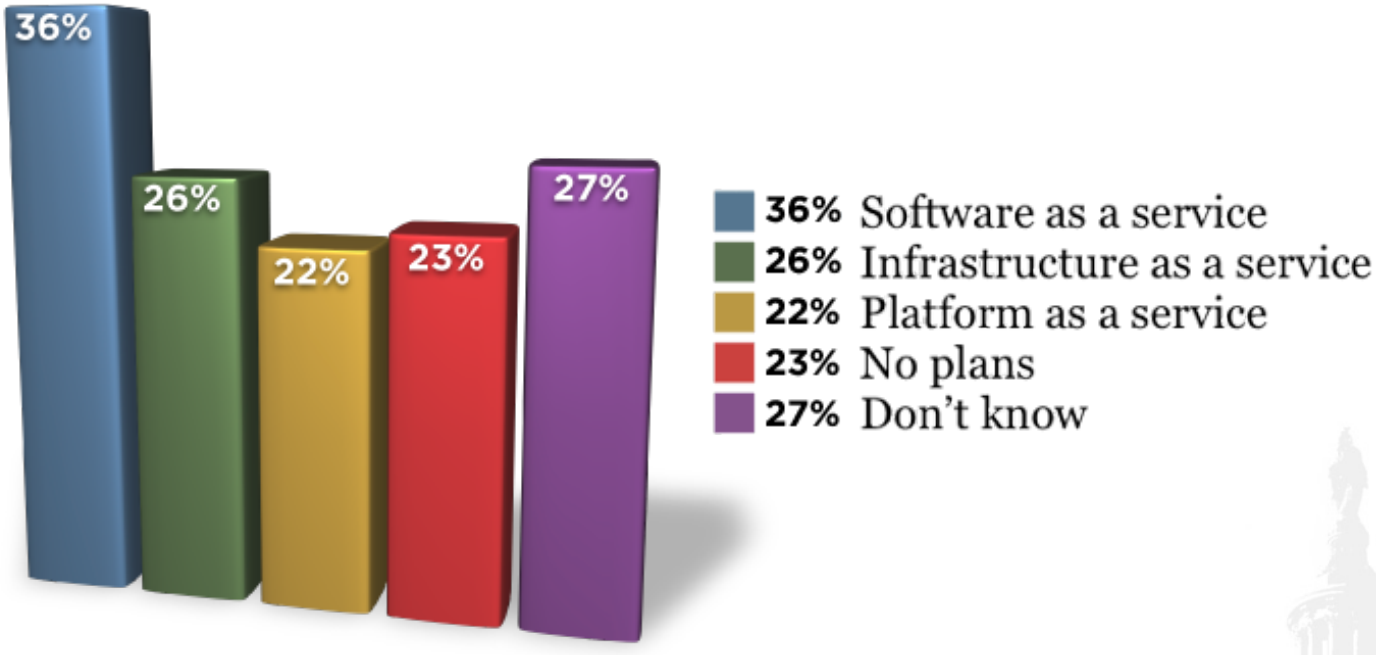
Cloud computing is hot, in part, because it's perceived as a way for agencies to reduce their IT costs. Indeed, half of the government IT security practitioners surveyed cite lower costs as a cloud computing benefit, far more than any other factor. A third of our survey takers also see the cloud as aiding in disaster recovery. Data on the cloud are likely stored on multiple severs, making recovery less problematic.

What are the biggest benefits cloud computing provides?



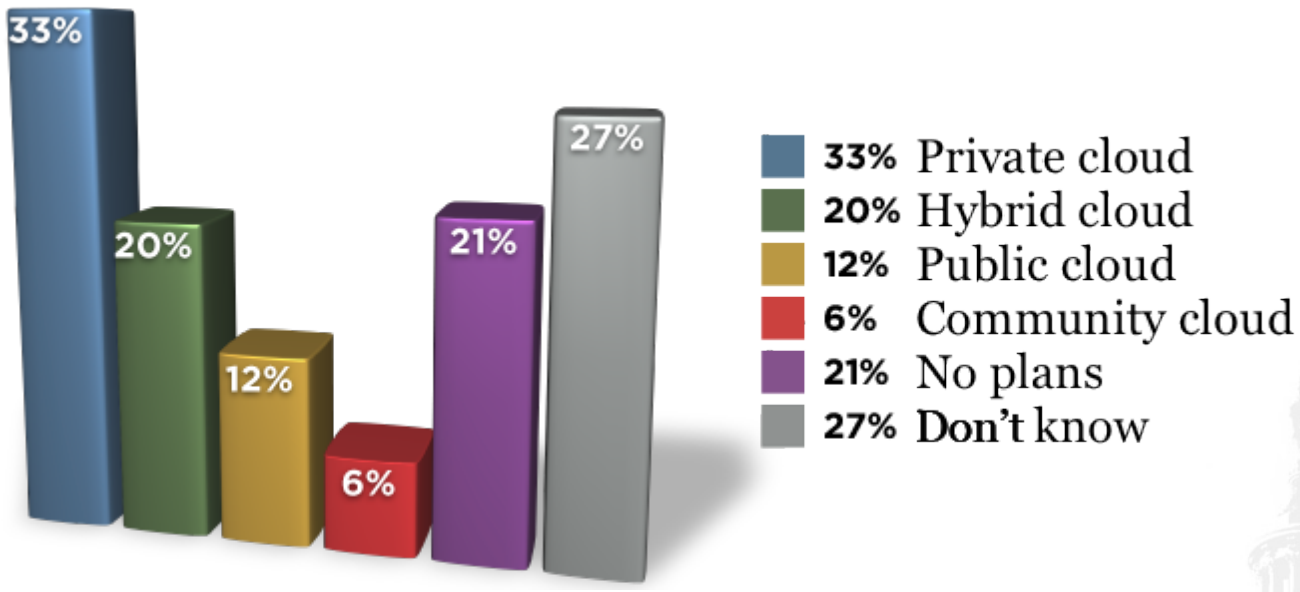
Among respondents whose agencies are considering cloud computing, more than one-third are contemplating software-as-a-service with one-quarter weighing infrastructure-as-a-service.

Based on the NIST definition of cloud computing, which service models are you considering?



The private cloud, with its servers dedicated to a single organization, is perceived to offer the greatest security, though as seen later, government IT security practitioners aren't totally sold on the security the private cloud offers.

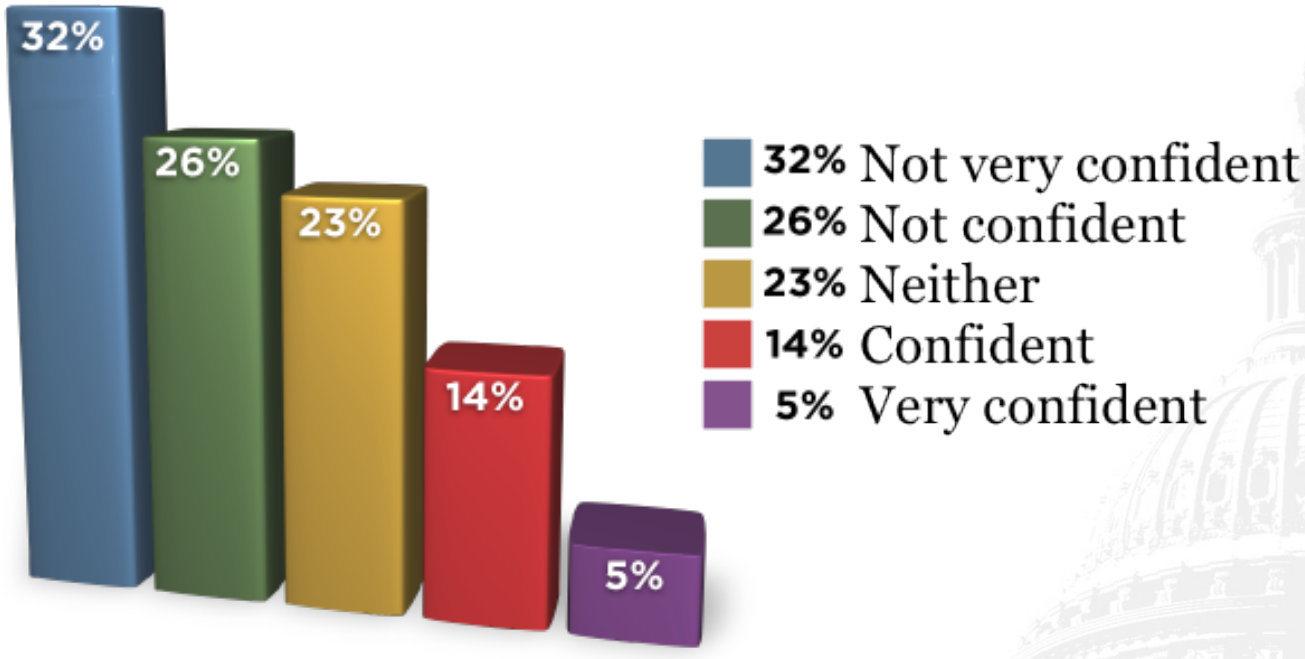
Based on the NIST definition of cloud computing, which deployment models are you considering?



Nearly 60 percent of our respondents say they lack confidence that data can be secured. "There are some very real risks associated with putting information out in the cloud, particularly if they're public clouds, to the extent that agencies will now have to rely on the security of the service providers," says Gregory Wilshusen, Government Accountability Office director of information security issues. What's key – whether for legacy systems or on the cloud – is proper controls be applied to secure data. "Until specific guidance and processes are developed to guide the agencies in planning for and establishing information security for cloud computing, they may not have effective information security controls in place for cloud computing programs," Wilshusen says.

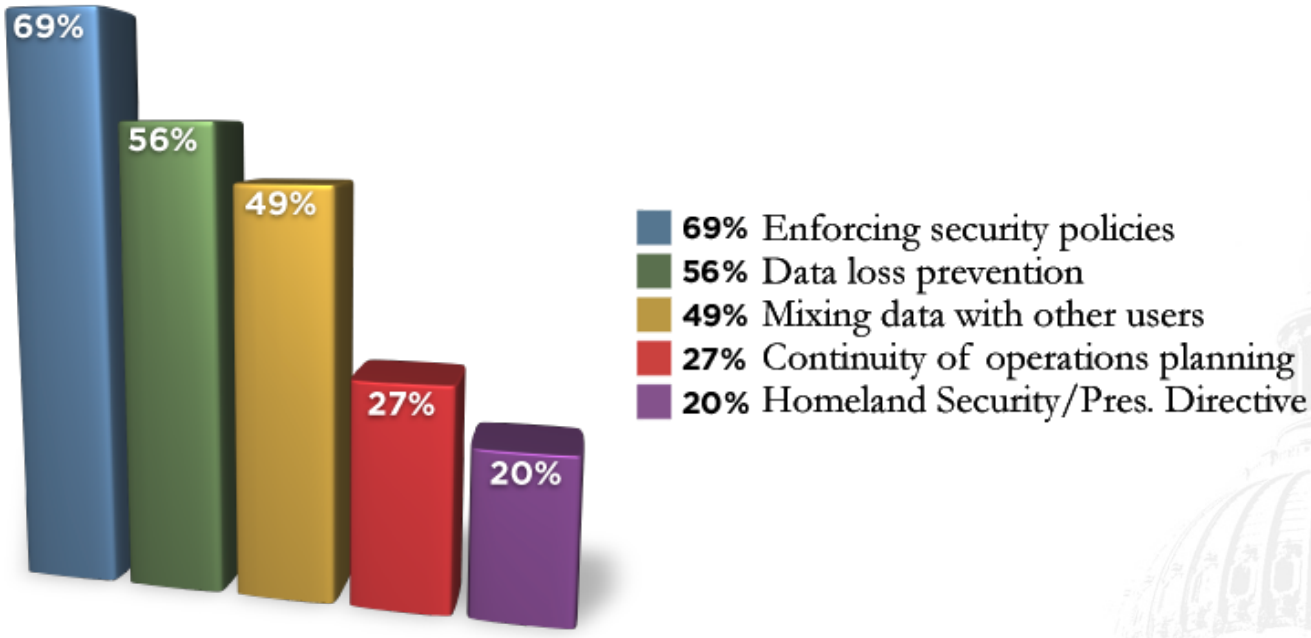
But Tomas Soderstrom, chief technology officer at NASA's Jet Propulsion Laboratory, is among those who believe the cloud can provide a secure environment: "I'll probably be hanged for this, but I really believe the cloud can be more secure than what we do today, because based on more resources, they certainly have a lot of redundancy, and redundancy comes in all shapes and sizes. And, it's fairly uniform, so if you apply a patch, you can apply it to everything at once."

How confident do you feel that sensitive data can be secured in the cloud?



Though concerns such as data loss and mixing data with other cloud users are considerable, the managerial and compliance aspect of cloud computing concerns most of our respondents. But, the biggest reservation our survey takers have with cloud computing is their ability to enforce security policy. “When you move things to cloud, you lose the concept of what applications and what data are where,” says Bret Hartman, chief technology officer of RSA, the IT security arm of storage vendor EMC. “It turns out for risk management and compliance purposes, knowing where a piece of data is on the planet must be really, really important, especially if you don’t want to violate laws or you want to deal with regulatory compliance.”

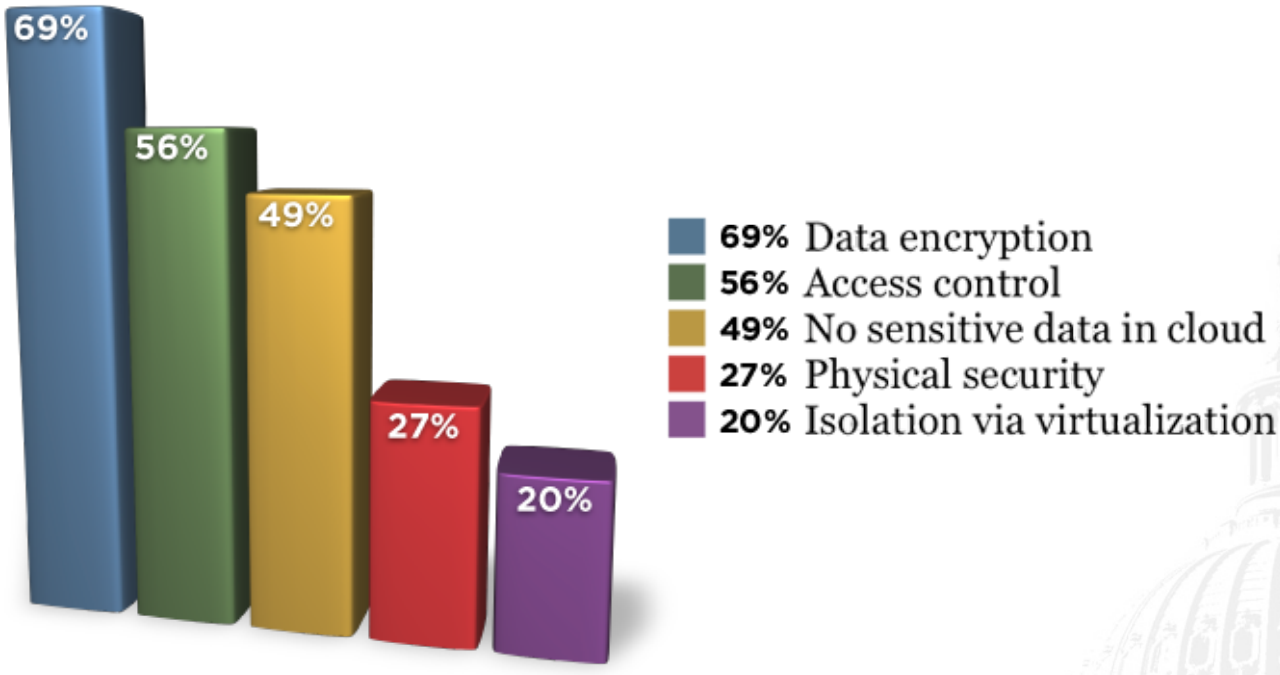
What are your biggest reservations about the cloud?



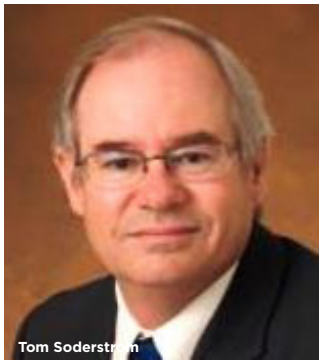
Many of the same technologies – encryption and access control – used to secure data in operations centers run by government agencies also will be employed on the cloud. "The cloud is not such a special technology necessarily that it is exempt from a security perspective, but is just another implementation of IT, and is a natural evolution of where we come from," Federal Chief Information Officer Vivek Kundra says.

Nearly half of the respondents say they'll protect sensitive information by just keeping such data off the cloud.

How will your agency secure sensitive data in the cloud?



NASA CTO Professes Faith in the Cloud



This transcript is an edited from an interview with Tomas Soderstrom, chief technology officer at NASA's Jet Propulsion Laboratory.

GOVINFOSECURITY.COM: What are some of the drawbacks JPL faced in executing its cloud initiative?

TOM SODERSTROM: When you're an early explorer, and we do a lot of that, you have some unintended consequences, often good, sometimes bad and also unexpected obstacles. We truly expected the security to be the biggest obstacle, and it really was not because we could work around it. Our security team at JPL is very much in the mode of "what do we do next?" and when. That has been a very positive experience.

I will probably be hung for this, but I really believe that the cloud can be more secure than what we do today. Because based on more resources, [cloud computing] certainly has a lot of redundancy, and redundancy comes in all shapes and sizes. And it's fairly uniform, so if you apply a patch, you can apply it to everything at once.

What we didn't expect was how difficult it would be for an institution that is used to negotiating individual contracts, to live with vendors. We had a really difficult time getting the license agreement signed with the big vendors. It turned out to be an educational process, from the engineers to the procurement organizations to the lawyers to the CIO. That took much longer than we had expected. Comparing stories with other enterprises, it is a very common challenge across industry.

What we did learn is if we were to do it again, which we will, we would have everybody sit down in the room at the same time, all the stakeholders and say, "here is what we're trying to do on the strategic side and we're just prototyping. We're not going to put any mission data in the cloud until we all agree that its ready, but in the meantime we want to prototype and move forward so let's get some of those agreements signed." I think that would have cut months off of the eventual time line.

GOVINFOSECURITY.COM: Is there any takeaway about IT security when it comes to a cloud initiative that people should have from NASA's experience?

SODERSTROM: Don't wait. Prototype now, try it now because then you will learn what IT security issues you have and then you can figure out which data you want to put in the cloud and not put in the cloud.

Make sure that the mission of the company is engaged. This is not an IT win. It's a business win, whatever the business or organization is. So we don't use IT terms but we use business terms. In our case it is exploring space. I would get all those stakeholders together for the strategy session and that would include security. Which data do we feel comfortable putting in the cloud now and how can we protect it? How can we see if somebody is accessing it inappropriately, etc.? Maybe the biggest one of all is to partner. Partner with everyone who will engage with you, and that's been really good for us, both with the mission side and other IT-type partners, and the vendors themselves. When everything is that new everybody is learning, but it has been a very good experience.

http://www.govinfosecurity.com/articles.php?art_id=3177

The Agenda

Challenges facing government IT security practitioners can seem insurmountable, but the situation is not as dire as it appears. It won't be easy, but steps can be taken to help those in the trenches to battle against vulnerabilities and threats.

1. Leadership

The White House must be more public about how it's tackling IT security challenges; its constituency of IT security practitioners demand it.

A perception many survey respondents have is that the federal government – or, for that matter, the Obama administration – isn't leading on government IT security. True or not – and the White House makes a case it's providing leadership – government IT security practitioners must not use a lack of leadership from Washington as an excuse not to do what must be accomplished. No doubt, the executive and legislative branches can do more, and should, but individual government IT security practitioners in the trenches have the smarts to accomplish much regardless of the leadership emanating from both ends of Pennsylvania Avenue.

2. Vulnerabilities

Be alert to vulnerabilities that originate from within your own organization.

"We have met the enemy and he is us."

The 1971 quote from the comic strip "Pogo" sums up one of the major challenges IT security practitioners face: the most consistent threats to IT security comes from within the organization. WikiLeaks proved that the insider is a major threat. Still, most damage from within the organization isn't malicious, so IT security practitioners must enforce policies to minimize if not purge careless practices. "Education and awareness are absolutely essential," say MS-ISAC founder Will Pelgrin.

But the Pogo quotation has another meaning: IT security practitioners must be vigilant to avoid practices that could do harm. Pelgrin cites statistics that millions of e-mail messages containing confidential data are transmitted unencrypted. "This should not be occurring at this point in time, yet it's happening way too often," he says.

3. Rules

Rules, regulations and guidance aren't perfect, but they provide sound advice that could prevent damage to government IT. Use them.

The Federal Information Security Management Act, despite its many flaws, remains an effective tool in combating IT security vulnerabilities.

Ron Ross, the NIST senior scientist and FISMA implementation project leader, says employing the checkbox approach of FISMA compliance won't guarantee safer IT systems. "What I can say, though, is complying with the provisions of FISMA, which include (NIST) standards and guidelines, will by definition, make your system more secure."

4. Personnel

Look to pool resources with other agencies and governments to address the shortage of qualified IT security personnel.

This may be the toughest nut to crack. For many organizations, the money isn't there to pay for needed IT security experts. Besides, there just aren't enough highly trained IT security experts to meet the needs of government and the private sector. This will require creativity, as Seattle Deputy CISO David Matthews says, such as collaborating with others to share the wealth of knowledge from practitioners working at other agencies and governments.

5. Beyond Washington

Exploit federal expertise, especially that provided by the National Institute of Standards and Technology.

Most local and state IT security practitioners recognize that NIST guidance provides a framework to govern sound IT systems.

Also, like personnel, money is at the heart of the IT security challenges facing local and state governments. And, like personnel, creativity will help, says Nevada CISO Christopher Ipsen:

"Government, and information security in government, need to rethink how we're approaching our service delivery to the citizens. ... How does IT change the abilities of government to deliver services better? For example, we have counties, cities and state governments, oftentimes doing the same thing. As a state, we need to look at how we can partner with our other governmental entities to communicate effectively with them, to define what roles each entity should have and to leverage the best-of-breed solutions from any of those entities for the maximum benefit of the citizens."

6. Buck Stops Here

Provide education and awareness training to the constituencies IT security organizations serve: The payoff would be worth the time and money invested in it.

IT security and the IT security organizations do not exist in a vacuum. Government cannot function efficiently unless its systems are secure. That's a point that must be driven home to non-IT agency and departmental leaders. This goes beyond cybersecurity awareness programs to a campaign to educate leaders on the synergy between IT security and the functioning of the enterprise. With cutbacks in discretionary spending, and competition heating up among programs for the limited taxpayers dollars available, IT security practitioners should not stand by idly.

7. Cloud Computing

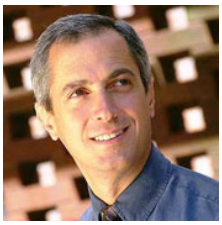
Just do it.

The cloud is here. Accept that fact, and do what must be done to make it secure.

Tom Soderstrom, the chief technology officer at NASA's Jet Propulsion Laboratory, suggests agencies should start small, and build on their initial efforts. JPL began by prototyping, learning from these early initiatives – what to avoid, how to work with vendors – and building upon them. "We're not going to put any mission data in the cloud until we all agree that its ready, but in the meantime we want to prototype and move forward so let's get some of those agreements signed. I think that would have cut months off of the eventual time line."

Resources

Learn more about the key issues driving the state of government information security in 2011 and beyond.



3 Infosec Challenges States Face

http://www.govinfosecurity.com/podcasts.php?podcastID=1018

Will Pelgrin, founder of the Multistate Information Sharing and Analysis Center, offers three IT security challenges states face: mobile devices, old infrastructure and insider threats, which he says tends to involve more carelessness than maliciousness. “Individuals may do something accidently, not intentionally; however, the consequence would be the same if it were intentional.”

IT Security Balancing Act

http://www.govinfosecurity.com/articles.php?art_id=1667

Chris Buse, chief information security officer for the state of Minnesota, relies on federal rules and guidance from the National Institute of Standards and Technology to help safeguard IT in the state. “By centering our program around the NIST model, by trying to follow the NIST guidelines, we think that we will be in a better position to ultimately demonstrate compliance with the FISMA Act requirements if that ever comes down to the state level. And, we also like the NIST documents and the NIST framework. I think the research that is put into NIST documents and the publications is simply outstanding. It is really good literature and NIST is well funded.”

Getting Out of the Infosec Budget Rut

http://www.govinfosecurity.com/articles.php?art_id=3079

Christopher Ipsen, chief information security office for the state of Nevada, says states must be more creative to address the fiscal shortfalls they face. “Government, and information security in government, need to rethink how we’re approaching our service delivery to the citizens. As a state, we need to look at how we can partner with our other governmental entities (local, county governments) to (a) communicate effectively with them, (b) to define what roles each entity should have and (c) to leverage the best-of-breed solutions from any of those entities for the maximum benefit of the citizens.”

IT Risk: Getting Top Leaders Involved

http://www.govinfosecurity.com/articles.php?art_id=3209

Ron Ross, senior computer scientist at the National Institute of Standards and Technology, sees a correlation between risk management and wisely spending limited funds. “In order for the organization to make good, credible risk-based decisions and invest dollars wisely, it really does take the involvement of everyone up the chain of command, especially with today’s advanced persistent threats that have the ability to really bring down an entire organization’s operations with some well-placed malware. The realization of this by senior leaders now has energized them and gotten them involved in the process of managing risk.”

Wipe Out: Data Vanish on Smart Phones

http://www.govinfosecurity.com/podcasts.php?podcastID=878

Elayne Starkey, chief security officer of the state of Delaware, is implementing new policies to address emerging technologies such as smart phones. “If that smart phone is indeed connected and synced to the state network, if it’s not password protected and gets lost or stolen and gets into the hands of someone, they literally have unfettered access to state data, which is the kind of stuff that causes me to lose sleep at night.”

About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.

This information is used by ISMG's subscribers in a variety of ways—researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

BANK INFO SECURITY®
.com | .co.uk | .eu | .in | .asia

CU Just for Credit Unions INFO SECURITY®

GOV INFO SECURITY®

HEALTHCARE INFO SECURITY®

Contact

Contact a sales representative for information on sponsorship opportunities:

ISMG Sales Team
(800) **944-0401**
sales@ismgcorp.com

ISMG INFORMATION SECURITY MEDIA GROUP
Information Security Media Group
4 Independence Way | Princeton, NJ 08540