

Technology

The cybersecurity agenda: An information security reality check

It's not enough to call cybersecurity a priority;
it's time to treat it like one

>
accenture

High performance. Delivered.

In collaboration with

iSMG
INFORMATION SECURITY
MEDIA GROUP

• Consulting • Technology • Outsourcing

Executive summary

Besieged by fraud threats from all vectors, the Obama Administration has driven a new national emphasis on improved cybersecurity. Read this paper to learn about:

- The current trends in cybersecurity;
- The criticality of situational awareness;
- The 5 key steps to guide your cybersecurity action plan.

What keeps President Obama awake at night? Cybersecurity certainly bubbles to the top of his list.

As fraudsters chip mercilessly away at the government's elastic perimeter, the nation's cyber infrastructure—and all the critical data it houses—lies at risk.

The fear is well-founded. There are an estimated 3 million indications of malicious activity per year in civilian government networks. Some 40,000 cyber attacks occurred against the Department of Defense alone in the first half of 2009; and cyber criminals have absconded with over \$100,000 from U.S. banks.

Legislation might help the President and U.S. government agencies get a better night's sleep, but a sound action plan, including situational awareness, is the way to get there—and ensure greater cybersecurity for all.

Beyond compliance

With so much at stake, the federal government is faced with a daunting challenge of locking down the nation's cyber infrastructure. The Federal Information Security Management Act of 2002 (FISMA) was the first legislative measure put in place to do just that.



"FISMA has forced agencies to establish programs for securing their information that includes dedicated management, oversight, accountability of agency heads, processes for securing IT systems, and mechanisms for measuring progress," says Patrick D. Howard, CISSP, CISM, and chief information security officer for the Nuclear Regulatory Commission, one of the federal agencies that follows FISMA guidelines.

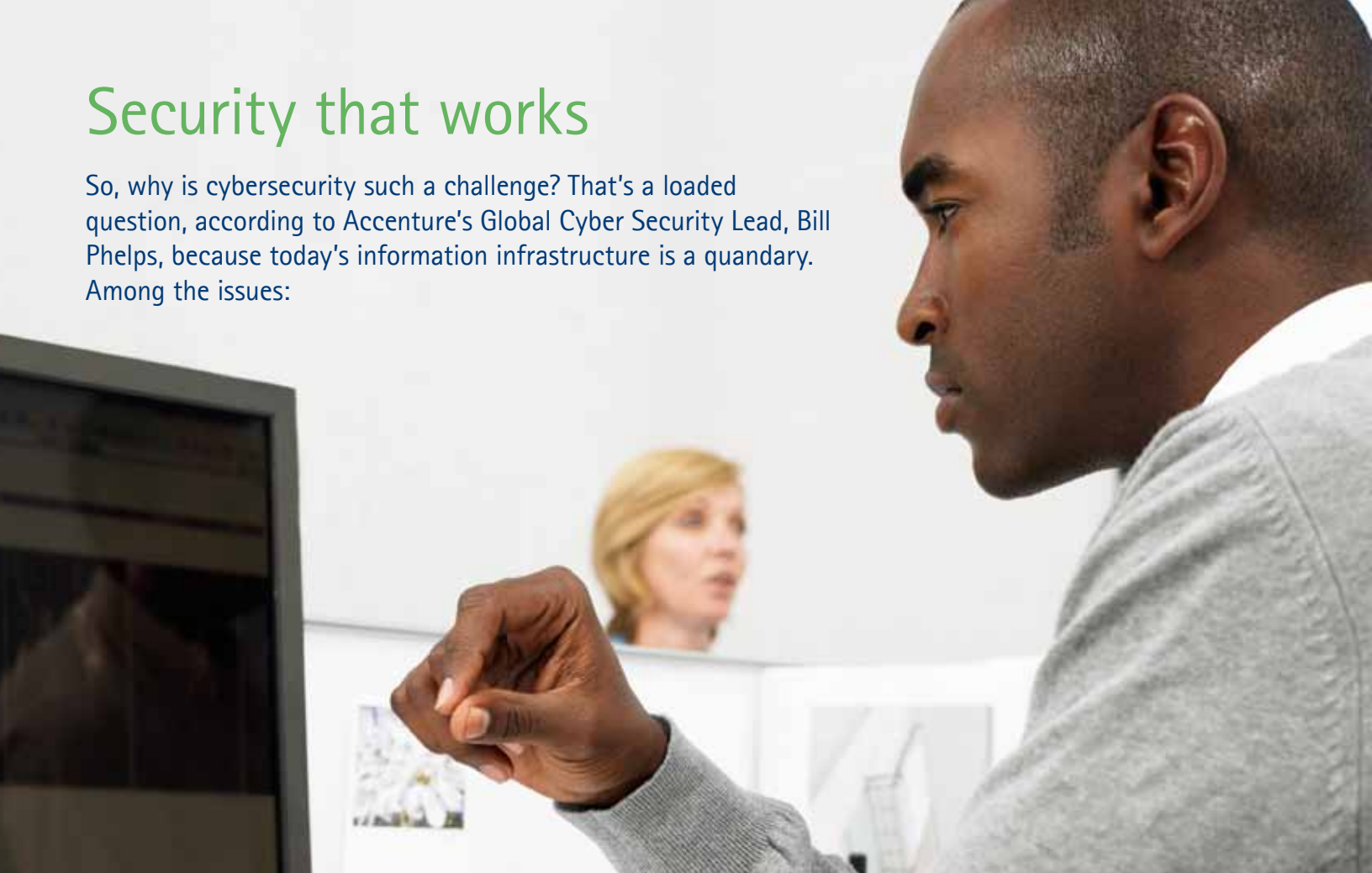
Of course, just meeting FISMA requirements doesn't mean an agency is secure. Recognizing its shortcomings, the Obama administration passed the Cybersecurity Enhancement Act, a measure that will, among other things, strengthen the role of the National Institute of Standards and Technology in shaping cybersecurity requirements.

The good news: The legislation is sparking big changes to FISMA guidance. The bad news: The NRC's Howard believes that such legislation has led to a focus on compliance rather than where it should be—risk management.

"I am pleased by the increased emphasis on cybersecurity by the Obama administration, and in Congress' intention to improve cybersecurity legislation," Howard says. "But legislation alone is never enough. It merely sets a tone, while its effectiveness is a function of how well it is implemented."

Security that works

So, why is cybersecurity such a challenge? That's a loaded question, according to Accenture's Global Cyber Security Lead, Bill Phelps, because today's information infrastructure is a quandary. Among the issues:



Advanced persistent threat

Cyber criminals have become more sophisticated, outpacing defensive measures. "Hackers constantly exploit weaknesses in popular products and pioneer new techniques using viruses, rogue antivirus software, keystroke loggers, botnets, and other tools, for immediate targets or time-triggered actions," says Phelps.

New dynamics

Agencies have completely changed the way they communicate, interact and accomplish their missions. They're sharing information in new, amazing and sometimes scary ways—from portals to social networking. They're even bringing trusted third parties into the fold. And their elastic IT model is introducing technology options that could present more risks, such as mobility and cloud computing.

Shared risk

All of this is extending the government's reach into the critical infrastructure. Yet, 85 percent of that infrastructure is in the hands of the private sector. Risk—to that infrastructure, information assets and private data—is rampant with potentially deep and catastrophic consequences.

"The fact is, agencies are giving more and more access to data and applications, a concept that runs counter to most government thinking," says Phelps. Traditional network security that relies on reactive measures simply isn't enough.

Needed: Situational awareness

One thing agencies can do to ratchet up security, Phelps notes, is enhance their situational awareness. "Agencies need to be able to anticipate what new threats may challenge the infrastructure, and which security elements can help to improve performance." Then, he says, the right security features can be incorporated into the agency's infrastructure and digital assets.

Situational awareness involves the development of a comprehensive, composite picture of one's security situation and proactive monitoring of cause and effect. That is, being aware of what is happening and understanding how information, events and corrective actions will impact agency goals and objectives, both now and in the future.

"You must maintain constant vigil over important information to understand the relationship among the various pieces of information monitored and then project this understanding into the near future to make critical decisions," says Seth Kulakow, former CISO for State of Colorado, in a recent blog for GovInfoSecurity.com. "Information security policies and procedures are developed with the best of intentions, but often fail because they were created without accounting for the dynamics of the environment and organization for which they were built."

The first part of the equation is an understanding of the risks. Agencies must have a full grasp of their vulnerabilities. Threats come from within and outside of the network perimeter. Some are malicious attacks, while others are unfortunate accidents, or human error. Risk spans the entire infrastructure—from desktops and mobile devices to datacenters and cloud applications. Agencies must also consider risk in the supply chain as partners handle more and more sensitive data.

So agencies must be ultra-diligent in their protective measures. It's important to recognize back doors and vulnerabilities that may slip through compliance efforts; and to understand complex and chained patterns in attacks. Agencies must expand the scope of vulnerability assessment or penetration tests and tackle the application-layer threat.

Threat intelligence from external sources is also important in preparing for zero-day exploits.

Agencies must also understand the potential impact a breach can have on the agency itself, as well as its missions and the nation on whole. What are the repercussions of a breached military plan? Can data be shared with trust models that protect civil liberties? Where will the government be if terrorists infiltrate financial institutions? What happens if the East Coast loses a power grid?

"The best information security professionals are situationally aware and attuned to what is happening to them and their environment," Kulakow declares. So it's all about being proactive. Instead of waiting and reacting to an attack, agencies must use all the information on hand to prevent damage before it occurs. That's the crux of good situational awareness and the only way to beat cyber hackers at their own game.

Questions for security leaders

Here's what every agency CISO should be asking of themselves and other senior leaders:

- Does each manager know what his or her responsibilities are with regard to information security?
- Do we assign ownership of and accountability for information security through a data governance program?
- Does our information strategy allow us to identify, track and control how data flows across all our systems and processes?
- Have we evaluated our privacy and protection technologies to confirm they are providing the necessary level of protection?
- Have we built a consistent level of awareness among employees?
- Have we provided them with the appropriate guidance and training for how to handle sensitive data and create secure passwords?
- Have we reexamined our data protection investments?
- Are we choosing business partners with care regarding their own security posture?
- Do we have formal incident response policies, procedures, and teams?

Cybersecurity action plan

So if the Cybersecurity Act is the agencies' starting point—a "to do" list to guide them toward thinking and acting more securely—where is the strategy to implement sound practices? Drawing on years of experience, Accenture provides these best practices to get agencies on the right course:

1. Identify and secure the IT assets, not just the perimeter.

To be successful, you need to know which assets and data are essential to operations and mission completion. Then you need to embed resilience and defensive capabilities across all those core elements. That kind of robust strategy will protect all assets and data—wherever it travels and wherever it lives—from being compromised. You should also consider a comprehensive test procedure to make sure your asset-level protection is effective.

2. Build a hard-nosed "culture of security."

To foster the right culture, you must implement an IT governance program that integrates the people, processes and technology needed to facilitate effective data management and enable responsible data-sharing. That starts by defining who has oversight and accountability for security and assigning responsibilities for data owners and stewards—perhaps even creating a privacy and protection council comprised of critical stakeholders. You should also establish a common set of data privacy and protection standards to reduce complexity and contain costs.

3. Pay closer attention to applications.

Whether off-the-shelf or home-grown, most applications are not engineered with security in mind, so you need to ensure trusted development processes to maintain their integrity. Today, that means adhering to requirements set-forth by Presidential legislation including the Cybersecurity Initiative and Homeland Security directives. Trusted delivery is

also critical—especially with innovations like cloud computing. Protecting the perimeter around applications is not a sufficient defense and you must extend security to the application layer. In every case, you need to be able to measure an application's ability to process and handle sensitive information throughout its deployment lifecycle.

4. Check and double-check user identity.

Identity and access management has become a top priority in government. Effective programs embed pervasive security without sacrificing functionality and ease of use. In terms of identity, cutting edge solutions are financially viable today—including biometrics and smartcards—and should be leveraged to strengthen authentication. And access control has evolved to include key capabilities such as single sign-on, immediate access revocation, self-service functionality and real-time analysis, all of which support mission needs while managing risk. Greatest value, though, will be realized by integrating those authentication and access management capabilities, effectively instituting full control over who has access to what and when.

5. Develop acute situational awareness.

If you're just reacting to suspicious events, you're going to be too late. Hackers and malicious entities start chipping away at vulnerabilities well in advance of a detectable event. You must keep ahead of threats by understanding the risks across the whole risk landscape, including the supply chain and business partner network. That means you have to continually assess partners' knowledge, practices and experience in managing sensitive data across organizational boundaries—as well as your own. Be sure to maintain a clear view of which risks might emerge, and have appropriate measurements in place to manage or mitigate these risks. You must also take into consideration risk's potential impact on the agency, its missions and the nation on whole.

Cybersecurity resource library



For more reading on cybersecurity challenges and solutions, please see:

Accenture resources

www.accenture.com/security

www.accenture.com/cybersecurity

Accenture cyber security PoV

http://www.accenture.com/Global/Technology/Technology_Consulting/Security-Solutions/R-and-I/Mounting-Security-Offensive.htm

Accenture Data Privacy and Protection research

http://www.accenture.com/Global/Technology/Technology_Consulting/Security-Solutions/R-and-I/How-Global-Data.htm

Government resources

U.S. Cybersecurity Caucus

<http://housecybersecuritycaucus.langevin.house.gov/>

S.773 – Cybersecurity Act of 2009

<http://www.opencongress.org/bill/111-s773/text>

Federal Information Security Management Act (FISMA) Implementation Project

<http://csrc.nist.gov/groups/SMA/fisma/index.html>

GAO: Federal Information Security Issues

<http://docs.govinfosecurity.com/files/external/2009June30-FISMAreform.pdf>

Obama IT Security Plan Praised

http://www.govinfosecurity.com/articles.php?art_id=1506

Testimony of Federal CIO Vivek Kundra

http://www.govinfosecurity.com/articles.php?art_id=2370

Interviews

Federal CIO Vivek Kundra

http://www.govinfosecurity.com/articles.php?art_id=2357

Melissa Hathaway, who led President Obama's "60-day" cyberspace policy review

http://www.govinfosecurity.com/articles.php?art_id=1972

Philip Reiting, top IT security official at the Department of Homeland Security

http://www.govinfosecurity.com/articles.php?art_id=2035

U.S. CERT Director Randy Vickers

<http://www.govinfosecurity.com/podcasts.php?podcastID=669>

Bruce McConnell, Counselor, DHS's

National Protection and Program Directorate, on the National Strategy for Trusted Initiative

http://www.govinfosecurity.com/articles.php?art_id=2781

Ron Ross, NIST senior scientist

<http://www.govinfosecurity.com/podcasts.php?podcastID=377>

Dickie George of the National Security Agency

http://www.govinfosecurity.com/articles.php?art_id=2005

About Information Security Media Group, Corp. (ISMG)

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focused on Risk Management, Compliance, Fraud, Security, and Information Technology. The company provides news, training, education and other related content for professionals in their respective industries. ISMG publishes BankInfoSecurity.com, CUInfoSecurity.com, GovInfoSecurity.com, HealthcareInfoSecurity.com, and a variety of other related online properties.

For more information on how Accenture can help your organization defend against cyber threats, visit accenture.com/cybersecurity

Copyright © 2010 Accenture
All rights reserved.

Accenture, its logo, and High Performance Delivered are trademarks of Accenture.

About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with approximately 204,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US\$21.6 billion for the fiscal year ended Aug. 31, 2010. Its home page is www.accenture.com.

Accenture has more than 20 years of experience helping governments across the globe use security to both defend against malicious threats and enable innovative processes for critical missions without increasing risk. By combining our security and technology know-how with industry-specific experience, we help our clients weave cyber resilience into their infrastructure, applications, and core processes—securing the fabric of their entire agency. To learn more, please visit www.Accenture.com