EMPLOYEE

Security

CONNECTION

Volume 23 **A quarterly awareness briefing for defense industry and government employees** Number 1

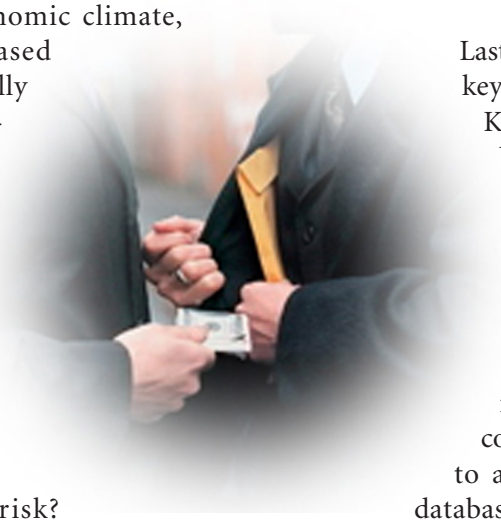
In this issue. . .

Page

Corporate Espionage on the Upswing

Corporate espionage on the home front, committed by foreign spies and global competitors, may be intensifying, security and law enforcement officials warn.

The difficult economic climate, coupled with increased layoffs that potentially lead to more disgruntled former workers, are fueling the situation. Now, more than ever, all employees must block espionage efforts to safeguard proprietary and sensitive information.



How real is the risk? Very; the cost, in terms of both monetary loss and jobs lost, can be staggering. Sure, you may not hear about many breaches – but that's because businesses keep such events hushed up, for obvious reasons.

Dozens of recent cases highlight the reality of corporate espionage. For example, an engineer at chipmaker Volterra told employers he was leaving the company to get married in Taiwan – but he was actually stealing data for a startup company there.

Last year, a man installed keylogging software on Kinko's stores in New York, then successfully stole login information from dozens of users.

And a Cisco Systems worker recently resigned, then used a co-worker's computer to access the company database and steal valuable product-development data. Make no mistake: the risk is real!

$45 billion!

Analysts say corporate espionage costs the world's 1,000 largest companies more than $45 billion each year. While all industries are vulnerable, firms in the defense and high-tech sectors need to be especially watchful. All told, U.S. businesses lose up to $250 billion in revenue as well as 750,000 jobs annually.

To help do your part to fight spying in

your organization, you need to understand the two basic types of threats: technical and non-technical.

Technical threats

Experts say that while businesses have worked hard to improve their networks and PCs with strong password policies and other measures, there is one glaring exception: the lowly printer. Once a worker sends a print job down the hall and forgets about it, the vital data sits there for all to see.

Keyloggers are another favorite tech tool of spies. They may be hardware or software devices, but once they're installed on a computer, they capture every keystroke – including passwords, of course – and relay this information back to the hackers, who can then easily access the network.

The explosive growth of wireless communication has also been a boon to corporate spies. They can often sit in company parking lots and intercept unencrypted wireless transmissions, and of course Wi-Fi hotspots are notorious havens for those who seek to steal information.

Non-technical threats

While the techie threats appear intimidating, analysts say you're actually more likely to fall victim to *non*-technical scams.

Perhaps the most common of these is simple and effective: disgruntled employees or former employees, taking advantage of sloppy access and password practices, steal vast amounts of product and customer data on their way out the door.

Sometimes, these thieves are hired or developed by foreign nations or competitors. Often, however, they make the decision to steal information on their own, out of a desire for revenge or financial gain, and then simply shop the info around. In either case, it's important that you keep an eye out for telltale signs of an inside job – a coworker who seems unbalanced or in dire financial straits, for example.

And by now, most workers are aware of the bag of spy tricks collectively known as social engineering. This occurs when thieves or spies use their knowledge of human nature to trick workers into divulging sensitive information. For example, social engineers may call on the phone pretending to be a company IT worker, and demanding your logon information.

Armed with this knowledge, here are some sensible countermeasures you can take when you suspect a spy. Experts stress that all employees at all levels of the organization bear some responsibility for halting corporate espionage.

Stop tailgaters. Tailgating is a favorite method of spies seeking physical access to a facility; they simply wait for an employee to use his or her access card, and slip in behind. Don't worry about being rude; if you suspect someone's tailgating you, report the incident.

Obey the basics. You've heard these tips a thousand times, but they bear repeating: Never click on unknown email attachments. Create strong passwords, and change them according to company policy. Don't transmit sensitive company data from unsecured wireless hotspots. Don't download freebie software like screensavers and games.

Be alert. As noted above, if you spot a coworker behaving in a manner that you fear may lead to insider theft, don't hesitate to report the suspicious activity to your security department.

Security Risks R Us

Think you know your stuff when it comes to spying? Try our quick quiz.

True or False: Because most data is stored digitally, "dumpster diving" is largely outmoded and is not considered a significant security threat.

True or False: If you recognize the sender's name in an email, it's safe to click on enclosed links even if you're not sure what they are.

True or False: Social networking sites like Facebook and LinkedIn are a growing security worry for businesses.

True or False: If your password is truly strong, it's okay to use it for multiple accounts, such as banking and work.

Answers

False. Trash is still a major source of company security breaches – shred sensitive documents!

False. Many computer worms automatically send themselves to everyone in the victim's address book.

True. Spies and scammers have developed sophisticated ways to "friend" people on Facebook, then use that trust to access sensitive information.

False. No matter how solid your password seems, it may be hacked – and if you use it for multiple accounts, thieves then know all your secrets!

Classified Data Sold

A Department of Defense official with top-secret security clearance allegedly provided an official working for the Chinese government with classified department data and documents. Experts say the alleged crime is a textbook case of insider theft.

Officials have charged James Wilbur Fondren Jr., deputy director for the U.S. Pacific Command Washington Liaison Office, with espionage conspiracy. Fondren allegedly sold the information to a Taiwanese-American man in the form of "opinion papers" via an at-home consulting business he ran on the side.

Fondren, 62, allegedly funneled the data to Tai Shen Kuo, who was one of his consulting clients. Kuo purchased reports from Fondren for anywhere between $350 to $800, eight of which included classified information. Among the classified data Fondren supplied Kuo was information about a joint U.S.-China naval exercise, U.S.-China military meetings, and a DoD draft report on China.

U.S. Military Technology Easy to Buy, Ship

Military hardware that can be used in nuclear devices and ground fighting can be easily purchased in the U.S. and shipped overseas, a government investigation has revealed.

The Government Accountability Office set up fake companies to obtain military and dual-use items – that is, items that have both military and commercial use – in the U.S. and ship them overseas. The domestic purchases allow buyers to avoid U.S. restrictions on sales to foreign entities.

Nuclear parts

Items purchased in the bogus transactions included parts for making nuclear devices and guiding missiles that could carry nuclear warheads, as well as night-vision devices, body armor, and other hardware for ground combat. Investigators say they learned that sensitive dual-use and military technology can be easily and legally purchased from U.S. manufacturers and distributors, then illegally exported, without detection.

Those investigators stressed that no laws were broken by any of the companies that sold items to the undercover GAO operation, and that the magnitude of trying to check all overseas travelers and shipments makes it impossible to halt illegal export of the items under current law.

When presented the GAO report, Congressmen said the lack of regulation or export controls made the situation particularly troubling.

Letter of the law

Undercover investigators complied with all required checks in purchasing the equipment, including the submission of end-user agreements that forbid exporting the equipment or using it in any nuclear, biological, or missile weapons. But such documents amount to nothing more than an honor system pledge rather than a true enforcement mechanism, experts say. Most of the transactions took place by e-mail and telephone calls.

The kind of front company and scheme used by GAO investigators are the kind being used by terrorist organizations today, the report says. This was not a hypothetical situation; this is being done.

The investigation shipped some of the dual-use items to a country that is a known trans-shipment point for terrorist governments and foreign governments attempting to acquire sensitive technology, according to the GAO.

Investigators would not name the country but said it's in southeast Asia and that the shipments were simple packages labeled "documents" and sent by regular mail.

Foreign Affairs

If your livelihood depends on having and maintaining a security clearance, you'll want to take note of this case: A federal judge has sentenced a civilian contractor from Houston to six months in prison for hiding his affair with a Chinese woman while he worked at the U.S. Embassy in Beijing.

Gregory W. Blackard, 37, was sentenced on one count of conspiring to make false statements. According to prosecutors and court documents, Blackard lied to federal agents about his 2005 to 2007 relationship with the woman when he was repeatedly asked whether he had frequent contact with any Chinese foreign nationals while working on a construction project at the embassy.

As part of having high-level security clearance to work on the project, Blackard was required to report any frequent contact he had with Chinese citizens.

SECURITYbriefs

Be Safe When Traveling Overseas

Overseas travel is exciting, whether you're packing for a pleasure trip or just hoping to do some sightseeing in conjunction with business travel. But now, more than ever, it's important to be prepared when you leave the U.S. Here are some tips and hints that will help you prepare:

Before you leave:

• **Make copies** of all personal documents you're taking with you: passport, credit cards, driver's license, and itinerary, for example.

• **Leave a detailed itinerary** with family or friends, so they know where you are. It's also wise to set up times to keep in touch via telephone – if you don't call at the appointed time, your family or friends can alert the authorities.

• **Leave your cellphone** at home. You may face truly insane roaming charges when making calls abroad. Experienced travelers buy a prepaid phone as soon as they touch down, and use it for the duration of their trip.

• **Alert your credit card companies** that you're about to depart. Overseas charges are a red flag for companies seeking to prevent fraud; if you fail to notify them, they may put a hold on your card, leaving you high and dry!

While you're abroad:

• **Try to blend in.** Sadly, there are many global hotspots where being an American makes you a potential victim. Avoid the "American uniform" of jeans, T shirt and baseball cap.

• **Maintain "situational awareness."** This means not climbing in sketchy-looking unmarked taxis, for example, and not following a "guide" into seedy areas of a city.

• **Get a hotel room** that's not on the ground floor; for obvious reasons, first-floor rooms are far less secure than those higher up.

Cybercrime Up

U.S. Internet fraud losses reached a record high $264.6 million in 2008, with more than 275,000 complaints received by the Internet Fraud Complaint Center.

The 2008 figure is a huge jump from $18 million in losses reported in 2001. And so far this year, from February to March, there was a 50% increase in reported Internet fraud complaints.

The amount of money lost per complaint has increased from about $325 per complaint in 2004 to $931 per complaint in 2008, according to the report.

Top 5 Home Security Mistakes

• **Unlocked doors and windows.** Even when you're at home, windows and doors should remain locked. By failing to secure the entries, you create an opportunity for someone to trespass or burglarize your family.

• **Leaving alarm systems off.** You wouldn't expect your car to run or your washing machine to clean your clothes if they weren't turned on, right?

• **Hiding keys on the property.** No matter how clever you are with your hiding place, leaving a key to your home on the exterior of your property is a huge risk.

• **Leaving sheds and garages unlocked.** Most people think burglars carry their own tools, but by leaving tool sheds unlocked, you create an opportunity for an unplanned break-in.

• **Ignoring ground maintenance.** Untrimmed hedges make great hiding places!

Did You Know That. . .

… U.S. military data, including launch procedures for a highly sensitive missile-defense system, were recently found on a hard drive bought second-hand on eBay. In a study, researchers found that fully 34% of all used drives contained sensitive information such as medical records, business plans, consumers' financial data, and Social Security numbers.

… Lost laptops cost organizations an average of $50,000 apiece. That result comes from a new study in which the maximum value of a stolen laptop came in at a cool $1 million – hardly surprising, experts say, given the extremely sensitive business information that typically resides on executives' computers today.

… Sensitive nuclear info was recently posted for all the world to see on the website of the Government Printing Office. Oops! The unclassified data included maps of fuel stockpiles for nuclear weapons. The slip occurred days after President Obama declared cyber-security a national security priority. Naturally, the information was quickly pulled down once the alarm was sounded.

Take the Fraud Alert Quiz

Everybody thinks they know enough to steer clear of online scams – but the number of victims keeps growing! Answer these questions to see how savvy you are.

Have you been informed that you were the winner of a foreign lottery, such as Canadian, Australian, El Gordo, or El Mundo, that you did not enter?

Have you been instructed to either wire, send, or ship money as soon as possible to a large U.S. city or to another country, such as Canada, England or Nigeria?

Have you been asked to pay money to receive a deposit from another country such as Canada, England, or Nigeria?

Have you responded to an email requesting you to confirm, update or provide your account information?

After using an online job-hunting service, have you been contacted by someone claiming to be hiring for a position that seems perfect in terms of salary, location, etc.?

Have you been contacted about starting a home-based business? If so, is there an upfront fee for getting your company started?

Have you been asked to run a package-forwarding business that requires little more than receiving and forwarding shipments?

Scoring for this quiz is simple: If you answer "yes" to *any* of the questions, you could be a fraud victim or on the verge of being scammed. Con artists are always promising potential victims the world; keep your eyes open and be wary of "opportunities" that seem too good to be true.

Resolve to Be Ready this Summer

With experts predicting more natural disasters this summer, be prepared:

Assemble a disaster supply kit. The Federal Emergency Management Agency recommends a kit with a three-day supply of non-perishable food, water, first aid supplies, a battery-powered radio, a flashlight, extra clothing and blankets, matches, photocopies of credit and ID cards, and essential medications.

Pick two safe meeting places. Choose a safe meeting place outside your home in case of a sudden emergency, such as a fire. Also, choose a second location outside your neighborhood in case you cannot return home for any reason.

Know how to shut off your home's natural gas, electricity, and water. Natural gas leaks and explosions are responsible for a significant number of fires following disasters; water also becomes a precious resource after many disasters.

Consider a portable generator. They can be crucial when temporary power is needed, but they can also be hazardous – never operate a generator indoors or in the garage.

Polygraph FAQ: Honesty Is the Best Policy

The very word "polygraph" strikes fear into the hearts of many who've been raised on a steady diet of detective movies and TV shows. But the polygraph is a useful tool for government intelligence agencies and other organizations today, and there's no reason you should fear it.

With that in mind, we'll take a look at some frequently asked questions about polygraphs; understanding the procedure will help ease your mind. Keep in mind that being honest and talking through any anxiety you may feel is the best advice.

Q: What is a polygraph?

A: It's a special test that can be administered to help determine an individual's eligibility for access to highly classified intelligence information.

Q: Do polygraphs work?

A: They are considered reliable in detecting the truth or falsity of the answers to objective questions, especially those that can be answered with a "yes" or "no" in reference to specific acts. Some experts believe subjective questions produce less reliable results. False positives and false negatives are rare when proper questioning procedures are followed.

Q: I've heard there are two types of polygraphs. What are they?

A: There are indeed two types:

In a **counterintelligence polygraph**, questions are restricted to topics such as espionage, sabotage, and terrorism.

In a **lifestyle polygraph**, questioning is more extensive and can involve all aspects of present and past behavior. The test process usually takes between one and three hours.

(A **full scope polygraph** combines the above types.)

Q: I have nothing to hide, but I'm nervous about getting a full scope lifestyle polygraph – the process itself is daunting! What can I expect?

A: Your nervousness is certainly understandable; polygraphs can be intimidating. But when you get down to it, the key is to be truthful and stay relaxed.

Q: Is it true I'll be asked all the questions *before* I'm hooked up to the machine?

A: Yes, this is a regulation. And it's one you can use to your advantage – before being hooked up, while the polygrapher is asking the questions, if there's anything you're concerned about, or anything that makes you nervous, this is the time to talk about and get past it. The idea is to get past anything that's causing you anxiety.

Q: Okay. So once the machine is hooked up, what happens?

A: The polygrapher will ask you the questions you went over initially in a yes or no format. Be honest and relax – that's the best way to handle it.

Q: How does one fail a polygraph?

A: The test is designed to look at physiological activities in a person. If you answer a question and your heart rate increases, the machine will pick this up, and the polygraph specialist may determine you are being deceptive or are hiding something. However, it could be that you are just nervous about the line of questioning. As noted above, the key to success with the polygraph is to talk out anything that may bother you *beforehand* with the polygraph specialist. This can definitely help you deal with any anxiety or nervousness that may cause the machine to read something.

Q: What happens if I fail my polygraph?

A: There's no sugarcoating it: if you fail a polygraph, that can be the end of that job. However, you can ask for and will sometimes be granted a second or third polygraph, depending on the agency and the circumstances. Always ask for an appeal and request another polygraph.

Q: What happens if I hold a Department of Defense clearance and already took a counterintelligence polygraph, but I later try to gain employment with an agency that requires a full-scope polygraph and I fail? Is access to all classified information consequently revoked?

A: If you already hold a clearance with the DoD and you try to go through the CIA or NSA process and fail, this does not take away your existing clearance.

State Department Spy Case Highlights Growing Insider Threat

In a case that has rocked the intelligence world, both a former State Department official with top-secret security clearance and his wife were recently arrested and charged with spying for communist Cuba for nearly 30 years.

Walter Kendall Myers, 72, and his wife Gwendolyn Steingraber Myers, 71, were charged with conspiracy to act as illegal agents and pass along classified information to the Cuban government. The affidavit suggests they were active as recently as April of this year. They're also charged with wire fraud.

Long history

Kendall Myers began working for the State Department in 1977 and traveled to Cuba in December 1978 for "academic purposes" after an invitation from the Cuban government. The couple were visited by Cuban officials while living in South Dakota, and prosecutors say they agreed in 1979 to spy for the communist country.

The Cuban Intelligence Service then allegedly directed Myers to resume his employment with the State Department, or to shift to the CIA. Myers returned to Washington with his wife and got a position that required a top-secret clearance.

The clandestine activity alleged by prosecutors, which spans nearly three decades, is incredibly serious and should serve as a warning to any others in the U.S. government who would betray their trust by serving as illegal agents of a foreign government, officials said.

Various methods

Myers is said to have told an FBI source that he typically removed State Department information by memory or by taking notes, and that he occasionally took documents home. Myers claims to have received "lots of medals" from the Cuban government and says he and his wife spent an evening with Fidel Castro in 1995.

The affidavit says the Cuban Intelligence Service often communicated with its U.S. agents by broadcasting encrypted radio messages on shortwave radio frequencies, and that the couple has "an operable shortwave radio in their apartment and they told an FBI source that they have used it to receive messages."

According to the Justice Department, the spy episode began to unravel in April when the FBI launched an undercover operation to convince the couple they'd been contacted by a Cuban intelligence officer and to ascertain the scope of their activities for the Cuban Intelligence Service.

An FBI source posing as a Cuban intelligence officer then approached Kendall Myers, saying that he had been sent to contact Myers by a Cuban intelligence official.

Recruitment techniques

Experts say this case, while it's garnered more attention than most, is hardly the first time U.S. citizens have spied for Cuba.

How does the communist nation find these spies? A former Cuban intelligence operative who recently defected to the U.S. has issued a report that offers a rare glimpse into Cuba's intelligence operations.

Jose Cohen Valdes was a Cuban intelligence officer employed in several areas of information acquisition and analysis in Havana. He has now documented his nation's penetration of U.S. universities in a report that has yet to be translated into English.

In the report, Valdes explains that the intended purpose of the spy recruits is not only to gather information, but to become agents of influence – individuals who can shape U.S. policy to assist a foreign nation and work against the best interests of the U.S.

He also points out that Cuba has been tied to virtually every major terrorist organization, from Hamas to Colombia's FARC communist guerrilla army.

Ex-Engineer Charged

A Chinese-born engineer stole trade secrets critical to the U.S. space program and passed them to China for three decades without being detected.

In the first economic espionage case to reach trial in the U.S., prosecutors charged Dongfan "Greg" Chung, 73 – who pleaded not guilty – with conspiracy, economic espionage, lying to federal agents, obstruction of justice, and acting as a foreign agent.

Chung allegedly gained the trust of Boeing Co. and his previous employer, Rockwell International, and used his job as a stress analyst at the companies to steal more than 250,000 pages of sensitive documents. The documents included trade secrets on a phased array antenna for the U.S. space shuttle and on the Delta IV booster rocket.

Audit Finds Flaws in Security Clearance Processing

Although the Defense Department has reduced the time it takes to process personnel security clearances, many clearance authorizations are still taking more than four months to complete – and some lack important information, according to a report from the Government Accountability Office.

The DoD and the Office of Personnel Management reported that the fastest 90% of initial security clearances for military and defense civilians were processed in an average of 124 days in 2008. But when the GAO studied all the initial clearances completed in 2008, it found 39% took more than 120 days to finalize, while 11% took more than 300 days.

The report also found that of the 3,500 top-secret clearances adjudicated in July 2008, 87% were missing at least one key piece of documentation (most often, employment verification). And 12% of those clearances also didn't include a personal interview.

Defense's clearance process has been on GAO's high-risk list since 2005. It's important to note that despite the flaws it found, the GAO concluded that both the Pentagon and OPM are now meeting timelines mandated in the Intelligence Reform and Terrorism Prevention Act of 2004.

'Derogatory information'

In less optimistic clearance news, the Pentagon may have issued top-secret clearances last year to as many as one-in-four applicants who had "significant derogatory information" in their backgrounds, including a record of foreign influence or criminal conduct, according to one audit.

The Pentagon granted more than 450,000 initial security clearances, as well as 180,000 renewals, to military personnel, civilian employees, and private contractors last year, based on the results of background investigations conducted by OPM.

The risks inherent in granting security clearances to the wrong people are illustrated by the case of Noureddine Malki, a naturalized U.S. citizen who worked as a contract translator in Iraq. Last year, Malki pleaded guilty to lying about his background in his application for a top-secret security clearance.

GAO auditors said their report concentrated on top-secret clearances because people with them "have access to information that, if improperly disclosed, could cause exceptionally grave damage to national security."

Cyber Espionage

Researchers at the University of Toronto have uncovered a computer spying operation they called GhostNet that was based primarily in China and had stolen documents from governments and private businesses around the world.

In another worrisome sign, there have also been recent credible reports that cyber spies from China, Russia, and other countries have penetrated the U.S. electrical grid with the aim of disrupting the system.

Moreover, cyber perpetrators are known to have sought access to information about the Pentagon's next-generation fighter aircraft, the $300 billion Joint Strike Fighter.

In the case of the Joint Strike Fighter project, attackers were able to copy and siphon off multiple terabytes of data related to the design and electronics systems, which could make it easier for hostile nations to defend against the aircraft.

Analysts agree that evidence points to China as being the base for spies responsible for the GhostNet attacks, and that they've hacked U.S. servers too.

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.

July – September 2009