

# Cybersecurity: Your Role, Your Agency's Role

President Obama has declared that cybersecurity represents one of the nation's most serious economic and national security challenges. The new cyber czar will have broad authority to develop strategy. Meanwhile, individual government workers and agency IT departments continue to play an important role in protecting government information and networks.

## The Individual's Role

Say your favorite niece has sent you an electronic birthday greeting card or posted a video on your Facebook page. Do you click the hyperlink?

"The risk is that the linked website will surreptitiously plant code on your computer that places your computer under someone else's control," says David Graziano, security solutions manager, Cisco. Then your computer can become a conduit to steal user names, passwords, and sensitive files and send spam.

That's why security professionals recommend you be cautious about clicking links in emails or on social networking sites, even if they appear to be from a trusted source. When in doubt, it's safest to type in the URL yourself.

## Your Agency's Role

External threats, including the personalized phishing attack described above, were identified as the most worrisome threat by federal government chief information security officers (CISOs) in a **2009 survey** conducted by (ISC)<sup>2</sup> and sponsored by Cisco and Government Futures, a consulting firm. Ranking next as the most dangerous to government are insider threat and software vulnerabilities.

The good news from the survey is that 90 percent of CISOs say agency officials act on their recommendations. "One reason is that the Federal Information Security Management Act (FISMA) scorecard has brought cybersecurity to the attention of Congress," Graziano says. But 40 percent of CISOs said they think that time spent on FISMA-mandated reporting and paperwork diverts agency resources from addressing known security vulnerabilities.

## What You Can Do Today

Regardless of how careful agency employees are, cybercriminals will continue to devise new threats that can expose government information and networks. Protecting against socially engineered threats delivered by email or on social networking sites requires a multilayered approach, or defense in depth. Here are five actions your agency can take today:

- **Block spam before it can get to employee desktops:** You can do this with an email gateway solution. Cisco IronPort Email Security Appliances, for example, block email based on senders' reputations. IronPort ascertains reputations by analyzing billions of email messages daily for more than 90 variables associated with spam. "Reputation-based filtering has been shown to produce a false-positive rate of much less than one in one million," says Graziano.
- **Block malicious websites:** If email with links to malicious websites does get through the agency's email gateway, you can use an Internet gateway solution to stop employees from clicking through. Be aware that the effectiveness of these gateways varies widely. "Checking the URL against whitelists of good sites and blacklists of bad sites isn't enough, because cybercriminals set up new sites constantly," Graziano says. That's why the Cisco IronPort Web Security Appliances also provides reputation filtering, which involves a real-time assessment of variables such as the website's country of origin and length in service.
- **Monitor and stop anomalous behavior on the desktop:** Even with the previous two measures in place, an employee might still manage to visit a website that deposits keystroke-logging software or other malware on the desktop. You can stop the malware from doing harm by using desktop intrusion prevention system software such as Cisco Security Agent. It immediately detects suspicious application behavior such as surreptitious software installation and asks you to confirm that the action is OK before allowing it. (You can also use Cisco Security Agent to enforce agency security policies such as not copying files to USB drives or pasting information into emails.)
- **Monitor and stop anomalous behavior on the network:** Use Cisco NetFlow, built into your existing Cisco routers, to look for anomalous behavior indicating a compromised desktop. One sign is sending large volumes of email.

- **Ensure that laptops comply with security policies:** Network Admission Control (NAC) solutions quickly scan desktops and laptops before allowing them to connect to the network, ensuring that they are infection-free and that they conform to the agency's security policy. Computers that are out of compliance are remediated automatically, without any involvement from the agency IT staff.

Protecting government information and networks from cybercriminals requires a joint effort from everyone in government. "When you use all five of these tools, you get defense in depth," Graziano says.

To watch a webcast discussing the results of the CISO survey, visit:

<http://mediazone.brighttalk.com/event/ISC2/02f657d55e-2569-intro>

To read about Cisco IronPort Web and Internet Security Appliances, visit: [www.cisco.com/web/products/ironport](http://www.cisco.com/web/products/ironport)



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV  
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)