



# WHARTON AEROSPACE & DEFENSE REPORT

Your Knowledge Source on the Aerospace & Defense Industry

## **Cyber Attacks: What Can Be Done to Stem the Tide of Defense Technology Theft?**

*March 27, 2009*

## **Cyber Attacks: What Can Be Done to Stem the Tide of Defense Technology Theft?**

Attacks on U.S. Defense computers are rising sharply in scope and sophistication, and yet the federal response has been feeble and uncoordinated at best, according to security experts. The lax response includes a surprising inattention to basic computer security best practices, and opens the U.S. up to a host of potentially crippling system failures and the theft of some of the nation's most advanced technologies, these experts note.

"2007 was perhaps the worst year for the United States when it comes to cybersecurity," said James Lewis, the director and senior fellow of the Technology and Public Policy Program at the Center for Strategic and International Studies in Washington, D.C., during an "Improving Cybersecurity" congressional hearing on March 19. "It may have been the long-awaited Electronic Pearl Harbor, despite the lack of explosions or casualties."

Even as the number of attacks continued to grow since 2007, the response has been nothing like the one President Franklin Delano Roosevelt launched after the attack on Pearl Harbor. Security experts contend that the politicians who can press for a concerted defense effort have not grasped the severity of the situation. Indeed, only a handful of the committee's two-dozen senators attended the March 19 Senate Commerce, Science and Transportation Committee session and heard the testimony of several highly regarded experts. "I'm mortified by the lack of attendance," said Jay Rockefeller (D-W.Va.), the chair of the committee. "I regard this as a profoundly and deeply troubling problem to which we are not paying much attention."

The missing senators would also, no doubt, be "deeply" troubled by the scope of the problem. When most people think of cyber attacks, they envision blatant hacks using digital viruses and worms to disable or corrupt systems. And certainly such attacks cause havoc, as the French experienced earlier this year when their fighter-jets were grounded after they became infected with the "Conficker" virus spreading across Microsoft Windows-based systems.

But more insidious are the attacks that infiltrate systems to steal cutting-edge research and designs for the technology that gives America a strategic advantage economically and militarily. Hackers have penetrated the computer networks of two of America's most advanced science labs, the Oak Ridge National Laboratory (ORNL) in Tennessee and Los Alamos National Laboratory in New Mexico. In the case of the ORNL, investigators found that the hackers had stolen the names and social security numbers of all the scientists who had visited the lab. That may have been a ploy, however, to mask the real goal of accessing more critical information.

"They are going after the most advanced technologies we depend on to maintain our air, sea and land military dominance," said Alan Paller, director of research for the SANS Institute, a Bethesda, Maryland-based research and educational organization devoted to security issues. "It's those technologies that are being stolen, manufactured and will at some point be used against us — it's the worst possible scenario."

### **Private Company Leaks**

It's not Defense Department computers and networks alone that hold this data and intellectual property that is of critical importance to the United States. The systems of private companies that work closely with the Armed forces are also targets. "These companies' computers are where the future technology is," said Paller. "They are building the next weapon system and some of the worst attacks were against the computers of

those companies — not against DoD computers."

Many defense companies — like Raytheon, Boeing and Lockheed Martin — have launched divisions that offer cybersecurity services to other companies — a new and growing market. Their expertise on this front comes from having to repel attacks against their own systems. "We have a security intelligence center that protects our own network infrastructure. We use what we have learned internally to protect our customers' infrastructure," said Mary Phillips, a senior manager at the Cyber Security & Technology Communications division at Lockheed Martin. "It starts inside and then we deliver externally what we are doing for ourselves internally."

Some security experts are skeptical of defense contactors' abilities to confront cyber attacks, however. They cite a surprising inattention to basic security practices that lead to lax or even unenforced standards — from conception through execution and final assessment of defense projects. While no security system can be perfect, some experts note, the current lax approach invites many security breaches that could easily be prevented.

It's worth noting that not all hacks are direct attacks on the networks. Sometimes, private companies or military services inadvertently leak information. The most common mistake is when people carry sensitive information on small flash memory-based thumbnail drives and then misplace them. Another way classified files are shared accidentally is through Peer-to-Peer (P2P) networks that link individual computers and enable them to share movies and music. Many people are not clear on how P2P software works and unwittingly expose many sensitive documents — like tax returns, social security numbers and payroll information. Hackers are all too aware of this and are on the prowl for this type of information.

In February, a security firm discovered sensitive engineering documents about the U.S. presidential helicopter on a computer in Iran, according to a Reuters report. The engineering and avionics data was for the existing VH-60 presidential helicopters produced by Sikorsky, a unit of United Technologies, and was not connected to the new generation of presidential helicopters being developed by Lockheed Martin. An investigation by a security firm indicated the breach occurred outside the office. The investigation concluded that in all likelihood, a high-level executive might have had the data on his home computer in a folder that shared music and videos over a P2P network.

### **Key Vulnerabilities**

During the March 19 "Improving Cybersecurity" hearing, Eugene Spafford, a professor and executive director at the Purdue University Center for Education and Research in Information Assurance and Security, outlined the top reasons why computer systems are so vulnerable. Understanding the reasons behind their vulnerabilities is a critical step in shoring up the defenses. Those reasons are as follows:

- Corporations and individuals have placed too much faith in the marketplace to develop defenses and forces to develop solutions. The strategy, Spafford contends, has failed largely because there is no liability for poor quality, and there is no penalty of consequence for continuing to sell faulty products.
- Technology departments are under pressure to maintain legacy systems and compatibility even when they know they have components that have security issues.
- To maintain those legacy systems, computer managers have to buy add-on security products to patch holes, entering the never-ending penetrate-and-patch cycle.

- Little effort is made to consider security and robustness as central design criteria, leading to implementation of software and hardware developed by vendors that have not been completely vetted. Spafford says that companies are under the misguided assumption that add-on security will address any problems.
- A misperception that security involves a fixed set of problems that can be "solved." The reality, Spafford says, is that systems continue to change and face adversaries that attack in novel ways to test evolving systems.
- Computers and networks are designed to provide speed and power at the lowest cost rather than implementing known, basic security principles.
- Law enforcement does not have the resources necessary to conduct forensic computing investigations.
- There is no political awareness to secure international cooperation to investigate and pursue cyber criminals operating outside U.S. borders. As a result, there is no effective deterrent to computer crime.
- Over-classification and restrictions on data and incidents make it difficult to gain an accurate view of the scope or nature of some problems. That also means that some research efforts might be inherently naive in focus because the researchers do not understand the true level of sophistication of their adversaries.
- There exists a critical misconception that the primary goal of intruders is to steal information or crash our systems. In reality, many adversaries seek to alter critical applications or data so that systems do not appear to be corrupted but fail at critical times — or worse, operate against our interests.
- We have too few people in government, industry and the general public who understand what good security is and this has a negative impact on the way computing is taught, designed, marketed and operated.

Spafford presented a daunting list of vulnerabilities, but security experts believe that the weaknesses can be strengthened. "There's no such thing as a perfect defense," said James Carafano, a senior research fellow for Defense and Homeland Security at the Heritage Foundation. "We should disabuse ourselves of this notion that somehow we are going to have no vulnerabilities if we spend gazillions of dollars to protect everything all the time." He added that we can take steps going forward, however, to build security assurance protocols to secure information networks.

Indeed, a new set of guidelines that help government agencies strengthen their defenses is now in the final stages of development. The Consensus Audit Guidelines, or CAG, were released in February by a coalition of public and private organizations, including various agencies within the Defense Department, the Homeland Security Department and the Energy Department. John Gilligan, a former Air Force and Energy Department chief information officer, is heading the project.

The idea simple: Instead of having wildly varying protections and responses for each department, CAG will serve as a foundation for a standardized approach to protecting the United States' critical computers, servers and networks.

The Sans Institute posted a draft of the guidelines for public comment through March. Many of the recommendations seem obvious, yet security experts say that few, if any, agencies observe them closely. The recommendations include terminating dormant accounts, controlling who has access to systems and at what level, and actually setting up boundary defenses. The other critical controls listed include the following:

1. inventory of authorized and unauthorized hardware
2. inventory of authorized and unauthorized software; enforcement of white lists of authorized software
3. secure configurations for hardware and software on laptops, workstations and servers
4. secure configurations of network devices such as firewalls, routers and switches
5. boundary defense
6. maintenance, monitoring and analysis of complete audit logs
7. application software security
8. controlled use of administrative privileges
9. controlled access based on need to know
10. continuous vulnerability testing and remediation
11. dormant account monitoring and control
12. anti-malware defenses
13. limitation and control of ports, protocols and services
14. wireless device control
15. data leakage protection
16. secure network engineering
17. red team exercises
18. incident response capability
19. data recovery capability
20. security skills assessment and appropriate training to fill gaps

Taking these standardized measures, security experts say, would help fortify government networks and computers against the growing number of attacks. This might be the only working solution because tracking where a cyber attack originated — the attribution — is nearly impossible.

"That is the Holy Grail. For all practical purposes, we can't guarantee who the attacker is," said Paller. "How would you retaliate? And against whom would you retaliate? Those are all big strategic questions."