China Has Increased Cyber-Spying On U.S., Says Commission

China has stepped up computer espionage attacks on the U.S. government, defense contractors, and American businesses, a congressional panel warns.

The top 10 U.S. defense contractors are believed to have been “victims of cyberespionage through penetrations of their unclassified networks,” the panel said in its annual report. The panel used its own analysts and investigators to compile information on data theft, based on input from defense, military, and intelligence agencies and specialists.

Spying on NASA

The security panel examined the implications of China’s pursuit of dominance not only in cyberspace, but in outer space. The Chinese have sought both military secrets from U.S. government networks and lucrative proprietary information from American corporations. The advantage China has gained from this espionage could reduce current U.S. conventional military dominance in future conflicts.

An example of Chinese espionage cited in the report involves an incident in 2005 in which Chinese cyber-burglars downloaded files about the propulsion system, fuel tanks, and solar panels of NASA’s Mars Reconnaissance Orbiter.

There has been concern about Chinese computer spying since 2002, when a large-scale series of cyber attacks was launched on U.S. government computer systems. In that attack, code-named Titan Rain by the U.S., the Chinese downloaded up to 20 terabytes of data – twice the amount stored in the entire print collection of the Library of Congress.

The security panel’s report urged Congress to spend more to protect the nation’s critical computer systems, and to monitor intrusions from abroad. It also recommended that Congress assess the security of the supply chain for computer equipment used in government and contractor
networks, and spend more to buy from trustworthy sources.

This raises another worry — the global supply chain for telecommunications items and electronic components manufactured in China. At least in theory, any such equipment is vulnerable to tampering by Chinese security services, the panel said. For example, the Chinese could implant in electronics malicious code that could be remotely activated on command, thus placing U.S. systems or the data they contain at risk of destruction or manipulation.

In spite of the enormous body of evidence to the contrary, China has always steadfastly denied engaging in any cyber-espionage or attempting to use cyberspace for military advantage.

Hackers hit White House

The White House computer network has been penetrated several times by Chinese hackers who viewed e-mails, according to a senior U.S. official. Cyberattackers penetrated the system for brief periods that allowed theft of information before government experts patched the system. The hackers got into an unclassified computer network, not the more secure classified one, but the attack was nonetheless deemed extremely serious.

Reports have also surfaced that the computer systems of Barack Obama and John McCain were hacked during the summer of 2008 as those men campaigned for the U.S. presidency. FBI and White House officials said they believe a foreign entity or organization, widely thought to be China, wanted to collect information about both candidates’ policy positions.

Employees targeted

Protecting sensitive information within the defense industry is difficult, given the number of employees and ways to access networks and information. Adversaries can use traditional human recruitment and social engineering attacks to gain access. Experts say employees are almost always the weak link in any security plan, and that continuing education and awareness training are key when it comes to securing valuable information.

Recent spy cases highlight China’s spy web in the U.S. In the past year alone, there have been at least a dozen criminal cases of Chinese espionage brought in the U.S. Notable examples include the following:

- Two engineers from China were recently sentenced to a year in prison for stealing computer chip designs from their Silicon Valley employers and trying to smuggle the secrets to China in order to launch a government-backed startup company there.
- In Newport News, Va., a Chinese-American scientist pleaded guilty to passing rocket technology to the Chinese government and bribing senior Chinese officials. The man helped the Chinese build a launch facility to send satellites and space stations into orbit.
- Motorola recently filed a civil suit against a former software engineer for the company, Chinese by birth, who already faces criminal charges as ring leader of a group that allegedly stole more than $600 million in sensitive corporate files.
- A Taiwan-born American was just sentenced to 15 years in prison after admitting he sent secret information on U.S. military purchases to Beijing.

The bottom line, analysts say, is that China’s ongoing espionage shows no signs of slowing.

Cyber Threat Forecast

Security experts predict that cyber attacks will increase in 2009.

Such attacks will “play a more shadowy role in attempts by antagonist nations to subvert the U.S. economy and infrastructure,” the Georgia Tech Information Security Center warns in its “Emerging Cyber Threats Report for 2009.”

Today, the nation’s critical infrastructure systems are fundamentally dependent on Internet-based technology, analysts agree. That means cyber attacks could disrupt U.S. power grids, water systems, transportation, communications, and other essential services.

And that makes cyber warfare attractive to U.S. adversaries — especially developing nations that lack significant military power but can nonetheless launch damaging attacks over the Internet.

The FBI recently revealed that it has thousands of open cases concerning cyber crimes. FBI officials explained that as many as two dozen nations have taken an “aggressive interest” in penetrating the U.S. government’s networks. And in the past year, that malicious activity has skyrocketed.

Malicious activity could come in the form of attacks that deny access to websites, that compromise sensitive information, or that introduce “botnets” that spread viruses and covertly co-opt computers to carry out data theft.
The Defense Department has imposed an immediate ban on the use of thumb drives and other easily portable devices that offer digital memory storage. DoD insiders believe the sudden announcement must have been caused by a security breach, though officials refused to confirm those suppositions.

The ban is part of a trend – NASA's Chief Information Officer recently sent the space agency's employees a memo severely curtailing use of thumb drives. The memo points out that recent months have seen a government-wide increase in the number of security threats originating from removable media, which can be used to infect systems with malicious code and/or remove sensitive data such as user names, passwords, and encryption keys from user systems.

NASA's new policy forbids workers from using personally owned thumb drives in government-owned computers, and vice versa. It also reminds employees to keep systems updated with security patches.

Allegations of trade-secret theft by an employee of chipmaker Intel have recently shed light on the surprising vulnerability of one of the world’s biggest and most sophisticated technology companies.

Biswamohan Pani, a low-level engineer at Intel, made off with information valued at more than $1 billion, according to an indictment.

Pani allegedly used a simple ruse to walk away with some of the chipmaker's most valuable, closely guarded information, and Intel later learned of the actions seemingly by chance.

The case provides an object lesson for companies hoping to keep their data from walking out the door with departing staff.

The facts alleged in the indictment reveal an overall lack of sophistication in Intel's efforts to safeguard the vital information, analysts say.

‘Mission-critical documents’

One intriguing aspect of the case is that Pani was able to remain an Intel employee—with access to sensitive company data—for days after beginning a job at rival Advanced Micro Devices.

Pani set June 11, 2008, to be his last day at Intel, but told managers he would be out of the office until that time, making use of accrued vacation time.

In reality, he began working at AMD on June 2. By remaining on Intel’s payroll, he maintained access to the company’s computer network.

Using his Intel-issued laptop, Pani remotely downloaded 13 highly sensitive documents, prosecutors allege. These included “mission-critical documents” describing in detail the procedures Intel uses for designing its newest generation of microprocessors.

Pani has claimed he acquired the information to help his wife, who was also an Intel employee. AMD did not ask Pani to take the information, or know he had taken it.

It was only by chance that Intel learned of Pani’s plans to work for a competitor and checked to see if he had made off with confidential files.

Just before Pani returned for his Intel exit interview, his boss heard a rumor that Pani had accepted a position at AMD.

This prompted a review of Pani’s actions, which revealed not only that he had downloaded sensitive material, but also that he had copied his Intel laptop’s hard drive onto an external storage device.

The new policy lowers a barrier that has long made it difficult for intelligence agencies to hire qualified area experts, linguists, and others simply because of their family ties.

Under the prior policy, one of the criteria for obtaining access to classified intelligence was that “the individual’s immediate family must also be U.S. citizens.” Although an exception to that standard could be granted by a senior official, it was only permitted in case of a “compelling need.”

Now, a clearance for those with foreign ties can be granted without a “compelling need,” though it may still involve additional processing.
Help Secure Yourself and Your PC in 2009

Every year, most of us pledge to eat healthier, get more exercise, and lose that extra weight. Although all these things help you feel better and give you peace of mind (if you actually follow through!), there’s another member of the household that also needs to stay healthy: the personal computer.

Here are the top things to do to help protect your PC and the vital data that lives on it:

• Use an Internet firewall. Firewalls help protect your computer from attackers who might try to delete information, crash the machine, or steal personal data. But remember, for a firewall to be effective, it needs to be turned on and set up properly.

• Run regular updates. Protect your computer against new threats by staying on top of security updates. When you first set up your new PC, be sure to accept automatic updates for all vital software. That way, all security updates will be installed without you having to worry about them, and you’ll be better protected from the latest attacks.

• Install and keep up to date an anti-virus program. Anti-virus software helps protect you from malware. As you know, viruses can slow your computer’s performance, cause a crash, or allow hackers to turn your PC into a “bot” that they use for malicious purposes. Of course, anti-virus programs, like all software, must be kept up to date so they can protect you from new threats as they emerge.

• Use anti-spyware software. Spyware is software that can, as the name implies, spy on computer users by collecting personal information. It can also change the configuration of your computer without your consent or control.

4 Fast Facts

Think all those warnings about identity theft are overblown? Consider these latest ID theft numbers, issued by the Federal Trade Commission:

1. In 2007, more than 8 million U.S. residents were victims of identity theft.
2. On average, victims spent $531 repairing the damage and 25 hours clearing up the situation with financial institutions.
3. The total cost of ID theft in the U.S. in 2007 was $49 billion.
4. This may surprise you: Arizona leads the nation in the most identity theft victims per capita.

Keeping Your Safe … Safe

As savers lose sleep over the financial crisis, consumers are increasingly taking their nest egg back to their nest — and into a safe. People are buying personal safes in record numbers as a place for cash, financial information, personal data, and medical records.

But there’s more than you might think to selecting a safe. Here are some factors the experts say you should keep in mind:

• Consider the weight of the safe. The more it weighs, the less likely a burglar can carry it out of your home.
• Place the safe in the basement to decrease the risk of it falling through the floor in the event of a fire.

When purchasing a safe, look for the Underwriters’ Laboratory certification mark, which indicates it’s gone through rigorous testing.
Did You Know That . . .

… The U.S. is especially vulnerable to security threats during the first months of a new presidency, analysts are warning. They point out that in recent times, there has been an unwelcome surprise early in every new President’s first term. Alarming, terrorists now have more weapons (physical and cyber) than ever before.

… Controlled but unclassified Defense Department information is leaking to the public from thousands of DoD-sponsored websites, according to Chief Information Officer John Grimes. Military experts are growing alarmed at the amount of vital, yet unclassified, data that is freely available online. Some of the data is being placed at risk by military contractors.

… Spy photos were recently found on a camera that was purchased – you guessed it – on eBay. The camera was bought for $30 by an Englishman who was stunned to find on it top-secret photos taken by British spies of Al Qaeda suspects. Images of rocket launchers were also stored on the camera.

Is Your Home an Easy Target for Thieves?

If a burglar wants to break into your house, he probably can. Fortunately, most burglars are lazy and fearful; they target the easy pickings. Here are some tips that’ll persuade burglars to skip your home:

• Keep your garage door closed as much as possible. Leaving the garage door open when you go out tells all who pass that there’s no car inside. And leaving the door open when you’re home is a bad idea, too – a burglar might figure out that your garage door is closed only when nobody’s home.

• Post a “Beware of Dog” sign. Dogs bark and bite. Crooks hate them. Post the sign even if you don’t have a dog. For similar reasons, a sign or sticker from a security company is a great deterrent, even if you do not use such a service.

• Leave a sandbox or tricycle in your yard – even if you don’t have young kids. Burglars prefer to stay away from homes that have young children. These homes are less likely to be vacant than others. A five-dollar yard-sale trike could save you thousands!

• Remove thick hedges and privacy fences. Burglars love to target homes with windows or doors that are not visible from the road or neighboring homes; they can take their time breaking into these houses without fear that they’ll be seen. If a high hedge or fence around your home provides potential cover for burglars, replace it with something shorter.

5 Tips to Prevent ID Theft in ’09

Here are some simple things you can do to protect yourself from identity theft in 2009 and beyond:

1. Invest in a shredder. Many people unwittingly leave a gold mine of information in their trash in the form of discarded credit card offers, old bank and credit card statements, etc.

2. Protect your mail. Stealing mail is another way ID thieves obtain personal information. Consider buying a lockable mailbox, or installing a mail slot if your mailbox is unsecured.

3. Limit what you share. Some people give away their info when they don’t need to by writing unneeded information on checks. Do not print your Social Security number, phone number, date of birth, or credit card account number on your checks.

4. Deactivate old credit cards. Close down any credit card accounts you have not used and don’t plan to use. These are easy targets for identity thieves once they have your personal information.

5. Monitor your credit report. Get your free reports every year. To order online: visit http://www.annualcreditreport.com; to order by phone, call (877) 322-8228.

Take Steps to Protect Sensitive Data from Hackers, Spies in ’09

It’s the start of a brand-spanking-new year, and that means we’ve all got a clean slate and a fresh start. That applies to information protection, too.

To get you off on the right foot, we’ve assembled a list of common security Problems, as well as Solutions that’ll help you do your best this year!

Problem: Securing sensitive information in today’s on-the-go world.

Solutions:
• Keep it on you. The best way to make sure your data doesn’t get stolen is to keep it with you at all times. If possible, don’t leave your laptop or other sensitive information in your hotel room. Resist the urge to ask the person next to you to keep an eye on your belongings when in a café or a restaurant.
• Encrypt It. The practice of scrambling data on your hard drive is standard among intelligence professionals, and it is just as important for business professionals. That way, if your laptop or PDA is lost or stolen, the information on it will be useless to others.
• Use a privacy filter. Remarkably simple and practically undetectable, privacy filters protect the data on your computer screen from prying eyes by making the screen visible to persons only directly in front of it.
• Be careful with thumb drives. Tiny, easily portable USB drives are a growing security risk. Before downloading data to one, check with your manager or IT department to find out what policies your employer has in place.

Problem: Despite the digital age, paper is still the biggest security risk.

Solutions:
• Shred all proprietary information with a cross-cut shredder. Desk-side shredders are ideal and affordable.
• Develop guidelines that outline the proper procedures for protecting sensitive information.
• Keep all sensitive information and files locked away. Restrict access to those who need it.
• Avoid leaving documents in communal copiers, shared printing spaces, conference rooms, or other open areas.
• At the end of each work day, all employees should log off their computers and lock their workstations or office doors. All confidential documents should be filed away rather than left on employees’ desks.

Problem: Dirty desks allow secrets to walk out the door.

Solutions:
• In general, keep your workspace clean. The problem with a sloppy work area is that if something does go missing, it’ll be harder for you to tell it’s gone.
• Lock sensitive documents and computer media in drawers or filing cabinets.
• Physically secure your laptop with a security cable. Your security or IT department will be happy to assist you in choosing an appropriate locking cable.
• Secure your workstation before walking away, even just for a bathroom break. It’s easy to password-protect your desktop to make sure nobody can sneak a peek at your computer while you’re away. In some cases, employees have even sent inappropriate email messages from a coworker’s computer.

Problem: Unauthorized visitors to the facility pose a security threat.

Solutions:
• Physical security starts with awareness and responsibility. Anytime you see anybody onsite without the appropriate security badge, it’s your duty to politely address them, and funnel them to security if necessary. Remember, social engineering hackers can only cause a breach if workers are too intimidated to approach them.
• Don’t get “tailgated.” This is the practice, commonly used by social engineers, of walking through a checkpoint, gate or door immediately behind a legitimate employee. If somebody tries to tailgate you, be polite (as usual!), but firmly guide them to the nearest security worker for the appropriate badge or card.
• Monitor and report any suspicious activity around your workplace’s access points. Common problem areas include loading docks, delivery entrances, parking lots, dumpster areas, and gates (if the building is fenced).
• Be aware that social engineers frequently pose as cleaning staff or technology employees as a way to cruise through offices unnoticed in search of secrets. Challenge anybody you don’t recognize.
Illegal exports of weapons, military equipment, and national security-related technology to potentially adversarial nations are on the rise. A crackdown on illegal exports of U.S. military technology led to a 32% increase in the number of arrests and criminal prosecutions in 2008, the Justice Department reports.

More than 145 U.S. and foreign businessmen as well as a few scientists, professors, and students were charged with illegal transfers in 2008, compared with 110 the prior year. Items illegally exported included rocket technology intended for China; fighter-jet and helicopter parts destined for Iran; and a “huge number” of firearms going to Mexico.

Part of the 32% increase was due to the prosecutorial crackdown, but experts say the worldwide demand for U.S. military technology is growing.

**Suspicions lead to arrests**

One positive sign is that many of the recent tech-transfer prosecutions came about because U.S. businesses grew suspicious about potential buyers, and notified law-enforcement agencies. In other cases, foreign buyers were busted when they attempted to make illegal purchases from undercover law-enforcement agents.

According to the Justice Department, efforts by some foreign governments to illegally obtain U.S. technology remain aggressive. Some nations have actually established front companies in the U.S. to acquire military items. Others target U.S. companies directly, or hire other firms (sometimes based in the U.S., sometimes overseas) to procure technology for them.

**Fallout from illegal transfers**

The threat posed by illegal technology transfers is very real, with ramifications for national security, U.S. competitiveness, employers – and individual employees.

Every day, foreign states, criminals, and terrorist groups seek arms, technology, and other materials to advance their technological capacity: weapons systems and (in some cases) weapons of mass destruction programs. With the U.S. producing the most advanced technology in the world, it has become a primary target of these illicit technology acquisition efforts.

Items sought are as diverse as missile technology, nuclear technology, assault weapons, trade secrets, source code, military aircraft parts, night vision systems, and technical know-how. The improper transfer of these items poses threats to U.S. allies, our troops overseas, and to Americans at home. It also undermines America’s strategic, economic, and military position in the world.

Illegal tech transfer also undermines the competitiveness of U.S. businesses, which more than ever must compete in the global market. Enterprises spend billions developing new products and technologies, and industrial espionage can cost them the advantages they’ve earned. And it stands to reason that the eventual fallout from illegal technology transfer reaches all the way to individual employees, who may face layoffs if business drops due to criminal exports.

**Doing your part**

So what can you do to make sure your employer steers clear of inadvertent illegal technology transfers? Here’s a checklist developed by experts that’ll help you spot potentially fishy transactions:

- The customer or purchasing agent is reluctant to offer information about the end-use of the item.
- The product’s capabilities don’t fit the buyer’s line of business.
- The item ordered is incompatible with the technical level of the country to which it is being shipped.
- The customer is willing to pay cash for a very expensive item when the terms of the sale would normally call for financing.
- The customer is unfamiliar with the product’s performance characteristics but still wants the product.
- Routine installation, training, or maintenance services are declined by the customer.
- Delivery dates are vague, or deliveries are planned for out-of-the-way destinations.
- A freight-forwarding firm is listed as the final destination.
- Packaging is inconsistent with the stated method of shipment or destination.
- When questioned, the buyer is evasive and unclear about whether the product is for domestic use, for export, or for re-export.
Security Quick Quiz

Think you know security? If so, then it’s time to test your knowledge of government security responsibilities and procedures.

1. True or False: Unauthorized entry into a classified, compartmented computer system may be grounds for revoking my security clearance.

2. True or False: My Secret security clearance gives me access to all information at the Secret level.

3. True or False: I may take classified material home overnight, and work on it at home, as long as I am certain to keep it under my personal control at all times.

4. True or False: Documents marked For Official Use Only have the lowest level of classification.

Answers

1. True. Whether motivated by the challenge of penetrating the system or by curiosity to “see what’s in there,” unauthorized entry into any computer file is a deliberate disregard for rules and regulations. It involves violation of the need-to-know principle or invasion of privacy.

   Some people assume unauthorized entry into a computer file isn’t a serious offense, but it can be a basis for revocation of your security clearance. Failure to comply with expected standards of personal conduct may cause your security clearance to be reevaluated.

2. False. Your security clearance gives you approved access only to information at the same or lower level of classification as the level of your clearance, and that you have a “need-to-know” in order to perform your work.

   Need-to-know is a fundamental security principle; it limits the damage that can be done by a trusted insider who goes bad.

   Failures in implementing the need-to-know principle have contributed to the damage caused by many recent espionage cases.

3. False. You must not take classified material home under any circumstances.

4. False. For Official Use Only (FOUO) is not a classification at all, and is not subject to the same controls as classified information. FOUO is a document designation used by the Department of Defense and other federal agencies to identify information or material which, although unclassified, may not be appropriate for public release.

By the Numbers

A new study spotlights common data-loss mistakes made by employees. Resolve to avoid the risks that can lead to the loss of sensitive information.

- About 70% of IT professionals say employee access of unauthorized applications and websites causes half of their companies’ data loss incidents.

- In the past year, 40% of IT pros say they’ve dealt with employees accessing unauthorized parts of a network or facility.

- In a sign that corporate trade secrets aren’t always secret, 24% of employees admit they’ve verbally shared sensitive information with non-employees.

- Almost half of the employees surveyed (44%) say they’ve shared work devices with others.

- Almost two of three employees admit they use work computers daily for personal use.

At least a third of employees leave computers logged on and unlocked when they’re away from their desk. These employees also tend to leave laptops on their desks overnight, sometimes without logging off, creating potential theft.

The Employee Security Connection (ISSN 0894-2080) is published quarterly by the National Security Institute, 116 Main Street, Suite 200, Medway, MA 02053. Subscriptions are $845 per year, telephone (508) 533-9099 for information concerning company/agency subscriptions. ©2009 National Security Institute. All rights reserved.

The subscribing facility is authorized to make this document available to its employees via its Intranet. Distribution is reserved exclusively for current subscriber companies/organizations of record and is not transferable. Posting of this document, or any portion thereof, via the Internet or an Extranet is strictly prohibited. Permission to reproduce copies for in-house distribution is reserved exclusively for current subscriber organizations of record and is not transferable. Reproduction of this material for purposes of incorporation in any publication intended for sale is prohibited without express permission of the publisher.

January – March 2009

Employee Security Connection

Yes, I accept your risk-free offer. I want to receive the best source for enhancing employee security awareness in my company. Please enter my full year’s subscription to the Employee Security Connection at just $899 per year for a single facility (Please call NSI at 508-533-9099 for inquiries re: multiple facility/enterprise-wide licensing). I understand that I will receive my own PDF version of the Employee Security Connection each quarter for the next 12 months. (Mass. residents please add 6.25% sales tax)

Name:_______________________________________________________________________

Title:________________________________________________________________________

Company:____________________________________________________________________

Address:_____________________________________________________________________

City:__________________________________    State_____    Zip_________________

Tel:_________________________________________________________________________

E-Mail:______________________________________________________________________

___ Payment enclosed ___ Bill my company -- PO#________________________________________

I prefer to charge my:  ___ VISA ___ MasterCard ___ AMEX

Card #:_________________________    Expiration Date:________________________

Name on card:_________________________________________________________________

Signature:_________________________________________________________________

National Security Institute

165 Main Street, Suite 215, Medway, MA 02053

Tel: 508-533-9099 - Fax: 508-507-3631 -- E-Mail: InfoCtr@nsi.org