RCUH Research Corporation of the University of Hawai'i

FOREIGN INTRUSION INTO ACADEMIC RESEARCH & TRAINING

FORUM REPORT

APRIL 29, 2021

INTRODUCTION

While most foreign students and researchers are studying and working in the United States for legitimate reasons, there is a small percentage who are actively working on behalf of other governments or organizations to steal intellectual property from university researchers. The objective of this forum was to educate attendees on how to protect their research and data from foreign intrusion.

Due to the COVID-19 pandemic, the 2021 RCUH forum was live-streamed to an audience of approximately 120 attendees from Hawai'i and the mainland United States. RCUH Executive Director Leonard R. Gouveia, Jr. served as the moderator for the fourth annual forum and introduced the three panelists:

NINA EPTON
Special Agent, Naval Criminal Investigative Service

Nina Epton is with the Hawai'i field office of the Naval Criminal Investigative Service (NCIS) and provides support to research, development, and acquisition programs for the U.S. Department of the Navy. Since 2009, she has supported U.S. Navy Systems Commands, Warfare Centers, and University Affiliated Research Centers, and cleared contractors throughout the United States.

SHAWN CASE
Counterintelligence Special Agent, Defense Counterintelligence and Security Agency

Shawn Case's career in counterintelligence has spanned more than 24 years, including 7 years of service in the U.S. Army. In his current position with the Defense Counterintelligence and Security Agency (DCSA), he focuses on education and training to cleared industry and supports numerous counterintelligence investigations and operations, both domestically and overseas.

JODI ITO
Chief Information Security Officer, University of Hawai'i System

Jodi Ito is responsible for the security and protection of information assets across all 10 campuses of the University of Hawai'i (UH) System and UH-affiliated research and education centers. She is also the chair of CyberHawaii and program director for the NSA's GenCyber Camps in Hawai'i, and she co-chairs several other cybersecurity committees.

FOREIGN INFLUENCE OVERVIEW

The large number of foreign students, researchers, scientists, and professionals in the United States, combined with current technological capabilities, allows foreign governments to contact and recruit individuals in the hopes of acquiring advanced technology without research costs.

In recent years federal agencies have issued statements expressing growing concerns over the potential for foreign influence in the following areas:

1. Diversion of intellectual property to foreign entities;
2. Sharing of confidential information by peer reviewers with others, including foreign entities;
3. Failure of researchers to disclose resources from other organizations, including foreign governments.

WHY HAWAIʻI?

Why might American adversaries be interested in targeting Hawaiʻi? According to a former Soviet officer, the most important data to collect was on policy and defense. When looking at our island state from that perspective, Hawaiʻi has several important Department of Defense commands, such as the U.S. Indo-Pacific Command and combatant commands, as well as corporations and universities that support a lot of the work to the DoD.

There is also a melding of cultures in Hawaiʻi that blends into our academic institutions and creates opportunities for collaboration. Specifically, the important research and work being done in the healthcare industry and environmental studies, along with the state's defense aspects and geographic location, make Hawaiʻi a high-value target for foreign intelligence entities and adversaries.

Some people claim that foreign intrusion isn't happening in Hawaiʻi, but it's absolutely happening here. There are J-1 visa applicants from China who are rejected because of their affiliations. There are UH personnel that China has tried to recruit for its Thousand Talents Program, which was designed to attract, recruit, and cultivate high-level scientific talent to further China's scientific development, economic prosperity, and national security. And while it's not illegal to participate in the Thousand Talents Program, there are implications when receiving federal research funds, as well as a potential (or actual) conflict of interest if that information is not disclosed.

"For decades, scientists at universities and research centers, supported by the Department of Defense (DoD), have made ground-breaking scientific discoveries that underpinned dramatic commercial and national security advances, significantly improving the lives of citizens here and abroad. DoD recognizes the contribution of research integrity principles, such as the free exchange of ideas, transparency, and collaboration across research communities as critical to our mutual success. Yet today, the ability to make similar advances is at risk, and research integrity is jeopardized through foreign governments' exploitation that intentionally target[s] U.S. and allied partner research and intellectual capital."

— Excerpt from October 2019 memo from the U.S. Undersecretary of Defense

TARGETING UNIVERSITIES

Foreign intelligence services are taking advantage of the U.S.'s spirit of openness and transparency as it pertains to innovation. They are specifically targeting universities (and their collaborative and cooperative environments) to steal information and to unethically divert intellectual capital from the U.S. to benefit themselves or other nations. Our U.S. research dollars are being invested into developing these technologies, so the federal government is getting better about publishing alerts in a timely manner and has even established the Cybersecurity and Infrastructure Security Agency to learn how we are being targeted.

In addition to universities, funding sponsors like the National Institutes of Health (NIH) and National Science Foundation (NSF) are experiencing similar trends, being targeted for their research and intellectual property.

CHINA, CHINA, CHINA...

There are 97 countries actively targeting the United States for information—the top four are China, Russia, Iran, and North Korea. The Chinese (i.e., the Chinese Communist Party) are the most aggressive at collecting intel. China has published 5-, 10-, and 15-year plans on how to gain a technological advantage and leapfrog into being a world leader. Through their aggressive (and some might say unfair) tactics in trying to accomplish this, they have become the most prolific collectors of information.

When the U.S. government assesses potential threats, it looks at intent and capability. While there may be a lot of countries that want to acquire data from the U.S., they don't have the capability. Or if they have capability, they may not be as aggressive in targeting the U.S., whereas both are true of China. China is probably considered the largest threat to our national defense in terms of how they're acquiring information and technology. And unfortunately the U.S. has little recourse based on the country's laws and views—if the U.S. tried to pursue a case through the Chinese court system, it would lose. For example, when New Balance sued for copyright infringement in China, the court basically said, "Too bad."

$600 BILLION

The estimated cost of intellectual property stolen annually from the United States. This number continues to increase each year, and China remains the principal offender, capitalizing on its defined technology transfer strategy and widespread access to U.S. intellectual property.

CASE STUDIES

There's a clear trend of the Chinese government targeting medical information in the U.S. And although that data may not be classified, it doesn't mean that the research is not important and doesn't need to be protected. Researchers need to control who has access to their information. Please view the following case studies for examples of research-related foreign espionage in higher education.

- RESEARCHERS CHARGED WITH VISA FRAUD AFTER LYING ABOUT THEIR WORK FOR CHINA'S PEOPLE'S LIBERATION ARMY (PLA)
- HARVARD UNIVERSITY PROFESSOR INDICTED ON FALSE STATEMENT CHARGES
- FORMER UNIVERSITY OF FLORIDA RESEARCHER INDICTED FOR SCHEME TO DEFRAUD NATIONAL INSTITUTES OF HEALTH AND UNIVERSITY OF FLORIDA
- FORMER WVU PROFESSOR PLEADS GUILTY TO FRAUD THAT ENABLED HIM TO PARTICIPATE IN THE PEOPLE'S REPUBLIC OF CHINA'S "THOUSAND TALENTS PLAN"
- NINE IRANIANS CHARGED WITH CONDUCTING MASSIVE CYBER THEFT CAMPAIGN ON BEHALF OF THE ISLAMIC REVOLUTIONARY GUARD CORPS

Star Advertiser B CITY EDITOR: David Butts / dbutts@staradvertiser.com / 529-4310
SATURDAY 3/24/18

local & business

Iranian agency steals U.S. secrets

The consulting firm hacks computers nationwide, including in Hawaii, the FBI says

Star-Advertiser staff and Los Angeles Times

Hawaii state email accounts were among thousands of government and university computers nationally that were hacked by nine Iranians working for the Iranian government, according to a federal indictment unveiled in New York.

The FBI and Department of Justice said an Iranian consulting firm worked for years to steal secrets from government agencies, universities and companies in the United States and around the globe, even hacking into the U.S. Department of Labor and the United Nations, according to federal officials who announced the charges Friday. The company also allegedly breached the computers of the Federal Energy Regulatory Commission and the states of Hawaii and Indiana, they said.

Hawaii's Office of Enterprise Technology Services posted a statement on its website Friday afternoon saying the hack of state computers involved 37 email accounts in the executive branch.

"As part of ETS's ongoing monitoring of the executive branch departments' email system, we noticed unusual activity involving 37 email accounts. We reacted quickly and resolved the situation," said the statement, which was attributed to state Chief Information Officer Todd Nacapuy and Chief Information Security Officer Vincent Hoang. "Law enforcement officials were contacted to assist in the investigation. According to the departments, the emails involved did not contain confidential information. Furthermore, the state's computer systems where confidential information is stored was not breached."

The "unusual activity" has no connection to the loss of data for 66,500 driver's license and state ID cardholders that was announced Thursday, Caroline Julian-Freitas, senior communications manager for the Office of Enterprise Technology Services, told the Honolulu Star-Advertiser.

She said Nacapuy and Hoang were not available for further comment. "However, I can confirm that Governor (David) Ige was not part of the 37 emails," she said in an email response to Star-Advertiser questions.

FBI officials said the Tehran-based Mabna Institute worked for Iran's Islamic Revolutionary Guard Corps and other clients in the Iranian government to steal academic research, proprietary secrets and government data, the indictment claims. The hacking went on since at least 2013, the Justice Department said.

A grand jury meeting in the southern district of New York charged nine people, all of them living in Iran. The Treasury Department also announced sanctions against the company and the employees.

According to federal

Please see **HACK,** *B5*

METHODS OF STEALING

OPEN-SOURCE INFORMATION

A cybersecurity company conducted a study that showed about 10% of phishing emails are successful, but if initial contact is made through a social media platform, the success rate increases to 33%.

Security agencies have found that social media platforms like LinkedIn are being exploited by foreign adversaries to find targets. For example, German intelligence services found multiple fake Chinese social media accounts on LinkedIn. The fraudsters used an attractive profile picture and acted as a headhunter or think tank employee to interest viewers. They then established a network of "friends" to get a better understanding of who their potential targets were and how they were connected, before determining whom to approach for additional information. But this practice isn't exclusive to China.

The North Koreans also created fake social media profiles, especially on LinkedIn, to target network security personnel. They were able to contact and build relationships with individuals and trick them into downloading malware onto their devices. It is important to note that the victims' devices were fully patched and updated at the time of the compromise. This indicates that North Korea is using advanced techniques like zero-day exploits in order to gain access to devices and networks.

Besides LinkedIn, foreign intruders can also view your Facebook, Instagram, or other accounts to look at your family members and close friends, and they may target an individual who doesn't have the same security awareness that you do. As long as they are able to attack that profile, they can get onto your home network or your work computer, and potentially the University's network.

Social media is an attractive way for adversaries to target individuals like Kevin Mallory, a retired CIA officer who was severely in debt. His LinkedIn profile stated that he was a China expert looking for work. Chinese intelligence services were able to hone in on him and see his vulnerabilities. Upon visiting China, Mallory agreed to work on behalf of the Chinese government by selling U.S. defense secrets.

Another platform being used is ResearchGate, which displays a researcher's articles, publications, and collaborators. Again, our adversaries are trying to create a network, and even if you're not the easiest target, they'll target someone close to you.

While the Cold War has ended, Russia continues to be a threat to our national security. It, too, is actively using open-source network intrusions to collect information through any sort of vulnerability they can find. The Russians are great at network-intrusion activities and coordinating efforts to steal intellectual property and research. When remote hacking efforts fail, they will send a group of intelligence officers to locations around the world where targets are physically located. For example, they sent seven highly trained intelligence officers to conduct a "man in the middle" attack in Amsterdam to target and disable a hotel's WiFi. This enticed guests to connect to the Russians' spoofed network, which happened to have a stronger connection, and resulted in their account credentials being stolen.

RECRUITMENT

When travel picks back up again and researchers begin attending international conferences, conventions, or trade shows (or other gatherings of subject-matter experts), be

RECRUITING INDIVIDUALS HELPS U.S. ADVERSARIES:

- Gain access to research and expertise for cutting-edge technology
- Benefit from years of scientific research conducted in the United States supported by federally funded grants and private funding
- Severely impact the U.S. economy

aware that is the ideal venue for intelligence services to operate. Foreign intruders are looking for these targets of opportunity, so even if you're going to a friendly city or country, you could still be targeted by adversarial intelligence services.

The ultimate goal of any intelligence service is to recruit an insider—someone who knows everything's that's going on. It doesn't have to be classified information; anything can provide greater detail about an organization—internal shifting of personnel, challenges with funding, a research method or methodology that is not going well and has been scrapped for an entirely different direction. All of that data is valuable to intelligence services.

A former Soviet case officer said his most valuable recruited source of information was the custodian of an office building. He just asked the person to do their job collecting the trash, but instead of putting it in the dumpster, he asked that it be given to him. The case officer would go through the trash for receipts, personal mail, etc. From the collection, the agent could develop a dossier of individuals who had access to important information, such as an administrative assistant or executive, anyone with a vulnerability that they could compromise.

MICE: MONEY, IDEOLOGY, COMPROMISE, EGO

Motivation is complex, but MICE is the classic model—Money, Ideology, Compromise, and Ego. For a lot of these big espionage cases, money proves to be a big motivator. Aldrich Ames was a 31-year veteran CIA case officer who spied for Russia for nine years. The Russians claim he was paid $1.88 million for the first four years of his service passing classified information.

Ana Montes, a senior analyst with the Defense Intelligence Agency, had sympathies towards Cuba and felt the U.S. government policy towards Cuba was unfair. She caught the attention of Cuban officials who recruited her and convinced her to leak classified U.S. military information for more than 16 years without any financial gain. Her motivation for spying was ideology, as she disagreed with U.S. foreign policy.

Compromise, like blackmailing an individual into providing information, is less prevalent in terms of recruitment, but ego has been a big motivator. An individual with a narcissistic personality may not recognize how their actions affect others. They may feel like they're doing something and can get away with it. To feed their ego, intelligence services will remind them how great and smart and wonderful they are, telling them that they're not appreciated enough by their home organization, but that the recruiting agency appreciates all of their efforts and contributions.

CYBER ATTACKS AT UNIVERSITIES

APT 40 LEVIATHAN ATTACK

The University of Hawai'i had an intrusion, the APT 40 Leviathan attack, that was reported in the *Wall Street Journal* and *Honolulu Star-Advertiser* in 2019, but it actually occurred two years prior. It was the first major attack, or Advanced Persistent Threat (APT), of a complicated magnitude by a hostile nation state. It was traced to China. UH and several other universities were targeted by the Chinese with the goal of infiltrating universities working on maritime projects.

We think that this attack group was doing reconnaissance on the University for months before the discovery. They are patient and methodical, and they know what they're doing. It was really eye-opening for us because after months and months of investigations, we were able to determine that seven computer systems and servers with personally identifiable information (PII) were compromised three months prior to being discovered. What was really interesting is that the malware was custom configured for each particular system. For example, in one database server, they hid their malware in directories with names that were associated with the database operations on that server.

Once they were on the actual network with these compromised servers (we suspect through a brute-force attack), they were able to identify what they wanted and move to another computer within the same network, also known as "pivoting." They installed programs that could look at the traffic in the network itself ("network sniffers" and "packet captures"), where they could identify accounts and passwords. The hackers were also able to log into a researcher's email account and observe the activity for several weeks. They read emails to understand the relationships between various contacts and then started to try to infiltrate others in the researcher's specific project unit. The hackers were finally discovered when they attempted to send malware-infected emails to the researcher's colleagues at other institutions. The systems of the researcher's colleagues were able to identify malware in the email and immediately notified UH.

Looking at our network traffic, we were able to see a spike in data leaving the network, but because the data was encrypted, we don't know what was exfiltrated or taken. Nevertheless, under Hawaii Revised Statute §487N-4, UH was required to inform the Legislature and notify individuals affected by the potential exposure. We also worked with our federal law enforcement partners and the Missile Defense Agency. UH is also in constant communication with those other universities because these attacks are ongoing.

OTHER TYPES OF ATTACKS

At UH, we are seeing an increase in the types of scans that are looking for vulnerabilities—any kind of remote access. Attackers are trying accounts and passwords until they're able to get in. Intruders are also burying their attacks in legitimate cloud services, so we're having a much more difficult time blocking them. For example, if we were to block an attack from Amazon, nobody at UH would be able to connect to Amazon to buy anything.

Federal agencies have suggested blocking traffic with China, but unfortunately, UH has legitimate transactions with China. It's also difficult for UH to determine which activity is illegitimate and block it. This occurred once when UH saw a huge spike in traffic leaving the network one weekend, so we immediately blocked it. And then we got a call from the Institute for Astronomy. They were transferring legitimate data to another site.

We are also seeing credential-stuffing attacks here at the university where the attacker uses stolen credentials to gain access. We're also seeing very targeted spear phishing attacks where malware is embedded in the email, or the email will direct the reader to a malware-infected website.

As a test, we had malware antivirus software installed on a computer and purposely clicked on some infected emails. This particular malware was able to be installed in spite of the protections, and it stole different types of information. If you were saving passwords in your browser, if you were doing remote logins and storing that information, if you had auto-fill information in your browser, it scooped all of that. Once the data was stolen, the malware sent the information to its Command and Control, that would then report back to have the malware perform additional actions or direct where to send the stolen information.

RANSOMWARE ATTACKS

Recently, we're seeing ransomware attacks, the financial aspect of cyber attacks, on universities. In 2020, the University of California, San Francisco was attacked with malware that encrypted several servers within the School of Medicine. While the incident did not affect its patient care delivery operations, overall campus network, or COVID-19 work, UCSF paid a ransom of $1.14 million to unlock and return the encrypted data. The University of Utah also paid a ransom of $457,000 in 2020.

There are dozens of ransomware gangs who leak stolen data. Because this is a billion-dollar business, ransomware operators are now organizing and forming cartels, joint partnerships, and profit-sharing arrangements. They'll segment a group to compromise the computers and networks, and they will then sell that data to ransomware operators.

HAVE I BEEN PWNED?

To track whether hawaii.edu email addresses have been leaked, breached, or exposed, the University of Hawai'i uses the website have I been pwned?

This website is a free resource that allows anyone to search whether their email account or phone number has been compromised, or "pwned," in a data breach.

BREACHES

- Jefit. In August 2020, more than 9 million email accounts were exposed, including 276 hawaii.edu accounts and passwords.

- Chegg.com. In April 2018, the textbook rental service suffered a data breach that impacted 40 million subscribers, which included almost 150,000 UH credentials and 4,000 UH passwords. More than 1,600 UH accounts had to be reset due to this breach.

If you suspect that your hawaii.edu email account has been compromised, click here to view next steps from the UH Information Technology Services Department.

SAFEGUARDING YOUR RESEARCH

USE EXISTING RESOURCES

Former Assistant Attorney General for National Security John Demers has said that it's not a crime to participate in China's Thousand Talents Program. However, it is the willful disregard for the disclosure requirements that causes issues. At the University of Hawai'i, you can turn to the Office of Research Compliance (ORC) and Office of Export Controls (OEC) for guidance on UH and federal sponsor disclosure requirements, export control regulations, and conflict of interest matters. They'll be able to tell you what a conflict of interest could potentially mean and provide assistance in complying with complex and ever-changing federal export control laws and regulations.

In general, export-control regulations cover four main types of University activities:

- **Transfers** of controlled information, including technical data to persons/ entities outside the U.S.
- **Travel** to certain sanctioned or embargoed countries for purposes of teaching or performing research
- **Shipment** of controlled physical items such as scientific equipment from the U.S. to a foreign country
- **Deemed Exports:** verbal, written, electronic, or visual disclosures of controlled scientific and technical information related to export-controlled items to foreign nationals in the U.S.

EXPORT-CONTROL CONCERNS AT UH

COLLABORATING AND USAGE

- With foreign colleagues in foreign countries OR U.S.
- With a foreign country subject to U.S. embargoes
- Research equipment on ships
- Signing Confidentiality Agreements or NDAs
- Creating, receiving, or working with encryption software

FOREIGN NATIONALS

- Exposure to export-controlled data
- Exposure to research projects and/ or labs involving Export Controls
- Training of foreign nationals on Export Control research protocols or equipment
- Application for J-1 Exchange Visitors, H-1B visas

RESEARCH

- Involving export-controlled data
- Contracts that require sponsor approval rights over publication, or that operate to restrict information
- Contracts in which sponsor limits participation of foreign nationals in classified research

SHIPPING

- Equipment to a foreign country
- Materials via Material Transfer Agreements

TRANSACTIONS

- Wiring funds to a foreign country
- Purchasing and/or using export-controlled software/equipment
- Receiving and sending export-controlled information by mail, electronically, verbally, etc.

TRANSPARENCY

The Deputy Director for Basic Research with the Office of the Secretary of Defense emphasized that transparency is the key to science. Being a responsible researcher means paying attention to quality assurance, which includes proper disclosure of all interests for possible biases. Disclosures are as important as verifying the references in a study and ensuring the data used is good data. If research is being funded by the public, then the public needs to trust in its integrity.

CONFLICTS OF INTEREST

As mentioned earlier, it's not illegal to engage with foreigners (e.g., foreign students, researchers, scientists, and professionals), but if it's not properly reported, you could get into trouble with the federal government. The Department of Defense is also tightening up its policies on hiring foreign nationals (e.g., the National Security Agency's GenCyber Program will not be allowed to hire any non-U.S. citizens effective next year).

Disclosures to the University (internal)

- Conflict of Interest disclosure
- Intellectual Property and Inventions disclosure

Disclosures to Sponsors (external)

- Current and pending support
- Foreign talent programs
- Foreign components

UH Conflict of Interest Policies

- UH Executive Policy 12.214: Conflicts of Interest and Commitment
- UH Administrative Procedure 12.304: Procedures for Disclosing and Addressing Conflicts of Interest Related with Extramurally-Funded Activities
- UH Administrative Procedure 5.504: Procedures for Disclosing and Addressing Conflicts of Interest and Commitment

NIH REPORTING REQUIREMENTS

In March 2021, NIH announced new disclosure requirements for U.S. researchers applying for NIH grants, effective May 25, 2021:

- Researchers must submit English-language copies of all "other support" received, including contracts, grants, and any other agreements specific to foreign appointments and/or employment with a foreign institution, regardless of whether or not they have a monetary value.
- The Biographical Sketch (Biosketch) submission has been modified to include scientific appointments in the section requiring disclosure of Positions and Honors.
- Researchers may now include in their Biosketch details of ongoing and completed research projects from the past three years to which they would like to draw attention.
- A signature block requiring researchers to attest to the accuracy of their submissions, under penalty of law, has been added to the disclosure forms.

REGULATIONS & RESOURCES

REGULATIONS IMPACTING UH

NDAA 889 / HHS 889

- Effective August 13, 2020, the government may not contract with an entity that uses certain telecommunications and video surveillance equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, produced by Huawei, ZTE, Hytera, Hangzhou Hikvision, Dahua, or their subsidiaries or affiliates.
- This applies to the University of Hawai'i across all departments because it is not specifically tied to a project.

Interim Defense Federal Acquisition Regulation Supplement (DFARS)

- 252.204-7012: Follow National Institute of Standards and Technologies (NIST) SP 800-171 which says to apply 110 controls to data classified as controlled unclassified information (CUI) in non-federal systems and organizations.
- 252.204-7020: If you have CUI, you must perform a self-assessment of NIST 800-171 compliance. The score must be inserted into the Suppliers Performance Risk System website before an award is made.
- 252.204-7021: Cybersecurity Maturity Model Certification (CMMC) has five levels. The contract solicitation will stipulate which level you need to be at. Level 1 is basic safeguarding of covered contractor information. Level 3 applies NIST 800-171 and 20 additional controls, and requires passing an audit by a third-party-certified assessor before proposal submission. By 2025, certifications will be required of all DoD contractors and awardees of DoD contracts. These regulations may apply sooner, if you have a subaward or subcontractor from a prime contractor that is required to flow down the requirements.

UH RESOURCES

- UH Chief Information Security Officer: Jodi Ito, jodi@hawaii.edu
- UH Facility Security Officer: Allie Zust, azust@hawaii.edu
- UH Information Technology Services: https://www.hawaii.edu/its/
- UH Institutional Data Governance: https://datagov.intranet.hawaii.edu/
- UH Office of Export Controls: https://researchcompliance.hawaii.edu/programs/export-controls/
- UH Office of Research Compliance: https://researchcompliance.hawaii.edu/
- Foreign Influence in University Research: https://www.hawaii.edu/research/foreign-influence/
- Protecting Research at UH Training: https://researchcompliance.hawaii.edu/webinar-protecting-uh-research-event-resources/

FEDERAL RESOURCES

- Cybersecurity and Infrastructure Security Agency
- Defense Counterintelligence and Security Agency
- Federal Bureau of Investigation
- Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise

RCUH RESOURCES

- RCUH Facility Security Officer: Leonard R. Gouveia, Jr., lgouveia@rcuh.com

FORUM Q&A

Q: Are U.S. territories and commonwealths considered foreign?

Shawn: They are not. If it doesn't belong to the U.S., then it's considered foreign.

Q: If there is one takeaway from today's presentation, what should it be?

Nina: For me it's maintaining vigilence. People will come in and say, "Hey, Nina, you know I'm probably being paranoid, but..." I always like to remind people that they're not being paranoid. Paranoia is an unsubstantiated fear that something is going on. There's plenty of evidence to indicate that universities are being targeted and they're being targeted aggressively.

Shawn: Trust your gut. If you have a feeling that something isn't quite right, let your Facility Securities Officer (FSO) know or someone in your chain know. Also trust in us that we're going to help people do the right thing. We understand academia and the problems and challenges that you face, and we're here to help.

Jodi: Ditto on what you both said, but the hard thing is how do you follow your gut feeling in a cyber environment? People aren't good about that. You have to pay attention and keep yourself educated. When these forums and opportunities for education come up, know that we're sharing the latest things that we're seeing and we're trying to synthesize it from the university side so you don't need to.

Q: What are the most common types of infiltration or attacks from foreign countries?

Nina: I haven't seen the data on percentages, but I've seen a lot of clever and very convincing spoofed emails and spearphishing emails. A lot of times these emails will come from a smaller corporation or company that may not have a strong or robust network defense system.

Shawn: Social media attacks and social media are pretty prevalent because of the COVID environment, a lack of travel, and the lack of interaction.

Jodi: For the University of Hawai'i, we don't know where an attack is coming from. We just know that we're being attacked. If you see something going on suspiciously on your computer, let your IT person know early on. They can contact the Information Security Team and we can try to help determine exactly what's going on. But because the University is so highly decentralized and because network computer systems are used and managed by projects, we centrally at the system level don't have visibility or control over that. We have tools and technologies available to the UH system, but a large part of watching for attacks is going to fall back on to the department or unit since everything is so decentralized within the university.

Q: Would any of the panelists recommend Tails, Whonix, or Qubes operating systems for travel?

Shawn: For foreign travel, depending on where you're going, I'd highly recommend you have disposable devices. For example, if you take your personal cell phone to China and you want to use their network to check your emails and contact your friends, you're going to have to download some updates to your software to use your phone on their network. Those updates basically give them

free access to your whole phone and all the information on your phone, so you can pretty much assume that any passwords, all your contacts, all your pictures, any conversations you have are being monitored and recorded. I know for a fact that a Chinese citizen who was talking bad about the Chinese government in a text group with his buddies was picked up by the local police a few hours later. If you think that you can go to China, use your devices with no repercussions and think there are no vulnerabilities, you are wrong. If you bring your cell phone, tablet, computer, I highly recommend having a clean device and creating an email address for your travel. Use an obscure password that you don't have on any other device and understand that you're going to have to either wipe it or just get rid of it when you get back.

Jodi: Whonix, Tails, and Qubes OS are basically anonymous operating systems that you can deploy in a virtual machine. I think it goes with the philosophy of sanitizing or having a clean environment, clean machine when you travel. The goal is don't take anything with you that has any information that could be of value. Assume that you are going to be compromised.

Q: What is the situation for green card holders? Did I hear Jodi say that we will not be able to hire non-citizens in the future?

Jodi: This guidance was given to me specifically from the NSA GenCyber Program. We were told that we cannot hire non-U.S. citizens next year for the GenCyber Program. This may not be the case for all types of grants and awards, so you have to check the requirement with the contracting officer of your sponsoring agency.

Q: What do you need to do if you've been "pwned"?

Jodi: If your information has been exposed, you should basically follow best practices and try to see where you've been using your username and password. Number one, change the password. Two, wherever you can employ multifactor authentication, do it. Third, make sure that you run remediation software on your computer (i.e., anti-malware software). For example, ITS distributes McAfee for free, so you can use that to try and clean it off. Sometimes these types of remediation tools don't always work on the first pass. It might take more than one pass to clean up as much of the malware as you can. Once your computer's been compromised, I personally think the safest thing to do is what we call nuke and rebuild, just reload everything from scratch. But many people cannot do that.

Q: What would be an indicator that an email could have a malware-infected attachment or have a link to a malware-infected website?

Jodi: UH's gmail web client has some built-in tools to identify well-known types of malware, but you really need to have anti-virus/anti-malware software installed on your computer to scan attachments. You should also ensure that applications cannot automatically be installed on your computer without your intervention. Make sure that you have to apply a password. For email, we say do not open the attachments by default; make sure you have something that was scanning it first before you open it. For a potential malware-infected website, hover over the link to check the URL. There are also web tools where you can input a link and it'll come up with a recommendation, i.e., if the site is clean or not clean.

Nina: This is a low-tech method: If you're not expecting an email from that person with a suspicious attachment or link, contact them through another means. Pick up the phone or text them to verify that they've sent you something. Don't email back to the same account.

Q: What is the importance of controlled unclassified information (CUI), particularly for universities?

Shawn: Currently, DCSA does not have a policy on CUI and how to implement the controls.

Jodi: I think the best thing you can do is look at the NIST 800-171 to become familiar with the controls that are being identified, so that you have an idea of what you need to do. Number one is inventory your equipment, your software, your people. You're going to have to put policies and procedures in place; have artifacts of evidence, e.g., prove that you have the firewall turned on, prove that you're logging on, prove that you're monitoring. Then, when the actual procedures come up, you won't be surprised.

Q: Do you have any recommendations as to what we should be looking for or worrying about with Chinese grad students, postdocs, collaborators? And how do we exercise proper care, while maintaining our core values?

Shawn: That's a challenging question because, again, the vast majority of the students are here for legitimate reasons. I would suggest you pay attention to news related to your research topic. For example, a lot of the cases we highlighted today dealt with healthcare. If you're working in that arena, you probably want to be a little more sensitive to whom you're bringing on and what kind of information you're looking at. It's not a bad practice to audit your data, to know who's accessing your data and when. If you see some strange behavior, then that might be something that you want to document or pay more attention to. If you're getting some off-the-wall questions, questions that shouldn't be asked or that are outside the scope of the work, again, that may be something that you want to pay attention to or be a little bit concerned about. Engineering, maritime, and healthcare are all really high-priority fields. Pay attention to the news. There's a lot of information out there. If you are working with ITAR restricted information, realize that you can't release that information to them or can't answer a question for them or help guide them in an area where you know ITAR restrictions apply because it's deemed an export.

Nina: You want to look at the behavior of the individual and not the ethnicity of the individual. If they're trying to access a space really early in the morning or late at night when nobody is around, or if their schedule changes and there's no reasonable explanation for it, those would be indicators and behaviors to be concerned about. If their actions are uncharacteristic of what they have going on in their lives, then that's a concerning behavior and should be looked at. If they're introducing devices onto a network, if they're bringing in cameras where it's not typically allowed or taking pictures with their cell phones, it should warrant a second look. If you have a data set that can be remotely accessed and your network administrator informs you that some strange IPs that haven't historically accessed that data set have opened it, it could be an indicator that data is being compromised. Look at anomalies.

Q: Many of us sail on research ships that travel in and out of foreign ports for short periods of time. How wary do we need to be about infiltration attempts in that setting?

Nina: In order to have a more informed response, I'd need to know more about the specific course. Generally, if you have a trip coming up and you know the scheduled stops, have a discussion with your FSO or through a point of contact, like Shawn or myself or our partners at the FBI. We'd be more than happy to have a discussion with you about the specific locations and the things you need to be aware of. It isn't always about intelligence concerns. It could be about political unrest, criminal

activity, or potential terrorism concerns. It would make you a better prepared and more informed traveler. My suggestion is just to come talk to us and then that way we can provide you specific information about where you're going as opposed to just kind of a general answer.

Jodi: Also, I'd suggest looping in Allie Zust, UH FSO. The more people that are aware of it, the better informed we can be and the better able to advise the broader community. It's all about collaboration and sharing.

Q: Teaching operational security to colleagues is hard in a fast-paced research environment, especially if colleagues do not have the same level of tech literacy, news engagement, or general caution. Any advice or resources, written or online, for helping co-workers develop better cyber safety habits?

Jodi: We are working on it! UH is working closely with the Office of Research Compliance, Office of Research Services, Data Governance, and RCUH to try to bring the information to the community in a very tangible way. This is why we actually split up and are doing these separate research-focused information briefings, because we can talk very specifically about the projects. Do we need to protect a sensor or buoy in the ocean? Or do we just need to worry about protecting the servers and systems where that data is being processed? It's very different from protecting our student information system. By focusing on these research types of operations, we hope that we can then make the information we share more relatable. Look for more of these coming. We are definitely going to be starting up a research security program, as was outlined in the JCORE report that came out recently.

HAVE ADDITIONAL QUESTIONS?

Please email rcuh@rcuh.com if you have any additional questions for the panelists and stay tuned for future trainings!

Prefer to chat over the phone? Please feel free to call RCUH Corporate Services at either of the following numbers:

- (808) 988-8314
- (808) 988-8311