HEARINGS

PREPARED STATEMENT OF SENATOR FRED THOMPSON
CHAIRMAN

COMMITTEE ON GOVERNMENTAL AFFAIRS

MAY 19, 1998

"WEAK COMPUTER SECURITY IN GOVERNMENT: IS THE PUBLIC AT RISK?"

The Governmental Affairs Committee today is holding the first of a series of hearings on the security of federal computer systems. The potential benefits promised by computers are contrasted with inherent risks to our security and public safety. While advances in computing power potentially can remake how the government does business and how future wars are fought, it also creates vulnerabilities which must be reduced. Today's hearing will address the darker side of the information revolution while exploring how we can better protect government information.

Computers are changing our lives faster then any other invention in our history. Our society is becoming increasingly dependent on information technologies, which are changing at an amazing rate. Consider a couple of examples:

> The singing greeting cards which you buy today for $2 have more computing power then existed in the world before 1950.
>
> A video camera which you buy today for less then $1000 has more computing power then a 1960s computer the size of this room.

Combine this rapid explosion in computing power with the fact that information systems are being connected together around the world without regard to geographic boundaries. The increasing ability of computers talking to each other offers both opportunities and challenges.

In today's hearing, we will discuss these challenges. We will hear that the nature of this challenge comes from the fact that our nation's underlying information infrastructure is riddled with vulnerabilities which represent severe security flaws and risks to our nation's security, public safety and personal privacy.

While "hacker attacks" receive much media attention, what worries me are the attacks that go unknown. The nature of attacks in the information age seems to allow a malicious individual or group to reach out and inflict extensive damage from the comfort and safety of their home.

We must ask whether we are becoming so dependent on communications links and electronic microprocessors that a determined adversary or terrorist could possibly shut down federal operations or damage the economy simply by attacking our computers.

At risk are systems that control power distribution and utilities, phones, air traffic, stock exchanges, the Federal Reserve, and taxpayers' credit and medical records. Unfortunately, government agencies are ill-prepared to address the situation. We as a nation cannot wait for the "Pearl Harbor" of the information age. We must increase our vigilance to tackle this problem before we are hit with a surprise attack.

Our witnesses today have substantial knowledge about what the problems really are and can recommend solutions. First, Dr. Peter Neumann, a recognized private-sector expert on computer security, will provide the Committee with an overview of information security issues and testify on the systemic security problems in the government's computer systems.

Then we will hear from L0pht -- seven members of a "hacker think tank" who identify security weaknesses in computer systems in an effort to persuade companies to design more secure systems. L0pht members will testify about specific weaknesses which enable hackers to exploit the nation's information infrastructure and government information.

340 DIRKSEN SENATE OFFICE BUILDING, WASHINGTON, D.C. 20510 (202) 224-4751

[Committee Members] [Subcommittees][Special Investigation]
[Jurisdiction] [Hearings] [Press Releases] [Sites of Interest]