EMPLOYEE
Security
CONNECTION

Volume 32 **A quarterly awareness briefing for defense industry and government employees** Number 4

In this issue. . .

This newsletter is brought to you by the NASA HQ Office of the Chief Information Officer and the Office of Protective Services.

Threats Posed by Careless Insiders, Foreign Governments at All-Time High

Careless and untrained insiders, as well as foreign governments, are the most common sources of security threats for federal agencies, and by extension businesses that work with them.

That finding headlines a recent survey from Market Connections, which polled federal technology leaders about a range of security threats: careless or untrained insiders, foreign governments, the general hacking community, hacktivists, malicious insiders, terrorists, for-profit criminals, and industrial spies.

In an unsettling turn, most of those threat sources were deemed to be at all-time highs in the recent study. As noted, the worst security threats turned out to be:

- Careless or untrained insiders, cited by 56%.
- Foreign governments, flagged by 52%.

Spying by hostile nation-states and hackers connected to them is a major problem, but at least the motive is easy to understand—they want to steal defense and industrial secrets (*see sidebar*).

But what is it that makes careless insiders an even greater threat—why is accidental exposure, deletion, or modification of data causing federal breaches? (By the way, about half of respondents say contractors' personnel present higher risks than actual federal employees.)

The insider risk is worsening – by accident

A related study, this one from Egress, includes the bombshell finding that 61% of CIOs believe employees leak sensitive information maliciously.

But in yet another study, performed by Dtex, about two-thirds of insider threats were found to be caused by users who introduce risk due to either careless behavior or human error. The Dtex researchers found that 13% of threats were due to compromised credentials, with only 23% caused by malicious intent.

So it's clear that when it comes to breaches, there's a major disconnect between tech leaders and workers. Consider the following:

- 79% of IT leaders say employees have put company data at risk accidentally in the last year. As noted, 61% believe they've done so maliciously.
- Meanwhile, over 92% of employees say they haven't violated data-sharing policy.
- 60% of IT leaders think they'll suffer an accidental insider breach in the next 12 months, and 46% believe they'll suffer a malicious one.
- Asked about leading causes of data breaches, IT leaders were most likely to name employee carelessness (60%). That was followed by a general lack of awareness (44%), while 36% blamed a lack of training.
- From the employee perspective, of those who had accidentally shared data, 48% said they had been rushing, 30% blamed a high-pressure work environment, and 29% said they were simply tired.
- The most common employee error was accidentally sending data to the wrong person (45%), while 27% had been fooled by phishing emails.

Drilling down on employee mistakes

So, what are some of the other non-malicious security mistakes made by workers? Let's break them down by category: email, password, and web security, which experts cite as the Big Three.

Email

– Opening attachments or clicking links that include malware. Far too many employees still do this, despite repeated warnings. Virtually all spearphishing and business email compromise attacks originate with such a click.

– Forwarding emails with suspicious links. This is no better than clicking the link yourself; it merely kicks the can, making the sketchy email somebody else's problem.

Passwords

– Easily guessed passwords. Researchers know, from studying widespread data breaches, that a disheartening number of workers still use such ridiculous passwords as 123456.

– Written-down or shared passwords. Employees also still write passwords on Post-It notes or scraps of paper. They may make a token effort to hide these notes—or they may actually pin them to cubicle walls.

– Reusing passwords. While it's not easy remembering the passwords for multiple accounts, using the same one over and over increases the harm if the password is breached.

– Leaving devices unprotected entirely. This is common on cellphones; to save time, people decline to create so much as a simple PIN. It's a major mistake, as that PIN, password, or fingerprint is your first line of defense if the device is lost or stolen.

Web security

– Clicking on advertisements. Sure, most ads are innocent—but those promising something too good to be true are often scams that may lead to data-theft sites.

– Surfing to sketchy sites or exploring the "deep web." The risk here is obvious. Your work computer should be used for business only; many deep web sites instantly track you and install malicious code.

– "Shadow IT," which is the practice of installing and using apps not approved by your employer. The problem here is that these software tools, while possibly useful, usually lack corporate-grade security features.

Bottom Line: When it comes to cybersecurity, people remain the weakest link in the organization. So please do your part to help ensure that government and company secrets are not compromised. ■

U.S. Universities Targeted

According to Accenture's iDefense unit, Chinese hackers recently targeted more than two dozen universities, many in the U.S., in an attempt to steal research about maritime technology. MIT and the Universities of Washington and Hawaii are among the victimized institutions.

Experts say the report is further evidence that Chinese cyberattacks intended to co-opt U.S. research on defense and military subjects are on the rise.

Following the pings

iDefense researchers learned which universities were being targeted by noting that their networks were "pinging" computer servers located in China. Those servers were controlled by a hacking group known by many names, including Mudcarp and Leviathan, to those in the security arena.

That group, linked to the Chinese government, is associated with breaches of Navy contractors that resulted in the theft of military information, including submarine missile plans.

As to the universities, nearly all have research labs that study undersea technology; many are linked to the Woods Hole Oceanographic Institute in Massachusetts. Researchers said the Chinese showed interest in these technologies, among others:

- Deployment of unmanned aerial drones from submerged submarines.
- Underwater modems and other systems related to undersea communication.

Contractor Pleads Guilty

Harold Martin, a former contractor who spent decades stealing classified information from both the National Security Agency and the Department of Defense, recently pleaded guilty. Martin, a 54-year-old Navy veteran, admitted that he stole and retained government documents from approximately 1996 until 2016, which is when he was arrested.

When federal agents raided Martin's Maryland home, they found 10 firearms—which his wife was unaware of—as well as about 50 terabytes of information. He went so far as to keep stolen papers and electronic documents in his car, according to prosecutors. Data in those files, from gaps in U.S. military capabilities to CIA intelligence collection sources, could cause grave harm to national security.

According to prosecutors, Martin also communicated online with people in Russian and other languages (it's not clear whether the stolen information fell into the hands of U.S. adversaries).

Former U.S. Counterintelligence Agent Charged with Espionage

Monica Elfriede Witt, a former U.S. service member and counterintelligence agent, was recently indicted by a federal grand jury for conspiracy to deliver and delivering national defense information to the Iranian government.

According to the Department of Justice, Witt helped Iranian intelligence services target her former fellow agents in the intelligence community. She also allegedly disclosed the code name and classified mission of a DoD Special Access Program.

Now 39, Witt defected to Iran in 2013 and remains at large. An arrest warrant has been issued for her.

Co-conspirators

The indictment charges four Iranian nationals with conspiracy, attempts to commit computer intrusion, and aggravated identity theft. Working on behalf of the Iranian Revolutionary Guard Corps, the four allegedly sought to deploy malware that would provide them access to U.S. intel community members' computers.

Arrest warrants have been issued for the conspirators, who also remain at large.

How did all this come about? According to the DOJ, Witt (a U.S. citizen) was an active-duty U.S. Air Force Intelligence Specialist and Special Agent of the Air Force Office of Special Investigations, who began duty in 1997 and left the U.S. government in 2008. She last worked as a contractor in 2010.

In 2012, Witt traveled to Iran for an anti-U.S. propaganda event. In the aftermath of this event, and due to contacts made during it, Witt apparently flipped. She re-entered Iran in 2013 and went on to disclose U.S. classified information to a contact, prosecutors say.

Turning on colleagues

As part of her work on behalf of the Iranian government, Witt conducted research about at least eight U.S. intel community personnel she had worked with, and used that information to draft "target packages" against these U.S. agents. Beginning in late 2014, her conspirators began a malicious campaign targeting these former co-workers and colleagues.

In one attack, the conspirators created a Facebook account said to belong to a former colleague of Witt. That bogus account caused several of Witt's former colleagues to accept friend requests.

Senior members of the U.S. intelligence community say Witt did serious damage, with one rating that damage a "seven or eight" out of ten.

Trade Secrets Theft

Remember how the formula for Coca-Cola was said to be a closely guarded secret? Well. A Chinese-born scientist formerly employed in connection with the beverage giant stands accused of seeking to swipe trade secrets from companies working with Coke in order to set up a rival venture—funded, in part, by China's government.

The claims against Xiaorong You, of Michigan, say her attempted theft exemplifies "the rob, replicate, and replace approach to technological development," a DOJ release notes. The trade secrets are said to be worth more than $100 million.

The trade secrets You is alleged to have stolen relate to the development of cans and food containers. Until 2017, she worked at an Atlanta company that did business with Coca-Cola. There, she was one of a limited number of employees who enjoyed access to those secrets.

SECURITYbriefs

Scammers Spoof DHS Caller ID

It's natural to take seriously a call from the Department of Homeland Security. After all, these are the folks safeguarding the nation in very turbulent times, right?

Well, yes. But the person on the other end of the line most likely is a criminal, not a DHS employee. The department recently alerted consumers that scammers are "spoofing" DHS phone numbers in an attempt to steal personal information.

In such a scam, your phone's caller ID displays a number that is indeed assigned to DHS. Make no mistake, though: the caller is a crook posing as a law enforcement or immigration official.

These scammers may claim you've been the victim of identity theft—and then demand that you "verify your personal information" by telling them your Social Security or bank account number. Don't fall for it!

The key is in the phone-number spoofing. Most consumers are wise to this, but in case you're not: *It is trivially easy for anybody to make any number pop up in Caller ID.*

Some tips on avoiding phone and spoofing ripoffs:

- Don't answer any call from an unknown number. If you do, you confirmed that your phone number is working, and you'll get many more calls.
- If the caller (or a recording) says you can push a button to stop receiving calls, resist the temptation and hang up instead.
- Never respond to questions, especially ones with a Yes or No answer.
- If you get a call from a legitimate company, hang up and call the number on your account statement or on the company's website to verify the original call.
- Do not allow the caller to force you into an immediate decision or action.

Social Engineering

Here, according to experts, are the three most common types of social engineering attacks. Guard against them all!

1. Phishing. These email attacks may look incredibly genuine, so always be skeptical.

2. Tailgating. This is a physical tactic in which a criminal tries to creep into a work space behind a legitimate employee.

3. Pretexting. In these attacks, someone approaches you, often over the phone, with a reason to extract sensitive information—for example, they claim to be an HR temp updating records.

'Smart Home' Security Risks

Here's an eye-popping number: According to a report from SonicWall, attacks on "smart home" devices rose by almost 220% last year!

It's just another indication that the internet of things has brought with it new security problems. Let's look at a few:

- **Sketchy manufacturers.** Everybody's jumping into the IoT space, and it's hard to tell which companies stand behind their products and take security seriously. In such a market, it's advisable to stick with brands you know.
- **Default passwords.** Makers of routers and various smart-home devices ship products with simple passwords that hackers know. Your first move should always be to create your own (strong!) password.
- **Lack of attention.** Who thinks about their thermostat? Their doorbell? Well, it's time to start; those IoT devices may be sending spam or launching cyberattacks.

Did You Know That. . .

Vetting of international travelers takes a step forward as new facial scanners in U.S. airports and other ports of entry come online. President Donald Trump recently signed a policy document calling for greater use of biometric tech, as well as increased data sharing, in an effort to prevent the travel of known or suspected terrorists.

Nineteen minutes is all Russian hackers require to move from an initial security breach to full control of a network. This recent CrowdStrike finding notes that it's a dizzyingly quick time. While most people focus on the initial intrusion, the speed with which Russian attackers parlay a hack into wider network access is far more worrisome.

Old USB drives contain recoverable information belonging to the previous owner about 67% of the time, according to a new Comparitech study. And oh boy, that data: nude pictures, tax documents, and highly sensitive work-related info were all easily found by researchers. Suggestion: smash old USBs with a hammer!

Cybersecurity and Remote Working

It's no secret that the massive growth of remote working has led to security woes. Indeed, a new OpenVPN study finds that 36% of businesses have dealt with security incidents caused by a remote employee—and to many experts, that figure seems low.

These breaches may be caused by vague policies or a lack of training. But let's turn the focus on what individual employees can do to avoid being part of the problem:

- **Know your employer's policies.** Yes, we just noted they're not always well communicated—but that's just more reason to learn what is expected of you whether working at home or engaged in business travel.
- **Take responsibility for your devices at all times.** That means PIN-protecting your phone, using your laptop for work only, and not letting your kids watch YouTube on your work tablet.
- **Use a VPN if possible.** A virtual private network creates a private tunnel beneath the public internet. It's a great way to keep your data secure.
- **Public wifi is a major risk.** You know this already, right? The hotspots located in coffee shops, airports, and convention centers are havens for eavesdropping attackers. Plan your sensitive communication accordingly.
- **Consider your apps.** Download only approved apps from the Apple Store or the Android Play Store. And even then, check out the end user agreement before downloading; many apps share a ridiculous amount of your data.
- **Pay attention to hygiene.** Security hygiene, that is! All software should be updated regularly.

10 Ways to Beef Up Your Home Security

Spring cleaning! While you're making your home look better, make it more secure too:

1. Replace burned-out lightbulbs around outside doors.

2. Trim trees and shrubbery so would-be burglars have no place to hide.

3. If you have a ladder stashed behind the house or garage, put it inside—otherwise, a crook can make use of it.

4. If you don't already, consider using gravel or pea-stone around your house. It crunches when stepped on, and burglars hate that.

5. Get an alarm system installed—or at least put an alarm-company *sticker* in a front window.

6. Make sure your locks work, and don't forget the garage—these buildings often house expensive tools and hobby gear.

7. Don't leave a spare key in the usual places, such as under a doormat.

8. Consider joining a Neighborhood Watch program. Members keep their eyes and ears open fo any suspicious activities.

9. Make sure any fencing is in good repair.

10. Don't tempt "porch pirates" by leaving Amazon deliveries in plain sight.

China Increasingly Using LinkedIn To Recruit Foreign Spies

LinkedIn is a favorite destination for those seeking to make professional connections—and that includes China's intelligence community.

Exhibit A: The case of a former Defense Intelligence Agency case officer Ron Hanson who recently pleaded guilty to attempted espionage. Hanson is thought to have been passing LinkedIn data on co-workers (among other information) to his Chinese handlers.

It's just the latest window into how Chinese intelligence agencies research and recruit Americans who can provide secrets that could benefit Beijing. Officials have long warned cleared personnel, and indeed anybody with access to sensitive data, about the potential pitfalls of social media.

Now, a handful of cases back up the warning, demonstrating that suspected Chinese spies are indeed exploiting LinkedIn to gather information about potential sources.

Hiding their true motives

Chinese operatives "may pose as a job recruiter or someone with a shared interest to make a connection to a target and lure them into a relationship," Dean Boyd, a spokesman for the National Counterintelligence and Security Center, said in a recent statement.

Concealing their state-sponsored role, he added, the spies "often attempt to elicit personal and professional information from their targets." Blue-ribbon targets are then tempted with offers of all-expense-paid trips to China, ostensibly for a speech or an exchange of research.

American intelligence experts point out that China is both patient and thorough. Hundreds, even thousands, of people in a targeted industry might be approached before one takes that bait. That person may be vulnerable for any number of reasons: bitterness over a missed promotion, difficult financial straits, or a drug or alcohol problem.

Evanina: China 'super aggressive'

Counter-intelligence chief William Evanina recently told reporters that China has launched a "super aggressive" campaign to recruit Americans on LinkedIn. He made it clear that LinkedIn has been "a victim" in this campaign.

Student Spies

According to intelligence officials and lawmakers, among the 350,000 students China sends to the U.S. each year are intelligence agents—sent by that nation's government to spy on U.S. industries and recruit others.

As a recent threat assessment from the U.S. intelligence community noted, "China's intelligence services will exploit the openness of American society, especially academia and the scientific community, using a variety of means."

A phenomenon long in the making

Law enforcement and intelligence agencies have warned for more than a decade that universities make easy targets for foreign intelligence services. With its long tradition of openness and the free exchange of ideas, they say, American academia was a problem waiting to happen.

Chinese students make up the largest foreign student body in the U.S., and it continues to grow. Accordingly, the State Department has discussed more stringent vetting measures on student visa applications.

Multiple recent cases also demonstrate that the U.S. is hardly China's only target. In October, French intelligence officials presented a report outlining how Chinese intelligence agents had contacted nearly 4,000 French government workers, corporate executives, and scientists via LinkedIn. And according to reports, as many as 10,000 German citizens were contacted by Chinese spies via social media—especially LinkedIn—last year.

To understand more about the practice, consider the case of Yanjun Xu, who is said to have been a regional deputy director at an agency controlled by China's Ministry of State Security until October.

What happened then? Xu became the first Chinese spy extradited to the U.S.; he was arrested in connection with a case in which Chinese spies used LinkedIn to message a GE Aviation engineer.

The sender, claiming to be from a prestigious science university, asked the engineer to travel to China. There, he would supposedly be asked to share ideas about developments in aerospace-related composite materials. All expenses would be paid, of course—and then there was the honorarium of $3,500.

Xu and other Chinese intel officers gave the targeted engineer plenty of helpful hints about "conceal[ing] the true nature of the information they were seeking from aviation companies and employees, including the use of codes and series of letters," according to the eventual indictment of Xu.

Protect Personal and Company Data With Digital Spring Cleaning

It's that time of year! Throw open a few windows, clear the dust kitties from under the bed, and generally freshen things up. While you're at it, why not perform a digital spring cleaning too, with an eye toward better protecting your own information—and your employer's? Here are tips in key categories:

The basics

- Make sure all your software applications are updated with the latest security patches; if you haven't already, set your software to automatically update.
- Protect your PC, tablet, and phone with anti-malware tools from a trusted company.
- Most of us have many apps on our phones that we virtually never use. Weed out unneeded apps to tighten up security and improve performance.
- Did you know the same advice applies to laptops? They ship with ridiculous applications aptly dubbed "bloatware," some of which may spy on you. Delete it!
- You've probably been hearing about multi-factor authentication for some time now; it's far more secure than a mere password. Sign up for MFA (sometimes called two-factor authentication) wherever possible.
- Security advice is never complete without a word of warning on passwords. This spring, take stock of yours. Are they long, strong, and not repeated across multiple accounts? Take action if necessary.

Device disposal

- Got old phones, tablets, or laptops lying around? Before selling or donating them, give them a good scrubbing.
- That doesn't merely mean deleting all your files. It's confusing, but hitting "Delete" doesn't actually delete anything. There are excellent tools available for all devices that truly eliminate data.
- Until recently, experts said that if you wanted to make an old hard drive useless, you should smash it with a hammer or drill a big hole in it. But even this isn't enough! To truly render a hard drive secure, pay a small fee to a reputed device-shredding service.

Business workspace

- Take a look around your office or cubicle. If you're like most people, there are at least a few usernames and passwords scribbled on Post-It notes. Now is the time to get rid of these!
- Password-protect your office computer so that when you step away even for a few seconds, it goes into screensaver mode. This will protect it from prying eyes.
- A tidy workspace is a secure workspace. Documents should not be left in plain view—and *sensitive* documents should be locked away.
- Most workers actually have far too many hardcopy documents for today's world, in which there's a digital copy of nearly everything. Take half an hour and make a big trip to the shredder.
- If you use a whiteboard, erase it promptly after each meeting. (You can snap a picture of it and write up the notes later.)

Home office

- If you don't already have one, buy a personal shredder ASAP. They're very affordable, and studies show that a huge percentage of identity fraud begins not with online trickery, but with theft of paper documents.
- While you're buying that shredder, purchase enough power strips to plug in your home-office devices. That way, you'll be protected against power surges.
- At work, your employer's IT department likely manages data backup. But how about at home? Most people pay almost no attention to backup. Either back up your devices to a dedicated hard drive on a regular basis, or sign up for an online backup service.
- Spring is a great time for a social cleansing. To stay secure, you should only be "friends" with folks you know from the real world. Go through your social media accounts and get rid of unwanted connections.

On the road

- Ask your IT department about a virtual private network, by far the most secure way to web-surf while traveling. Even if your employer doesn't offer a VPN, you can inexpensively sign up for one on your own.
- Public wifi hotspots are data-privacy disasters! Avoid them, use a VPN as described above, or, at the very least, don't transmit sensitive information over them.

Security Clearances and Marijuana: What You Need to Know

Not long ago, business titan Elon Musk very publicly smoked a doobie on a popular podcast. This took place in California, where marijuana is legal.

Here's the problem: In connection with SpaceX, Musk holds a security clearance. In the wake of his televised toking, an investigation was launched (pardon the pun) into whether he should retain that clearance.

With marijuana now fully legal, partially legal, or decriminalized in a majority of states, many people are wondering about ramifications for security clearances. Here are answers to some common questions:

Q: Is pot now treated just like alcohol where clearances are concerned?

A: No, not at all, and this is the important thing to remember. The reason? Under *federal* law, marijuana is still considered a controlled substance—and security clearances are, of course, a federal matter. This is true regardless of the amount of pot or the form in which it is ingested. In 2015, when states began loosening laws, the Office of Personnel Management issued a guidance specifically addressing the issue, noting that changes at the state level "do not alter federal law, existing suitability criteria, or Executive Branch policies regarding marijuana."

Q: With pot remaining fully criminalized in only 15 states, will this change eventually?

A: Many experts say it will—but for now, marijuana use can still harm your chance at obtaining or retaining a security clearance.

Q: Are there any extenuating circumstances that make marijuana use less of a red flag?

A: Certainly. The Security Executive Agent Directive 4 guidelines mention cases that happened so long ago, and so infrequently, that they do not cloud a candidate's judgment or trustworthiness. Additionally, the guidelines note that candidates who can demonstrate measures they've taken to disassociate themselves from past drug use should not be ruled out.

Q: What about hemp, CBD oil, and products based on them?

A: Cannabidiol, or CBD oil, is extracted from cannabis plants. It does not get users high, and has lately become a popular treatment for a wide variety of medical issues, from stress to arthritis. Like hemp, CBD oil has been legalized or decriminalized in many states—but it remains illegal under federal law, and thus its use will impact a security clearance application.

Shrinking Backlog

For some time now, the long wait for security clearances—and resulting backlog—has been a thorn in the side of the federal government, its contractors, and employees.

Caution remains the watchword, but recent process and responsibility changes appear to have a positive effect:

OPM's National Background Investigations Bureau has trimmed the number of pending investigations from 725,000 a year ago to 542,000, according to NBIB Director Charlie Phalen.

Of those waiting for an initial clearance, about 103,000 are at work, operating under an interim security clearance.

NBIB is exploring the use of artificial intelligence to speed the process. Already, AI has trimmed by 52% the number of hours investigators need in the field to complete an investigation.

There's more to a clearance than an investigation, and work remains to be done on the adjudication process. While adjudicating an initial security clearance takes, on average, 37 days, adjudicating periodic reinvestigations takes an average of 113 days.

The Employee Security Connection (ISSN 0894-2080) is published quarterly by the National Security Institute, 165 Main Street, Suite 215, Medway, MA 02053. Subscriptions are $998 per year, telephone (508) 533-9099 for information concerning company/agency subscriptions. ©2019 National Security Institute. All rights reserved.

April - June 2019

Agency Point of Contact

NASA Office of the Chief Information Officer and Office of Protective Services Points of Contact

Michael Witt, Associate CIO for IT Security and Senior Agency Information Security Official (SAISO), (202) 358-0622 *michael.witt@nasa.gov*

Willie Crenshaw, Governance, Risk & Compliance, (202) 358-0947, *willie.d.crenshaw@nasa.gov*

*NASA Security Operations Center: soc@nasa.gov
**Agency-Wide service provider located at Ames Research Center.*

Office of Protective Services
Counterintelligence Division Director:
Darrell Slone, (202) 358-2007, darrell.d.slone@nasa.gov

Ames Research Center:
Chris Knoth, (650) 604-2250,
christopher.d.knoth@nasa.gov

Armstrong Flight Research Center:
Frank Sutton, (661) 276-7476,
frank.a.sutton@nasa.gov

Glenn Research Center:
George Crawford, (216) 433-8458,
george.s.crawford@nasa.gov

Goddard Space Flight Center:
Christian Breil, (301) 286-1533,
christian.m.breil@nasa.gov

Headquarters:
Arthur Payton, (202) 358-4645,
arthur.r.payton@nasa.gov

Jet Propulsion Laboratory:
John O'Malley, (818) 354-7828,
john.omalley@nasa.gov

Johnson Space Center:
Tony Dietsch, (281) 483-7921,
robert.dietsch-1@nasa.gov

Kennedy Space Center:
Ronald Storey, (321) 867-2568,
ronald.e.storey@nasa.gov

Langley Research Center:
Benjamin Marchione, (757) 864-3403,
benjamin.marchione@nasa.gov

Marshall Space Flight Center:
Ron Smith, (256)544-7808,
ronald.l.smith@nasa.gov

Stennis Space Center:
David Malcom, (288) 688-1683,
david.a.malcom@nasa.gov

Cyber Threats/Concerns
Stefan Morgan, (202) 358-1294,
stefan.j.morgan@nasa.gov