May 2005

INFORMATION SECURITY

Emerging Cybersecurity Issues Threaten Federal Information Systems

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-231, a report to congressional requesters

Why GAO Did This Study

Federal agencies are facing a set of emerging cybersecurity threats that are the result of increasingly sophisticated methods of attack and the blending of once distinct types of attack into more complex and damaging forms. Examples of these threats include *spam* (unsolicited commercial e-mail), *phishing* (fraudulent messages to obtain personal or sensitive data), and *spyware* (software that monitors user activity without user knowledge or consent). To address these issues, GAO was asked to determine (1) the potential risks to federal systems from these emerging cybersecurity threats, (2) the federal agencies' perceptions of risk and their actions to mitigate them, (3) federal and private-sector actions to address the threats on a national level, and (4) governmentwide challenges to protecting federal systems from these threats.

What GAO Recommends

GAO recommends that the Director, OMB, ensure that agencies address emerging cybersecurity threats in their FISMA-required information security program and coordinate with DHS and the Department of Justice to establish guidance for agencies on how to appropriately address and report incidents of emerging threats. OMB representatives generally agreed with our findings and conclusions and indicated their plans to address our recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-05-231.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

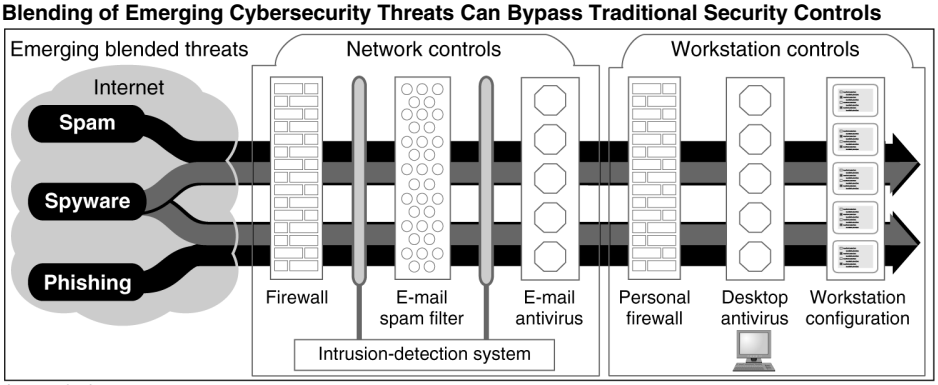
Spam, phishing, and spyware pose security risks to federal information systems. Spam consumes significant resources and is used as a delivery mechanism for other types of cyberattacks; phishing can lead to identity theft, loss of sensitive information, and reduced trust and use of electronic government services; and spyware can capture and release sensitive data, make unauthorized changes, and decrease system performance. The blending of these threats creates additional risks that cannot be easily mitigated with currently available tools (see figure).

Agencies' perceptions of the risks of spam, phishing, and spyware vary. In addition, most agencies were not applying the information security program requirements of the Federal Information Security Management Act of 2002 (FISMA) to these emerging threats, including performing risk assessments, implementing effective mitigating controls, providing security awareness training, and ensuring that their incident-response plans and procedures addressed these threats.

Several entities within the federal government and the private sector have begun initiatives to address these emerging threats. These efforts range from educating consumers to targeting cybercrime. Similar efforts are not, however, being made to assist and educate federal agencies.

Although federal agencies are required to report incidents to a central federal entity, they are not consistently reporting incidents of emerging cybersecurity threats. Pursuant to FISMA, the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) share responsibility for the federal government's capability to detect, analyze, and respond to cybersecurity incidents. However, governmentwide guidance has not been issued to clarify to agencies which incidents they should be reporting, as well as how and to whom they should report. Without effective coordination, the federal government is limited in its ability to identify and respond to emerging cybersecurity threats, including sophisticated and coordinated attacks that target multiple federal entities.

Blending of Emerging Cybersecurity Threats Can Bypass Traditional Security Controls



Source: GAO.