The 2009 State of Cybersecurity from the Federal CISO's Perspective — An (ISC)²® Report

April 2009

20 (ISC)² years of excellence

Government Futures

CISCO

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

EXECUTIVE SUMMARY

Governments around the world are recognizing the urgent need to address cyber security issues. The U.S. government has a variety of roles to play globally, but its key role is to secure its own information and systems. Chief Information Security Officers (CISOs) are on the front lines of securing federal information and information systems. They provide a unique window into this critical task, and their perspective on the challenges they face and progress they see can tell us much about the true state of play in this arena. For this reason, Cisco, Government Futures, and (ISC)² surveyed a broad cross-section of federal agency CISOs to gather their views on the current environment and their recommendations for future priorities and directions.

The survey provides a front-line perspective on the current and future state of agency programs, network and systems security, and the CISO's view on developing an effective information security workforce. The CISO role is evolving and growing rapidly, but CISOs remain the principal officials responsible for overseeing and promoting the security of agency information and information systems.

KEY SURVEY RESULTS

As the data in the following pages show, federal CISOs are feeling empowered. They say they are generally listened to and that the agencies act on their recommendations. This increased influence is a welcome sign from years past, when cybersecurity was not viewed as a management priority. And yet, CISOs continue to face organizational challenges, including, in their view, inadequate resources to do the job, undue focus on compliance reporting and unnecessary paperwork at the expense of actually addressing the many known problems. Notwithstanding these shortcomings, CISOs are, for the most part, highly satisfied with their jobs and strongly motivated by the importance of their missions.

Foremost on CISOs' minds is the threat. In particular, external attacks are seen as the most serious threat, with data loss and exploits presenting the greatest concerns in this category. The insider threat and software vulnerabilities are next in importance, but at a lower level.

Governance issues are next in line. As one CISO said, "We're fighting ourselves," reflecting continued ambiguity of roles within organizations. Principal concerns expressed in this area were the need for even more senior management buy-in, the persistence of organizational stovepipes, the lack of sound metrics, and the relative absence of risk management in a compliance-focused oversight system.

There is progress on key initiatives, including those contained in the Bush Administration's Comprehensive National Cybersecurity Initiative (CNCI), yet CISOs are divided on the issue of where the federal agencies actually stand in the battle to secure agency information and systems. Half the CISOs believe the government is "not getting ahead" of the attackers, while the other half believes we "are turning the corner."

The rest of the report provides details on these and other opinions and on specific recommendations that the CISOs advocate to improve the federal government's security posture. The recommendations touch on human capital, tools and technologies, budget, and, of course, governance.

IMPLICATIONS OF THE SURVEY DATA

Despite these concerns, CISOs believe progress is being made on several fronts and feel they are in a position to influence and lead. But is the direction optimal? Based on this and supplemental research, this report recommends four significant changes in direction to help the CISOs become even more successful on behalf of their agency clients and the American people.

First, the compliance culture, which tends to keep score in binary fashion (i.e., one is "in compliance" or "not in compliance"), must be replaced with a risk-management culture. The Federal Information Security Management Act (FISMA) requires a risk-based approach to security[1], yet the CISOs and their overseers in the agencies, in Congress, and in OMB have more work to do in educating policy and program officials that risks cannot be eliminated. They can only be managed.

[1] *Agencies are required "to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency, or information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." (44 U.S.C. 3543(a)(2))*

Second, the overemphasis on threats, in particular on external attacks leading to data loss, distorts priorities in a pernicious manner. This overemphasis is understandable given the current tsunami of denial of service attacks, viruses and worms, and botnets, coupled with the well-documented "exfiltration" (i.e., stealing) of sensitive government data from federal systems. It may underestimate, however, the ultimately more serious internal attacks – the insider threat present. The history of physical security teaches that the inside job, more often that not, proves to be the final undoing to the best-laid external security plans. More immediately, the focus on preventing incoming attacks (and the obsolete concept of a security "perimeter") have detracted focus from the data that is going out of the agency.

Third, the minimal attention given to what is being left behind by the attackers, unknown time bombs waiting to be activated at some future date (possibly in conjunction with a physical attack), must be corrected. Admittedly, this problem often lies in the realm of the "unknown unknowns" and thus is most difficult to manage and measure. But without leadership attention to this dimension of the problem, we face an unmanaged risk of potentially enormous dimensions.

Finally, CISOs – along with the private sector cybersecurity industry – remain in a reactive, not proactive, stance. This explains why CISOs are of two minds regarding where we stand. The highly asymmetric nature of the threat environment means that trying to keep up with it will be frustrating at best. We are like a mule with a carrot that is dangled on a stick in front of it to keep it moving. We will not reach that goal. Instead, we must reverse the odds by architecting systems that are inherently secure and not rely on fixing one that was designed to be fundamentally insecure. This is the longer term challenge that the survey data suggests – and one that is well beyond the control of the CISOs we surveyed.

CONCLUSION

Our work revealed a community of motivated CISOs who, while frustrated by some of the bureaucratic and leadership obstacles to success, are hard at work to improve the situation. There are many bright spots in the data, and the increasing influence of CISOs in their organizations is a key one of those.

Countering the bright spots is the need for the changes in direction suggested above and an increasingly demanding environment ahead – one that will require strong leadership and unprecedented collaboration across agencies and with the private sector.

INTRODUCTION

Governments around the world are recognizing the urgent need to address cyber security issues. The U.S. government has a variety of roles to play globally, but its key role is to secure its own information and systems.

CISOs are on the front lines of securing federal information and information systems. They provide a unique window into this critical task, and their perspective on the challenges they face and progress they see can tell much about the true state of play in this arena.

> ***"It's no secret that terrorists could use our computer networks to deal us a crippling blow."***
>
> *- Barack Obama, July 2008*

For this reason, Cisco, Government Futures, and (ISC)² surveyed a broad cross-section of federal agency CISOs to gather their views on the current situation and their recommendations for future priorities and directions.

MORE EMPOWERED, BUT THE EFFORT REMAINS UNEVEN

CISOs say they are listened to and that agency officials act on their recommendations. CISOs are satisfied with their positions – they love the mission and intend to stay in government – but wish they had more resources to accomplish their goals and even more support from senior management.

While most report directly to the CIO, some report at a lower level. None report to the CFO, COO, or Chief Risk Officer, and some see this structure as reducing their overall effectiveness.

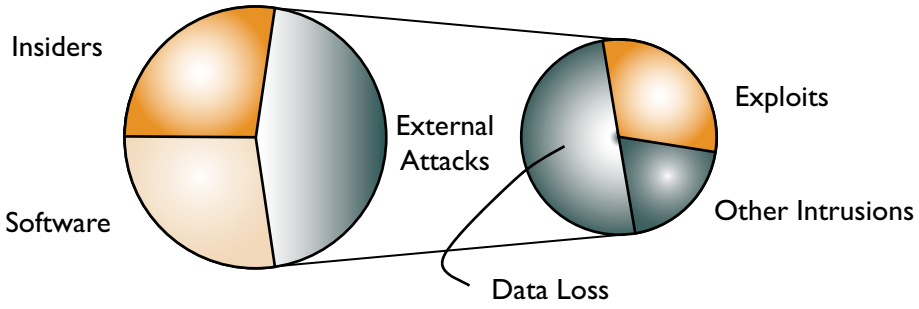
FISMA is generally viewed as having had a positive effect, but two in five CISOs believe it has become misdirected or is a time-wasting exercise. The CISOs give high marks to guidance and assistance from NIST, and to a lesser extent NSA, but do not view OMB and DHS as highly effective leaders.

> ***"CISOs should not be reporting to the CIO. Instead, they should be reporting to the COO or another non-biased executive."***
>
> *- Civilian Agency CISO*

PRIORITIES: THREATS, GOVERNANCE, COMPLIANCE

Threats are top of mind for CISOs. In particular, 48% view external attacks as the biggest threat, with insider threats and software vulnerabilities following at 26% each. Data loss is the biggest concern from external attacks, followed by exploits.

CISO Threat Priorities



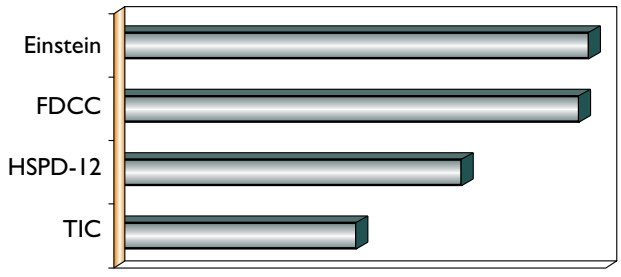
Improving governance is next on the priority list, including getting more buy-in from agency leadership, eliminating security stove pipes, developing sound metrics, improving IT inventory, and implementing a risk management program.

Compliance rounds out the top three, with key objectives including better relations with the Inspector General, expanding work on material weaknesses, and achieving certification and accreditation goals.

MEASURING PROGRESS AND THE CNCI

CISOs see good progress implementing two key programs: Einstein and the Federal Desktop Core Configuration (FDCC). They view the Trusted Internet Connection (TIC) and Homeland Security Presidential Directive 12 (HSPD-12) programs as less successful to date.

More generally, CISOs support a shift to continuous monitoring. There is less enthusiasm for FISMA reports. Other favored metrics included patch management, incident management, and risk exposure (Note: this survey was conducted before the Consensus Audit Guidelines had been finalized).



Degree of Progress

Many CISOs are frustrated with the previous administration's Comprehensive National Cybersecurity Initiative (CNCI). The CNCI was largely seen as having "an external focus" and not devoting enough funds to fixing longstanding agency security problems. In addition, desires for greater attention to authentication, reduced classification of information, and better access to Einstein data were expressed by more than half the respondents.

CISOs DIVIDED

Half the CISOs believe we are making progress but are still "not getting ahead of the attackers." The other half believe "we are turning the corner." Clearly, the agencies are divided.

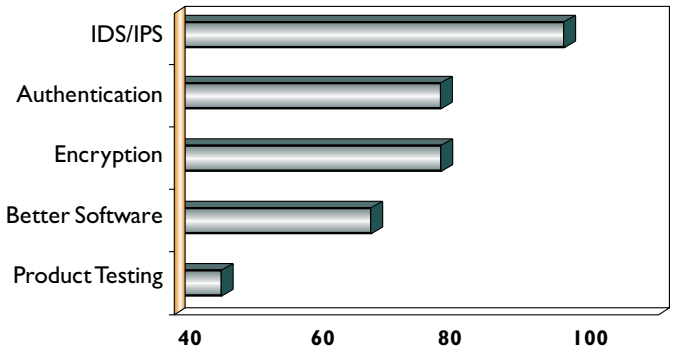
> ***"Our counter-measures are still deficient."***
>
> *- Science Agency CISO*

The CISOs see external attacks as the most significant threat to government information and information systems. Their top priorities are to address those threats, along with improving cybersecurity governance and meeting compliance objectives.

To improve the situation, they propose several changes to the current way the government approaches cybersecurity, including a shift from compliance reporting to continuous monitoring and the imposition of strict security requirements whenever major IT systems are acquired.

TOOLS AND TECHNOLOGIES

Stronger intrusion detection and prevention top CISOs' list of desired tools. Strong authentication and the use of encryption across all forms of communications are a strong second, followed by improvements in the security of commercial software products. Improved product testing is viewed as less important.



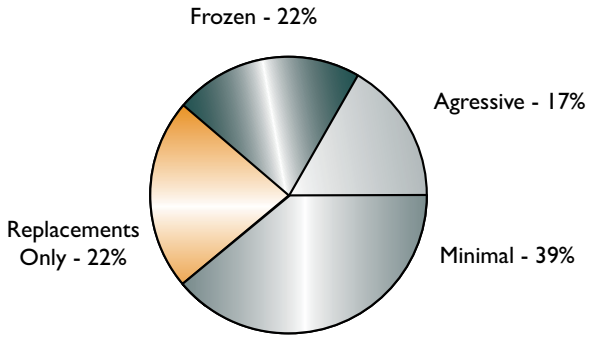
Percentage of CISOs Advocating Each Technology

GETTING THE RIGHT PEOPLE

The current economic crisis will increase risks because of the pressure to deploy money – and systems – quickly, therefore reducing time for testing and assuring systems integrity, but there's a silver lining. It will be easier for government to retain key security staff. While hiring remains minimal at this point, when they do look for staff, CISOs emphasize experience, communication skills, professional certifications, and security clearances.

Three-quarters of CISOs say that mandatory professional certification, as is required under Department of Defense Directive 8570.1, should be extended across government.

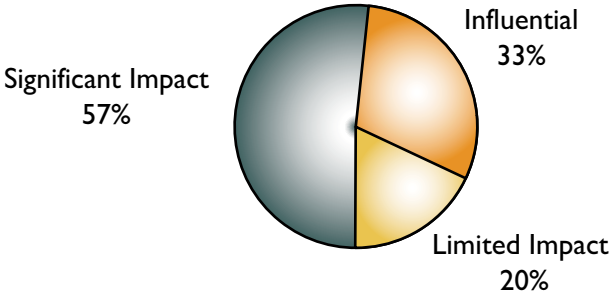
Federal Hiring Posture - Still Weak



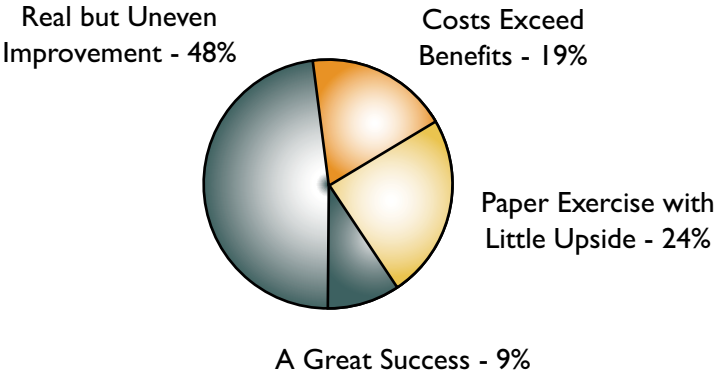
Three-quarters of the CISOs say that mandatory professional certification, as is required under Department of Defense Directive 8570.1, should be extended across government.

BACKGROUND DATA

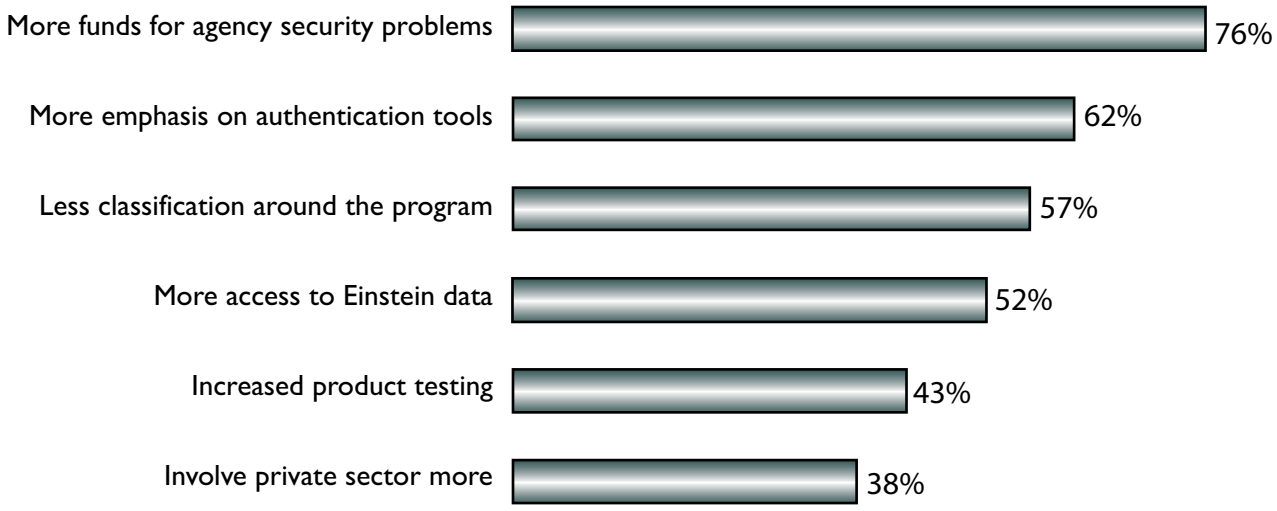
How would you rate your ability to impact the security posture of your department/agency?



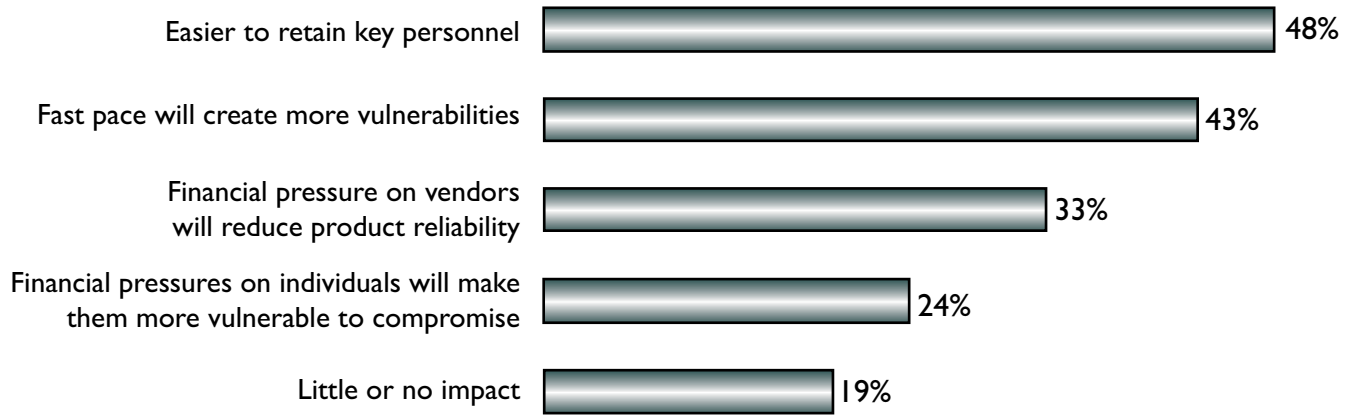
How would you characterize the FISMA process?



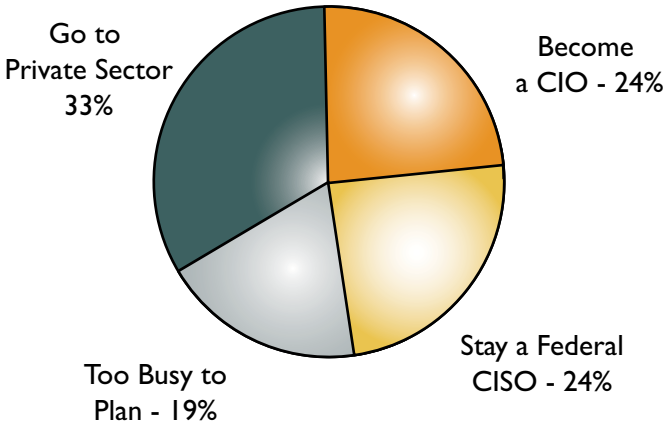
What changes would you make to the CNCI?



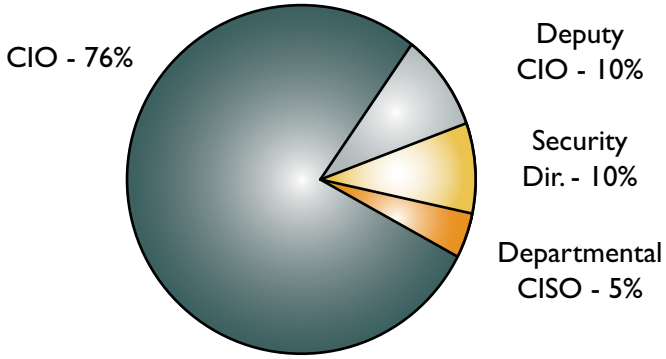
How do you think the economic crisis will affect your agency's IT security?



What do you envision will be your next job?



Who do you report to?



METHODOLOGY AND ACKNOWLEDGEMENTS

This first annual federal CISO survey was conducted during Q1 2009 with 40 federal agency and bureau-level CISOs. Responses were gathered by telephone and in-person interviews and were supplemented by e-mail responses. The responses came primarily from civilian, law enforcement and intelligence agency CISOs. We hope this report provides valuable insight at a time when significant events are transpiring that may have a substantial impact on the federal CISO community, including the results of the 60-day review being conducted under the direction of President Obama and several pieces of legislation that have been or are about to be introduced into Congress. We greatly appreciate the cooperation of these front-line CISOs in advancing our knowledge about our federal information and information systems security.

Lynn McNulty, CISSP, Interviewer

Bruce McConnell, Analyst

SPONSORS

(ISC)²® is the not-for-profit global leader in educating and certifying information security professionals. We have over 60,000 certified members in more than 130 countries. (ISC)² issues the Certified Information Systems Security Professional (CISSP®), Certified Secure Software Lifecycle Professional (CSSLP™), Certification and Accreditation Professional (CAP®), and Systems Security Certified Practitioner (SSCP®) credentials to those meeting necessary competency requirements. *www.isc2.org*

Cisco Federal Thought Leadership Program

With the information security landscape evolving on a daily basis, it's critical for security leaders to stay on top of the latest in industry news, analysis, and opinions. Through its Federal Thought Leadership Program, Cisco provides federal executives exclusive access to a wealth of security resources on an ongoing basis.

The federal community's one-stop shop for market intelligence, tools and breakthrough security thinking: www.cisco.com/go/tlc/security.

Government Futures, a part of McConnell International LLC, believes that dramatic changes are needed if the federal government is going to deliver on the policy, service, and security needs of this country. We see the blurring of public and private sector roles and the rise of "Web 2.0" tools and culture as two emerging trends that will drive the necessary changes. Government Futures highlights the convergence of those trends to build a community of thought leaders that will enable people and organizations to understand and shape the future. *www.governmentfutures.com*