United States Government Accountability Office

GAO

Report to Congressional Requesters

May 2005

INFORMATION SECURITY

Emerging Cybersecurity Issues Threaten Federal Information Systems

G A O

Accountability ★ Integrity ★ Reliability

GAO
Accountability·Integrity·Reliability

Highlights

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

May 2005

INFORMATION SECURITY

Emerging Cybersecurity Issues Threaten Federal Information Systems

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

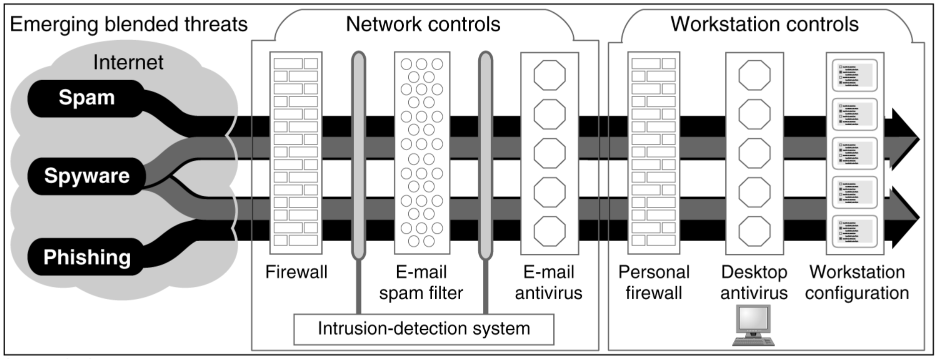
Spam, phishing, and spyware pose security risks to federal information systems. Spam consumes significant resources and is used as a delivery mechanism for other types of cyberattacks; phishing can lead to identity theft, loss of sensitive information, and reduced trust and use of electronic government 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.

Contents

Appendixes

Tables

Figures

Abbreviations

AOL	America Online, Inc.
BHO	browser help object
CAN SPAM Act	Controlling the Assault of Non-Solicited Pornography and Marketing Act
CERT/CC	CERT Coordination Center
CFO	chief financial officer
CFR	Code of Federal Regulations
CIO	chief information officer
DHS	Department of Homeland Security
EULA	end-user license agreement
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FedCIRC	Federal Computer Incident Response Capability
FISMA	Federal Information Security Management Act of 2002
FTC	Federal Trade Commission
ICE	Immigration and Customs Enforcement
IG	inspector general
IP	Internet Protocol

IRS	Internal Revenue Service
I-SPY PREVENTION Act	Internet-Spyware Prevention Act
IT	information technology
NCSA	National Cyber Security Alliance
NCSD	National Cyber Security Division
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PC	personal computer
SLAM-Spam	simultaneously layered approach methodology–Spam
SPY Act	Securely Protect Yourself Against Cyber Trespass Act
USA PATRIOT	Act Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
US-CERT	United States Computer Emergency Readiness Team
Win2K Pro	Windows 2000 Professional

GAO

Accountability ★ Integrity ★ Reliability

United States Government Accountability Office
Washington, D.C. 20548

May 13, 2005

The Honorable Tom Davis
Chairman, Committee on Government Reform
House of Representatives

The Honorable Adam Putnam
House of Representatives

This report describes the threats of emerging cybersecurity issues such as 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). Specifically, the report discusses (1) the potential risks to federal information systems from emerging cybersecurity threats such as spam, phishing, and spyware; (2) the 24 Chief Financial Officers Act agencies' reported perceptions of these risks and their actions and plans to mitigate them; (3) government and private-sector efforts to address these emerging cybersecurity threats on a national level, including actions to increase consumer awareness; and (4) governmentwide challenges to protecting federal information systems from these threats.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the date of this letter. At that time, we will send copies of this report to the Ranking Minority Member of the Committee on Government Reform and to other interested parties. In addition, the report will be made available at no charge on GAO's Web site at http://www.gao.gov.

If you have any questions concerning this report, please call me at (202) 512-6244 or send e-mail to wilshuseng@gao.gov. Major contributors to this report are listed in appendix V.

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Executive Summary

Purpose

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).

Spam, phishing, and spyware, while once viewed as discrete consumer challenges, are being blended to create substantial threats to large enterprises, including federal systems. According to security researchers' and vendors' 2004 annual security reports, phishing and spyware were identified among the top emerging threats of last year, and they are predicted to increase in 2005. Federal and private-sector security experts are observing the rapid evolution of attack technologies and methods. The increasing sophistication and maliciousness of cybersecurity threats create unique challenges to federal systems and governmentwide cybersecurity efforts.

To more effectively understand and address these issues, the Chairman, House Committee on Government Reform, and Representative Putnam asked GAO to determine (1) the potential risks to federal information systems from emerging cybersecurity threats such as spam, phishing, and spyware; (2) the 24 Chief Financial Officers (CFO) Act agencies' reported perceptions of these risks and their actions and plans to mitigate them; (3) government and private-sector efforts to address these emerging cybersecurity threats on a national level; and (4) governmentwide challenges to protecting federal information systems from these emerging cybersecurity threats.

Background

The same speed and accessibility that create the enormous benefits of the computer age can, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with computer operations from remote locations for mischievous or malicious purposes, including fraud or sabotage. Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence-gathering, and acts of war. As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood increases that information attacks will threaten vital national interests.

The sophistication and effectiveness of cyberattacks have steadily advanced. These attacks often take advantage of flaws in software code, use exploits that can circumvent signature-based tools[1] that commonly identify and prevent known threats, and social engineering techniques designed to trick the unsuspecting user into divulging sensitive information or propagating attacks. These attacks are becoming increasingly automated with the use of botnets—compromised computers that can be remotely controlled by attackers to automatically launch attacks. Bots (short for robots) have become a key automation tool to speed the infection of vulnerable systems.

Several laws have been implemented to improve the nation's cybersecurity posture. The requirements of the Federal Information Security Management Act of 2002 (FISMA) present a framework for agencies to use in improving their capabilities to protect federal systems and information against cyberattack. The act also assigns specific responsibilities to the Office of Management and Budget (OMB), which include developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, and, at least annually, reviewing and approving or disapproving agency information security programs. FISMA also charged the Director of OMB with ensuring the operation of a central federal information security incident center that would be responsible for issuing guidance to agencies on detecting and responding to incidents, compiling and analyzing information about incidents, and informing agencies about current and potential information security threats, among other responsibilities. Other laws, such as the Homeland Security Act and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act),[2] also address actions that the government can take to increase national cybersecurity awareness and preparedness, including the roles and responsibilities of key agencies such as the Department of Homeland Security (DHS). FISMA also requires that the National Institute of

[1] Signature-based tools compare files or packets to a list of "signatures"—patterns of specific files or packets that have been identified as a threat. Each signature is the unique arrangement of zeros and ones that make up the file.

[2] USA PATRIOT Act, October 26, 2001 (Public Law 107-56).

Standards and Technology (NIST) establish standards, guidelines, and requirements that can help agencies improve the posture of their information security programs. NIST has issued several publications relevant to helping agencies protect their systems against emerging cybersecurity threats.

Results in Brief

Spam, phishing, and spyware pose security risks to federal information systems. Spam is a problem not only because of the enormous resources it demands, but also because it now serves as a means for other types of attack. Phishing can lead to identity theft and loss of sensitive information; it can easily result in reduced trust in and therefore use of electronic government services, thereby reducing the efficiencies that such services offer. Phishers have targeted federal entities such as the Federal Bureau of Investigation (FBI), Federal Deposit Insurance Corporation (FDIC), and the Internal Revenue Service (IRS). Spyware threatens the confidentiality, integrity, and availability of federal information systems by capturing and releasing sensitive data, making unauthorized changes to systems, decreasing system performance, and possibly creating new system vulnerabilities, all without the user's knowledge or consent. The blending of these threats creates additional risks that cannot be easily mitigated with currently available tools.

Agencies reported varying perceptions of the risks of spam, phishing, and spyware. In addition, many agencies have not fully addressed the risks of emerging cybersecurity threats as part of their required agencywide information security programs, which include performing periodic assessments of risk; implementing security controls commensurate with the identified risk; ensuring security-awareness training for agency personnel; and implementing procedures for detecting, reporting, and responding to security incidents. An effective security program can assist in agency efforts to mitigate and respond to these emerging cybersecurity threats.

Several entities within the federal government and the private sector have begun initiatives directed toward addressing spam, phishing, and spyware. These actions range from targeting cybercrime to educating the user and private-sector community on how to detect and protect systems and information from these threats. While the initiatives demonstrate an understanding of the importance of cybersecurity and emerging threats and represent the first steps in addressing the risks associated with emerging threats, similar efforts are not being made to assist 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, OMB and 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.

Principal Findings

Spam, Phishing, Spyware, and Other Emerging Threats Put Federal Agencies at Risk

Federal agencies are facing a set of emerging cybersecurity threats that are the result of changing sources of attack, increasingly sophisticated social engineering techniques designed to trick the unsuspecting user into divulging sensitive information, new modes of covert compromise, and the blending of once distinct attacks into more complex and damaging exploits.

Advances in antispam measures have caused spammers to increase the sophistication of their techniques to bypass detection; the frequency and sophistication of phishing attacks have likewise increased, and spyware has proven to be difficult to detect and remove.

The risks that agencies face are significant. Spam consumes employee and technical resources and can be used as a delivery mechanism for malware[3] and other cyberthreats. Agencies and their employees can be victims of phishing scams, and spyware puts the confidentiality, integrity, and availability of agency systems at serious risk. Other emerging threats include the increased sophistication of worms, viruses, and other malware, and the increased attack capabilities of blended threats and botnets.

[3] Malware (malicious software) is defined as programs that are designed to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded into useful programs so that users are induced into activating them. Malware can include viruses, worms, and spyware.

Many Agencies Do Not Fully Identify and Address Security Risks of Emerging Threats

Agencies reported varying perceptions of the risks and effects of spam, phishing, and spyware. Most agencies (19 of 24) identified nonsecurity effects from spam, including reduced system performance and the costs of filtering e-mail. Of these 19 agencies, 14 reported that spam consumed network bandwidth used to transmit messages or consumed disk storage used to store messages. However, only one agency identified the risk that spam presents for delivering phishing, spyware, and other threats to their systems and employees.

Also, 14 of 24 agencies reported that phishing had limited or no effect on their systems and operations. Two agencies indicated that they were unaware of any phishing scams that had specifically targeted their employees, while 6 agencies reported a variety of effects, including the increased need for help desk support and instances of compromised credit card accounts.[4] In addition, 5 agencies reported that spyware had minimal effect on their systems and operations, while 11 noted that spyware caused a loss of employee productivity or required increased usage of help desk support. Of the remaining 4 agencies that reported spyware effects, 2 noted the decreased ability for their users to utilize agency systems: 1 agency noted that users had been unable to connect to an agency network, while the other indicated that users had experienced a denial of service after an antispyware tool had been implemented. Finally, one agency reported the costs associated with developing and implementing antispyware tools, and another stated that spyware was simply a nuisance to its users.

Many agencies have not fully addressed the risks of emerging cybersecurity threats as part of their agencywide information security programs (including periodic risk assessments; security controls commensurate with the identified risk; security awareness training; and procedures for detecting, reporting, and responding to security incidents). For example, 17 of the 24 agencies indicated that they have not assessed the risk that the agency name or the name of any of its components could be exploited in a phishing scam. Also, several agencies reported that current enterprise tools to address emerging cybersecurity threats are immature and therefore impede efforts to effectively detect, prevent, remove, and analyze incidents. For example, although most agencies (20 of 24) reported implementing agencywide approaches to mitigating spam, some agencies

[4] The remaining two agencies did not provide a response to our survey question regarding the risks of phishing to agency systems and operations.

reported concerns that these tools could not be relied upon to accurately distinguish spam from desired e-mails.

Agencies also reported that employee awareness was a significant challenge as they worked to mitigate the risks associated with phishing and spyware. Of the 24 agencies we surveyed, 13 reported that they have or plan to implement phishing awareness training this fiscal year, 3 reported plans to implement training in the future, and 3 had no plans to implement phishing awareness training. Agency officials also reported that they issue correspondence to inform employees of specific incidents and have made general information available on how to detect and report suspicious e-mail or activity characteristic of these threats. However, officials consistently confirmed that user awareness of emerging threats is still lacking and that significant improvements must be made. Lastly, our review of agencies' incident-response plans found that while they largely address the threat of malicious code, they do not fully address phishing or spyware. Specifically, our analysis of the incident-response plans or procedures provided by all 24 agencies showed that none specifically addressed spyware or phishing. Further, one agency indicated that spyware is not considered significant enough to warrant reporting it as a security incident.

Efforts to Combat Cybersecurity Threats Are Directed toward the Private Sector and Consumers

Recognizing the potential risks emerging cybersecurity threats pose to information systems, several entities within the federal government and the private sector have begun initiatives directed toward addressing spam, phishing, and spyware. These efforts range from combating cybercrime to educating the user and the private-sector community on how to detect and protect systems and information from these threats. While the initiatives demonstrate an understanding of the importance of cybersecurity and emerging threats and represent the first steps in addressing the risks associated with these threats, similar efforts are not being made to assist federal agencies.

Both the public and private sectors have noted the importance of user education and consumer awareness relating to emerging cybersecurity threats. The Federal Trade Commission (FTC) has been a leader in this area, issuing consumer alerts and releasing several reports on spam as well as guidance for businesses on how to reduce identity theft. In addition, FTC has sponsored various events, including a spam forum in the spring of 2003, a spyware workshop in April 2004, and an e-mail authentication summit in the fall of 2004. Also notable is its Identity Theft Clearinghouse, an online resource for taking complaints from consumers. Organizations such as the

Anti-Phishing Working Group, the Phish Report Network, and the United States Internet Service Provider Association have also been actively involved in combating these emerging cyberthreats, as has the Federal Deposit Insurance Corporation in consumer education. Finally, the Department of Justice and FTC are involved in criminal investigations and law-enforcement activities related to spam, phishing, and spyware.

Lack of Coordinated Incident Reporting Limits Federal Capability to Address Emerging Threats

Agencies are not consistently reporting emerging cybersecurity incidents such as phishing and spyware to a central federal entity; while some report cyber incidents to DHS's United States Computer Emergency Readiness Team (US-CERT) as required,[5] other agencies report incidents to law enforcement agencies, while still others do not report incident information outside their agency. Discussions with US-CERT officials confirmed that they had not consistently received incident reports from agencies and that the level of detail that accompanies an incident report may not provide any information about the actual incident or method of attack. US-CERT officials also noted that agencies' efforts to directly report incidents to law enforcement could be duplicative, as US-CERT forwards incidents with a high level of severity to either the FBI or the Secret Service.

As of March 2005, neither OMB nor US-CERT had issued guidance to federal agencies on the processes and procedures for reporting incidents of phishing, spyware, or other emerging malware threats to US-CERT. The most recent guidance to federal agencies on incident-reporting roles and processes was issued in October 2000—prior to the establishment of US-CERT. Lacking the necessary guidance, agencies do not have a clear understanding of which incidents they should be reporting, as well as how and to whom they should report. Moreover, 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.

[5] FISMA charged the Director of OMB with ensuring the operation of a federal information security center. The required functions are performed by DHS's US-CERT, which was established to aggregate and disseminate cybersecurity information to improve warning and response to incidents, increase coordination of response information, reduce vulnerabilities, and enhance prevention and protection.

Recommendations for Executive Action

In order to more effectively prepare for and address emerging cybersecurity threats, we recommend that the Director, Office of Management and Budget, take the following two actions:

- ensure that agencies' information security programs required by FISMA address the risk of emerging cybersecurity threats such as spam, phishing, and spyware, including performing periodic risk assessments; implementing risk-based policies and procedures to mitigate identified risks; providing security-awareness training; and establishing procedures for detecting, reporting, and responding to incidents of emerging cybersecurity threats; and

- coordinate with the Secretary of Homeland Security and the Attorney General to establish governmentwide guidance for agencies on how to (1) address emerging cybersecurity threats and (2) report incidents to a single government entity, including clarifying the respective roles, responsibilities, processes, and procedures for federal entities—including homeland security and law enforcement.

Agency Comments and Our Evaluation

We received oral comments on a draft of our report from representatives of OMB's Office of Information and Regulatory Affairs and Office of General Counsel. These representatives generally agreed with our findings and conclusions, and they supplied additional information related to federal efforts to address emerging cyber threats. This information was incorporated into our final report as appropriate.

In commenting on our first recommendation, OMB stressed that the agencies have the primary responsibility for complying with FISMA's information security management program requirements. Nevertheless, OMB indicated that it would incorporate emerging cybersecurity threats and new technological issues into its annual review of agency information security programs, and it plans to consider whether the programs adequately address emerging issues before approving them.

OMB told us that our second recommendation was being addressed by a concept of operations and taxonomy for incident reporting that it is developing with DHS's US-CERT. The final document is planned to be issued this summer. OMB officials indicated that the completed document will establish a common set of incident terms and the relationships among those terms, and will also clarify the roles, responsibilities, processes, and procedures for federal entities involved in incident reporting and response—including homeland security and law enforcement entities.

Additionally, the Departments of Defense, Homeland Security, and Justice provided technical comments via e-mail, which were incorporated as appropriate.

Chapter 1

Introduction

The same speed and accessibility that create the enormous benefits of the computer age can, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with computer operations from remote locations for mischievous or malicious purposes, including fraud or sabotage. We reported in March 2004 that federal agencies continue to show significant weaknesses in computer systems that put critical operations and assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.[1]

The increasing sophistication and maliciousness of cybersecurity threats create unique challenges to federal systems and governmentwide cybersecurity efforts. Security experts are observing the rapid evolution of attack technologies and methods. Unsolicited commercial e-mail (spam) has been an annoyance to Internet users for several years. However, over the past few years, this mass-marketing tool has evolved from a mere nuisance to a delivery mechanism for malicious software programs (commonly referred to as malware) that hijack computers, and e-mail that deceives recipients into divulging sensitive information, such as credit card numbers, login IDs, and passwords (phishing). One emerging form of malware, known as spyware, is installed without the user's knowledge to surreptitiously track and/or transmit data to an unauthorized third party.

Security researchers' and vendors' 2004 annual security reports reportedly identified phishing and spyware as among the top emerging threats of last year, and they were predicted to increase in 2005. These threats have targeted our government; for instance, in 2004, federal entities such as FDIC, the Federal Bureau of Investigation (FBI), and IRS were used in phishing scams in which their agency names were exploited. Although spam, phishing, and spyware were once viewed as discrete consumer challenges, they are now being blended to create substantial threats to large enterprises, including federal systems. For example, the number of phishing scams that are often spread through spam has significantly increased.

Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism,

[1] GAO, *Information Security: Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements*, GAO-04-483T (Washington, D.C.: Mar. 16, 2004).

foreign intelligence gathering, and acts of war. According to the FBI, terrorists, transnational criminals, and intelligence services are quickly becoming aware of and using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, and degrade the integrity of or deny access to data.[2] As larger amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood increases that information attacks will threaten vital national interests. Table 1 summarizes the sources of emerging cybersecurity threats.

[2] A virus is a program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. A Trojan horse is a computer program that conceals harmful code. It usually masquerades as a useful program that a user would wish to execute. A worm is an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. A logic bomb is a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event, such as termination of the programmer's employment, occurs. A sniffer, synonymous with packet sniffer, is a program that intercepts routed data and can be used to examine each packet in search of specified information, such as passwords transmitted in clear text.

Table 1: Sources of Emerging Cybersecurity Threats

Threat	Description
Terrorists	Terrorists may use phishing scams or spyware/malware in order to generate funds or gather sensitive information.
Criminal groups	There is an increased use of cyber intrusions by criminal groups that attack systems for monetary gain; further, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities.
Spyware/malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware.
Hackers	Hackers sometimes break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
Insider threat	The disgruntled organization insider is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors. Employees who accidentally introduce malware into systems also fall into this category.
Botnet operators	Botnet operators are hackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems to enable them to coordinate attacks and distribute malware, spam, and phishing scams. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam or phishing scams, etc.).
Phishers	Individuals or small groups that execute phishing scams in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Individuals or organizations that distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing scams, distribute spyware/malware, or attack organizations (i.e., denial-of-service).

Source: GAO analysis.

The sophistication and effectiveness of cyberattacks have steadily advanced. These attacks often take advantage of flaws in software code, circumvent signature-based tools[3] that commonly identify and prevent known threats, and use stealthy social engineering techniques designed to trick the unsuspecting user into divulging sensitive information. These

[3] Signature-based tools compare files or packets to a list of “signatures” (patterns) of specific files or packets that have been identified as a threat. Each signature is the unique arrangement of zeros and ones that make up the file.

attacks are becoming increasingly automated with the use of botnets[4]—compromised computers that can be controlled remotely by attackers to automatically launch attacks. Bots have become one of the key automation tools that speed the location and infection of vulnerable systems.

Laws and Other Policies Aim to Improve Federal Agency Cybersecurity Capabilities, Increase National Awareness, and Deter Cybercrime

Several laws have been implemented to improve the nation's cybersecurity posture. The Federal Information Security Management Act of 2002 (FISMA) requires agencies to implement an entitywide risk-based approach to protecting federal systems and information against cyberattack. Other laws, such as the Homeland Security Act and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), among others, also address actions that the government can take to increase national cybersecurity awareness and preparedness, including the roles and responsibilities of key agencies such as DHS. Additionally, recent legislation, both enacted and pending, that specifically addresses spam, phishing, and spyware has included civil and criminal penalties to deter cybercrime.

FISMA Charges Agencies to Improve Information Security Capabilities

FISMA establishes clear criteria to improve federal agencies' cybersecurity programs. Enacted into law on December 17, 2002, as title III of the E-Government Act of 2002, FISMA requires federal agencies to protect and maintain the confidentiality, integrity, and availability of their information and information systems.[5] It also assigns specific information security responsibilities to the Office of Management and Budget (OMB), the Department of Commerce's National Institute of Standards and Technology (NIST), agency heads, chief information officers (CIO), and inspectors

[4] Bots (short for "robots") are programs that are covertly installed on a targeted system. They allow an unauthorized user to remotely control the compromised computer for a variety of malicious purposes. Attackers often coordinate large groups of bot-controlled systems known as bot-networks, or botnets.

[5] According to FISMA, information security is defined as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information. (44 U.S.C. Section 3542(b)(1)(A-C)).

general (IG). For OMB, these responsibilities include developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, as well as reviewing, at least annually, and approving or disapproving, agency information security programs. FISMA required each agency including agencies with national security systems, to develop, document, and implement agencywide information security programs to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Specifically, this program is to include

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;

- risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system;

- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;

- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;

- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency’s required inventory of major information systems;

- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

- procedures for detecting, reporting, and responding to security incidents; and

- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

FISMA requires each agency to report annually to OMB, selected congressional committees, and the Comptroller General on the adequacy of information security policies, procedures, and practices, and on compliance with FISMA's requirements.

FISMA also charges the Director of OMB with ensuring the operation of a central federal information security incident center with responsibility for issuing guidance to agencies on detecting and responding to incidents. Other responsibilities include compiling and analyzing information about incidents and informing agencies about current and potential information security threats. Prior to FISMA, the CIO Council (then chaired by OMB's Deputy Director for Management) issued a memorandum to all agency CIOs instructing agencies to follow specific practices for appropriate coordination and interaction with the Federal Computer Incident Response Capability (FedCIRC).[6] OMB's statutory requirement supported FedCIRC, and OMB received quarterly reports from FedCIRC on the federal government's status on information technology security incidents.

Following the establishment of DHS and in an effort to implement action items described in the National Strategy to Secure Cyberspace, FedCIRC was dissolved as a separate entity and its functions absorbed into the United States Computer Emergency Readiness Team (US-CERT), which was created in September 2003. US-CERT was established to aggregate and disseminate cybersecurity information to improve warning about and response to incidents, increase coordination of response information, reduce vulnerabilities, and enhance prevention and protection. US-CERT analyzes incidents reported by federal civilian agencies and coordinates with national security incident response centers in responding to incidents on both classified and unclassified systems. US-CERT also provides a service through its National Cyber Alert System to identify, analyze, prioritize, and disseminate information on emerging vulnerabilities and threats.

[6] Chief Information Officers Council, *Memorandum for Chief Information Officers of All Agencies: Agency Interaction with GSA's Federal Computer Incident Response Capability (FedCIRC)* (Washington, D.C.: Oct. 29, 2000). FedCIRC was established in 1996 to provide a central focal point for incident reporting, handling, prevention, and recognition for the federal government.

On August 23, 2004, OMB issued FISMA reporting instructions to the agencies.[7] This guidance reinforces the requirement for agencies to test and evaluate their security controls annually, at a minimum, to promote a continuous process of assessing risk and ensuring that security controls maintain risk at an acceptable level. Further, agencies' 2004 FISMA reporting guidance requires them to report on their incident-detection and incident-handling procedures, including methods used to mitigate information technology security risk and internal and external incident-reporting procedures. OMB also issued a memorandum to the agencies on personal use policies and "file sharing" technology.[8] In this guidance, OMB directs agencies to establish or update their personal use policies and to train employees on these policies to "ensure that all individuals are appropriately trained in how to fulfill their security responsibilities."

FISMA Requires NIST to Provide Guidance on Protecting Federal Systems

FISMA also requires NIST to establish standards, guidelines, and requirements to help agencies improve the posture of their information security programs.[9] NIST has issued several publications relevant to assisting agencies in protecting their systems against emerging cybersecurity threats. For instance, Special Publication 800-61, *Computer Security Incident Handling Guide*, advises agencies to establish an incident-response capability that includes establishing guidelines for communicating with outside parties regarding incidents, including law enforcement agencies, and also discusses handling specific types of incidents, including malicious code and unauthorized access. Additionally, NIST Special Publication 800-68 (Draft), *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, describes configuration recommendations that focus on deterring malware, countermeasures against security threats with malicious payload, and specific recommendations for addressing spyware.

[7] Office of Management and Budget, *Memorandum for Heads of Executive Departments and Agencies: FY 2004 Reporting Instructions for the Federal Information Security Management Act*, Joshua B. Bolten, Director, M-04-25, August 23, 2004.

[8] Office of Management and Budget, *Memorandum for Chief Information Officers: Personal Use Policies and 'File Sharing' Technology,* Karen S. Evans, Administrator, IT and E-Gov, M-04-26, September 8, 2004.

[9] NIST had previously been required to develop computer security standards by the Computer Security Act of 1987, Public Law 100-235, which was superseded by FISMA.

NIST has also issued guidance on various controls that agencies can implement, such as *Guidelines on Electronic Mail Security*[10] and *Guidelines on Securing Public Web Servers*.[11] The electronic mail security guide discusses various practices that should be implemented to ensure the security of a mail server and the supporting network infrastructure, such as

- organizationwide information systems security policy;
- configuration/change control and management;
- risk assessment and management;
- standardized software configurations that satisfy the information systems security policy;
- security awareness and training;
- contingency planning, continuity of operations, and disaster recovery planning; and
- certification and accreditation.[12]

In its publication on securing public Web servers, NIST discusses methods that organizations can take to secure their Web servers. This includes standard methods such as hardening servers, patching systems, testing systems, maintaining and reviewing logs, backing up, and developing a secure network. It also includes selecting what types of active content

[10] NIST, *Guidelines on Electronic Mail Security,* Special Publication 800-45 (Gaithersburg, Md.: September 2002).

[11] NIST, *Guidelines on Securing Public Web Servers*, Special Publication 800-44 (Gaithersburg, Md.: September 2002).

[12] *Certification* is the comprehensive evaluation of the technical and nontechnical security controls of an IT system that provides the information necessary for a management official to formally declare that an IT system is approved to operate at an acceptable level of risk. This management approval, or *accreditation*, is the authorization of an IT system to process, store, or transmit information, and it provides a form of quality control and challenges managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements. The accreditation decision is the implementation of an agreed-upon set of management, operational, and technical controls, and by accrediting the system, the management office accepts the risk associated with it.

technologies to use (e.g., JavaScript and ActiveX), what content to show, how to limit Web bots (i.e., bots that scan Web pages for search engines), and discusses authentication and cryptographic applications. The publication also notes the importance of analyzing logs, in order to notice suspicious behavior and intrusion attempts.

Further, NIST is currently drafting a guide on malware that includes a taxonomy of malware, incident prevention, incident response, and future malicious threats to assist agencies in improving the security of their systems and networks from current and future malware threats. NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, emphasizes the importance of technical, managerial, and operational security controls to protect the confidentiality, integrity, and availability of a system and its information. The security controls defined in the publication were recommended for implementation in the context of a well-defined information security program, which should include periodic risk assessments and policies and procedures based on risk assessments.[13] For a comprehensive listing of NIST publications that can be used to protect agency networks and systems against emerging threats, see appendix I.

Additionally, agencies are required by various other laws to protect specific types of information, such as programmatic, personal, law enforcement, and national security data. For example, agencies are required to protect employee and personal data under the Privacy Act of 1974, and the IRS is mandated to protect individuals' personal tax records.[14] Further, security-sensitive transportation and other critical infrastructure information is required to be protected under a variety of laws. If this information is made available to or accessed by an attacker, agencies may be failing to implement the necessary management controls to protect against unauthorized access. Securing federal systems and the information that they process and store is essential to ensuring that critical operations and missions are accomplished.

[13] *NIST Special Publication 800-53* defines risk assessments to include the "magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization."

[14] 26 U.S.C. § 6103; Taxpayer Browsing Protection Act, Public Law 105-35, August 5, 1997, 26 U.S.C. § 7213A.

Other Laws and Policies Highlight Cybersecurity as a National Priority

The Homeland Security Act of 2002 established key roles in cybersecurity for DHS.[15] In 2002 the Homeland Security Act created DHS, which was given responsibility for developing a national plan; recommending measures to protect the critical infrastructure; and collecting, analyzing, and disseminating information to government and private-sector entities to deter, prevent, and respond to terrorist attacks. The act also increased penalties for fraud and related criminal activity performed in connection with computers. Additionally, the act charged DHS with providing state and local government entities and, upon request, private entities that own or operate critical infrastructure, with

- analysis and warnings concerning vulnerabilities and threats to critical infrastructure systems,
- crisis management support in response to threats or attacks on critical information systems, and
- technical assistance with respect to recovery plans to respond to major failures of critical information systems.

The President's National Strategy to Secure Cyberspace was issued on February 14, 2003, to identify priorities, actions, and responsibilities for the federal government as well as for state and local governments and the private sector, with specific recommendations for action by DHS. This strategy established priorities for improving analysis awareness, threat reduction, and federal agency cybersecurity. It also identified the reduction and remediation of software vulnerabilities as a critical area of focus. Specifically, the strategy identifies the need for

- a better-defined approach on disclosing vulnerabilities, to reduce their usefulness to hackers in launching an attack;
- creating common test beds for applications widely used among federal agencies;
- establishing best practices for vulnerability remediation in areas such as training, use of automated tools, and patch management implementation processes;

[15] Public Law 107-296, November 25, 2002.

- enhanced awareness and analysis for identifying and remedying cyber vulnerabilities and attacks; and

- improved national response to cyber incidents and reduced potential damage from such events.

Homeland Security Presidential Directive 7 defined responsibilities for DHS, sector-specific agencies, and other departments and agencies to identify, prioritize, and coordinate the protection of critical infrastructure to prevent, deter, and mitigate the effects of attacks. The Secretary of Homeland Security is assigned several responsibilities, including establishing uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors.

Homeland Security Presidential Directive 5 instructed the Secretary of Homeland Security to create a new National Response Plan; this plan, completed in December 2004, was designed to align federal coordination structures, capabilities, and resources into a unified, national approach toward incident management. One component of the plan is the Incident Annexes, which address situations requiring specialized application of the plan, such as cyber, biological, and terrorism incidents. Specifically, the Cyber Incident Response Annex established procedures for a multidisciplinary, comprehensive approach to prepare for, remediate, and recover from cyber events of national significance that impact critical national processes and the economy. Key agencies given responsibilities for securing cyberspace and coordinating incident response include DHS and the Departments of Defense and Justice.

The USA PATRIOT Act increased the Secret Service's role in investigating fraud and related activity in connection with computers. In addition, it authorized the Director of the Secret Service to establish nationwide electronic crimes task forces to assist law enforcement, the private sector, and academia in detecting and suppressing computer-based crime; increased the statutory penalties for the manufacturing, possession, dealing, and passing of counterfeit U.S. or foreign obligations; and allowed enforcement action to be taken to protect our financial payment systems while combating transnational financial crimes directed by terrorists or other criminals.

Recent Legislation Targets Spam, Phishing, and Spyware to Deter Cybercrime

The growing attention of the significant problems caused by spam, phishing, and spyware has resulted in legislation that imposes civil and criminal penalties to deter cybercrime. The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003, the first federal law addressing the transmission of commercial electronic messages, went into effect on January 1, 2004.[16] This act did not ban unsolicited commercial e-mail, but, rather, established parameters for distributing it, such as requiring that commercial e-mail be identified as advertisement and include the sender's valid physical postal address. It prohibits, among other actions,

- the use of deceptive subject headings;
- the use of materially false, misleading, or deceptive information in the header or text of the e-mail;
- transmitting e-mail to accounts obtained through improper or illegal means; and
- sending e-mail through computers accessed without authorization.

The act also required labels on sexually oriented material and an opt-out mechanism that prohibits the sender from transmitting commercial e-mail to the recipient more than 10 days after the recipient opts out. Further, it established civil and criminal penalties, including fines of up to $6 million and a maximum prison term of 5 years. This act was intended to deter spammers from distributing unsolicited commercial e-mail but, according to media sources, has received criticism for its lack of enforceability.

The following list highlights civil and criminal prosecutions at the federal and state level under the CAN-SPAM Act in 2004:

- On March 20, four major Internet service providers filed the first lawsuits under the CAN-SPAM Act.
- In April, Michigan conducted the first criminal prosecution under the CAN-SPAM Act, and charged four men with sending out hundreds of

[16] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act of 2003), December 16, 2003 (Public Law 108-187).

thousands of fraudulent, unsolicited commercial e-mail messages advertising a weight-loss product.

- In September, the “wireless spammer” became the first person convicted under the CAN-SPAM Act.

States have also developed their own legislation to combat these threats. According to the National Conference of State Legislatures, 36 states had enacted legislation regulating unsolicited commercial e-mail. However, some or all of their provisions may be pre-empted by the CAN-SPAM Act.[17]

The Fair and Accurate Credit Transaction Act of 2003[18] provided additional provisions to protect consumers against forms of identity theft, which includes phishing. However, increased awareness and interest among legislators and growing recognition that current law may not sufficiently respond to phishing and spyware have propelled the introduction of phishing and spyware bills during the 109th Congress:

- The SPY ACT (Securely Protect Yourself Against Cyber Trespass), H.R. 29, introduced by Representative Mary Bono on January 4, 2005, details specific actions that would be deemed unlawful if performed by anyone who is not the owner or authorized user of a protected computer, such as taking control of the computer, manipulating the computer’s settings, installing and deleting programs, collecting personally identifiable information through keyloggers,[19] and others. It also would prohibit the collection of certain information without notice and consent from the user, and would require software to be easy to uninstall. The Federal Trade Commission would be charged with enforcing the act with civil penalties set for various violations. This bill was originally introduced during the last Congress and was approved by the House Committee on Energy and Commerce.

[17] Section 8(b)(1) of the CAN-SPAM Act states: “This Act supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.”

[18] Public Law 108-159, December 4, 2003.

[19] Keyloggers have the capability to store all characters typed at the keyboard.

- The I-SPY (Internet-Spyware) Prevention Act, H.R.744, introduced by Representative Bob Goodlatte on February 10, 2005, would deem as a criminal offense any intentional unauthorized access, including access exceeding authorization, of a computer that causes a computer program or code to be copied onto the computer for advancement of another federal criminal offense or intentional obtainment or transmission of "personal information" with the intent of injuring or defrauding a person or damaging a computer. It would also incriminate the intentional impairment of the security protections of a computer. The bill imposes prison terms of up to 5 years and also authorizes $10 million to the Department of Justice to combat spyware and phishing scams. The bill was referred to the House Committee on the Judiciary.

- The Anti-phishing Act of 2005, S. 472, introduced on February 28, 2005, by Senator Patrick Leahy, would impose penalties for phishing and pharming.[20] The bill would prohibit the creation or procurement of a Web site or e-mail message that falsifies its legitimacy and attempts to trick the user into divulging personal information with the intent to commit a crime involving fraud or identify theft. This bill would allow prosecutors to seek fines of up to $250,000 and jail terms of up to 5 years. The bill has been referred to the Judiciary Committee prior to action by the full Senate.

- The Anti-phishing Act of 2005, H.R. 1099, introduced on March 3, 2005, by Representative Darlene Hooley, would criminalize phishing scams and certain other federal or state crimes of Internet-related fraud or identity theft, including the creation of a Web site that fraudulently represents itself as a legitimate online business. The bill includes criminal penalties of fines and/or up to 5 years of imprisonment. The bill was referred to the House Committee on the Judiciary.

- The Software Principles Yielding Better Levels of Consumer Knowledge (SPY BLOCK) Act, S. 687, introduced on March 20, 2005, by Senator Conrad Burns, would prohibit a variety of surreptitious practices that result in spyware and other unwanted software being placed on

[20] Pharming redirects a user to a spoofed Web site by "poisoning" the local domain name server (DNS). Poisoning a DNS server involves changing the specific record for a domain, which results in sending the user to a Web site different from the one intended, unbeknownst to the user. This type of attack involves Trojan horses, worms, or other technologies that attack the browser address bar, thus redirecting the user to a fraudulent Web site when the user types in a legitimate address.

consumers' computers. The bill also includes criminal penalties for certain unauthorized computer-related activities, such as fines and/or up to 5 years of imprisonment for the illicit indirect use of protected computers. The bill was referred to the Senate Committee on Commerce, Science, and Transportation.

Objectives, Scope, and Methodology

Our objectives were to determine (1) the potential risks to federal information systems from emerging cybersecurity threats such as spam, phishing, and spyware; (2) the 24 Chief Financial Officers (CFO) Act agencies' reported perceptions of these risks and their actions and plans to mitigate them; (3) government and private-sector efforts to address these emerging cybersecurity threats on a national level, including actions to increase consumer awareness; and (4) governmentwide challenges to protecting federal information systems from these emerging cybersecurity threats.

To determine the potential risks to federal systems from emerging cybersecurity threats, we first determined effective mitigation practices by conducting an extensive search of professional information technology security literature. In addition, we met with vendors of commercial antispam, antiphishing, and antispyware tools to discuss and examine their products' functions and capabilities. We also reviewed research studies and reports about these emerging cybersecurity threats. Further, with the assistance of our chief information officer (CIO), we conducted a spyware test to determine specific risks of spyware, including the types of Web sites that distribute spyware, the types of spyware that can be installed, and the types of sensitive information that can be relayed to a third party.

For our spyware test, we created a laboratory of six workstations networked together and connected to the Internet. All six computers were identically configured on the Microsoft Windows XP operating system. One group of computers (three machines) served as the control group (i.e., knowledgeable user), and the other group served as the test group (i.e., uneducated user). Each computer within the control and test groups was set up with a different Web browser. Specifically, within each group, one computer had Microsoft's Internet Explorer installed, the second had Mozilla Firefox installed, and the third had Netscape Navigator installed.

Testers ran a series of nine sessions on each machine using its respective Web browser. Each session consisted of navigating various groups of selected Web sites. After visiting a group of Web sites, we then ran five antispyware tools to detect spyware that may have been installed while visiting those sites. The testers on each computer visited the same Web sites, in the same order, and within the same time frame. The testers were provided with respective rules of behavior when visiting these sites using the control and test group computers (e.g., whether to click on banners, run independent code, install browser add-ons, etc.). The selected groups of Web sites included typical work-related and nonwork-related sites. The selected sample of sites was based on the following factors:

- Web sites that team members had visited for this engagement, including the Web sites for each of the 24 CFO Act agencies;

- government and personnel Web sites for federal employees;

- nonwork-related Web sites as selected by team members; and

- corroboration by reports generated from our CIO department's Web-filtering tool.

From among the identified sites that met these criteria, we used our professional judgment and selected the following Web site groups: (1) government agencies/services, (2) news media, (3) streaming media, (4) financial institutions/e-banking, (5) gambling, (6) games, (7) personals/dating, (8) shopping, and (9) Web search. After our 2-week test period was concluded, we analyzed log data and formed general conclusions about the security risks and effects of the spyware that was downloaded from our Web site navigations.

To determine the 24 CFO Act agencies' reported perceptions of the risks from spam, phishing, and spyware and their actions and plans to mitigate them, we developed a series of questions about emerging cybersecurity threats including spam, phishing, and spyware that were incorporated into a Web-based survey instrument. We pretested our survey instrument at two federal departments and internally at GAO through our CIO. For each agency to be surveyed, we identified the CIO office, notified each of our work, and distributed a link to access the Web-based survey instrument to each via e-mail. In addition, we discussed the purpose and content of the survey instrument with agency officials when requested. All 24 agencies responded to our survey. We did not verify the accuracy of the agencies' responses; however, we reviewed supporting documentation that agencies provided to validate their responses. We contacted agency officials when necessary for follow-up information. We then analyzed agency responses to determine agencies' perception of risks from spam, phishing, spyware, and other malware, as well as their practices in addressing these threats.

Although this was not a sample survey, and, therefore, there were no sampling errors, conducting any survey may introduce errors, commonly referred to as nonsampling errors. For example, difficulties in how a particular question is interpreted, in the sources of information that are available to respondents, or in how the data are entered into a database or were analyzed can introduce unwanted variability into the survey results. We took steps in the development of the survey instrument, the data collection, and the data analysis to minimize these nonsampling errors. For example, a survey specialist designed the survey instrument in collaboration with subject-matter experts. Then, it was pretested to ensure that the questions were relevant, clearly stated, and easy to comprehend. Because this was a Web-based survey, 23 of the 24 respondents entered their answers directly into the electronic questionnaire, thereby eliminating the need to have much of the data keyed into a database and thus minimizing an additional potential source of error. For the remaining agency, which provided a separate file of its survey responses, the data entry was traced and verified.

To determine the government and private-sector efforts under way to address spam, phishing, and spyware on a national level as well as the governmentwide challenges to protecting against these threats, we conducted literature searches, reviewed available federal and private-sector documentation, and solicited agencies' input on incident reporting in our survey. In addition, we met with security experts in the private sector and federal officials from homeland security, law enforcement, and the intelligence community to discuss their experiences, practices, and challenges in addressing these threats.

We conducted our work in Washington, D.C., from September 2004 through March 2005, in accordance with generally accepted government auditing standards.

Chapter 2

Emerging Cybersecurity Threats to Federal Agencies

Federal agencies are facing a set of emerging cybersecurity threats that are the result of changing sources of attack, increasingly sophisticated social engineering techniques designed to trick the unsuspecting user into divulging sensitive information, new modes of covert compromise, and the blending of once distinct types of attack into more complex and damaging forms.

Spam, Phishing, and Spyware: Emerging Cybersecurity Threats

Spam, phishing, and spyware are examples of emerging threats that are becoming more prominent. Advances in antispam measures have caused spammers to evolve their techniques to bypass detection. Also, the frequency and sophistication of phishing attacks increased rapidly in the past year. Further, spyware has proven to be difficult to detect and remove.

Spam Delivers Unwanted Content to Organizations and Employees

For several years, the distribution of unsolicited commercial e-mail—commonly referred to as spam—has been a nuisance to organizations, inundating them with e-mail advertisements for products, services, and inappropriate Web sites. The Anti-Spam Technical Alliance reports that while spam has been an annoyance to Internet users for many years, the spam nuisance today is significantly worse, both in the quantity and the nature of the material received. Experts have stated that spam makes up over 60 percent of all e-mail.

Two fundamental issues underscore the spam problem. First, spam is a profitable business. Experts have commented that unsolicited commercial e-mail continues to be a problem because it is profitable: not only is sending spam inexpensive, but a percentage of targeted consumers open the messages, and some purchase the advertised items and services. Second, e-mail messages do not contain enough reliable information to enable recipients to determine if the message is legitimate or forged. As a result, spammers can forge an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.

Advances in antispam measures have caused spammers to make their techniques more sophisticated to bypass detection and filtration. Some of these methods include inserting random text, using alternate spellings, using various characters that look like letters, disguising the addresses in e-mails, and inserting the text as an image so that the filter cannot read it. Further, compromised systems are regularly being used to send spam, with experts estimating that such systems deliver 40 percent of all spam. Not only has this made it more difficult to track the source of spam, but the potential for financial gain has resulted in spammers, malware writers, and hackers combining their respective methods into a blended attack.

Phishing Combines "Social Engineering" with Internet Technology to Commit Fraud

Phishing is a high-tech scam that frequently uses spam or pop-up[1] messages to deceive people into disclosing their credit card numbers, bank account information, Social Security number, passwords, or other sensitive information.[2] The frequency and sophistication of phishing attacks increased rapidly in 2004. As defined by the FTC,[3] phishers send an e-mail or pop-up message that claims to be from a business or organization that users deal with—for example, Internet service providers, banks, online payment services, or government agencies. The message typically says that users need to "update" or "validate" their account information, and might threaten some dire consequence if users do not respond. The message directs users to a Web site that looks just like a legitimate organization's site, but is not. The fraud tricks users into divulging personal information so the phishers can steal their identity. Phishing is conducted through spam, malware, and blended threats, as well as through e-mail.

Phishing scams use a combination of social engineering and technical methods to deceive users into believing that they are communicating with an authorized entity. In social engineering, an attacker uses human interaction—or social skills—to obtain or compromise information about an organization or its computer systems. In addition to using their social skills, phishers use technical methods to create e-mail and Web sites that appear legitimate, often copying images and the layout of the actual Web site that is being imitated. Further, phishers exploit software and system vulnerabilities to reinforce users' perceptions that they are on a legitimate Web site. For example, phishers use various methods to cause the

[1] A type of window that appears on top of (over) the browser window of a Web site that a user has visited. Pop-up advertisements are used extensively in advertising on the Web, though advertising is not the only application for pop-up windows.

[2] The word "phishing" comes from the analogy that Internet scammers are using e-mail bait to fish for passwords and financial data from the sea of Internet users. The term was coined in 1996 by hackers who were stealing America Online (AOL) accounts by scamming passwords from unsuspecting AOL users. Since hackers have a tendency to replacing "f" with "ph," the term phishing was derived. The term has evolved over the years to include not only obtaining user account details but access to all personal and financial data.

[3] FTC Consumer Alert, *How Not to Get Hooked by a 'Phishing' Scam*, June 2004.

browser's Web address display to show a legitimate site's address instead of the actual Web address of the fraudulent site. Phishers also use browser scripting languages to position specially created graphics containing fake information over key areas of a fraudulent Web site, such as covering up the real address bar with a fake address. In addition, phishers can fake the closed lock icon on browsers that is used to signify that a Web site is protecting sensitive data through encryption.[4]

"Pharming" is another method used by phishers to deceive users into believing that they are communicating with a legitimate Web site. Pharming uses a variety of technical methods to redirect a user to a spoofed Web site when the user types in a legitimate Web address. For example, one pharming technique is to "poison" the local domain name server (DNS), which is an Internet service that translates domain names like www.congress.gov into unique numeric addresses.[5] Poisoning a DNS involves changing the specific record for a domain, which results in sending users to a Web site very different from the one they intended to access—without their knowledge. DNS poisoning can also be accomplished by exploiting software vulnerabilities. Other pharming methods use malware to redirect the user to a fraudulent Web site when the user types in a legitimate address.

A growing trend in phishing scams is the use of malware to steal information from users. These scams depend on system characteristics (e.g., existence of specific vulnerabilities, lack of security controls) to deploy payload mechanisms, such as viruses and Trojan horses. Social engineering is used to convince users to open an e-mail attachment or visit a malicious Web site, causing the malware to install. The malware could record users' account details when they visit an online banking Web site, and the captured information is then sent to the phishers.

[4] The lock icon is associated with the Secure Socket Layer (SSL) Web security technology that utilizes security certificates. For a closed lock icon to appear on a Web site, phishers can use fraudulent security certificates or even graphically replicate the closed lock image.

[5] The Internet domain name system is a vital aspect of the Internet that works like an automated telephone directory, allowing users to reach Web sites using easy-to-understand domain names, instead of the string of numbers that computers use when communicating with each other.

Spyware Gathers Information Surreptitiously

A widely accepted definition of spyware does not currently exist; various definitions and descriptions of spyware have been proposed by security experts and software vendors, and the definition of spyware has even varied among proposed legislation. These definitions vary based on factors such as whether the user has consented to the downloading of the software to his or her computer, the types of information it collects, and the nature and extent of the harm caused. However, the gathering and dissemination of information by spyware can be grouped into two primary purposes: advertising and surveillance.

Spyware can be used to deliver advertisements to users, often in exchange for the free use of an application or service. It can collect information such as a user's Internet Protocol address, Web surfing history, online buying habits, e-mail address, and software and hardware specifications. It often provides end users with targeted pop-up advertisements based on their Web-surfing habits. Spyware has also been known to change browser domain name system settings to redirect users to alternate search sites filled with advertisements. Some spyware places highlighted advertising links over keywords on normal Web pages.

Other spyware is used for surveillance and is designed specifically to steal information or monitor information access. It may range from keyloggers to software packages that capture and transmit records of virtually all activity on a system.

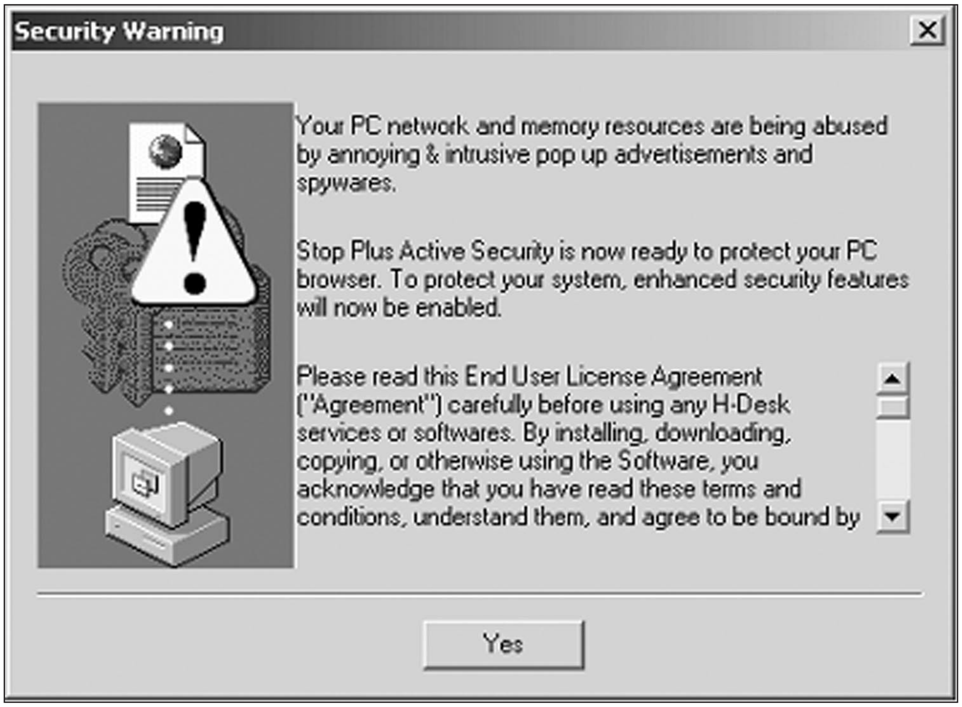
Software that is used to advertise or collect information has both legitimate and illegitimate uses. Various experts classify software used for advertising as either adware or spyware, depending on the previously mentioned factors. Additionally, surveillance applications can be used by organizations as legitimate security devices. This further underscores the difficulty in defining spyware. The FTC defines spyware as "software that gathers information about a person or an organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over computers without the consumer's knowledge."[6] For the purposes of this report, we are substituting the word "user" for "consumer."

[6] Transcript from FTC's Public Workshop, *Monitoring Software on Your PC: Spyware Adware, and Other Software* (Washington, D.C.: Apr. 19, 2004).

Spyware Uses Deceptive Techniques to Install onto Systems

Users are deceived into installing spyware onto their systems because spyware authors and distributors use various social engineering techniques to induce users to install their spyware. For example, users could receive pop-up advertisements claiming that their systems are infected with spyware and advising them that they should download the displayed software to remove the spyware; however, instead of downloading removal software, users end up downloading spyware itself. See figure 1 for an example of such a deceptive pop-up window.

Figure 1: Deceptive Pop-Up Advertisement for Software Purported to Provide Antispyware Protection; It Is Actually Spyware Itself



Your PC network and memory resources are being abused by annoying & intrusive pop up advertisements and spywares.

Stop Plus Active Security is now ready to protect your PC browser. To protect your system, enhanced security features will now be enabled.

Please read this End User License Agreement ("Agreement") carefully before using any H-Desk services or softwares. By installing, downloading, copying, or otherwise using the Software, you acknowledge that you have read these terms and conditions, understand them, and agree to be bound by

Source: Internet Security Systems.

Security experts have noticed spyware that presents a user with a pop-up asking if the user wants to install the application; however, regardless of what the user chooses, spyware is installed. Further, peer-to-peer software—programs that facilitate file sharing—are often packaged with numerous spyware applications. While the behavior of the bundled spyware is often mentioned in the end-user license agreement (EULA), the EULA is typically long and confusing. EULAs often use large text print in small windows; in some cases users would have to page down more than 100 times to read it all. Additionally, the descriptions of what the application installs are often hidden or incomplete.

While some spyware tricks users into installing, other spyware spreads by exploiting security vulnerabilities and low security settings in e-mail and Web browsers—for example, when a user on a system with known software flaws opens a malicious e-mail or visits a malicious Web site. Further, low-security settings of Web browsers may allow malicious scripts to install spyware onto systems. Additionally, some variants of worms and viruses install spyware after they have infected a system. Persons with access can also physically install spyware onto a system.

Spyware is Difficult to Detect, Remove

Spyware is difficult to detect by users. A study by the National Cyber Security Alliance and America Online found that 89 percent of users who were found to have spyware on their systems were unaware that it was there.[7] Even if users notice changes to their systems, they may not realize what caused the change and may not consider that there is any risk—thus the incident may go unreported. Additionally, browser helper objects[8] can be especially difficult for users to detect because their operations are generally invisible to users. Spyware also employs techniques to avoid detection by antivirus and antispyware applications that search for specific "signature strings" that characterize known malicious code.

Beyond the problem of detection, the removal of spyware is an additional difficulty. It typically does not have its own uninstall program, forcing users to manually remove spyware or use a separate tool. Many spyware programs install numerous files and directories and make multiple changes to key system files. Some spyware will install multiple copies of itself onto a system, so that when a user removes one copy, another copy reinstalls itself. Spyware has also disabled antivirus and antispyware applications, as well as firewalls, to avoid detection.

[7] America Online, Inc. and National Cyber Security Alliance (NCSA), *AOL/NCSA Online Safety Study* (Washington, D.C.: Oct. 25, 2004).

[8] Browser helper objects (BHO) are small programs that run automatically every time an Internet browser is launched. Generally, a BHO is placed on the system by another software program and is typically installed by toolbar accessories. It can track usage data and collect any information displayed on the Internet.

Spam, Phishing, and Spyware Are Threats to Federal Agencies

Agencies face significant risks from these emerging cybersecurity threats. Spam consumes employee and technical resources and can be used as a delivery mechanism for malware and other cyber threats. Agencies and their employees can be victims of phishing scams. Further, spyware puts the confidentiality, integrity, and availability of agency systems at risk.

Spam Consumes Resources and Is Used as a Delivery Mechanism for Other Forms of Attacks

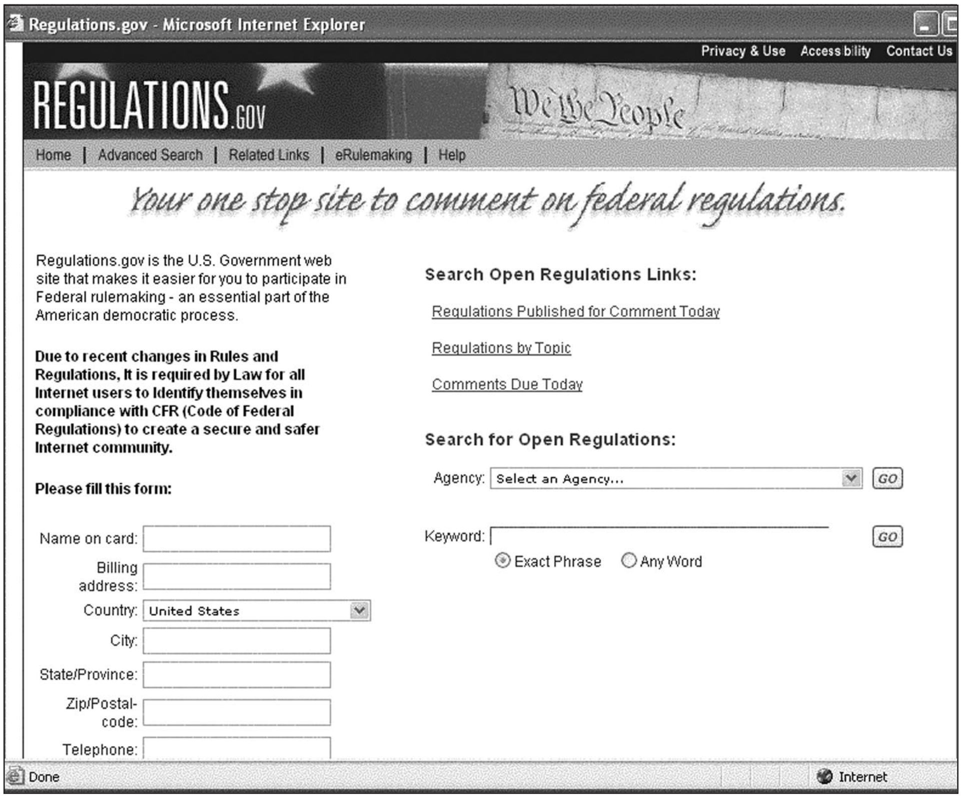
Spam is a growing security problem for organizations, users, and networks because it has the potential to breach the confidentiality, integrity, and availability of information systems when used as a delivery mechanism for other threats. While spam is often used for marketing, it is also used to distribute malware, including viruses, worms, spyware, and Trojan horses, as well as phishing scams. Once delivered, these threats can violate the confidentiality, integrity, and availability of systems. Moreover, spam can be used to cause a denial-of-service attack.[9] Spam may also deliver offensive materials that can create liability concerns for organizations. Further, the sheer quantity of spam hampers productivity, requires technical support, and consumes bandwidth. Spam has made it necessary for organizations to allocate additional resources to manage its risk, including antispam software and increased storage space.

Phishing Can Lead to Identity Theft, Loss of Sensitive Information, and Reduced Trust in E-Government Services

Federal agencies and employees can be victims of phishing scams. We identified two main categories of phishing based on their threats and victims: (1) employee-targeted phishing that is received by employees of agencies and (2) agency-exploiting phishing that spoofs the identity of an agency to facilitate a phishing scam. Although phishing scams have exploited the identities of online financial and auction sites such as US Bank, Citibank, eBay, and PayPal, phishers have also exploited federal agencies and Web portals such as the FBI, FDIC, IRS, and the Regulations.gov Web site (see fig. 2).

[9] A denial-of-service attack is an attack in which one user takes up so much of a shared resource that none of the resources is left for other users. Denial-of-service attacks compromise the availability of the resources.

Figure 2: Image of Fraudulent Web Site Used in the Regulations.gov Phishing Scam


Regulations.gov - Microsoft Internet Explorer
Privacy & Use
Accessibility
Contact Us
REGULATIONS.GOV
We the People
Home | Advanced Search | Related Links | eRulemaking | Help
GO
GO
Done
Internet

Your one stop site to comment on federal regulations.

Regulations.gov is the U.S. Government web site that makes it easier for you to participate in Federal rulemaking - an essential part of the American democratic process.

Due to recent changes in Rules and Regulations, It is required by Law for all Internet users to Identify themselves in compliance with CFR (Code of Federal Regulations) to create a secure and safer Internet community.

Please fill this form:

Name on card:

Billing address:

Country: United States

City:

State/Province:

Zip/Postal-code:

Telephone:

Search Open Regulations Links:

Regulations Published for Comment Today

Regulations by Topic

Comments Due Today

Search for Open Regulations:

Agency: Select an Agency...

Keyword:

● Exact Phrase ○ Any Word

Source: Anti-Phishing Working Group.

A phishing scam can result in the exposure of user access information, which can lead to unauthorized access and the loss and manipulation of sensitive data. Employee-targeted phishing scams can result in the release of personal employee or agency information, such as usernames and passwords. Employees who fall for phishing scams can also become victims of identity theft. Additionally, as a part of a phishing scam, a user could visit a Web site that installs malicious code, such as spyware.

Phishing is a risk to public and private-sector organizations alike. Phishers often pose as reputable organizations such as banks or federal agencies to appear as legitimate requests for information. According to Gartner, Inc., the direct phishing-related loss to U.S. banks and credit card issuers in 2003 is estimated at $1.2 billion.[10] Indirect losses are considered to be much higher, including customer service expenses, account replacement costs, and higher expenses due to customers' decreased use of online services. Consequently, agency-exploiting phishing scams may go beyond the purview of the agency CIO. For example, one agency CIO noted that although he had the ability to apply FISMA-required practices to his agency's systems and networks, the agency's response was not limited to the CIO's actions. He indicated that the agency's public affairs department, federal law enforcement agencies, and Internet service providers were all affected by the phishing scam. Researchers have noted the potential for phishing scams to disrupt the growth of electronic commerce in general. Phishing scams that exploit a federal agency's identity could cause citizens to lose trust in e-government services.

Spyware Threatens the Confidentiality, Integrity, and Availability of Federal Information Systems

Spyware threatens federal information systems by compromising their confidentiality, integrity, and availability through its ability to capture and release sensitive data, make unauthorized changes to systems, decrease system performance, and create new system vulnerabilities. Spyware can allow attackers to obtain sensitive information and gain unauthorized access to sensitive information. Both advertising and surveillance spyware can collect information. Advertising spyware typically collects information such as a user's browsing habits and demographic information to produce targeted advertisements. However, both types of spyware are capable of collecting user names and passwords, personally identifiable information, credit card numbers, e-mail conversations, and other sensitive data. NIST notes that spyware can collect just about any type of information on users that the computer has stored. For example, certain remote administration tools can take control over a Webcam[11] and microphone, capturing both visual and vocal activity.

Spyware can change the appearance of Web sites and modify what pages users see in their Web browsers. For example, spyware can modify search results and forward users to Web sites with questionable content, such as malicious and pornographic sites, potentially resulting in liability risks. In

[10] Gartner, Inc., provides research and analysis on the global information technology industry.

[11] A Webcam is a video camera, usually attached directly to a computer, whose current or latest image is requestable from a Web site.

addition, spyware can change system configurations to make systems more vulnerable to attack by, for example, disabling antivirus and antispyware software and firewalls.

Spyware is often responsible for significant reductions in computer performance and system stability through its consumption of system and network resources. Users have reported dramatic decreases in their computer and Internet performance, which can be attributed to multiple instances of spyware. Network administrators have also noticed a loss of bandwidth as a result of spyware. Additionally, poorly programmed spyware applications can result in application and system crashes. Microsoft estimates that spyware is currently responsible for up to 50 percent of all computer crashes. Further, improper uninstalls of spyware have been known to disable a system's Internet connection, and reductions in the availability of systems and the network could decrease employee productivity.

Spyware creates major new security concerns as malicious users exploit vulnerabilities in spyware to obtain unauthorized system access. If an organization or user does not know that spyware is on the computer, there is effectively no way to address the associated vulnerabilities. For example, spyware often includes, as a part of an update component, capabilities to automatically download and install additional pieces of code without notifying users or asking for their consent, typically with minimal security safeguards. Additionally, researchers at the University of Washington found that in a certain version of spyware, it was possible for attackers to exploit the update feature to install their own malicious code. Spyware can also redirect users to Web sites that infect systems with malicious code or facilitate a phishing scam. Remote administration tools are intended to provide remote monitoring and recording capabilities, but they also provide malicious users with the means to remotely control a machine. Changes to system configurations could allow spyware to not only remain undetected, but also make systems more vulnerable to future attacks from worms, viruses, spyware, and hackers.

Other Threats Are Also Emerging

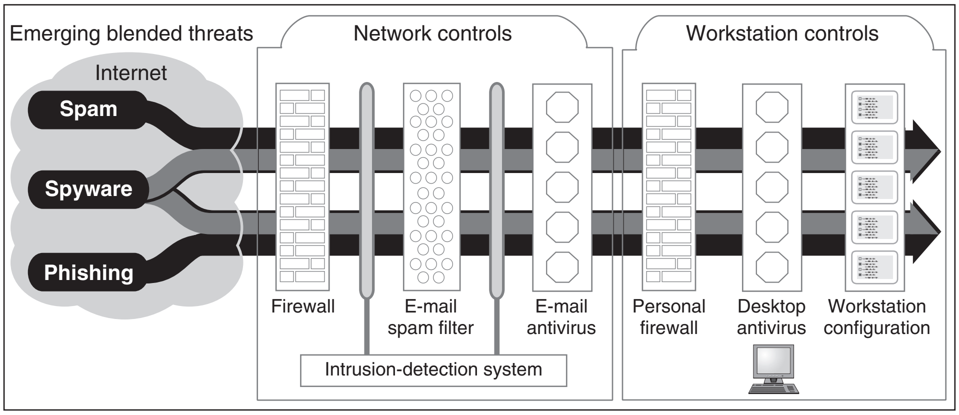
In addition to spam, phishing, and spyware, other threats are also emerging, including the increased sophistication of worms, viruses, and other malware and the increased attack capabilities of blended threats and botnets. Malware continues to threaten the secure operation of federal information systems. The CERT Coordination Center (CERT/CC) reported that 3,780 new vulnerabilities were found in 2004.[12] In recent years, security experts have noted that the time between a released vulnerability and an exploitation is decreasing, so that the average time frame between the announcement of vulnerability and the appearance of associated exploitation code is down to 5.8 days. More than 10,000 new viruses were identified in 2004. Agencies are now faced with the formidable task of patching systems and updating security controls in a timely and appropriate manner.

New forms of worms and viruses pose challenges to the security of networks. Antivirus software provides protection against viruses and worms. However, polymorphic, metamorphic, and entry-point-obscuring viruses are reducing the effectiveness of traditional antivirus scanning techniques. Polymorphic viruses are self-mutating viruses that use encryption. Specifically, a small decoder, which changes periodically, decrypts the viruses' main bodies prior to execution. Metamorphic viruses change the actual code of the virus between replications, resulting in significantly different patterns, thus causing it to be undetected by the signature-based tool. Entry-point-obscuring viruses are making detection more difficult by placing the malicious code in an unknown location. Further, these techniques are often used to infiltrate and hide code in a victim's computer as a base for further criminal activity. Combating these types of viruses requires diligence in maintaining updated antivirus products that employ algorithms to detect these new threats.

Blended threats are an increasing risk to organizations. Security analysts have noticed an increase in the number of blended threats, as well as increasingly destructive payloads. Such threats combine the characteristics of different types of malicious code, such as viruses, worms, Trojan horses, and spyware. The multiple propagation mechanisms often used in blended threats allow them the versatility to circumvent an organization's security in a variety of ways. As a result, blended threats can infect large numbers of systems in a very short time, with little or no human intervention, causing widespread damage very quickly. They can then simultaneously overload system resources and saturate network bandwidth. Figure 3 depicts the ability of some blended threats to bypass security controls. (Other combinations of threats are also possible.)

[12] CERT/CC is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

Figure 3: Blended Threats May Bypass Traditional Security Controls



Source: GAO.

Examples of recent blended threats include MyDoom, Netsky, Sasser, and Sobig. The Sobig worm exemplifies one of the dangers of blended threats. When Sobig successfully infects a computer, it downloads spyware from a Web site, including a keylogger. The keylogger monitors the system for any banking, credit card purchases, or other financial activity and captures user information, passwords, and cookies and sends them back to the authors. Additionally, Sobig downloads an unlicensed copy of the Wingate proxy server, allowing any malicious user who knows the Internet protocol address of the infected machine to channel actions through the system anonymously. Spammers used the proxy to anonymously send unsolicited e-mail.

Security experts have noted an increase in the manipulability of attacks. Malicious users are infecting vulnerable systems with bots, which then allow the users to remotely control the systems.[13] Malicious users can command botnets to distribute spam, phishing scams, spyware, worms, viruses, and launch distributed denial-of-service attacks. For example, last year the Department of Justice reportedly found that botnets on government computers were sending spam. The short vulnerability-to-exploitation window makes bots particularly dangerous; once a means of exploiting a vulnerability is known, the owner of the botnet can quickly and easily upgrade the bots, which can then scan target systems for the

[13] Machines compromised with bots are often referred to as “zombies.” Multiple machines under a user’s control are referred to as a “bot network” or “botnet.”

vulnerability in question, vastly increasing the speed and breadth of potential attacks.

Many Agencies Do Not Fully Identify and Address Security Risks of Spam, Phishing, and Spyware

Agencies' responses to our survey indicated varying perceptions of the risks of spam, phishing, and spyware. Many agencies have not fully addressed the risks of emerging cybersecurity threats as part of their agencywide information security programs, which include FISMA-required elements such as performing periodic assessments of risk; implementing security controls commensurate with the identified risk; ensuring security-awareness training for agency personnel; and implementing procedures for detecting, reporting, and responding to security incidents. An effective security program can assist in agency efforts to mitigate and respond to these emerging cybersecurity threats.

Agencies' Responses Indicated Varying Perceptions of Risks and Effects of Emerging Threats

According to agency responses, most agencies (19 of 24) identified nonsecurity effects from spam. They identified several incidents of spam that reduced their systems' performance and the productivity levels of their users and their information technology staff. Other costs associated with spam include the use of network resources and the costs of filtering e-mail. Of these 19 agencies, 14 reported that spam consumed network bandwidth used to transmit messages or consumed disk storage used to store messages. However, only 1 agency identified the risk that spam presents for delivering phishing, spyware, and other threats to their systems and employees.

Also, 14 of 24 agencies reported that phishing had limited to no effect on their systems and operations. Two agencies indicated that they were unaware of any phishing scams that had specifically targeted their employees, while 6 agencies reported a variety of effects, including the increased need for help desk support and instances of compromised credit card accounts.[1] Further, in a follow-up discussion, an agency official noted that phishing is primarily a personal risk to employees and that employees who fall victim to phishing scams could face personal security issues related to identity theft that could reduce their productivity.

In addition, 5 agencies reported that spyware had minimal to no effect on their systems and operations, while 11 noted that spyware caused a loss of employee productivity or increased usage of help desk support. Of the remaining 4 agencies that reported spyware effects, 2 noted the decreased ability for their users to utilize agency systems: 1 agency noted that users

[1] The remaining two agencies did not provide a response to our survey question regarding the risks of phishing to agency systems and operations.

had been unable to connect to an agency network, while the other indicated that users had experienced a denial of service after an antispyware tool had been implemented. Finally, 1 agency reported the costs associated with developing and implementing antispyware tools, and another stated that spyware was simply a nuisance to its users.

Agencies' Information Security Programs Do Not Fully Address Emerging Cybersecurity Threats

As discussed in chapter one, FISMA charges agencies with the responsibility to create agencywide information security programs that include periodic assessments of risk; implement security controls that are commensurate with the identified risk; conduct security awareness training for agency personnel, including contractors; and implement procedures for detecting, reporting, and responding to security incidents. However, according to their survey responses, agencies have not fully addressed the risks of emerging cybersecurity threats as part of their agencywide security programs.

Most Agencies Did Not Assess the Risk of Phishing Scams

While risk assessments are a key information security practice required by FISMA, most surveyed agencies reported not performing them to determine whether the agency name or its employees are susceptible to phishing scams. Of the 24 agencies we surveyed, 17 indicated that they have not assessed this risk. In addition, 14 agencies reported that at least one employee experienced a phishing scam. By not performing risk assessments, agencies are vulnerable to unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of their respective agencies. In fact, several agencies have had their identities exploited in phishing scams, as summarized in table 2.

Table 2: Federal Entities Exploited by Emerging Cybersecurity Threats

Entity	Exploit
Immigration and Customs Enforcement (ICE) (DHS)	E-mail claiming to be from an ICE agent referred users to ICE's official Web site in an effort to steal money from relatives of U.S. soldiers killed in Iraq.
FBI (Department of Justice)	Spoofed e-mail claiming to be from the FBI requested users to verify their information to avoid further investigation. The Web address contained in the e-mail was deceptive and led to a fraudulent Web site.
FDIC	Spoofed e-mail forwarded users to a fraudulent Web site that used FDIC's logos, fonts, and colors to request users to submit bank account information, as well as credit card and Social Security numbers.
IRS (Department of the Treasury)	Spoofed e-mail claiming to be from the IRS and an official-looking Web site were used in an attempt to trick recipients into disclosing their personal and financial data.
Bureau of the Public Debt (Department of the Treasury)	Spoofed e-mail from what appeared to be Public Debt e-mail addresses contained links to rogue Web sites. These sites claimed to be legitimate private commercial banking Web sites and attempted to obtain financial information from individuals.
Operators of the regulations.gov Web site: Environmental Protection Agency, Food and Drug Administration, Government Printing Office, and National Archives and Records Administration/Office of the Federal Register	Regulations.gov is a Web site where consumers can participate in government rulemaking by submitting comments. The e-mail included a link to a Web site that mimics regulations.gov and asked readers to provide their personal and financial information.
State Department	Spoofed e-mail claiming to be from security-abroad@state.gov and maintained by the department's Bureau of Public Affairs attempted to dupe recipients into clicking a link to download an executable file that would change access to specific folders and files.

Source: GAO analysis of agency data.

NIST Guidance Available to Assist Agencies in Their Assessment of Risk

NIST has issued guidance to agencies on risk management and has developed a security self-assessment guide. NIST's *Risk Management Guide for Information Technology Systems*[2] defines risk management as the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. The guide provides a foundation for the development of an effective risk management program for assessing and mitigating risks identified within IT systems. Additionally, NIST's Security Self-Assessment Guide for Information Technology Systems[3] provides a method for agency officials to determine the current status of their information security programs and, where necessary, establish a target for improvement.

[2] NIST, *Risk Management Guide for Information Technology Systems*, Special Publication 800-30 (Gaithersburg, Md.: July 2002).

[3] NIST Special Publication 800-26.

Further, as part of its FISMA requirements, NIST issued its *Standards for Security Categorization of Federal Information and Information Systems*,[4] which establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur that jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

Agencies Noted Challenges in Using Existing Security Controls to Effectively Mitigate Risks of Spam, Phishing, and Spyware

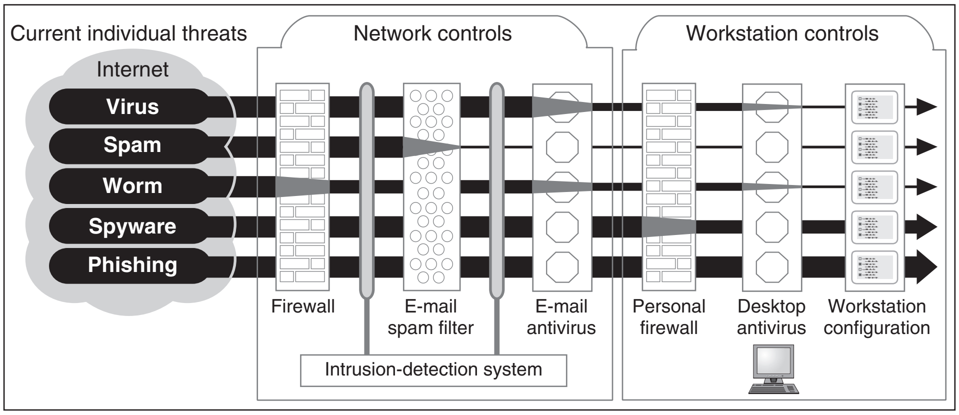
Vendors are increasingly providing automated tools to mitigate the risks of spam, phishing, and spyware at an enterprise level. However, according to several agencies responding to our survey, current enterprise tools to address emerging cybersecurity threats are immature and therefore impede efforts to effectively detect, prevent, remove, and analyze incidents. Officials at the Department of Justice noted that although there was a lack of enterprise software solutions that could rapidly detect and analyze behavioral anomalies, in the absence of a purely technological solution, system administrators could exercise greater control over federal systems by implementing tighter security controls. For example, agencies could limit users' rights to modify and change certain features on their computers. This control could greatly reduce agencies' susceptibility to compromise from these types of exploits. Indeed, one agency noted that they were able to keep most spyware out of their systems by enforcing policy and user privileges at the network level.

Further, we and NIST have advised agencies on how to protect their networks from these threats by using a layered security (defense-in-depth) approach. Layered security implemented within an agency's security

[4] NIST, *Federal Information Processing Standards Publication: Standards for Security Categorization of Federal Information and Information Systems*, FIPS PUB 199 (Gaithersburg, Md.: December 2003).

architectures[5] includes the use of strong passwords, patch management, antivirus software, firewalls, software security settings, backup files, vulnerability assessments, and intrusion detection systems.[6] Figure 4 depicts an example of how agencies can use layered security controls to mitigate the risk of individual cybersecurity threats.

Figure 4: Layered Security Mitigates the Risk of Individual Cybersecurity Threats



Source: GAO.

Agencies Noted the Unreliability of Antispam Tools

Most agencies (20 of 24) reported implementing agencywide approaches to mitigating spam. Enterprise antispam tools are available to filter incoming e-mails. These tools enable agencies to reduce the amount of spam that reaches employees and use various techniques to scan e-mail to determine if it is spam. Filters can also use antivirus technologies to detect malicious code. E-mail services can be outsourced, fully or in part, to companies that

[5] We define security architectures to include enterprise architecture, enterprise security architecture, and network security architecture. Generally speaking, an enterprise architecture connects an organization's strategic plan with program and system solution implementations by providing the fundamental information details needed to guide and constrain implementable investments in a consistent, coordinated, and integrated fashion. For more information on enterprise architectures, see GAO, *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management* (Version 1.1), GAO-03-584G (Washington, D.C.: Apr. 1, 2003).

[6] We previously reported on available technologies to secure federal information systems, including antivirus software, firewalls, and intrusion detection systems. See GAO, *Information Security: Technologies to Secure Federal Systems*; GAO-04-467 (Washington, D.C.: Mar. 9, 2004).

manage the e-mail operations, including filtering for spam, phishing scams, and malware. See appendix II for more detailed information on antispam tools and services.

However, agencies reported concerns that these tools could not be relied upon to accurately distinguish spam from desired e-mails. Some observed that spammers are evolving and adapting their spamming techniques to bypass the filtering rules and signatures that antispam tools are based on. One agency reported that false positives were a larger concern than false negatives, as users place a high priority on receiving all legitimate e-mails and do not accept lost messages as a result of faulty e-mail filtering. Furthermore, the agency reported that outgoing e-mails could be falsely blocked by antispam tools used by the intended recipients. Consequently, federal agencies are challenged to continually monitor and adjust their filtering rules to mitigate false positives and false negatives. Many agencies stressed that the constant evaluation and modification that are required by current spam filtering solutions demand a significant investment in resources.

Agencies Reported Limited Tools to Identify Phishing

Although phishing scams are typically distributed through mass e-mail (much like spam distribution), several agencies reported that limited technical controls are available to effectively scan e-mail in order to identify a phishing message. One agency related challenges in determining how to utilize an automated tool to control employees' Internet browsing behaviors—without also restricting Internet access that is needed to perform job-related functions.

Agencies can also utilize traditional enterprise antispam tools to mitigate the risks from employee-targeted phishing, as these tools are increasingly providing antiphishing capabilities that can also detect and block known phishing scams using content-based or connection-based techniques.

Agencies cannot rely on these tools as a complete solution; because antiphishing tools typically quarantine suspected phishing e-mail, a person must review each quarantined message in order to make a final determination of the message's legitimacy. DHS's Homeland Security Advanced Research Projects Agency recognized the need for additional tools and techniques that defend against phishing and in September 2004 published a solicitation for proposals to research and develop these technologies. The solicitation notes that antiphishing solutions must work for all types of users and, most importantly, for less sophisticated users, who are those most likely to fall for phishing scams. The agency also warned that any technology that requires end-users to change their behavior will face hard challenges and that the solutions must be easily integrated into existing information infrastructure.

Agencies can also take steps to reduce the likelihood of having their identities used to facilitate a phishing scam. For example, organizations can actively search for abuse of their trademarks, logos, and names. These searches typically focus on trademark or copyright infringement, but have also proven useful in proactively discovering phishing scams. However, one federal official noted that agencies are not using Web-crawling[7] tools to proactively identify potential agency-exploiting phishing and felt that the reluctance to use such tools comes, in part, from privacy and legal concerns.

Establishing clear communication practices with customers can also reduce the success rate of phishing scams. Good communication policies reduce the likelihood that consumers will confuse a phishing scam with a legitimate message. Good communication practices include having a consistent look and feel, never asking for passwords or personal information in e-mail, and making e-mail more personalized.

Responding quickly and effectively can reduce the damage of phishing scams. Because phishing scams are typically hosted and operated outside of an organization's network, a response plan to phishing scams will often require cooperation with external entities such as Internet service providers. The response could include shutting down a Web site and preserving evidence for subsequent prosecution of the phishers. Other practices include notifying consumers by e-mail or a Web site warning when an incident occurs to inform consumers about how to respond. Further, experts recommend that organizations contact law enforcement.

Properly secured e-government services could reduce the risk of an agency's identity being used in a phishing scam. Phishers exploit vulnerabilities in the code of Web sites in order to facilitate their scams; secure code reduces the likelihood that an attack of this type will be successful. NIST offers guidance to agencies on how to secure their

[7] A Web-crawling tool is a software program that browses the Internet in a methodical, automated manner and maintains a copy of all the visited pages for later processing.

systems, including Web servers, and considerations that should be made when using active content.[8]

FDIC has made several recommendations that financial institutions and government could consider applying to reduce online fraud, including phishing.[9] FDIC recommends that financial institutions and government consider (1) upgrading existing password-based single-factor customer authentication systems to two-factor authentication; (2) using scanning software to proactively identify and defend against phishing attacks; (3) strengthening educational programs to help consumers avoid online scams, such as phishing, that can lead to account hijacking and other forms of identity theft, and taking appropriate action to limit their liability; and (4) placing a continuing emphasis on information sharing among the financial services industry, government, and technology providers. The further development and use of fraud detection software to identify account hijacking, similar to existing software that detects credit card fraud, could also help to reduce account hijacking.

Agencies Reported Limited Enterprisewide Antispyware Tools

In response to our question on spyware-related challenges, about one-third of surveyed agencies highlighted the immaturity of enterprisewide tools and services that effectively detect, defend against, and remove spyware. Six agencies also emphasized the spyware-related challenges of identifying or detecting incidents.

Traditional security tools, including firewalls and antivirus applications, offer only limited protection against spyware. While firewalls are used to protect a network or a PC from unauthorized access, firewalls are limited in their ability to distinguish spyware-related traffic from other, harmless Web traffic. For example, browser helper objects are not stopped by firewalls, because firewalls see them as Web browsers. Additionally, spyware is typically downloaded by a user onto a system, which enables the spyware to bypass typical firewall protection. However, firewalls can at times detect spyware when it attempts to request access to the Internet.

[8] National Institute of Standards and Technology, *Guidelines on Securing Public Web Servers*, Special Publication 800-44 (Gaithersburg, Md.: September 2002) and *Guidelines on Active Content and Mobile Code*, Special Publication 800-28 (Gaithersburg, Md.: October 2001).

[9] FDIC, *Putting an End to Account-Hijaking Identity Theft*, December 14, 2004.

Antivirus applications have limited capabilities to detect and remove spyware. Antivirus vendors are beginning to include spyware protection as a part of their overall package; however, Gartner, Inc., reports that major antivirus vendors continue to lag on broader threats, including spam and spyware. The behavior of spyware is different from that of viruses, such that antivirus applications could fail to detect spyware. NIST includes antispyware tools as part of its recommended security controls for federal information systems. Antispyware tools detect and remove spyware, block it from running, and can prevent it from infecting systems.

Although desktop antispyware tools are currently available, their use by agencies would cause additional problems, such as difficulties in enforcing user utilization and updating of the tools. Agencies confirmed NIST's recommendation to consider the use of multiple antispyware tools because the technologies have different capabilities and no single tool can detect all spyware.[10] The results of our spyware test confirmed these variances; the scans from five antispyware tools consistently identified different spyware. According to several agency responses, some of the most effective antispyware tools are freeware applications, but they do not have the capability to centrally manage a large deployment of systems. In addition, officials at one agency noted that it is difficult to track data being transmitted by spyware. Although current tools such as firewalls may assist in tracking incidents, spyware incidents are difficult to measure because spyware transmits using the same communications path as legitimate Web traffic. Indeed, our spyware test proved the difficulty in analyzing such spyware transmissions; the Internet traffic logs from a single hour of Web browsing resulted in more than 30,000 pages of text that could not be effectively reviewed without automated analysis tools.

Software vendors have recognized the need for enterprise antispyware applications. Antivirus and intrusion-detection vendors have recently added antispyware features to their base products, and corporate applications have recently been placed on the market to detect and block known spyware while providing larger enterprises with centralized administration. These enterprise antispyware tools enable network administrators to combat spyware from a central location. With an enterprise solution, an antispyware program is installed on each computer system (client) and communicates with a centralized system. The central system updates individual clients, schedules scans, monitors the types of

[10] NIST Special Publication 800-53, p. 100.

spyware that have been found, and determines if the spyware was successfully removed. As with many antivirus efforts, a major limitation for some antispyware tools is that in order to detect the spyware, the tool has to have prior knowledge of its existence. Thus, as with many antivirus tools, certain antispyware tools must be updated regularly to ensure comprehensive protection. Evolving enterprisewide tools may provide the ability to establish rules that can address various categories of potential spyware behavior. For more information on antispyware tools, see appendix III. Without an ability to centrally detect spyware, agencies will have a difficult time fulfilling FISMA's incident-reporting requirements.

Agencies Identified Need for Continuing Efforts to Improve Employee Awareness

Agencies reported that employee awareness was a significant challenge as they worked to mitigate the risks associated with phishing and spyware. As discussed in chapter 1, agencies are required by FISMA to provide security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency. However, of the 24 agencies we surveyed, 13 reported that they have or plan to implement phishing awareness training this fiscal year, 3 reported plans to implement training in the future, and 3 had no plans to implement phishing awareness training.[11] Agencies reported efforts to increase their employees' awareness of phishing scams and the risks associated with revealing personal information over the Internet. Specifically, 10 agencies reported utilizing bulletins, notices, or e-mails to alert users to the methods and dangers of phishing scams. Further, 16 agencies indicated that they had implemented or planned to implement agencywide phishing guidance this fiscal year. Nevertheless, agencies reported a variety of user awareness challenges, including training their users to avoid visiting unknown Web sites, to verify the source of any request for sensitive or personal data, to be knowledgeable of new phishing scams, and to report any scams to the agency. Other challenges noted were the increased sophistication of phishing scams and the need for users to be continually updated about the changing threat.

Further, of the 11 agencies that responded to our question on spyware awareness training, 7 indicated that they had or planned to implement training this fiscal year, 1 reported plans to implement training in the future, and 3 indicated that they had no plans to implement training. Five

[11] Five agencies did not respond to our survey question on implementing phishing awareness training.

agencies reported plans to distribute agencywide spyware guidance in the form of bulletins or e-mails. However, when asked to identify spyware-related challenges, 6 agencies highlighted the difficulty of ensuring that their employees are aware of the spyware threat. One agency noted that users inadvertently reintroduce spyware; this could be mitigated if users were made aware of the browsing behaviors that put them at risk for downloading spyware. Moreover, agency officials confirmed that user awareness of emerging threats is still lacking and that significant improvements must be made.

Agencies' Incident-Response Plans or Procedures Do Not Fully Address Phishing and Spyware Threats

FISMA requires agencies to develop and implement plans and procedures to ensure continuity of operations for their information systems. In addition, NIST guidance advises agencies that their incident-response capability should include establishing guidelines for communicating with outside parties regarding incidents and also discusses handling specific types of incidents, including malicious code and unauthorized access.[12]

However, our review of agencies' incident-response plans found that while they largely address the threat of malware, they do not fully address phishing or spyware. Specifically, our analysis of the incident-response plans or procedures provided by the 20 agencies showed that none specifically addressed spyware or phishing. However, all of these plans addressed malware and incidents of unauthorized access (which are potential risks for phishing and spyware). Further, 1 agency indicated that spyware is not considered significant enough to warrant reporting it as a security incident. Determining what an incident is and how it should be tracked varies considerably among agencies. For example, 1 agency noted that each intrusion attempt is considered an incident, while another agency reported that one incident can involve multiple users or systems.

Because spyware is not detected and removed according to a formalized procedure, much of the information on the local machine would be destroyed and not maintained as evidence for an investigation of a computer crime. As a result, this information would not be available to aid in discovering what happened or in attributing responsibility for the crime.

[12] NIST Special Publication 800-61.

Chapter 4

Existing Efforts to Combat Cybersecurity Threats Are Directed toward the Private Sector and Consumers

Recognizing the potential risks that emerging cybersecurity threats pose to information systems, several entities within the federal government and private sector have begun initiatives directed toward addressing spam, phishing, and spyware.

These efforts range from targeting cybercrime to educating the user and the private-sector community on how to detect and protect systems and information from these threats. While the initiatives demonstrate an understanding of the importance of cybersecurity and emerging threats and represent the first steps in addressing the risks associated with emerging threats, similar efforts are not being made to help federal agencies address such risks.

Federal and Private Sector Emphasize Consumer Education and Protection Initiatives

Both the public and private sector have noted the importance of user education and consumer protection relating to emerging cybersecurity threats. FTC has been a leader in this area, issuing consumer alerts and releasing several reports on spam, as well as providing guidance for businesses on how to reduce the risk of identity theft. FTC also updates and maintains useful cybersecurity information on its Web site at www.ftc.gov, including its Identity Theft Clearinghouse, an online resource for taking complaints from consumers. This secure system can be accessed by law enforcement, including the Department of Justice. In addition, FTC has sponsored various events, including a spam forum in the spring of 2003, a spyware workshop in April 2004, and an e-mail authentication summit in the fall of 2004.

Efforts to Increase Consumer Awareness of Phishing

As the threat of phishing has increased, so has the number of groups aimed at informing and protecting consumers against this emerging cybersecurity threat. The Anti-Phishing Working Group, created in the fall of 2003, is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and e-mail spoofing. The working group provides a forum for discussing phishing issues, defines the scope of the phishing problem in terms of hard and soft costs, and shares information and best practices for eliminating the problem. Where appropriate, the working group also shares this information with law enforcement.

Additionally, the Phish Report Network, a recently formed group, enables companies to reduce online identity theft by safeguarding consumers from phishing attacks. Claiming to be the first worldwide antiphishing aggregation service, the Phish Report Network provides subscribers with a mechanism for staging a united defense against phishing. Industry experts agree that the escalating phishing problem, if unabated, will continue to result in significant financial losses. The Phish Report Network aims to significantly reduce these losses by preventing online fraud and rebuilding consumer confidence in online channels. The network is comprised of senders and receivers. Any company being victimized by phishing attacks, such as a financial services or e-commerce company, can subscribe to the Phish Report Network as a sender and begin immediately and securely reporting confirmed phishing sites to a central database. Other companies, such as Internet service providers, spam blockers, security companies, and hosting companies, can join the Phish Report Network as receivers. Subscribing as a receiver provides access to the database of known phishing sites submitted by the senders. Using this information, receivers can protect consumers by blocking known phishing sites in various software, e-mail, and browser services. Additionally, real-time notifications of new phishing sites are available to receivers to ensure up-to-the-minute protection against the latest attacks.

Further, the United States Internet Service Provider Association serves both as the Internet service provider community's representative during policy debates and as a forum in which members can share information and develop best practices for handling specific legal matters. Association officials plan to produce guidance on spam and phishing. Currently, the association focuses on taking down sites that have been spoofed and contacts banking institutions for their coordination when necessary. It also offers insight to federal agencies in the case of a phishing incident, noting that enterprises/agencies need to act quickly when they detect a problem and contact the relevant providers and try to preserve potential evidence. Going to the authorities, such as the FBI, will not stop a phishing attack or a botnet immediately. Law enforcement is an important component, but enterprise/agency security officials need to plan for responding to attacks and coordinating their efforts with their contractors and Internet service providers.

Lastly, FDIC states that the only real solution for combating phishing is through consumer education. FDIC officials believe phishing is a very dangerous threat because it undermines the public's trust in government. For this reason, FDIC's public affairs office has instituted a toll-free telephone number for customers to call with questions about the legitimacy of communications purported to come from FDIC. In addition, FDIC maintains a Web page to warn consumers of phishing fraud.

Efforts to Address the Growing Problem of Spyware

In April 2004, the Congressional Internet Caucus Advisory Committee[1] held a workshop on spyware, designed to help Congressional offices reach out and educate their constituents on how to deal with spyware. A variety of educational materials was distributed to assist offices in responding to constituent complaints about spyware. These included a tool to assist offices in posting to their Web sites basic spyware prevention tips for computer users; newsletters on several issues including computer security, spam, and privacy; and materials from other sources—including FTC—for producing a district town hall meeting on spyware and computer security.

In March, the FTC revisited the issue of spyware with a follow-up report to its April 2004 workshop.[2] According to the report, the FTC concluded that spyware is a real and growing problem that could impair the operation of computers and create substantial privacy and security risks for consumers' information. FTC also stated that the problems caused by spyware could be reduced if the private sector and the government took action. The report suggested that technological solutions such as firewalls, antispyware software, and improved browsers and operating systems could provide significant protection to consumers from the risks related to spyware. The report recommended that industry identify what constitutes spyware and how information about spyware should be disclosed to consumers, expand efforts to educate consumers about spyware risks, and assist law enforcement. The report further recommended that the government increase criminal and civil prosecution under existing laws of those who distribute spyware and increase efforts to educate consumers about the risks of spyware.

[1] The Congressional Internet Caucus Advisory Committee is a group of public interest, nonprofit, and industry groups that aims to educate Congress and the public about important Internet-related policy issues.

[2] Report of the Federal Trade Commission Staff, *Spyware Workshop: Monitoring Software on Your Personal Computer: Spyware, Adware, and Other Software* (Washington, D.C.: March 2005).

Criminal Investigations and Law Enforcement Actions Also Under Way

The Department of Justice and FTC have law enforcement authority over specific aspects of cybercrime that relate to spam, phishing, spyware, and malware. When a cybercrime case is generated, FTC first handles the civil component and Justice—including the FBI—follows by addressing the criminal component. Justice and FTC initiatives have resulted in successful prosecutions, but also have highlighted challenges that are specific to the enforcement of cybercrime.

Department of Justice Targets Spam and Phishing

FBI's Cyber Division, established in 2002, coordinates, supervises, and facilitates the FBI's investigation of those federal violations in which the Internet, computer systems, and networks are exploited as the principal instruments or targets of criminal, foreign intelligence, or terrorist activity and for which the use of such systems is essential to that activity. The Internet Crime Complaint Center, formerly the Internet Fraud Complaint Center, is the unit within the FBI responsible for receiving, developing, and referring criminal cyber crime complaints. For law enforcement and regulatory agencies at the federal, state, and local levels, the Center provides a central referral mechanism for complaints involving Internet-related crimes. It places significant importance on partnering with law enforcement and regulatory agencies and with industry. Such alliances are intended to enable the FBI to leverage both intelligence and subject matter expert resources, pivotal in identifying and crafting an aggressive, proactive approach to combating cybercrime.

The Internet Crime Complaint Center has put forth several initiatives in an attempt to fight cybercrime related to spam and phishing:

- The simultaneously layered approach methodology–Spam (SLAM-Spam) initiative, which began in September 2003, was started under the CAN-SPAM Act and developed jointly with law enforcement, industry, and FTC. This initiative targets significant criminal spammers, as well as companies and individuals who use spammers and their techniques to market their products. The SLAM-Spam initiative also investigates the techniques and tools used by spammers to expand their targeted audience, to circumvent filters and other countermeasures implemented by consumers and industry, and to defraud customers with misrepresented or nonexistent products.

- Operation Web Snare, another joint effort with law enforcement, targets criminal spam, phishing, and spoofed or hijacked accounts, among other criminal activities. According to officials at the Department of Justice, this sweep, which began in June 2004, has so far resulted in 103 arrests and 53 convictions.

- Operation Firewall, a joint investigation with several law enforcement agencies and led by the Secret Service, targeted a global cybercrime network responsible for stealing personal information about citizens from companies and selling this information to members of the network. According to Justice officials, this investigation began in July 2003 and resulted in the indictment of 19 cybercriminals and several additional arrests for identity theft, credit card fraud, and conspiracy in October 2004.

- Finally, Digital PhishNet, a cooperative effort among private-sector companies and federal law enforcement, is an FBI-led initiative to create a repository of information for phishing-related activities in order to more effectively identify, arrest, and hold accountable perpetrators of phishing scams.

Phishing is currently being handled by two organizations within Justice's Criminal Division: the Fraud Section, which deals with identity theft and economic crimes, and the Computer Crime and Intellectual Property Section, which focuses extensively on the issues raised by computer and intellectual property crime. According to Justice officials, the department continues to respond to the challenges presented by spam, phishing, and other emerging threats with new initiatives, investigations, and prosecutions.

FTC Takes Court Action to Address Spyware

FTC's enforcement authority is derived from several laws, including the Federal Trade Commission Act, the CAN-SPAM Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act, among others.[3] This authority has recently led FTC to sue Seismic Entertainment, its first

[3] See the Federal Trade Commission Act and the CAN-SPAM Act of 2003, Public Law 108-187, December 16, 2003. Also see the Telemarketing and Consumer Fraud and Abuse Prevention Act (15 U.S.C. §§ 6101-6108) and the Telemarketing Sales Rule, 16 CFR Part 310, which implements the act.

spyware case.[4] FTC officials claim that Seismic Entertainment placed malicious code on the Seismic Entertainment Web site, which exploited a vulnerability in Internet Explorer such that when a user visited the Web site, software would install, without user initiation or authorization, onto the user's computer. As a result, the user would receive numerous pop-up advertisements, the user's homepage changed, and other spyware was installed. Further, certain pop-up advertisements would provide the user with an offer to purchase a product in order to stop the pop-ups from appearing. The FTC was issued a temporary injunction that forces Seismic Entertainment to remove the malicious code from the Web site server and prohibit the dissemination of the software.

Another recent case involved Spyware Assassin, an operation that offered consumers free spyware detection scans that "detected" spyware—even if there was none—in order to market antispyware software that does not work.[5] The FTC claims that Spyware Assassin and its affiliates used Web sites, e-mail, banner ads, and pop-ups to drive consumers to the Spyware Assassin Web site, ultimately threatening consumers with dire consequences of having spyware on their machines—such as credit card and identity theft—if they did not accept the free "scan." The free "scan" displays an "urgent error alert," indicating that spyware has been detected on the machine and prompts the user to install the latest free update to fix these errors, in which case Spyware Assassin software is installed. FTC has requested that Spyware Assassin and its affiliates be barred from making deceptive claims and is seeking a permanent halt to the marketing scam as well as redress for consumers.

[4] Federal Trade Commission, Plaintiff, v. Seismic Entertainment Productions, Inc., SmartBot.net, Inc., and Sanford Wallace, Defendants., United States District Court, District of New Hampshire (FTC File No. 042 3125).

[5] Federal Trade Commission, Plaintiff, v. MaxTheater, Inc., a Washington Corporation, and Thomas L. Delanoy, individually and as an officer of MaxTheater, Inc., Defendants, United States District Court, Eastern District of Washington (FTC File No. 042 3213).

Federal Agencies Have Received Minimal Guidance on Addressing Spam, Phishing, and Spyware

As of March 31, 2005, DHS's National Cyber Security Division (NCSD) had produced minimal guidance to federal agencies on how they should protect themselves from spam, phishing, spyware, or other emerging threats. NCSD supports and enhances other federal and private-sector groups that examine cybersecurity-related issues by looking at what other groups are doing and providing assistance if needed. As NCSD's operational arm, US-CERT has several initiatives under way to share information on cybersecurity issues and related incident-response efforts. However, NCSD's communications and efforts pertaining to emerging cybersecurity threats have primarily been directed to the private sector and the general public.[6] For example, we found that almost all of the US-CERT alerts, notices, and bulletins that provided specific guidance on how to address spam, phishing, or spyware were written to help individual users. In fact, the one relevant publication that was targeted to federal agencies was issued over 2 years ago.[7] Further, because this publication focused on instructing agencies on how to filter out a specific spam message, there is no current US-CERT guidance that addresses the security risks of spam to federal agencies—including its capacity to distribute malware.

Similarly, law enforcement entities have not provided agencies with information on how to appropriately address emerging cybersecurity threats. For example, the FBI has not issued any guidance to federal agencies or provided any detailed procedures for responding to spam, spyware, phishing, or botnets that would maintain evidence needed for a computer crime investigation. Also, the Secret Service has not created any initiatives specifically examining the risk of phishing attacks against the federal government or the fraudulent use of federal government identities. Further, the Secret Service has not distributed information to federal agencies about what measures they can take to protect their agencies from being targeted in a phishing scam.

[6] See appendix IV for selected publications on the US-CERT Web site that are relevant to addressing spam, phishing, or spyware.

[7] *FedCIRC Informational Notice: High Volume of Spam Being Received by Federal Agencies* (2003-01-01, Jan. 2, 2003).

Lack of Coordinated Incident Reporting Limits Federal Capability to Address Emerging Threats

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, OMB and 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.

Lack of Federal Guidance Impedes Consistent Agency Reporting of Emerging Threats

Agencies are not consistently reporting emerging cybersecurity incidents such as phishing and spyware to a central federal entity. As discussed in chapter 1, agencies are required by FISMA to develop procedures for detecting, reporting, and responding to security incidents—including notifying and consulting with the federal information security incident center for which OMB is responsible. OMB has transferred the operations for this center to DHS's US-CERT.

However, our analysis of the incident response plans and procedures provided by 20 agencies showed that none specifically addressed phishing or spyware. Further, general incident reporting varies among the agencies; while some report cyber incidents to US-CERT, other agencies report incidents to law enforcement entities, while still others do not report incident information outside their agency. Indeed, the inspector general for one agency reported that more than half of the agency's organizations did not report malicious activity, federal law enforcement was notified only about some successful intrusions, and attacks originating from foreign sources were not consistently reported to counterintelligence officials. Discussions with US-CERT officials confirmed that they had not consistently received incident reports from agencies and that the level of detail that accompanies an incident report may not provide any information about the actual incident or method of attack. Further, they noted that agencies' efforts to directly report incidents to law enforcement could be duplicative, because US-CERT forwards incidents with criminal elements to its law enforcement division. According to DHS officials, these incident reports are always passed to the FBI and the Secret Service.

The agencies' inconsistent incident reporting results from the lack of current federal guidance on specific responsibilities and processes. As of March 2005, neither OMB nor US-CERT had issued guidance to federal agencies on the processes and procedures for reporting incidents of phishing, spyware, or other emerging malware threats to US-CERT. As previously discussed, OMB's FISMA responsibility to ensure the operation of a central federal information security center—US-CERT—involves ensuring that guidance is issued to agencies on detecting and responding to incidents, incidents are compiled and analyzed, and agencies are informed about current and potential information security threats. However, the most recent guidance to federal agencies on incident-reporting roles and processes was issued in October 2000—prior to the establishment of US-CERT. According to officials at US-CERT, the level of detail that accompanies an incident report may not provide any information about the actual incident or method of attack. In fact, the incident reporting guidelines on US-CERT's Web site only provide agencies with the time frames for reporting incidents and do not specify the actual incident information that should be provided. For example, while the guidance indicates that spam e-mail is to be reported to US-CERT on a monthly basis, it does not clarify whether agencies should simply report the number of spam e-mails received or if they should include the text of the spam e-mails as part of the incident report. Without the necessary guidance, agencies do not have a clear understanding of which incidents they should be reporting or how and to whom they should report.

In addition to the lack of specific guidance to agencies, the federal government lacks a clear framework for the roles and responsibilities of other entities involved in the collection and analysis of incident reports—including law enforcement. Homeland Security Presidential Directive 7 requires that DHS support the Department of Justice and other law enforcement agencies in their continuing missions to investigate and prosecute threats to and attacks against cyberspace, to the extent permitted by law. Rapid identification, information sharing, investigation, and coordinated incident response can mitigate malicious cyberspace activity. In 2001, we recommended that the Assistant to the President for National Security Affairs coordinate with pertinent executive agencies to develop a comprehensive governmentwide data collection and analysis framework. According to DHS officials, US-CERT is currently working with OMB on a concept of operations and taxonomy for incident reporting. This taxonomy is intended to establish a common set of incident terms and the relationships among those terms and may assist the federal government in clarifying the roles, responsibilities, processes, and procedures for federal entities involved in incident reporting and response—including homeland security and law enforcement entities. According to OMB officials, the final version of the concept of operations and incident reporting taxonomy is to be issued this summer.

The lack of effective incident response coordination limits the federal government's ability to identify and respond to emerging cybersecurity threats, including sophisticated and coordinated attacks that target multiple federal entities. Without consistent incident reporting from agencies, it will be difficult for US-CERT to perform its transferred FISMA responsibilities of providing the federal government with technical assistance, analysis of incidents, and information about current and potential security threats.

Chapter 6

Conclusions and Recommendations

Conclusions

Emerging cyberthreats such as spam, phishing, and spyware present substantial risks to the security of federal information systems. However, agencies have not fully addressed the risks of these threats as part of their FISMA-required agencywide information security programs. Although the federal government has efforts under way to help users and the private-sector community address spam, phishing, and spyware, similar efforts have not been made to assist federal agencies. Consequently, agencies remain unprepared to effectively detect, respond, and protect against the increasingly sophisticated and malicious threats that continue to place their systems and operations at risk.

Moreover, although OMB and DHS share responsibility for coordinating the federal government's response to cyberthreats, guidance has not been provided to agencies on when and how to escalate incidents of emerging threats to DHS's US-CERT. As a result, incident reporting from agencies is inconsistent at best. Until incident reporting roles, responsibilities, processes, and procedures are clarified, the federal government will be at a clear disadvantage in effectively identifying, mitigating, and potentially prosecuting sophisticated and coordinated attacks that target multiple federal entities.

Recommendations

In order to more effectively prepare for and address emerging cybersecurity threats, we recommend that the Director, Office of Management and Budget, take the following two actions:

- ensure that agencies' information security programs required by FISMA address the risk of emerging cybersecurity threats such as spam, phishing, and spyware, including performing periodic risk assessments; implementing risk-based policies and procedures to mitigate identified risks; providing security-awareness training; and establishing procedures for detecting, reporting, and responding to incidents of emerging cybersecurity threats; and

- coordinate with the Secretary of Homeland Security and the Attorney General to establish governmentwide guidance for agencies on how to (1) address emerging cybersecurity threats and (2) report incidents to a single government entity, including clarifying the respective roles, responsibilities, processes, and procedures for federal entities—including homeland security and law enforcement entities.

Agency Comments and Our Evaluation

We received oral comments on a draft of our report from representatives of OMB's Office of Information and Regulatory Affairs and Office of General Counsel. These representatives generally agreed with our findings and conclusions and supplied additional information related to federal efforts to address emerging cyber threats. This information was incorporated into our final report as appropriate.

In commenting on our first recommendation, OMB stressed that the agencies have the primary responsibility for complying with FISMA's information security management program requirements. Nevertheless, OMB indicated that it would incorporate emerging cybersecurity threats and new technological issues into its annual review of agency information security programs and plans to consider whether the programs adequately address emerging issues before approving them.

OMB told us that our second recommendation was being addressed by a concept of operations and taxonomy for incident reporting that it is developing with DHS's US-CERT. As we indicated earlier in our report, the final document is planned to be issued this summer. OMB officials indicated that the completed document will establish a common set of incident terms and the relationships among those terms and will also clarify the roles, responsibilities, processes, and procedures for federal entities involved in incident reporting and response—including homeland security and law enforcement entities.

Additionally, the Departments of Defense, Homeland Security, and Justice provided technical comments via e-mail, which were incorporated as appropriate.

Relevant NIST Special Publications

NIST is required by FISMA to establish standards, guidelines, and requirements that can help agencies improve the posture of their information security programs. The following table summarizes NIST special publications that are relevant to protecting federal systems from emerging cybersecurity threats.

Table 3: NIST Special Publications Relevant to Emerging Cybersecurity Threats

Title	Description
Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005	Security controls are the management (e.g., risk assessments, certification and accreditation, etc.), operational (e.g., personnel security, incident response, system and information integrity, etc.), and technical (e.g., identification and authentication, access control, etc.) protections prescribed for an information system to safeguard the confidentiality, integrity, and availability of the system and its information. In conjunction with and as part of a well-defined information security program, NIST recommends implementing security controls such as the organization's overall approach to managing risk, security categorization of the system, activities associated with customizing the baseline security controls, and potential for supplementing the baseline security controls with additional controls, as necessary, to achieve adequate security.
DRAFT Special Publication 800-70, *The NIST Security Configuration Checklists Program for IT Products*, August 2004	A security configuration checklist can establish "benchmark settings" that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the federal government. This guide is intended for users and developers of IT product security configuration checklists, so that organizations and individual users can better secure their systems. While this document does not have specific guidance in handling spam, phishing, and spyware, it does note the threat of malicious code spread through e-mail, malicious Web sites, and file downloads.
DRAFT Special Publication 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist,* June 2004	An IT security configuration checklist applied to a system in conjunction with trained system administrators and a well-informed security program can reduce vulnerability exposure. This guide provides information about the security of Windows XP and security configuration guidelines for the operating system and commonly used applications. The guide also provides methods that system administrators can use to implement each recommended security setting in four types of environments: small/home offices, enterprise, high security, and legacy.
Special Publication 800-61, *Computer Security Incident Handling Guide*, January 2004	New types of security-related incidents emerge frequently. Thus, an incident response capability is necessary to rapidly detect incidents, reduce loss and destruction, mitigate the vulnerabilities that were exploited, and restore computing services. This publication provides guidance on how agencies can detect, analyze, prioritize, and handle incidents through its discussion of how to organize a computer security incident response capability and handle various types of incidents, including denial of service, malicious code, unauthorized access, inappropriate usage, and multiple-component incidents.
Special Publication 800-42, *Guideline on Network Security Testing*, October 2003	An effective security testing program within federal agencies is critical to keeping their networked systems secure from attacks. Testing serves several purposes, including (1) filling the gap between the state of the art in system development and actual operation of these systems and (2) understanding, calibrating, and documenting the operational security posture of an organization. Testing is an essential component of improving an organization's security posture.

(Continued From Previous Page)

Title	Description
Special Publication 800-43, *Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System*, November 2002	The principal goal of the document is to recommend and explain tested, secure settings for Windows 2000 Professional (Win2K Pro) workstations, with the objective of simplifying the administrative burden of improving the security of Win2K Pro systems. This guide provides detailed information about the security features of Win2K Pro, security configuration guidelines for popular applications, and security configuration guidelines for the Win2K Pro operating system. It discusses methods that system administrators can use to implement each recommended security setting.
Special Publication 800-44, *Guidelines on Securing Public Web Servers*, September 2002	The Web server is the most targeted and attacked host on most organizations' networks. As a result, it is essential to secure Web servers and the network infrastructure that supports them. The publication discusses methods that organizations can use to secure their Web servers, such as hardening servers, patching systems, testing systems, maintaining and reviewing logs, backing up, and developing a secure network. It also discusses what types of active content technologies to use (e.g., JavaScript, CGI, ActiveX), what content to show, how to limit Web bots (i.e., bots that scan Web pages for search engines), and authentication and cryptographic applications.
Special Publication 800-45, *Guidelines on Electronic Mail Security,* September 2002	Securing e-mail servers is an important aspect of protecting against emerging threats because compromised e-mail servers can be used to assist phishers and spammers distribute malware and carry out further attacks on a network. The publication discusses, among other things, e-mail standards and their security implications, filtering e-mail content, and administering the mail server in a secure manner.
Special Publication 800-40, *Procedures for Handling Security Patches*, August 2002	Effective patch management can help mitigate the threat of spam, phishing, spyware, worms, viruses, and other types of malware. This guide provides a systematic approach for identifying and installing necessary patches or mitigating the risk of a vulnerability, including steps such as creating and implementing a patch process, identifying vulnerabilities and applicable patches, and patching procedures, among others.
Special Publication 800-46, *Security for Telecommuting and Broadband Communications*, August 2002	Systems used by telecommuters may not have the same quality of spam filtering, patches, hardening of systems, and general network security as an employer's systems. Thus malware, including spyware and other emerging threats, could be installed onto systems and introduced into an organization's network by remote users. This publication helps organizations address security issues by providing recommendations on securing a variety of applications, protocols, and networking architectures.
Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002	Risk management is the process of identifying, assessing, and mitigating risk to an acceptable level. Managing risk can enable an organization to improve the security of IT systems and facilitate well-informed risk management decisions. This guide describes the risk assessment process, including identifying and evaluating risks, their impact, and risk-reducing measures; risk mitigation, which includes prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process; and the ongoing assessment process and key steps for implementing a successful risk management program.
Special Publication 800-28, *Guidelines on Active Content and Mobile Code*, October 2001	Active content refers to the electronic documents that can carry out or trigger actions automatically without an individual directly or knowingly invoking the actions. While active content has many useful functions, it has also been used to run malicious code and to install programs such as spyware. This guide recommends key guidelines to federal departments and agencies for dealing with active content.

Source: GAO analysis of NIST reports.

Antispam Tools

What the Technology Does

Antispam tools scan, inspect, filter, and quarantine unsolicited commercial e-mail, commonly referred to as spam, while allowing the delivery of legitimate e-mail. These tools can block and allow e-mail sent from specific Internet Protocol (IP) addresses that have been identified as distributors of spam or other connection- or content-based rules.

How the Technology Works

When a spam filtering solution scans e-mail messages, it uses various techniques to detect spam. The most common filtering methods used are whitelists, blacklists, challenge/response systems, content analysis, textual analysis, heuristics, validity checking, and volume filtering. A whitelist accepts mail from users and domains designated by the user or system administrator. These e-mail messages will typically bypass the filter even if they exhibit characteristics that may define them as spam. Similarly, blacklists, also referred to as blocklists, prevent e-mail from specific domains, IP addresses, or individuals from being accepted. Many vendors maintain their own lists and provide optional subscriptions to third-party blacklist services.

Content analysis capabilities allow the tools to scan the subject line, header, or body of the e-mail message for certain words often used in spam. Mail that contains certain keywords, executables, or attachments with extensions commonly associated with malware can be filtered. A more sophisticated form of this approach is lexical analysis, which considers the context of words. Such content controls can help organizations enforce their own policy rules.

Spam fingerprinting identifies specific spam e-mail with a unique fingerprint, or signature, so that these messages can be recognized and removed. Reverse domain name server lookup allows the receiving mail server to look up the IP address of the sending server to determine if it matches the header information in the e-mail. This allows the tool to determine if the sender is attempting to spoof the mail organization information. This form of validity checking is not commonly used because many systems are not correctly configured to accurately respond to this type of lookup.

An increasingly common feature is heuristical analysis, which employs statistical probabilities to determine if the characteristics of an e-mail categorize the message as spam. Each spam characteristic is assigned a score, or spam probability, and if the cumulative score exceeds a designated threshold, the message is labeled as spam. Most heuristic analysis includes adaptive filtering techniques, which can generate rules to identify future spam. A more advanced heuristics-based approach is bayesian filtering, which makes an assessment of both spam-like versus legitimate e-mail characteristics, thereby allowing it to distinguish between spam versus legitimate e-mail. Its self-learning filter is adaptive in learning the e-mail habits of the user, which can allow the tool to be more responsive and tailored to a specific individual.

Because a salient characteristic of spam is the bulk quantity in which it is distributed, spam filtering solutions also check for the volume of e-mail sent from a particular IP address over a specific period of time. Other spam protection capabilities include challenge/response systems, in which senders must verify their legitimacy before the e-mail is delivered. This verification process typically requires the sender to respond to a request that requires a human (rather than a computer) to respond. Tools can also employ traffic pattern analysis, which looks for aberrant e-mail patterns that may represent a potential threat or attack.

Antispam tools can handle spam in various ways, including accepting, rejecting, labeling, and quarantining messages. Messages that are labeled or quarantined can usually be reviewed by the user to ensure that they have not been misidentified.

These tools also have the capability of providing predefined or customized reports, as well as real-time monitoring and statistics. Increasingly, antispam tools provide antiphishing capabilities that can also detect and block phishing scams.

Effectiveness of the Technology

Automated antispam solutions yield false positive rates—that is, they incorrectly identify legitimate e-mail as spam. In such instances, a user may not receive important messages because they have been misidentified. Tools can also produce false negatives, which incorrectly identify spam as legitimate e-mail, thereby allowing spam into the user's inbox. Additionally, the current vendor market is still immature, as it is composed of many smaller vendors with limited history in this market. The rise of botnets also increases the challenge in determining legitimate spam because with more networks distributing smaller amounts of e-mail, it is not as easy to determine the legitimacy of the messages based on the quantity distributed. Further, antivirus vendors have launched or licensed more advanced spam-filtering capabilities into their antivirus engines, thereby providing a more comprehensive tool and increasing competition for point-solution vendors. Finally, because spammers are constantly evolving their techniques, vendors may lag behind in providing the most current capabilities.

Appendix III

Antispyware Tools

What the Technology Does

Antispyware tools provide protection against various potentially unwanted programs such as adware, peer-to-peer threats, and keyloggers, by detecting, blocking, and removing the unwanted programs and also by preventing the unauthorized disclosure of sensitive data. Antispyware solutions protect computer systems against the theft of sensitive information at a central location (desktop or enterprise level).

How the Technology Works

Antispyware tools typically work by scanning computer systems for known potentially unwanted programs, thus relying on a significant amount of prior knowledge about the spyware. These antispyware solutions use a signature database, which is a collection of what known spyware looks like. Therefore, it is critical that the signature information for applications be current.

When a signature-based antispyware program is active, it searches files and active programs and compares them to the signatures in the database. If there is a match, the program will signal that spyware has been found and provide information such as the threat level (how dangerous it is).

Some tools are able to block spyware from installing onto a system by using real-time detection. Real-time detection is done by continuously scanning active processes in the memory of a computer system and alerting a user when potentially hostile applications attempt to install and run. A user can then elect to stop the spyware from installing onto the system.

Once spyware is found, a user can chose to either ignore it or attempt to remove it. In order to remove a spyware application, a tool has to undo the modifications that were made by the spyware. This involves deleting or modifying files and removing entries in the registry. Some tools can block the transmission of sensitive information across the Internet. For example, one tool allows users to input specific information that the user wants to ensure is not transmitted (e.g., credit card number) by an unauthorized source. The tool then monitors Internet traffic and will warn a user if a program attempts to send the information.

Effectiveness of the Technology

Antispyware solutions cannot always defend against the threat of spyware unless they have prior knowledge of its existence and also the required frequent updating for signature files. Even then, antispyware tools vary in their effectiveness to detect, block, and remove spyware. For example, one tool that prevents installed spyware from launching does not actually remove the spyware from the system. NIST recommends that organizations consider using antispyware tools from multiple vendors.

Relevant DHS Publications

DHS issues a variety of publications related to cybersecurity threats and vulnerabilities on the US-CERT Web site (www.us-cert.gov). The following table summarizes selected publications that are relevant to the emerging cybersecurity threats of spam, phishing, and spyware.

Table 4: Selected DHS/US-CERT Publications Relevant to Spam, Phishing, or Spyware

Title	Description
Cyber Security Tip: Risks of File-Sharing Technology (ST05-007, Mar. 30, 2005)	Warns that file-sharing technology may introduce security risks, including the installation of spyware and the exposure of sensitive information. Identifies good security practices that users can take to minimize these security risks.
Cyber Security Tip: Recovering from Viruses, Worms, and Trojan Horses (ST05-006, Mar. 16, 2005)	Warns that many users are victims of viruses, worms, or Trojan horses, and highlights spyware as a common source of viruses. Provides steps that users can take to recover from these threats, including using antispyware tools.
Cyber Security Alert: Security Improvements in Windows XP Service Pack 2 (SA04-243A, Jan. 10, 2005)	Describes how Microsoft Windows XP Service Pack 2 can improve a computer's defenses against attacks and vulnerabilities. Notes that the service pack includes changes in Internet Explorer that can help defend against phishing attacks.
Federal Informational Notice: Safe Online Holiday Shopping (FIN04-342, Nov. 30, 2004)	Warns of a potential increase in phishing scams that target online shoppers and describes the risks that online fraud, phishing scams, and identity theft pose to individuals. Recommends steps that end-users can take to mitigate this threat.
Cyber Security Tip: Recognizing and Avoiding Spyware (ST04-016, Sept. 15, 2004)	Defines spyware and provides a list of symptoms that may indicate that spyware has been installed on a computer. Provides individuals with steps they can take to prevent and remove spyware.
Cyber Security Tip: Avoiding Social Engineering and Phishing Attacks (ST04-014, July 28, 2004)	Defines social engineering and phishing attacks and identifies steps that individuals can take to avoid becoming a victim and what to do if one suspects that sensitive information has been compromised.
Cyber Security Tip: Protecting Your Privacy (ST04-013, July 14, 2004)	Identifies steps that individuals can take to ensure that the privacy of personal information submitted online is being protected.
Cyber Security Tip: Browsing Safely: Understanding Active Content and Cookies (ST04-012, June 30, 2004)	Defines "active content" and "cookies," and notes that active content can be used to run spyware or collect personal information. Provides advice on how individuals can more safely browse the Web.
Cyber Security Tip: Reducing Spam (ST04-007, May 26, 2004)	Defines spam and discusses how individuals can reduce the amount of spam they receive.
Cyber Security Alert: Continuing Threats to Home Users (SA04-079A, Mar. 19, 2004)	Identifies four specific threats of malicious code and also warns home users of the risk of phishing scams. Provides suggested protective measures that individuals can take to mitigate these threats.
Vulnerability Note: Microsoft Internet Explorer Does Not Properly Display URLs (VU#652278, Feb. 17, 2004)	Identifies a specific software vulnerability that could be exploited by an attacker to run a phishing scam. Provides solutions to address the vulnerability and identifies affected systems.
FedCIRC Informational Notice: High Volume of Spam Being Received by Federal Agencies (2003-01-01, Jan. 2, 2003)	Notes that federal agencies had reported receiving a high volume of spam promoting a particular Web site. Provides recommendations for filtering e-mail for these spam messages.

Source: GAO analysis of DHS/US-CERT publications.

Appendix V

GAO Contact and Staff Acknowledgments

GAO Contact

J. Paul Nicholas, Assistant Director, (202) 512-4457, nicholasj@gao.gov.

Acknowledgments

In addition to the individual named above, Scott Borre, Carolyn Boyce, Season Dietrich, Neil Doherty, Michael Fruitman, Richard Hung, Min Hyun, Anjalique Lawrence, Tracy Pierson, and David Plocher made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON ♻ RECYCLED PAPER