

Testimony of Alan Paller
Director of Research, The SANS Institute

Before the
Oversight and Investigations Subcommittee of the House Committee on
Financial Services
Hearing on
“Oversight of the Office of Financial Research and the Financial Stability
Oversight Council”

July 14, 2011

Chairman Neugebauer, Ranking Member Capuano, Vice Chairman Fitzpatrick, and members of the Subcommittee, as we sit before you today, the computers of federal government agencies and their contractors are under constant attack. Government computers are being infiltrated and taken over by malevolent organized crime groups and by nation-state actors; they are being infected by malicious code; and they are being retasked to gather and redirect sensitive information so that it can be mined and repurposed. The losses from such data theft is massive. Unfortunately, this is generally unknown by the public or by members of Congress because agency and contractor personnel keep these damaging attacks a secret in order to avoid the embarrassment associated with public disclosure.

I have the honor of running SANS, the largest cybersecurity school in the world, with 120,000 alumni working at institutions ranging from the NSA, the FBI and DoD, to banks, insurance companies, colleges, hospitals, and high-tech organizations in 70 countries. I also oversee the Internet Storm Center, an early warning system for the Internet, and guide the annual compilation of the most dangerous new attack vectors. These responsibilities give me direct and indirect access to information about nonpublic cybersecurity attacks as well as to the promising practices and tools available to help mitigate the threats. In my testimony today, I will frequently use data from secondary sources. I can assure you that these data provide an incomplete but very accurate picture of what is happening in cybersecurity.

In the next few minutes I'll very briefly answer several questions:

- Who is attacking the computers of U.S. government agencies and contractors?
- What are they after, and how much information have they already taken?
- How do the attacks work, and why don't current defenses stop them?

- How do cybersecurity practices differ in federal government agencies and contractors from common practices in the private financial industry?

Who is carrying out these attacks?

Teams of spies, paid by national governments, are behind most of the damaging attacks on U.S. government computers. Some are employed by the sponsoring foreign governments as civilian or military personnel; others are private contractors who also may be conducting cybercrime and economic espionage against nongovernmental organizations, either independently or on behalf of their government sponsors.

Organized crime groups also target government agencies but do far less damage to governments than they do to other commercial organizations. For example, they generally steal credit card data and other personal information and sell the data and/or extort money in return for not revealing the theft to the company's clients.

What are these attackers after, and how much information have they taken?

The nation-state-sponsored attacks have three primary objectives:

- Theft of military technology and other military secrets.
- Placement of malicious computer code on sensitive computers to gain access to additional data and to change data — to change what people believe is real. General Keith Alexander, Commander of the US Cyber Command, calls these malicious programs “remote sabotage tools.” These malicious programs are also being placed on computers inside power plants and communications networks.
- Theft of critical financial and technical data that can be used to gain unfair advantage in international negotiations involving other companies and governments.

Government is not the only target of these nation-state-sponsored attacks. An epidemic of intellectual property cybertheft is plaguing U.S. corporations and their law firms, especially those doing business with Asian nations. Unfortunately, US companies were never told of the scale or virulence or effectiveness of these attacks. But British companies were: The head of MI-5 (the UK Security Service) sent a letter to the managing directors of the 300 largest companies in the United Kingdom in late 2008. The letter said that if their companies were engaged in any negotiations or business with a major Asian power, they were being attacked with the same cyber weapons being used against military targets. As MI-5 reported, the attackers' goal is to gain an economic advantage by gaining valuable intellectual property — that is, to give their home-country companies or government officials a leg up in negotiations or even to eliminate the need to negotiate at all through the use of cyber theft. That letter also warned British companies that their law firms were also being targeted. Many hundreds of US companies have also had their systems penetrated and their data stolen and remote control software installed. You've heard about the Google attack but there are hundreds more. Some of the largest US law firms have also been deeply penetrated; their entire databases of all client records and client communication have been stolen.

Most cyberattackers seek financial and business planning data from such powerhouse corporations as Exxon or Google, but the recent attack on the International Monetary Fund and the 2010 attack on NASDAQ show that financial data held by governments and quasi-governmental organizations are also high-value and vulnerable targets.

How much information have they taken? These cyberattackers appear to be highly effective. General William Lord, Director of Information, Services and Integration in the Air Force's Office of Warfighting Integration, hinted at the extent of the losses when he inadvertently provided some classified information to a journalist. While giving a talk in a classified meeting in August 2006, General Lord left the room to take a lengthy call. While he was out, the meeting turned to some unclassified items, and a newspaper reporter joined the meeting. Upon his return, General Lord, who did not know that journalist had joined the audience, reported that "China has downloaded 10 to 20 terabytes of data from the NIPRNet. They're looking for your identity so they can get into the network as you. There is a nation-state threat by the Chinese."

Here are just a few key examples of the types and scope of information lost in such attacks:

- Nation-state-sponsored attackers gained access to technical plans for key components of the \$300 billion F-35 Joint Strike Fighter — America's most expensive weapons system. Importantly, this breach was not in the DoD itself, but against a defense contractor.
- According to Time magazine, another attack involved "a huge collection of files that had been stolen from Redstone Arsenal, home to the Army Aviation and Missile Command. The attackers had grabbed specs for the aviation-mission-planning system for Army helicopters, as well as Falconview 3.2, the flight-planning software used by the Army and Air Force."
- The IMF attack this spring demonstrates that sophisticated attackers are after governmental financial data. As the New York Times reported on June 11, "The global agency [IMF] has highly confidential information about the fiscal condition of many nations. As such, the IMF's files contain 'political dynamite' that could affect global markets."
- A senior official of the Commerce Department, testifying before a House Subcommittee in April, 2007, reported that the computers of the Commerce Department's Bureau of Industry and Security (BIS) were taken over by attackers believed to be stationed in China. The BIS division at Commerce decides which American technologies are too sensitive to export. BIS has data on what each technology is, why it is too sensitive, who makes it, and the other details that another nation would need to replicate the technology. When asked whether he knew how widely the infection had spread inside the Commerce Department or whether he was confident they had gotten rid of it, the witness said, "no."

Sadly, similar losses are occurring in nearly every major federal agency and in many smaller ones

How do the attacks work, and why don't current defenses stop them?

The vast majority of the data theft attacks are made in six steps:

Step 1: The attackers fool a person – usually a person with more access than the average user – to cause that person (the “victim”) to open an attachment to an email. I’ll show you how and why that works in a moment using your own office as an example.

Step 2: The attachment runs a hidden program that exploits a weakness on the victim’s computer.

Step 3: The victim’s computer is forced to contact the attacker’s computer, and as a result is given detailed instructions for what to search and where to look.

Step 4. The victim’s computer, now completely under the control of the attacker, gathers sensitive information, compresses it, and sends it to a site controlled by the attacker.

Step 5. The victim’s computer gets additional instructions to spread its infection to other computers that then are also forced to contact the attacker’s computer for instructions.

Step 6. The malicious software programs on these systems bury themselves very deep and erase any evidence of their existence. They sit, nearly idle, checking only infrequently with the attacker’s system for additional instructions.

This sequence of steps works in attacks against government agencies and against large government contractors, all of which process an enormous amount of information collected by and on behalf of the federal government. They also work against many corporations.

Security awareness training is ineffective in stopping these nation-state, because the attacker can send hundreds of emails and only has to fool one person. And, when the attackers are working for a nation-state with a large budget, they can spend as much as \$200,000 or more to gather intelligence

about a single intended victim and can thus craft an email that can be utterly convincing as having come from a trusted colleague. For example, a cyberattack against a congressional office may target the one person with administrative rights to all the servers in the office. The attackers would likely spend weeks or months (and a lot of money) to get close to this staff person, to learn something that is happening in the office that would not be known outside, and then to send a counterfeit email that appears to be from that person’s superior. The

Cybercrime is also lucrative for terrorists. Imam Samudra, the Bali Bomber, who exploded a bomb and murdered 200 young vacationers from Australia and New Zealand in October 2002, used cybercrime to get money to buy bomb-making supplies. In his autobiography, written while on death row, Samudra gave Al Qaeda recruits detailed instructions for using cybercrime to “make more money in a few hours of work than a policeman can make in three to six months of work.” He went on to say, “Please do not do that for the sake of money alone! I want America and its cronies to be crushed in all aspects.” [from “Hacking: Why Not!” a chapter in the jailhouse autobiography of Imam Samudra]

employer-employee relationship, combined with the inside information used in the email, provides an overwhelming incentive to open the email attachment.

In addition to gathering information directly from the government computers, cyberattackers also seek to infect government and other websites so that visitors have their computers infected and lose a lot of sensitive data or become zombies. Government computers have been caught two ways in this type of attack. As one example, a Department of Homeland Security website was infected and subsequently tried to infect every visitor to the site—a site visitors should have been able to trust. The second way that government computers are affected is that government users may be pointed toward infected websites and their computers made into zombies that can be used to gather data inside an agency network. A particularly virulent example occurred several years ago when the American Enterprise Institute website, a policy-oriented site often visited by White House personnel and other national leaders, was infecting so many visitors that the US Computer Emergency Response Team put out a warning to all federal users. Sadly, many nonfederal users were never alerted; some of them only came to know their systems were infected if they were overwhelmed and stopped functioning.

Finally, cyberattackers take advantage of the high volume in federal systems. One such case involved the IRS. Many websites offer to submit electronic tax returns for individual taxpayers, and some of these advertise through Google to draw in customers. Several of those sites were run by organized crime groups that took the data from individuals, filled out the tax returns, and submitted them—but with one important change: the criminals substituted foreign bank routing data for the taxpayers' banking information. The attack was like illegally tapping an oil pipeline, only in this case, the pipeline had electronic cash running through it.

Users cannot be expected to foil such attacks. The only powerful way to make these attacks less effective is to follow the lead of intelligence agencies and some careful financial institutions by configuring the technology to protect the users. Although many federal cybersecurity professionals know what needs to be done, it doesn't seem to get done. The great shame is that doing security right can cost less than what we spend now to do it wrong. The waste was documented by a Senate oversight subcommittee chairman, who pointed out that billions are being paid to contractors, at the rate of more than \$1,000 per page, for millions of pages of useless reports documenting out-of-date and generally less important security problems.

A much better approach is continuous automated monitoring, which means daily monitoring and correction of vulnerabilities in software and other security flaws. This has already been documented by the Office of Management and Budget as massively more effective than the out-of-date reports, but agencies just keep paying their contractors to keep producing paper reports.

Almost every federal agency outsources the bulk of its information processing to contractors—many of which have already lost sensitive data to cyberattacks. Two such attacks were disclosed this past Monday. Defense contractors have lost so much unclassified data that Secretary of Defense Robert Gates created a new DoD program to force contractors to disclose attacks, to learn from them, and to use the knowledge to try to improve defenses. The program, which is entirely voluntary, has done some good, but the contractors are reluctant to make more important changes needed to protect their systems. A new regulation

has just been proposed to force all DoD contractors to do a better job protecting their unclassified networks, but press reports say the contractors are complaining loudly and, as a result, the contractors expect to be relieved of much of the responsibility for protecting the data they keep for the government.

As I mentioned earlier, the people who know about these attacks won't tell unless compelled to do so. This secrecy allows agencies and contractors to avoid embarrassment, but it also means that critical security problems are not being fixed because the public and Congress do not know about the attacks and do not demand action. A related challenge partially caused by the secrecy, is the national shortage of people with deep technical security skills needed to make the technology more secure. This shortage plagues government and industry and is so severe that contractors at one intelligence agency will steal the skilled people from another contractor at the same or another agency, in a practice Bloomberg News labeled "fratricide" this past March. Another important aspect of this shortage is that the majority of people now working in the federal government as security professionals, and many who work for government contractors, lack the critical skills to identify or fix the type of software security flaws that routinely lead to the loss of critical data and lack the forensics and reverse engineering skills to find malicious code that has managed to penetrate their systems. Many of these "soft-skilled" people are very good at writing reports; they just are not good enough at securing computers.

How do cybersecurity practices differ in federal government agencies and contractors from common practices in the private financial industry?

One useful rule of thumb in cybersecurity is that the quality of security is proportional to the amount of money at risk. Financial institutions, because they can lose a lot of money very quickly, have better security practices than most other organizations. They implement rigorous configuration control and automated continuous monitoring and mitigation. Most federal agencies don't have those controls in place, despite a common awareness of the value of such measures.

The primary cause of this difference is the lack of consequences for federal workers and contractors who oversee and audit systems that lose critical data. It's almost unheard of for a federal worker or a government contractor to be disciplined in the aftermath of a damaging cyberattack. Banks have a long tradition of conducting after-incident analysis and meting out appropriate penalties. The tradition began with the first huge cyber heist from a bank. In 1994, a Russian named Vladimir Levin used stolen access codes and passwords to steal more than \$10 million from Citibank. In the aftermath, the top internal auditor with security responsibilities left Citibank, directly as a consequence of his missing the key risk, according to his colleagues. In federal agencies, there are no consequences for auditors who fail to see or act on the risks. Inspectors general in federal agencies rely on out-of-date checklists, often keeping their agencies from making critically needed changes. Yet, I do not recall any oversight hearing at which the IG was asked why his or her office missed the risk that led to huge losses of critical information.

The Bottom Line

In sum, cyber attacks against government sites are very hard to stop, but federal agencies could do a far better job than they are doing. As long as security remains so lax inside government, there is great risk that any data gathered by government would be easy prey for financial criminals and nation-states bent on cyber mischief. This concern applies particularly to small agencies that may lack the scale to implement first-class cybersecurity protections. For example, if the Office of Financial Research moves data from well-protected financial sites to less well-protected government or contractor sites, they will put that data at risk.

If you choose to empower OFR to gather sensitive information from financial institutions then you would sleep a lot better at night if they implement world-class cyber defenses that would include the following:

- Continuous (daily) monitoring of the twenty key controls in the Consensus Audit Guidelines (the “CAG”) and the exclusive use of tools that strictly adhere to the automation and interoperability requirements of the security configuration automation protocols developed by NIST and NSA.
- Implacable adherence to operating system and software configurations defined in the Universal Gold Master configurations approved by the DoD’s Joint Consensus Working Group.
- Rigorous multi-factor identity validation of every user without exceptions.
- A team of at least eight “hunters and tool builders” who use constantly updated scripts to monitor OFR system logs and network information continuously to find evidence of penetrations and then reverse engineer, and eliminate malicious programs that make it through the perimeter.
- Software code analysis and penetration testing for all software that accesses sensitive information and any that allows access to the systems, such as web sites.
- Auditors who verify these defenses are in place and substantial consequences for auditors if they miss well-known problems.
- If the risk to the nation’s financial system is great enough, determine whether the collected data should be treated as, and protected as classified data.

Biographical Information

Alan Paller is founder and research director of the SANS Institute, a graduate degree granting college and security training and research institution with more than 120,000 alumni in seventy countries. At SANS, he oversees the Internet Storm Center (an early warning system for the Internet), NewsBites, (the semi-weekly security news summary that goes to 210,000 people), @RISK (the authoritative summary of all critical new vulnerabilities discovered each

week), and the publication of the “Seven Most Dangerous New Attack Vectors” being discovered each year. He also leads a global security innovation program that identifies people and practices that have made a measureable difference in cyber risk reduction, and illuminates those innovations so other security practitioners can take full advantage of them to improve security in their enterprises.


He has testified multiple times before both the US Senate and House of Representatives. In 2000 President Clinton recognized his leadership by naming him as one of the initial members of the President’s National Infrastructure Assurance Council. Under President Bush, the U.S. Office of Management and Budget and the Federal CIO Council named Alan as their 2005 Azimuth Award winner, a singular lifetime achievement award recognizing outstanding service of a non-government person to improving federal information technology. In May of 2010, the Washington Post named seven people as “worth knowing, or knowing about” in cyber security. The list included General Alexander who heads the US Cyber Command, Howard Schmidt, the White House Cyber Coordinator, other national leaders, and Alan.

Earlier in his career Alan helped build a software company, took it public, and merged it into a larger company listed on the New York Stock Exchange. His degrees are from Cornell University and the Massachusetts Institute of Technology.

United States House of Representatives
Committee on Financial Services

"TRUTH IN TESTIMONY" DISCLOSURE FORM

Clause 2(g) of rule XI of the Rules of the House of Representatives and the Rules of the Committee on Financial Services require the disclosure of the following information. A copy of this form should be attached to your written testimony.

<p><i>(Faint text: Name of the witness)</i></p>	
<p>Alan Paller</p>	<p>SANS Institute</p>
<p><i>(Faint text: Title of the witness)</i></p>	
<div style="background-color: black; width: 100px; height: 20px; margin: 0 auto;"></div>	
<p><i>(Faint text: Have you ever received any financial benefit from the subject of your testimony?)</i></p>	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
<p><i>(Faint text: Have you ever received any financial benefit from the subject of your testimony?)</i></p>	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
<p><i>(Faint text: Have you ever received any financial benefit from the subject of your testimony?)</i></p>	
<p>Approximately 1,400 federal employees and and contractors have attended school at SANS, paying an average of \$3,500 EACH, ANNUALLY. we are a school and take no other federal contracts except for training.</p>	
	

Please attach a copy of this form to your written testimony.