Week 3

Andrew Councill for USA TODAY

Defense efforts: Dan Lidor, left, and Aaron Hixson participate in the Department of Homeland Security's largest cyber security exercise Thursday.

Bush pushes cyber security
President wants to raise funding to $7.3 billion

By Richard Wolf
USA TODAY

WASHINGTON — A sudden spike in the number of successful attacks against federal government information systems and databases has led President Bush to propose a multibillion-dollar response.

The number of incidents reported to the Department of Homeland Security rose by 152% last year, to nearly 13,000, according to a new government report. The security breaches, more than 4,000 of which remain under investigation, ranged from the work of random hackers to organized crime and foreign governments, says Tim Bennett, president of the Cyber Security Industry Alliance.

The increase and severity of data breaches prompted Bush to recommend a 10% increase in cyber security funding for the coming fiscal year, to $7.3 billion. That's a 73% increase since 2004.

"The president's put a lot of emphasis on this recently," says Robert Jamison, undersecretary for national protection and programs at the Department of Homeland Security. "We're concerned that the threats are real and growing. ... We're more vulnerable as a nation."

Members of Congress and experts in the private sector say the government's new initiative is overdue.

"There are more and more bad guys out there," says Sen. Tom Carper, D-Del., who chaired a Senate Homeland Security subcommittee hearing this week on government information security risks. In 31% of the infiltrations, he says, "agencies do not know who took the information or how much information was taken."

Rep. Jim Langevin, D-R.I., who chairs the House Homeland Security subcommittee with jurisdiction over

the issue, says the Bush administration "has not paid nearly enough attention to cyber security" until this year. Now, he says, "they're at least trying to move in the right direction."

Homeland Security Secretary Michael Chertoff has made improving cyber security one of his top four goals for 2008. "It's the one area in which I feel we've been behind where I would like to be," he told reporters here last week.

A focus on China

The Defense Department and federal intelligence agencies are on the warpath against increasing numbers of cyberattacks.

To combat the threat, the government is rolling out a system this year that reduces external connections to the Internet, detects intrusions in and out of federal networks and enables faster patching of holes.

Even so, the Government Accountability Office reported this week that 20 of 24 major federal agencies are deficient in protecting against cyberattacks. Gregory Wilshusen, the GAO's director of information security issues, cited past instances in which the State Department network was breached by a malicious code inside an e-mail; a Transportation Security Administration hard drive with employment records was found missing; and an idled nuclear power plant's private computer network was infected by a virus, disabling a

safety monitoring system.

Deputy Defense Secretary Gordon England noted last week that Estonia was victimized by a series of attacks for three weeks in 2007 that forced its largest bank to shut down its online banking network. "Cyberwarfare is already here," England told a Veterans of Foreign Wars conference.

Much of the attention focuses on China, which could be infiltrating U.S. government information technology systems despite denials by Beijing. In its annual report to Congress last week on China's military power, the Pentagon said several cyberspace attacks around the world in 2007 were sourced back to China.

Director of National Intelligence Mike McConnell told the Senate Intelligence Committee last month

that several nations, including China and Russia, "have the technical capabilities to target and disrupt elements of the U.S. information infrastructure and for intelligence collection." He recommended "proactive measures to detect and prevent intrusions from whatever source, as they happen, and before they can do significant damage."

"The Chinese have a lot of resources, and they're willing to spend it to break in," says James Lewis, a cyber security expert at the Center for Strategic and International Studies.

Alan Paller, director of research at the SANS Institute, which specializes in information security research and training, says preventing cyberattacks is as important as preventing physical attacks. "Owning our computers is a

Cyberattacks on the rise

Incidents of security breaches reported by federal agencies to the U.S. Computer Emergency Readiness Team:

Type of incident	FY 2005	FY 2006	FY 2007
Under investigation	82	912	4,056
Improper usage	370	638	3,305
Unauthorized access	304	706	2,321
Attempted access	976	1,388	1,661
Malicious code	1,806	1,465	1,607
Denial of service	31	37	36
Total	3,569	5,146	12,986

Source: Office of Management and Budget

powerful weapon in a war," Paller says. "We need to get them out."

Practicing for attacks

To test security against about 100 possible attacks, the Department of Homeland Security today is completing a week-long series of simulations called "Cyber Storm II." The event presumed a coordinated cyberattack on information technology, communication, chemical and transportation systems. Participants from five countries, nine states, 18 federal agencies and more than 40 private companies participated.

"They remarked somewhat sheepishly how much of a stretch this has been for them," Greg Garcia, assistant secretary for cyber security at the Homeland Security Department, said Thursday during a tour of the event at Secret Service headquarters here.

Karen Evans, administrator for electronic government and information technology at the Office of Management and Budget, says part of the 152% increase in security breaches in 2007 was due to more accurate reporting, but she acknowledges that much of it represents a real rise.

Industry officials want a greater government role in preventing cyberattacks. Bennett says, "With global attacks on data networks increasing at an alarming rate, in a more organized and sophisticated manner, and often originating from state-sponsored sources, there is precious little time to lose."

Discussion

1. What startling statistics have prompted Bush to propose a multi-billion dollar response to cybercrime?
2. Why do you think cybersecurity is one of Homeland Security Secretary Michael Chertoff's top four goals for 2008?
3. Alan Paller, director of research at the SANS Institute, says that "owning our computers is a powerful weapon in a war." Brainstorm how a foreign enemy could use our computers against us in a war.
4. The participants of "Cyber Storm II" felt that the exercise was "a stretch" for them. Why do you think they felt this way? How do you think they would feel if they participated in this kind of exercise on a regular basis?
5. Why do industry officials want the government to take a greater role in preventing cyberattacks?

Activity

The Director of National Intelligence, Mike McConnell, says that the U.S. needs to protect its computer networks before cybercriminals "can do significant damage." And according to McConnell, China and Russia, along with several other nations, "have the technical capabilities to target and disrupt elements of the U.S. information infrastructure and for intelligence collection." Get into a group of three. Imagine that you are on McConnell's team and that you have been assigned to give a brief to the president on foreign cyberthreats against the U.S.'s information infrastructure. Create a three-minute oral presentation that answers the following questions: How can foreign governments disrupt the U.S.'s information infrastructure? For what purposes might a foreign government choose to do so? What measures should the U.S. put in place to detect and prevent such an intrusion? Present your brief to the class.

STAYSAFEONLINE.org
National Cyber Security Alliance

Homeland
Security

USA TODAY
Education

Lesson objectives:

Week 3

In this lesson, students will:
- ▶ Read about foreign threats to the U.S.'s information infrastructure.
- ▶ Identify reasons why foreign countries might want to invade the U.S.'s information infrastructure.
- ▶ Determine what measures the U.S. could take to prevent cyberattacks.
- ▶ Practice their oral communication skills.

Time requirements:

Step 1: Read the article (10 minutes).
Step 2: Answer the discussion questions (10 minutes).
Step 3: Create a three-minute oral brief (15 minutes).
Step 4: Present to the class (3 minutes per group – about 25 minutes).
Total: 60 minutes

Recommendations:

▶ Step 2: It is best to facilitate a whole class discussion to ensure student understanding of the concepts. Push students to consider multiple answers to Questions 2 and 3.

▶ Step 3: Before students begin creating their brief, make sure they know what three questions they must answer. To stretch their thinking on the subject, encourage them to provide multiple answers to each of the questions.

▶ Step 4: To close the lesson, have students present their briefs. You may wish to create a class list of answers to the three questions on the board. This will provide the most comprehensive view of the foreign threat against the U.S.'s information infrastructure.

▶ Homework: You may wish to have students explore the Department of Homeland Security's Critical Infrastructure resources on their website (link below) to help them better understand the nature of the threat and the ways in which the U.S. government plans to prevent or combat a cyberattack. In your next class session, students can share what else they would have added to their briefing, in light of the new information they gained from the website.

Links:

- ▶ National Cyber Security Alliance — StaySafeOnline www.staysafeonline.org
- ▶ The Department of Homeland Security's Critical Infrastructure/Key Resources Protection Resources www.dhs.gov/xprevprot/programs/editorial_0211.shtm
- ▶ The Office of the Director of National Intelligence: About the Intelligence Community www.dni.gov/faq_intel.htm
- ▶ United States Computer Emergency Readiness Team www.us-cert.gov
- ▶ i-SAFE www.i-safe.org
- ▶ Wired Safety Organization www.wiredsafety.org
- ▶ Federal Trade Commission: OnGaurdOnline onguardonline.gov
- ▶ Multi-State Information Sharing and Analysis Center www.msisac.org/awareness