SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

Oversight Hearing

"Worm and Virus Defense: How Can We Protect the Nation's Computers from These Serious Threats?"

Wednesday, September 10, 2003
10:00 a.m.

Opening Statement

Chairman Adam Putnam (R-Fl)

Good morning. A quorum being present, this hearing of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census will come to order.

Today we continue our in-depth review of cyber security issues affecting our nation. There are several things unique to cyber attacks that make the task of preventing them particularly difficult. Cyber attacks can occur from anywhere around the globe: from the caves of Afghanistan to the war fields of Iraq, from the most remote regions of the world or simply right here in our own back yard.

The technology used for cyber attacks is readily available and changes continually. And, maybe most dangerous of all, is the failure of many people – including many of those who are critical to securing these networks and information from attack -- to take the threat seriously, to receive adequate training, and to take proactive steps needed to secure their networks. A severe cyber attack could have serious repercussions throughout the nation both in a physical sense and in very real economic dollars.

The initial plan for this hearing was to focus primarily on strategies and methodologies within the agencies of the federal government for identification and mitigation of computer vulnerabilities through a system of "patch management". However, recent events caused us to expand the boundaries of this hearing to include computer systems throughout our nation. This summer everyone -- once again -- realized just how vulnerable our computer networks are to cyber attack. The Blaster worm and SoBigF virus brought home the reality that unsecured computer systems are all too prevalent and that – as a nation – across all levels, government, business and home users, we absolutely must take computer security more seriously.

The Blaster worm infected over 400,000 computers in less than five days. In fact, about one in three Internet users are infected with some type of virus or worm every year. The speed at which worms and viruses can spread is astonishing. What's equally astonishing is the lethargic pace at which people deploy the patches that can prevent infection in the first place. Microsoft announced the vulnerability, and had the patch available… weeks before the exploit appeared.

The recent viruses and worms have been blamed for bringing down train signaling systems throughout the East, affecting the entire CSX system, which covers 23 states. Additionally, new information coming to light shows that the Blaster worm is being linked to the severity of the power blackout of last month. The North American Electric Reliability Council blames another worm, Slammer, for impairing bulk electric system control by bringing down networks. We learned last week that The U.S. Nuclear Regulatory Commission issued a formal Information Notice to nuclear power plant operators warning them about an incident in January in which the Slammer computer worm penetrated networks at Ohio's Davis-Besse nuclear plant and disabled two important monitoring systems for hours.

A recent Gartner study predicts that by the year 2005, 90 percent of cyber attacks will attempt to exploit vulnerabilities for which a patch is available or a solution known. So, why aren't systems patched and anti-virus programs kept up to date? This hearing will examine the issues surrounding these incidents, including how vulnerabilities are discovered, how the public is notified about potential vulnerabilities, the mechanisms that exist for protecting systems, the real and potential problems presented by patching systems, and the scope of the problem confronting the federal government, the business community and the general public.

System administrators are often times overwhelmed with simply maintaining all the systems they have responsibility for overseeing. Challenges that organizations face in maintaining their systems are significant: with an estimated 4,000 vulnerabilities being discovered each year, it is an enormous challenge for any but the best-resourced organizations to install all of the software patches that are released by the manufacturer. Not only is the sheer quantity of patches overwhelming for administrators to keep up with, but patches can be difficult to apply and also have potentially unexpected side effects on other system components that administrators must then evaluate and address. As a result, after a security patch is released, system administrators often take a long time to fix all their vulnerable computer systems. Obviously, small organizations and home users, who lack the skills of system administrators, are even less likely to be able to keep up with the flow of patches.

The Department of Homeland Security's (DHS) Federal Computer Incident Response Center recently awarded a $10.8 million, five-year contract for a government-wide patch

management service to notify agencies about security holes in commercial software for systems on their networks, and the availability of patches to fix them. The service is known as the Patch Authentication and Dissemination Capability (PAD C).

The goal is to simplify patch management by providing administrators only with information relevant to their IT systems and ensuring that patches are genuine and effective. PAD C went on-line in January of this year.

According to officials, once agency system administrators have provided a profile of their systems and software, PAD C will alert them to potential vulnerabilities, provide interim security advice until a patch is made available, disseminate available patches, and keep management informed of available patches and which ones their systems administrators have downloaded.

Large organizations, such as business and educational institutions, often rely on commercial firms to notify them of vulnerabilities. For example, there are several firms that offer vulnerability notification, combined with analysis of the customer's computer systems for vulnerabilities. These firms also provide information on where to get the patches and prioritize them for the system administrators.

In addition, the commercial critical infrastructure sectors depend on information from their Information Sharing and Analysis Centers (ISACs) to help them respond to potential cyber threats. These ISACs are designed to allow members of a sector to share information about incidents to help increase preparedness and vigilance. The progress of Blaster demonstrates the importance of the early warning systems that ISACs are tasked with developing.

Independent researchers discover most vulnerabilities. These researchers may be academics, consultants or black hats. The Organization for Internet Security is working with software vendors, consultants and other interested parties to formalize procedures for dealing with vulnerabilities, including vendor notification and controlled disclosures. There is a very important role for government to play in the disclosure procedures. It is simply not acceptable for vendors to determine on their own schedule who gets notified and when. Given the potential national security risk that could emanate from the exploitation of a vulnerability, it is imperative that the appropriate government entities be involved in this process from the very beginning.

Vulnerabilities in software, and the worms and viruses that exploit them, have become a fact of life for the Internet. The government, law enforcement and private industry must develop…and continue to update… a plan to deal with these emerging threats. How can we educate home and small business users to minimize the risk posed by zombie computers? How can researchers, the government and the software industry work together to identify and remedy vulnerabilities in the most constructive manner? How will the federal government evolve an effective patch management program? What can be done to expedite the discovery and prosecution of cyber criminals who release worms and viruses? And, most important of all, how can the federal government, law enforcement and industry work together to protect the vital infrastructure of the Internet?

We have an excellent line-up of witnesses this morning who will share with use their expertise as we explore Worms and Viruses, how can be better protect the Nation's computers?