EMPLOYEE

Security

CONNECTION

Volume 24 **A quarterly awareness briefing for defense industry and government employees** Number 1

In this issue. . .

Page

3 Unseen Security Risks Reside in Copiers

4 Top 10 Scams to Avoid in 2010

5 6 Safety Tips for Social Networking

6 U.S. Cracks Down on Classified Info Leaks

7 How U.S. Protects, Tracks Its Secrets

8 Checklist Before You Leave on Vacation

Report: Cyber Spies Attack Defense Contractors 'Every Hour'

Defense contractors are under constant attack by foreign intelligence services attempting to gather technology secrets, according to a Defense Security Service report.

The report finds that foreign nations are increasingly exploiting the Internet, including social networking sites, to conduct industrial espionage against Defense Department contractors. "Defense-related technologies and information are under attack each day, every hour and from multiple sources," says the report. "The attack is pervasive, relentless and unfortunately, at times, successful."

The Defense Security Service oversees security at 13,000 contractor facilities; contractors are required to detail suspicious contacts with foreign nations or commercial organizations to the agency.

Vast quantities of data

Just how large is the threat? Here's one way to look at it: the U.S. is losing enough data in cyber attacks alone to fill the Library of Congress many times over, experts say. The report finds that more than 100 foreign spy agencies are working to gain access to U.S. computer systems, as are criminal organizations. Even terrorist groups are known to have cyber attack capabilities.

U.S. computer systems are probed thousands of times a day and scanned millions of times a day, government computer analysts have informed Congress.

Hackers have already penetrated the U.S. electrical grid and have stolen intellectual property, corporate secrets, and money, according to the FBI's cybercrime unit. In one incident, a bank lost $10 million in cash in one day.

The scale of the losses, including the theft of sensitive and unclassified data, is staggering, experts admit.

Direct attacks

The report says direct requests for information sent via email were the most

ORED OFFICE OF RESEARCH AND ECONOMIC DEVELOPMENT
MISSISSIPPI STATE UNIVERSITY
Facility Security Office

prevalent type of attempt to obtain information on U.S. defense systems, followed closely by "suspicious Internet activity," a category that included intrusions into unclassified contractor networks.

The attacks came from nations considered both friendly and otherwise. Countries in East Asia and the Pacific, including China, the two Koreas, and Vietnam, dominated Internet attempts. Email messages requesting price quotes and system information were the preferred method to attempt to steal information on U.S. technologies.

Users also sent multiple email requests for the same information to different individuals working for the same contractor.

Worker info vulnerable

The report warns that the abundance of personnel information on contractor websites, as well as the growing use of social networking sites such as Facebook and Twitter, "give a likely targeting advantage to East Asia and Pacific cyber actors exploiting the Internet."

Hackers from East Asia and the Pacific region focused their attention on information systems, accounting for 29% of suspicious contact reports, according to the report. More than a third of the attacks (36%) from European countries (including Russia, France, Germany, and the UK) tried to obtain information on aeronautical systems, while 12% targeted data on information technology.

Attempts to obtain information on unmanned aerial vehicles (UAVs), which the military has used successfully in Iraq and Afghanistan, have increased to an extent that the report devotes a special section to them. Bottom line: the U.S. is fending off constant, exhaustive efforts to steal UAV-related technologies and information.

'Friendly' Nations Spying

Adding insult to injury, not all of these info-seeking bids come from countries viewed as enemies; NATO allies have tried a variety of Internet probes to obtain information on UAV technology, including offers to buy entire systems and suspicious requests asking to team with a contractor or to create a joint venture.

Social-networking sites present a massive risk to defense contractors, the report says. Amazingly, many potentially sensitive UAV-related videos can simply be watched on YouTube. Modern spies also maintain a presence on Twitter, Facebook, and LinkedIn.

LinkedIn is considered especially risky by many because many large U.S. defense corporations use it to glean personal information on potential hires. LinkedIn provides detailed personal information that can make the recipient of a phishing email think it's from a legitimate sender.

As sites like Facebook continue to grow in popularity, many employers have set policies in place aimed at making sure workers don't post sensitive company data either intentionally or by accident. One common espionage ploy today is to create an account (often with the name and photo of an attractive young woman), then send "friend" requests to everybody at a given company or department.

Because social networking users tend to trust the "friends" they make at such sites, they are likely to let down their guard and reveal potentially sensitive data about their workplace. Experts say all employees, especially those whose work involves sensitive information, should understand and follow their company's policy on social networking sites. ❑

Russian Spy Ring

Eleven people have been arrested for allegedly serving as secret agents of the Russian government with the goal of penetrating U.S. government policymaking circles.

The arrests culminate a multi-year investigation that turned up allegations of a vast undercover network designed to collect critical information for Moscow, including new U.S. nuclear weapons research.

The alleged spy ring's members were given the single, primary goal of becoming "sufficiently 'Americanized'" to gain access to the U.S. government's planning and policy apparatus, the FBI said in an affidavit.

To underscore that point, U.S. officials said they decrypted a 2009 message sent to two of the alleged co-conspirators.

"You were sent to USA for long-term service trip," the intercepted message read. "Your education, bank accounts, car, house etc. — all these serve one goal: fulfill your main mission, i.e., to search and develop ties in policymaking circles in U.S. and send intels [intelligence reports] to C.'" "C" was identified as the Russian foreign intelligence headquarters in Moscow, also known as "Moscow Center.'"

The group, dubbed the "illegals," was accused of being tasked by the Russian intelligence agency SVR to enter the United States, assume false identities, and become "deep-cover" Americans, according to the Justice Department.

Facebook Spy Scam

A number of Israeli soldiers reportedly fell victim to a recent Facebook spy scam, demonstrating the security risks inherent in social networking sites.

The soldiers thought they were "friending" a young woman – who may actually have been a Hezbollah operative. A Facebook profile belonging to one "Reut Zuckerman" was used to lure soldiers to reveal sensitive information over the course of a year. "Zuckerman," whose photograph showed an attractive woman lounging on a sofa, pretended to be in the Israeli army herself.

Some soldiers are said to have given out such sensitive information as their friends' names, military jargon, secret codes, and detailed descriptions of their bases. Eventually, the "Zuckermann" profile was taken off Facebook after some heads-up soldiers reported it to their superiors. Espionage experts say it's now common practice for spies to use Facebook and LinkedIn to seek sensitive data.

Unseen Security Risks Reside in Copiers

The hard drives in copy machines hold thousands of images and are rarely erased when sold. Believe it or not, these humble machines may constitute one of the biggest security risks at any company.

Unless a copier contains a security program to scramble the information, or the hard drive is purged, all the documents on it can be retrieved.

Workplace risk

The potential security risks for businesses are frightening. Let's face it, we've all walked past the shared office copier and raised our eyebrows at the material we found atop it or forgotten inside: job reviews, sensitive planning memos, info on future campaigns, etc.

Where printers and copiers are concerned, security is usually an afterthought. And if the copiers operate on a network, physical access to the hard drive is not even necessary – access can be gained through the network.

These security risks can be remedied with a program that scrambles the data on the hard drive. But too often, organizations skimp on this security feature. In one recent investigation, researchers retrieved thousands of documents from publicly available copiers. Many documents contained highly sensitive data and could just as easily have been stolen by identity thieves or corporate spies.

Congress, FTC concerned

Analysts say securing the lowly copier is one of the next challenges for businesses and other organizations, and they're not alone. Some congressmen want to know more about the vulnerabilities presented by copiers, as does the Federal Trade Commission.

It's unclear whether Congressional hearings, new regulations, or both will follow, but the call to better understand and control copier risks is gathering steam.

In the meantime, experts say all workers should do their part to ensure the safety of photocopied sensitive information.

- If your organization has policies regarding which copiers may be used for sensitive data, be sure to follow them.

- If you send jobs to a printer/copier electronically, it's a good idea to take a quick walk beforehand to make sure the machine isn't jammed or in use.

- Never send a job twice (many workers do this when they're not sure the job went through), and of course never leave the original document on the copier.

Security Breach Cost

Underscoring the importance of safeguarding sensitive data, the average cost of an information security breach has nearly tripled in the past two years, according to a recent survey by PricewaterhouseCoopers.

The survey reveals that 92% of businesses have experienced security incidents over the past year, ranging from hacking attacks to accidental leaks of data. Each incident costs between $402,000 and $980,000 to remedy – a massive increase from $129,000 - $244,000 in 2008.

The growth in incidents reflects the growing reliance businesses have on computer systems and the Internet. Some 61% of large companies detected attempts to break into their systems, up from 31% two years ago. One in six say an intruder managed to get through their defenses. Large companies are dealing with an average of 45 incidents a year, up from 15 two years ago.

SECURITYbriefs

Top 10 Scams to Avoid in 2010

Con artists never sleep! Here are some scams experts say you should watch out for this year:

'Free trial.' According to the Better Business Bureau, companies that peddle diet pills, teeth whitening strips, and so on show no sign of slowing.

Vishing and Smishing. These phishing attacks exploit Voice over Internet Protocol and SMS messages. Scammers pose as financial institutions and claim your credit card or bank information has been compromised.

Health insurance scams. In the wake of federal healthcare changes, ripoffs are surging. One survey found 57% of state fraud bureaus reported a rise in healthcare-related scams.

Mortgage madness. Phony forensic auditors and attorneys are calling consumers and claiming they can get them off the mortgage hook – for upfront fees.

Loan modification scams. This one's similar to the mortgage ripoff; scammers promise desperate homeowners they can avoid eviction in exchange for fees.

Online car ads. Online classified sites are hotbeds of fraud. Common tricks include scams in which buyers are asked to deposit money in a fake escrow service, and the "price too good to be true" con.

Travel trouble. Watch out for con artists selling bogus travel insurance or impossibly cheap vacations.

Scholarship scams. Financial aid scammers claim millions of dollars in private scholarship money goes unused. In truth, private scholarships tend to be reserved for specific individuals.

Job-search jerks. Fake recruiters trawl the web for desperate job seekers. Many misrepresent their services, promote fictitious job openings, or charge high advance fees.

Work-at-home scams. These have been around forever, but the poor economy makes them tempting. Be warned; these "opportunities" are almost never legitimate.

Lost Luggage

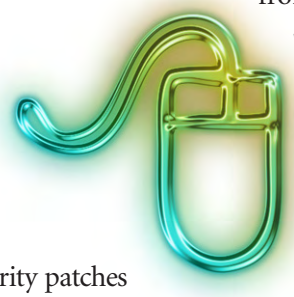
Did you know about 30 million bags failed to arrive at their destinations on time last year? Make sure yours do get there:

- Attach a sturdy ID tag to your bag with your contact information, including a cell phone number.
- Also put contact information inside the luggage, in case the tag gets knocked off.
- Put a distinctive ribbon or sticker on your luggage so you can find it quickly at baggage claim.

4 Summer Computer Tips

It's natural to let down your guard in the lazy, hazy summertime – but it's also dangerous! Stay secure with these tips:

1. Pay close attention to your email. It's still the most commonly used channel for spreading threats.



2. Install the latest security patches for your applications. Cyber-crooks frequently launch attacks that exploit security holes in common programs. Software companies continually make security patches available, but they only work if you install them!

3. Don't download programs from dubious Internet sites. Summer always brings a rise in the number of downloads people make; it's important to make sure yours are safe.

4. Exercise caution with social networks. Don't publish details like the day you'll be going on vacation, especially if details of your address are available on the same social network.

Did You Know That. . .

… A confessed spy was convicted recently of smuggling and other charges after he tried to acquire sensitive encryption gear from eBay and other sources. Chi Tong Kuok, of Macao, says he was acting on behalf of the Chinese government, and that the gear was to be used to monitor U.S. communications.

… Airport body scanners are okay with most U.S. travelers, according to a recent survey. Nearly two-thirds (65%) said they approve of full-body scans as a tradeoff for improved airline safety. The Transportation Security Administration will soon deploy more than 450 new scanners despite questions surrounding their accuracy and effectiveness.

… Cyberattacks are viewed by many experts as the biggest threat to the power grids in both the U.S. and Canada. A new report warns that if sophisticated attackers target multiple key nodes in the system, the resulting failure could exceed present-day repair capabilities. The report calls for better coordination between power companies and the government.

6 Safety Tips for Social Networking

By now, most people know that social networking sites such as Facebook, Twitter, and LinkedIn pose security risks. To help you stay safe on these sites, we offer the following tips:

1. Think about how different sites work before deciding to join one. Some sites allow only a defined community of users to access posts; others allow anyone to view them.

2. Think about keeping some control over the information you post. Consider restricting access to your page to a select group of people – for example, friends from school, your club, your team, or your family.

3. Keep sensitive information to yourself. Don't post your full name, Social Security number, address, or phone number. Be cautious about posting information that could be used to identify or locate you offline.

4. Make sure your screen name doesn't say too much about you. Don't use your actual name, your age, or your hometown. Even if you think your screen name makes you anonymous, it doesn't take a genius to combine clues to figure out who you are and where you can be found.

5. Post only information you're comfortable with others knowing. Many people can see your page, including your parents, your teachers, the police, and the company you might want to work for in five years!

6. Remember that once you post information online, you can't take it back. Even if you delete the information from a site, older versions exist on other people's computers.

5 Steps to Emergency Preparedness

Nobody likes to think about them, but disasters do happen. Your family should create a plan for fires, natural disasters, and other unforeseeable events. Here are some steps to get you started; learn more at www.fema.gov.

1. Decide how you will get in touch with other family members if you're alone when a disaster strikes.

2. Name a friend or relative you can all contact in the event the family is separated. Choose a person who lives in another town or state that won't be affected by the same disaster.

3. Contact your children's school principal and learn what emergency plan is in place. Let your kids know that in case of an emergency, they should remain calm and listen to their teacher or principal.

4. Keep contact numbers, emergency numbers, medical numbers, and insurance information taped inside binders, notebooks, book bags, wallets, etc. Write the list in waterproof ink.

5. Learn what your community's plans are in the event of evacuation.

U.S. Cracks Down on Classified Information Leaks

Each year, unauthorized leaks cause severe damage to U.S. national security and expose our intelligence activities and capabilities. Some of the worst damage comes not from penetration by spies, but from unauthorized leaks by those with access to classified information.

Experts say the White House is quietly ratcheting up its campaign against national security leaks, and indeed some recent stiff sentences appear to bear this out. Anybody entrusted with sensitive information would do well to take note.

Examples abound – There are, unfortunately, plenty of examples of damaging information leaks in today's headlines.

Military officials recently confirmed they arrested an Army intel analyst for allegedly giving classified U.S. combat videos to the website Wikileaks. Specialist Bradley Manning also claims to have released hundreds of thousands of diplomatic cables from the State Department, which is studying what damage the leak may have caused.

The Justice Department recently indicted a former National Security Agency official for allegedly leaking information about a mismanaged computer program. Thomas A. Drake fancied himself a whistleblower who spoke to a reporter only after failing to convince government agencies they were squandering hundreds of millions of dollars, but he now faces years in prison and 10 felony charges involving the mishandling of classified information.

Prosecutors secured a 20-month prison sentence against an FBI linguist who leaked to a blogger. That's the longest sentence ever handed down to a government employee for passing national security secrets to the media, and is widely considered a signal that the Obama administration plans to get tough with leakers.

All told, the FBI says it identified 14 leakers of sensitive information in the past five years. Starting with 183 "referrals" (possible leaks), the agency opened 26 investigations and concluded that 14 warranted suspect status.

Unintentional leaks – Most experts agree that while intentional, criminal leaks of sensitive data are a major problem (as shown by the examples above), unintentional breaches are actually far more common, and just as potentially damaging.

Social-networking sites such as Facebook, LinkedIn, and Twitter have all been channels for these accidental leaks, as have blogs and, of course, email.

Facebook's sky-high popularity has made the site a magnet for all sorts of spies. One popular gambit is to create a bogus account supposedly belonging to an attractive young woman, then seek to "friend" U.S. soldiers or employees who work with sensitive data. The spies then slowly, methodically gain the trust of these online "friends," with a goal of eventually learning classified (as well as personal) information.

The federal government itself recently confessed to an accidental, and potentially catastrophic, breach: it made public a lengthy report, clearly marked "highly confidential," with detailed info on the nation's civilian nuclear sites and programs.

Fortunately, there are some simple steps you can follow to make sure you don't accidentally disclose corporate or government secrets:

Remember "need to know." Possessing the appropriate clearance level is only half the equation; remember that everybody, including your co-workers, must have a *need to know* classified data.

Lock the laptop. One recent study found that over half of government workers took a laptop computer home to access data that was supposed to stay in the office.

Paper is king. Sure, you need to secure digital data, but keep in mind paper still presents the greatest risk. Shred or lock up sensitive documents.

Know your responsibilities. If you access classified information, you signed a contract requiring you to accept certain obligations as a condition of your continued employment. Keep this in mind!

Loose lips. On the walls of the Intelligence Committee room are framed posters from World War II that remind of the dangers of leaks. "Loose lips might sink ships," warns one. Another poster shows a ship in flames and reads: "A careless word … a needless sinking." The ghosts of leaks past serve as potent reminders of the dangers of leaks today.

Report Shows How U.S. Protects, Tracks Its Secrets

The national security classification system hit both highs and lows in 2009, the Information Security Oversight Office (ISOO) disclosed in its latest annual report to the president.

The total number of reported national security classification actions skyrocketed to a record 54.8 million, a startling 135% increase over the year before, according to the report. However, this increase isn't as alarming as it may seem; it was largely due to a change in reporting practices to include email and other electronic products that were excluded from previous reports.

Numbers actually falling

In fact, the ISOO pointed to several positive developments in 2009 in terms of limiting classification activity. The actual number of wholly new secrets, or "original classification actions," decreased 10% to about 183,000. (The large majority of classification actions are known as "derivative classifications," which means they incorporate or reproduce in a new document information that was previously classified.)

The number of "original classification authorities" – that is, individuals who are authorized to designate information as classified in the first place – also decreased 37% to about 2,600. That's the lowest number of authorized classifiers reported since ISOO began keeping statistics 30 years ago.

More good news: in 2009, agencies assigned a maximum duration for classification of 10 years or less to 67% of newly classified records, the highest fraction ever. The number of pages that were declassified declined by 8% in 2009, to 28.8 million pages, although the number of pages that were reviewed (52 million pages) actually increased slightly.

The ISOO's annual report is widely viewed as a touchstone for assessing the state of national security secrecy each year; it provides a unique public compilation of agency data on classification activity.

Concerns

In addition to the positive developments in its report, ISOO noted many concerns and challenges:

Oversight efforts continue to identify shortcomings in agency implementation of basic requirements. Of particular concern are requirements related to implementing directives, security education and training, classification guides, and self-inspections.

Sustained vigilance on the part of senior leadership within the agencies is critical to success. That must be why they call it bureaucracy: in the Executive branch alone, there are nearly 2,400 classification guides in use. And only 54% have been updated in the past five years. Clearly, streamlining the number of guides and updating them more frequently should be a goal.

Mission: Reduce overclassification

The story behind the story of the ISOO's 2009 report begins with a directive from President Obama to reduce the amount of classification in government documents, which skyrocketed after the terror attacks of September 11, 2001.

Obama's executive order made several changes to the classification system. For example, it allows different agencies to more easily share classified data with one another, and it directs employees to use the lowest possible level of classification.

Those trying to implement the changes compare the process to reversing a battleship; it's not going to happen instantly. In essence, a sweeping cultural change is needed, as the model that prevailed until now focused on secrecy.

The government spent $8.3 billion last year to create and safeguard classified information, and $43 million to declassify it, according to ISOO. The figures don't include data from the principal intelligence agencies, which is classified.

Declassification

Naturally, in the search for more openness, the *de*classification of data takes on new importance. The ISOO's report contains plenty of encouraging news here, including the following:

In 2009, agencies reviewed nearly 52 million pages (!) and declassified about 29 million pages of records. Overall, the ISOO has reason to be proud of its progress. Analysts agree the next several years will tell if the shift is a long-term trend.

Security Checklist Before You Leave on Vacation

Summertime, and the living is … risky.

Sad but true; burglars and identity thieves look forward to these months as much as you do; they know people often let down their guard around vacation time.

To make sure you don't pay for a thief's summer getaway, we offer some expert tips.

Before you leave home:

Trim the shrubs. You may think dense shrubbery around the house offers privacy, but it creates cover for burglars.

Create light and sound. Use automatic timers for your lights inside and motion detector lighting outside your house. New timers have a random on/off time and battery backup in case of power outages. It's a good idea to attach radios to these timers to create noise.

Leave a key with a trusted friend or neighbor so they can check, at least once every 48 hours, on your home.

Create that lived-in look. For lengthy trips, have a neighbor park a car in your driveway, keep your front door clear of newspapers/brochures, and arrange to have your lawn mowed.

Lock up. This sounds obvious, but people overlook it! Ensure all windows, doors, and garage doors are locked. You might also disconnect power to automatic garage doors.

While traveling:

Streamline your purse or wallet. Bring only the credit and debit cards you'll truly need and a driver's license. That way, you limit your risk if your purse or wallet goes missing.

Go easy on the debit card. If a thief "skims" this card, he can empty your bank account immediately. Credit cards, on the other hand, have many consumer protections built in.

Remember that vacation rentals such as beach cottages are virtually impossible to secure, because so many renters have keys and the locks are usually cheap. When you're leaving for the beach, consider locking valuable items such as laptops and cameras in your car – it's probably more secure.

Hotel rooms aren't much better. If you're in a hotel, it's probably not wise to leave expensive electronics and jewelry in your room.

Report This!

You are the first line of defense against espionage. The government relies on you to safeguard national security by reporting behavior that may relate to the unauthorized disclosure of classified information.

If you spot the following behaviors, it's important that you report them to your security department immediately:

- A colleague has contact with an individual known or suspected to be associated with a foreign intelligence service.
- A co-worker asks you to obtain classified information to which he lacks authorized access.
- You learn a colleague has been keeping classified material at home or in some other unauthorized place.
- You spot someone removing classified material from the work area without appropriate authorization.
- You observe someone improperly removing the classification markings from documents.
- A colleague begins extensively using the office copier or fax machine to reproduce or transmit sensitive information.
- You learn that a co-worker is facing extreme financial pressures due to divorce, debts, or alcohol and drug abuse.

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 $899 per year, telephone (508) 533-9099 for information concerning company/agency subscriptions.

July – September 2010