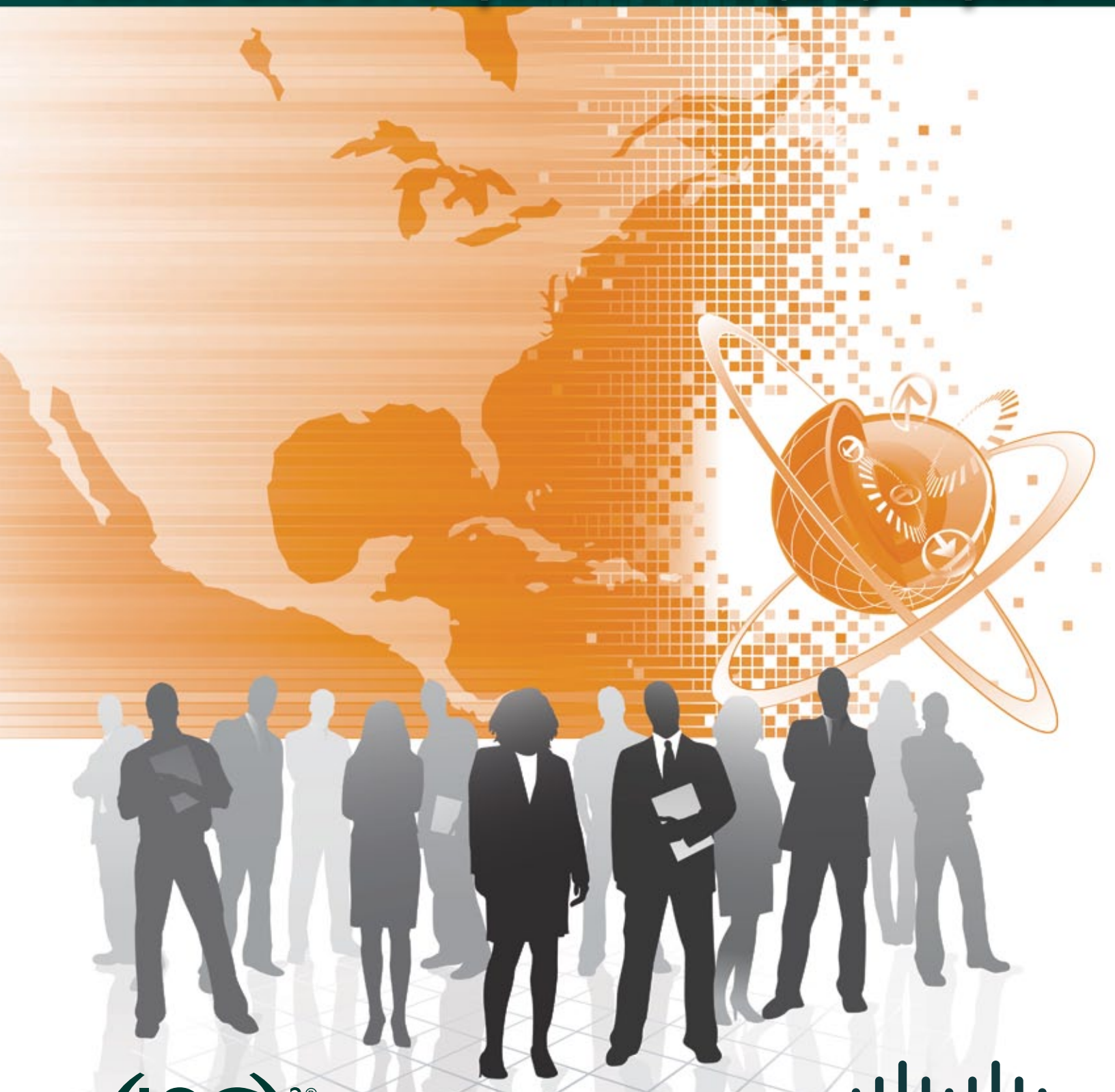
The 2010 State of Cybersecurity from the Federal CISO's Perspective — An (ISC)² Report



(ISC)²®

GARCIA STRATEGIES, LLC

CISCO™

The 2010 State of Cybersecurity from the Federal CISO's Perspective – An (ISC)²® Report

EXECUTIVE SUMMARY

In May 2009, President Barack Obama, in the first-ever presidential speech dedicated entirely to cybersecurity, proclaimed that the nation's digital infrastructure should be considered a "strategic national asset." Those weighty words affirmed what specialists in the Internet security field have long recognized and built careers around. But the fact that those words were uttered by the President of the United States in a nationally televised address ushered in a new era of national awareness – and perhaps government activism — about the ongoing and pervasive vulnerabilities and threats that government, business, academic and personal users face in our online world every day.

The federal government's cadre of chief information security officers (CISOs) – no strangers to the ebb and flow of political tides that affect their mission – currently view this emergent national awareness with an ambivalent mix of hope and wonder. They see greater awareness but still insufficient resources to protect our networks; better tools and training but increasing threats and attacks on our infrastructures; and more security initiatives within and across the agencies, but organizational structures not yet equipped to get ahead of our adversaries and our own operational flaws.

> ***"There is more attention to and awareness of the magnitude of the problem; attention leads to resources and action."***

We are seeing measurable progress; indeed, trend lines are favorable, as suggested in the survey findings of the second annual "State of Cybersecurity from the Federal CISO's Perspective – An (ISC)² Report". A joint effort between (ISC)², Cisco and Garcia Strategies, this report is intended as a tool to track developments in our ability to assess and protect the security of those strategic national assets entrusted to our public servants. On the front lines of this ongoing battle are the nation's federal CISOs, and we present these findings to reflect their views for the benefit of their peers, policymakers and the public.

KEY SURVEY FINDINGS

If there is one theme that characterizes the results of this year's survey, we turn to the well-known aphorism by Socrates - "know thyself" - which suggests that in order for us to truly understand the world, we must first understand ourselves. In cybersecurity, this means that awareness of our challenges and opportunities is the first step toward being able to do something about it - to change the status quo.

This survey organizes CISOs' perspectives into four categories: security posture, workforce effectiveness, resources and tools and policy and emerging initiatives.

First, what federal CISOs see in the nation's security posture in 2010 is not significantly different from that reported in 2009. Half believe we're better off than last year, while the other half see that we're worse off or no better in our ability to protect our networks.

Half of the CISOs in 2010, fewer than in 2009, report that they feel they have a significant ability to impact the security posture of their agency. Yet they continue to see vulnerabilities and incidents. They identify software, poorly trained users and/or insider threats as continuing problems that they rate as even more severe than external threats such as nation states, Website vulnerabilities and spear phishing.

Looking at security through the lens of workforce effectiveness, CISOs continue to show overall satisfaction with their jobs, yet their job requirements have evolved beyond the technical, with half of the respondents being asked to deliver more managerial, policy and political responsibilities in their roles. So they rely heavily on well-trained staff with highly valued professional certifications and are turning to Scholarship for Service students and contractor conversions for many of their hiring needs.

Outside of their own control, CISOs must rely on a variety of internal and external tools and resources to get their jobs done – whether it's technology, Congressional funding, bureaucratic operations or cross-agency protective initiatives. Among these areas, CISOs' satisfaction is mixed. They continue to deploy intrusion detection and intrusion prevention technologies and, compared to 2009, have an improved view of the cross-agency "Einstein" IDS/IPS program managed by the Department of Homeland Security's U.S.-CERT. And while many are taking advantage of the Information Systems Security Line of Business (ISS-LOB), only 10 percent are satisfied with their own agency HR and procurement operations to facilitate their mission execution, and even less have any confidence in the ability of Congress to understand their mission and provide adequate resources.

These results square with CISOs' perspectives about policy and emerging initiatives, in which more than half of the CISOs would advise the new White House Cybersecurity Coordinator, Professor Howard A. Schmidt, CISSP, CSSLP, Fellow of (ISC)², to place increased agency funding and enforcement of security mandates at the top of his priority list. This suggests the need for a strong and proactive educational outreach strategy with Congress. As for emerging initiatives, cloud computing

may be a part of a broad government initiative, but almost ¾ of respondents admit they're not using the cloud because of the range of security concerns they need to understand before deploying their data and applications in the cloud. Those same concerns, however, have not stopped adoption of Web 2.0 social networking applications to enhance the ubiquity and usability of government services. Seventy-eight percent of CISOs who use Web 2.0 services say they have enforced security policies in place, suggesting considerable alignment of new services with security policies.

RECOMMENDATIONS

These survey results suggest that, from a broad perspective, the issue of cybersecurity has matured in the minds of the American public and the federal stewards of our information infrastructure, such that we are coming to "know thyself," with the awareness of our challenges as a starting point for improvement. From the results of this survey and the trends that emerged from last year's report and other sources, we can advance a few key recommendations that will build on the progress CISOs have made over the last several years.

First, if our digital infrastructure is indeed a strategic national asset, then it is incumbent upon Congress to give CISOs sufficient funding to protect government networks. Digital pennies can save us analog dollars. Then, CISOs must use the appropriate tools for measuring risk and security and be held accountable for meeting their agency's mission requirements. They cannot be held accountable for poorly defined and unfunded mandates.

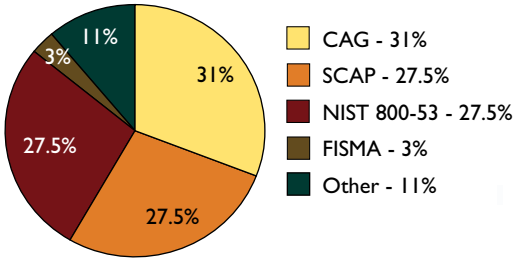
Second, CISOs need to be given the flexibility and creativity it takes to be competitive with the private sector in recruiting qualified and motivated staff. While CISOs clearly see certifications as an important measure of qualification, other factors like the ability to offer strong in-house training and hands-on experience must factor into hiring decisions. Third, CISOs and the government officials who support them need to do a better job of educating the Congress about the business case for how better security will improve government services, reduce costs for software maintenance and incident response and protect critical, sensitive data. If they succeed, the additional attention they receive from lawmakers may raise their visibility within their organizations and result in better operational support from functions such as human resources and procurement.

Finally, consistent with one of the recommendations we made in 2009, there needs to be a continuing and stronger emphasis on protection and management of data, distinct from focusing too heavily on threats and attacks. As practitioners, CISOs report that they can maintain strong security in a way that protects privacy without infringing upon it, that we can have an open government policy of transparency while keeping security policies in place to protect sensitive information and that outsourcing services to the cloud does not mean outsourcing truly critical data. Decisions on security policy and implementation need to be considered through this prism of data management imperatives.

SURVEY DETAILS

DESPITE INCREASING ATTENTION TO TOOLS AND METRICS, THREATS STILL LOOM

Most Useful Metric Tools



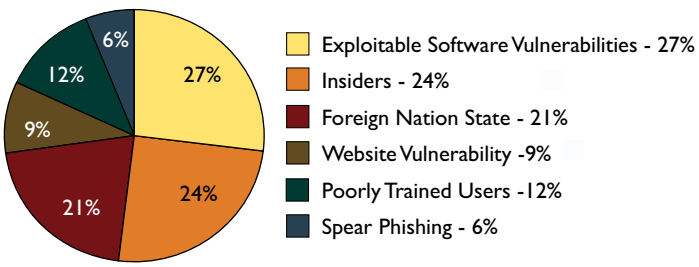
Federal CISOs are seeing greater awareness of their missions but not enough improvement in the security posture of the federal domain. Almost 50 percent of respondents say they have significant ability to impact the security of their organization, but the same number say the security problem is either worse or the same as it was one year ago. But CISOs believe we are potentially poised to see much better gains in our security posture. As one CISO observed, "There is more attention to and awareness of the magnitude of the problem; attention leads to resources and action."

To build on their ability to improve their agency's security posture, CISOs point to several useful tools in their arsenal. The Consensus Audit Guidelines (CAG), Security Content Automation Protocol (SCAP) and the NIST 800-53 guidelines all receive high marks for being most useful. In addition, they almost universally (94 percent) believe that the government should include specific, mandatory security requirements in every major IT procurement. In this environment, 85 percent of these practitioners reported that continuous monitoring is the most useful metric for measuring the level of security. However, the ongoing evolution of threats makes measurement of our progress difficult. As one CISO observed, "Metrics are unclear because of our inability to link compliance with reduction of impact."

> ***"Metrics are unclear because of our inability to link compliance with reduction of impact."***

Asked to rank the number one threat in terms of severity, 27 percent identified exploitable software vulnerabilities, followed by 24 percent for insiders. Interestingly, however, 43 percent of CISOs blame insecure software for less than a quarter of detected security breaches. Only one in 15 respondents was able to claim that 75-100 percent of those breaches were due to insecure software. This suggests a possible anomaly based on the complexity of managing multi-layered network security – that widely held assumptions about software vulnerabilities aren't easily linked to attributable security incidents.

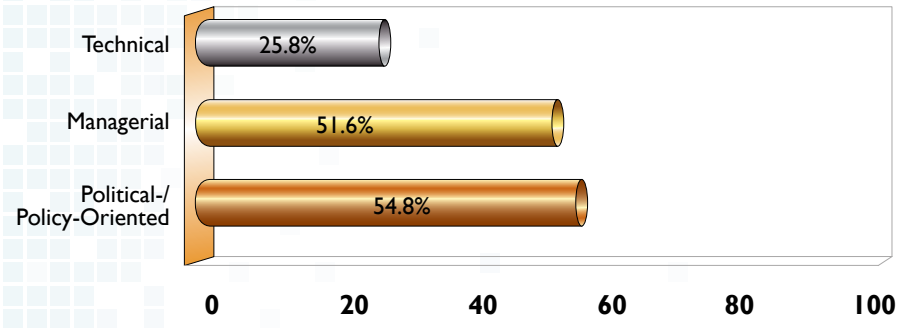
Most Severe Threats



THE NEED FOR FLEXIBILITY IN MANAGING OUR MOST IMPORTANT ASSET

Many organizations today, whether government or private sector, have adopted the mantra, "people are our most important asset." It is no different among federal CISOs, whether they're concerned with their own job satisfaction or the quality of the people they need to manage their infrastructure. When asked about their level of job satisfaction, 63 percent of the CISOs confirmed they were either satisfied or very satisfied with their jobs, which is attributable in part to their strong belief that they have a significant impact on the security of their organizations. A motivated workforce is often a successful one.

CISOs See Their Duties Becoming More:

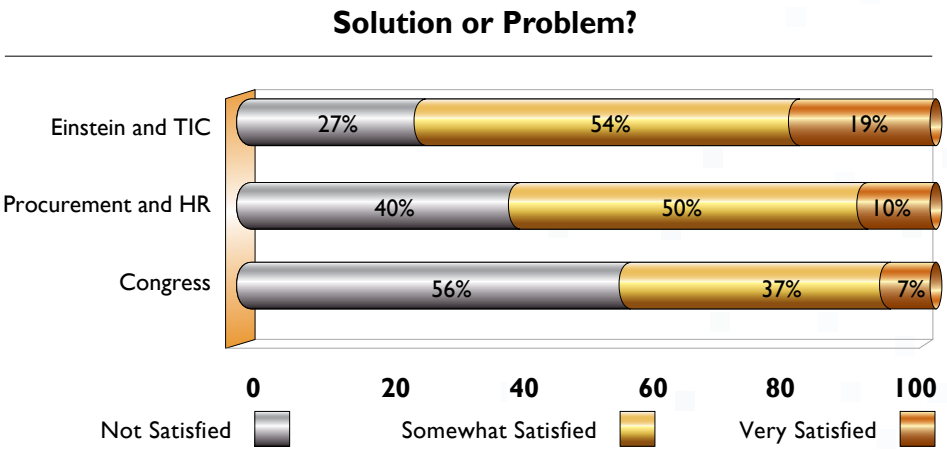


Still, half of the CISOs see their jobs taking on more managerial, policy and political elements on top of their existing technical duties, and they know they can't do it all alone. They, accordingly, lean significantly on a well-trained and experienced staff. Sixty-eight percent of respondents say they have adequate training resources, but equally important to them are professional certifications, which more than 70 percent ranked as high or very high in importance when hiring or promoting employees. A similar number believe that security certifications should be mandatory for security professionals across the government. This tracks closely with 2009 data, which showed 75 percent of CISOs advocating mandatory certifications across the government. The most prevalent certification held among the CISOs responding is the CISSP® (62 percent), followed by CISM (25 percent) and NSA-IAM (13 percent).

Looking ahead to staff augmentation, CISOs estimate that contractor conversions and the private sector will each make up 30 percent of their hires, with a similar number from internal sources. In terms of tapping the talent of our next generation's workforce in the Scholarship for Service (SFS) program, 44 percent of the CISOs expect to hire one to five SFS students, 12 percent will hire more than six, while another 44 percent will not take advantage of this resource.

OUTSIDE RESOURCES: PART OF THE SOLUTION OR PART OF THE PROBLEM?

This is likely the question many CISOs regularly ask about the outside influences that can help or hurt execution of their mission – whether it's their internal HR and procurement department, security lines of business which allow agencies to outsource security expertise to other agencies, the DHS Einstein and TIC program for monitoring network traffic in and out of the .gov domain or mission authorization and appropriations from Congress.

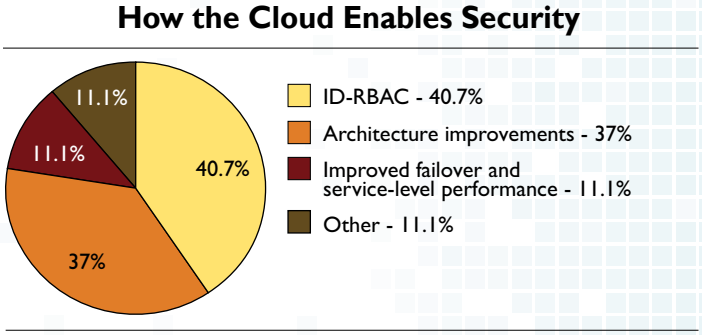


Looking at the numbers, CISOs are showing more confidence in the Einstein program, which was characterized in last year's report as frustrating and too externally focused. In 2010, almost ¾ of the respondents report they are satisfied to somewhat satisfied with this cross-agency intrusion detection/prevention program, which may be due in part by the fact that the same number are complementing the effort with the use of IDS and IPS on their networks, as well as automated ID management and many other sophisticated security tools.

Relying on others to support their efforts, CISOs are outsourcing select security expertise to other agencies through the ISS-LOB, with 62 percent participating in the program and 10 percent serving as lines of business for other agencies.† That level of CISO confidence, however, is not so strong among their own agency human resources and procurement functions, which they depend on for timely and high-quality hiring and technology acquisitions, with 40 percent expressing no satisfaction with those performance functions. Similarly, when it comes time to "show me the money," 57 percent of CISOs are not confident that Congress understands their mission well enough to provide sufficient funding – either for hiring or technology. There may be some promising signs, however, in pending legislation that recognizes these recruitment challenges by requiring an annual report on hiring effectiveness.

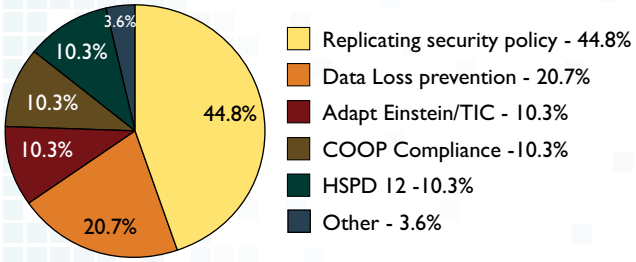
HEY, YOU, GET ON TO MY CLOUD

The continual march of technology brings a stampede of vulnerabilities. CISOs must constantly assess how new technologies and capabilities can enable or enhance their agency missions without introducing new, unacceptable risks. Looking at some of these emerging technologies facing CISOs, cloud computing and Web 2.0 services



† *The ISS-LOB designates agencies as "shared service centers" for lines of business in FISMA reporting; certification and accreditation; IT security awareness training; and Trusted Internet Connections Access Providers (TICAPs).*

Biggest Security Concerns with the Cloud



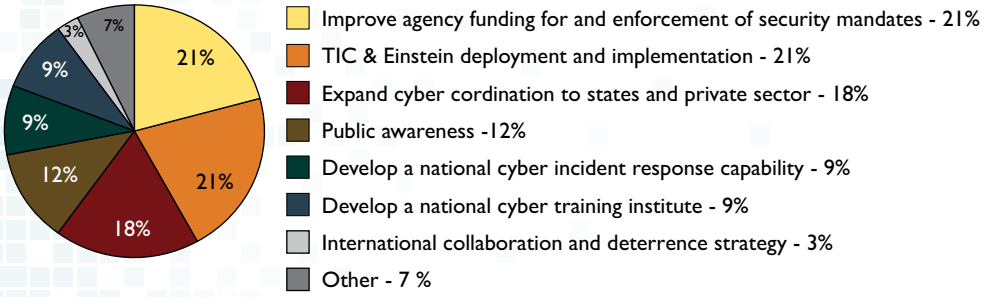
show business promise but security peril. 72 percent of CISOs in the survey report that they do not yet use cloud computing because of the high levels of uncertainty around being able to replicate IT security policy in the cloud (45 percent) and data loss prevention (21 percent).

Those who see promise in cloud computing, conversely, also see potential for improving security, particularly through ID-based network solutions that employ role-based access controls, or RBAC (41 percent), as well as design improvements that enable the cloud with a strategic architecture (37 percent). All CISOs reporting that they do use cloud computing services for mission delivery say they have enforced security policies in place, which suggests there could be some useful templates in place as reference for other CISOs wanting to explore their options.

While experience continues to show that we need to be circumspect in the use of Web 2.0, social networking and P2P technologies, many CISOs see less complication in the security issues surrounding them, as 62 percent are using those services as part of their mission delivery system. Almost 80 percent of those using those services claim to have enforced security policies in place. This suggests a general recognition of the power of those tools in implementing the Obama Administration's Open Government initiative as long as there is control over distributed usage among employees. The Marine Corps, for example, announced on March 29, 2010, that it is lifting the ban on the use of social networking to allow those out in the field to maintain communications with home.

In balancing the sometimes competing demands between information transparency and protection and information security and privacy, responding CISOs do not feel as conflicted as the policy debates would suggest. Three-quarters of CISOs report that they have data security policies in place to balance the needs of transparency and information protection. About the same number do not believe that privacy protections undermine the needs of security or that security monitoring technologies necessarily

White House Cybersecurity Coordinator for a Day Recommended Highest Priorities



encroach on privacy rights. This perhaps goes to the heart of reconciling what we are trying to protect versus what we are trying to stop.

Finally, CISOs were asked to be the White House Cybersecurity Coordinator for a day and make recommendations for what should be the highest priorities for that office. Not surprisingly, improved agency funding ranks highest, followed by effective TIC/Einstein deployment to protect agency networks. Almost as many – 18 percent – acknowledge the importance of expanding cybersecurity coordination to states and the private sector.

CONCLUSION

In our vastly interconnected digital world, national understanding of "cybersecurity" as an issue and a discipline has evolved from ignorance to discovery, to what is now sober yet somewhat disorganized attention. CISOs, policymakers, corporate America and the general public are each at different stages of "knowing thyself" – knowing their risks and responsibilities in the digital infrastructure. Our challenge is to coalesce around a shared understanding and a unity of purpose toward a security regimen that in the end becomes habit.

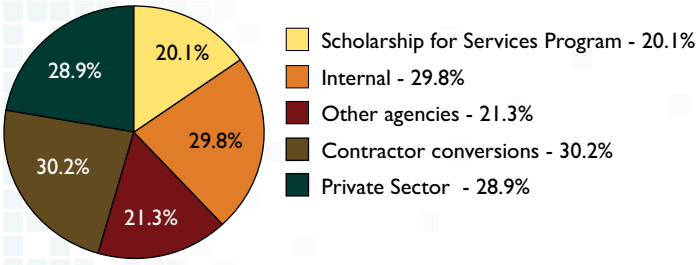
The good news from the survey is that CISOs know what their challenges are, and most have a firm understanding of what needs to be done to overcome them. They know they need to build a workforce with a diversity of talents, using a variety of technological tools. They're also aware that their biggest threat continues to come from internal vulnerabilities. Moreover, knowing that their success depends on a network of support mechanisms within and outside their agencies, such as security lines of business or US-CERT's Einstein program, many federal CISOs express a general sense of cautious optimism.

But they know we're not there yet. Less auspicious in the findings is the fact that we've not yet organized that awareness into an effective culture of cybersecurity across the government's political and operational communities. CISOs understand they're working in an environment where all of the moving parts, such as agency business operations, Congressional buy-in and funding, evolving technologies and standards of practice, need to be moving together in the same direction. Yet they point out a continuing lack of unified momentum. Observed from above, these moving parts might be seen as taking two steps forward, one step back and one to the side before righting themselves forward again.

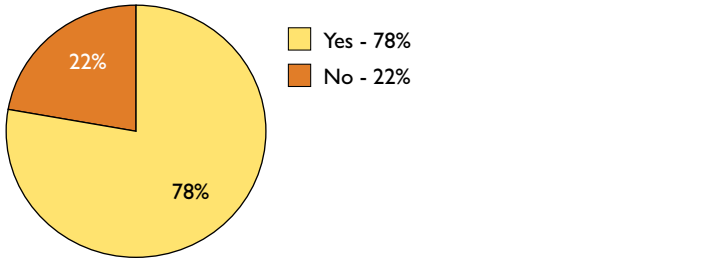
In the short term, CISOs will look to the power behind the White House Cybersecurity Coordinator's office to drive the changes that will ultimately show improvement. Their hope is this: first, make the case to the Congress; second, secure the funding stream; and third, hold CISOs accountable to clear and measurable standards of security improvement. It will be an honest deal and good governance and would show the business community and the general public that the government can lead by example.

BACKGROUND DATA

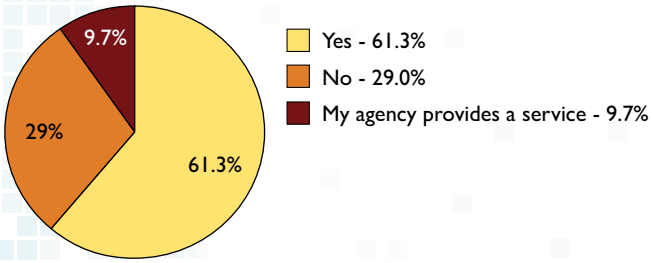
In your staffing plans, what percentage of your hires will come from:



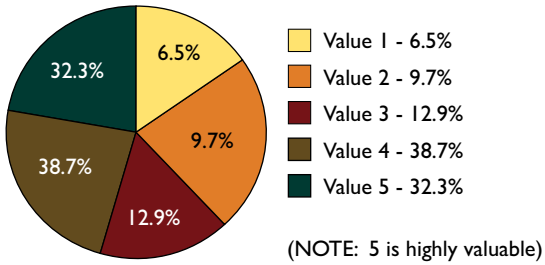
If your agency is using Web 2.0/social networking services, do you have enforced security policies in place?



Is your agency taking advantage of the Security Lines of Business provided by other agencies?

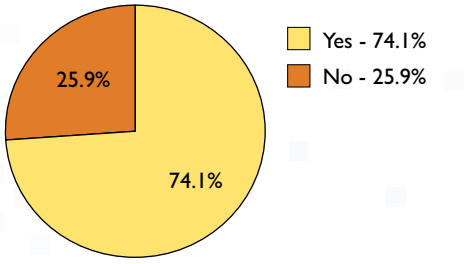


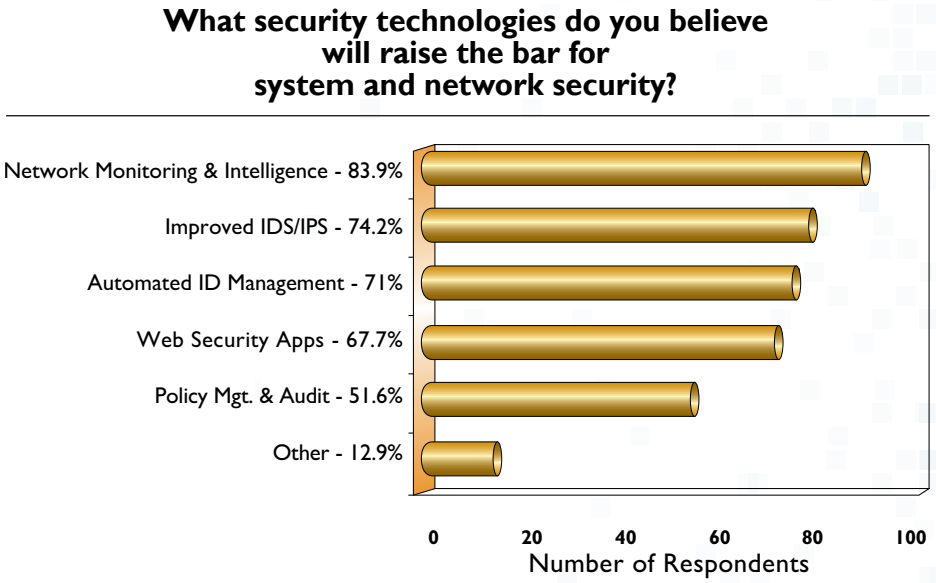
What value do you place on professional certifications when hiring or promoting employees?



(NOTE: 5 is highly valuable)

For the President's Open Government Directive, does your agency have data security policies in place to reconcile the needs for information transparency and information protection?





METHODOLOGIES AND ACKNOWLEDGEMENTS

This second annual federal CISO survey was made available to a cross-section of 85 federal agency and bureau-level chief information security officers (CISOs) and information security officers (ISOs) during the 1st quarter of 2010. Thirty-six of those reached participated by using an online survey tool that gathered anonymous responses to 31 questions. The survey request went out to personnel from defense, civilian, law enforcement and intelligence agencies. We greatly appreciate the cooperation of these front-line CISOs in advancing the state of knowledge about our federal information and information systems security.

Greg Garcia, President, Garcia Strategies, LLC

W. Hord Tipton, CISSP-ISSEP, CAP, CISA, Executive Director of (ISC)^2

SPONSORS

(ISC)²® is the not-for-profit global leader in educating and certifying information security professionals throughout their careers. With over 68,000 certified members in more than 135 countries, (ISC)² issues the Certified Information Systems Security Professional (CISSP®) and related concentrations, Certified Secure Software Lifecycle Professional (CSSLP®), Certification and Accreditation Professional (CAP®), and Systems Security Certified Practitioner (SSCP®) credentials to those meeting necessary competency requirements. Learn more at www.isc2.org.

Cisco is the worldwide leader in networking and IT infrastructure that transforms how governments connect, communicate and collaborate with secure voice, video and data to constituents, end-users and other governments.

Cisco's Cybersecurity solutions enable government employees to access information securely from any client across any network. Cisco Collaboration, Virtualization, Video and Secure Borderless Network technologies enable governments to meet their mission. Learn more at www.cisco.com/go/federal.

GARCIA STRATEGIES, LLC

Garcia Strategies, LLC provides strategic business development and government affairs advisory services for companies contributing to the national cybersecurity and emergency interoperable communications missions. The firm's founder, Gregory T. Garcia, was the nation's first Presidentially appointed Assistant Secretary for Cybersecurity and Communications with the U.S. Department of Homeland Security from 2006-2008.

(ISC)²®

SECURITY TRANSCENDS TECHNOLOGY®