CYBERSECURITY:
PROTECT, DETECT, RESPOND

FORUM REPORT

APRIL 6, 2018

UH Mānoa IT Center

RCUH Research Corporation of the University of Hawai'i

University of Hawai'i System

UHARI

FORUM REPORT

The 2018 RCUH forum was held at the UH Mānoa IT Center conference room and livestreamed throughout Hawai'i. A total of 500 people registered for the forum, 100 in-person attendees and 400 live-stream participants.

RCUH Executive Director Sylvia Yuen welcomed attendees and thanked the forum co-sponsors, the University of Hawai'i (UH) and the University of Hawai'i Association of Research Investigators. Dr. Richard Rocheleau, Director of the UH Hawai'i Natural Energy Institute, introduced the panel moderator, RCUH Board Chair Gene Bal, and the three panelists:

- *Brian Tuskan, Senior Director of Security, Microsoft Corporation*
- *Will Bales, Supervisory Special Agent - Cyber, FBI Honolulu*
- *Garret Yoshimi, VP for information Technology/CIO, UH System*

BRIAN TUSKAN

Senior Director of Security, Microsoft Corporation

Microsoft has a huge footprint that encompasses over 190 countries and consists of 730 physical locations, 224,000 employees and partner contractors, and 100 or so retail stores. The physical security at these locations is pretty standard—access control, card key, and videos. However, with its physical and cybersecurity teams working together, Microsoft is changing the way it provides physical security. How do you protect the Redmond site, which has a 13 million square-foot footprint, accommodates 16,000 people for events, and has an open environment? Microsoft is moving towards a frictionless environment which provides greater safety and security with fewer barriers. In the new environment, card-key access will be replaced by facial recognition and other means of identification. The security guard looking at multiple screens will also be replaced as this model is not very effective and offers a false sense of security.

How do you take a tremendous amount of data from various sources and make sense of it? Converged connected security provides a risk-based artificial intelligence (AI) solution that sits on the cloud. It crawls open source channels (e.g., law enforcement, social media, news reports) looking for risks, and if a situation occurs, like a break-in, it will disseminate a risk report based on machine learning. This enables the human operator to behave more smartly and intuitively because the high-risk situation is brought to his/her attention with camera views and location, which allows for a more precise response.

> **"When you have a large campus environment, you want to have an integrated solution, especially for physical security."**

There are other security changes underway at Microsoft. Chat bots with AI machine learning will be used to raise the risk profile and enable security officers to do their jobs better. Robots will augment what humans can do, rather than replace

Panelist Brian Tuskan showcased innovative physical security technology that Microsoft is creating and using at their Cyber Defense Operations Center in Redmond, Wash.

them. For example, Microsoft has piloted autonomous robots with sensors and cameras to undertake what a human cannot physically do, like enter a room where a fire is smoldering or detect gunshots. Security guards in a shack or driving around a large campus are expensive and not very effective. However, sensors around a campus perimeter coupled with drones that are immediately dispatched when the perimeter is breached, automatically locking in the target and notifying the operations center with photos, allow a more precise response and greater security.

(A mixed-reality demonstration was presented using the hololens, which brings holograms into the real world. It uses technology to make the holograms look and sound like they are actually part of the environment you are in.)

Even with the best cyber program in the world, the greatest vulnerability is someone within the organization—the person who unwittingly leaves the back door open for hackers and/or the insider who does something to harm the network. It's important for everyone in the organization to practice good cyber hygiene.

FUTURE OF AI SECURITY

> **Risk-Based AI Systems:** These search for risks through social media, news reports; if there is an emergency, they will immediately alert the operator to a risk so he/she can make a precision response.

> **Chat bots:** These machine-learning programs receive communications and can decipher different languages. They can detect key words that pop up in any communication, such as "gun" and "school," and report them to the operator.

> **Autonomous Robots:** These augment what humans can do; they have sensors and cameras and can do things humans can't (e.g., detect temperature, gun shots).

> **Drones:** They are self-contained, with sensors that allows them to automatically deploy and lock on a target if an area is breached.

WILL BALES

Supervisory Special Agent - Cyber, FBI Honolulu

Cyber threats are one of the top threats our nation is facing, and you may be targeted by criminal or national security actors. The U.S. agencies that work on cyber crimes are the Departments of Justice, Homeland Security, and Defense. All have different roles for tracking cybercrimes. The Presidential Policy Directive established the "lanes" in which the different agencies operate. The FBI is essentially your one-stop shop for cybercrimes, whether it's criminal or nation-state actors. Many people do not call the FBI when they've been hacked or have a ransomware incident, but they should, even if they're embarrassed or believe no recovery is possible. The FBI is the "police" for cybercrimes and investigates what happened and tracks the subjects.

The hacking process can take minutes, although exfiltration to maintain presence can take years, depending on how sophisticated the hackers are.

Traditionally, criminal actors move through the process quickly as they want to secure as much data as possible and don't care about being "noisy" per se, since once they get the data, they can do what they want with it.

On the other hand, nation-state actors are focused on the intelligence gathering, so they are going to be slow and methodical because they don't want to raise suspicion and want to learn what you are currently learning. Here are some other differences between national security and criminal intrusions:

- National-security intrusions: terrorism and espionage. Both of these are important for everyone here today, especially for those affiliated with universities. Both criminals and nation-state actors are interested in things being worked on at universities.
- Criminal intrusions: financially motivated; insider; hacktivists. Hacktivists usually have some type of social cause or reason for disruption. They often commit DDOS (distributed denial of service) attacks, bring down networks or servers—something that brings visibility to their cause.

North America will continue to be one of the most heavily targeted areas in the world for financially motivated actors (for instance, Sony, Equifax, Target, and eBay were targets). Education/universities comprised 13% of all hits with over a hundred different types of incidents. In 2017, almost 2 billion records were compromised. Unfortunately, with so many hacks in the news, people are becoming immune to them now.

THE REALITY OF DATA BREACHES

> 1,901,866,611 data records compromised in the first half of 2017

> 10,507,550 records lost or stolen every day, or 122 records per second

> 74% of breach incidents were identity theft

> When looking at the number of breaches by industry, healthcare accounted for 25% of incidents, followed by the financial sector (14%), and education (13%)

> 88% of data breaches occurred in North America

"You are targeted. It doesn't matter who you are, you are a target of a criminal or national security actors."

If you are confronted with ransomware, the FBI's official position is that you should not pay the ransom. It will encourage the criminals to continue to demand ransom. However, if you do pay, provide the FBI with the necessary information: the "wallet" in which the ransom was deposited; the email address you were communicating with; and other information that will enable law enforcement to track down the bad guys. By industry sector, almost 20% of reported ransomware was in education.

Nation-state intrusions are motivated by terrorist ideology and target specific individuals or organizations to steal sensitive information. These intrusions can be done anonymously, super cheaply, very quickly, with little risk and high reward. The fight is uneven with nations against a corporate IT department which often consists of 1 or 2 people. But corporations can secure their systems to mitigate intrusions if they have the resources to do so. One successful intrusion can steal gigabytes or more of information worth millions of dollars and years and years of work.

Potential targets of hackers: anyone with access to sensitive or proprietary data or technology that foreign governments or companies may find beneficial. Government/ law enforcement, cleared defense contractors, manufacturers, health insurers, law firms, and universities are some of the targets.

Targeted data: IP/research; contracts; personal identifiable information; military secrets; industrial control systems; and financial data.

ANATOMY OF A HACK

Hacktivism
> Hactivists use computer network exploitation to advance their political or social causes

Crime
> Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain

Insider
> Trusted insiders steal proprietary information for personal, financial, and ideological reasons

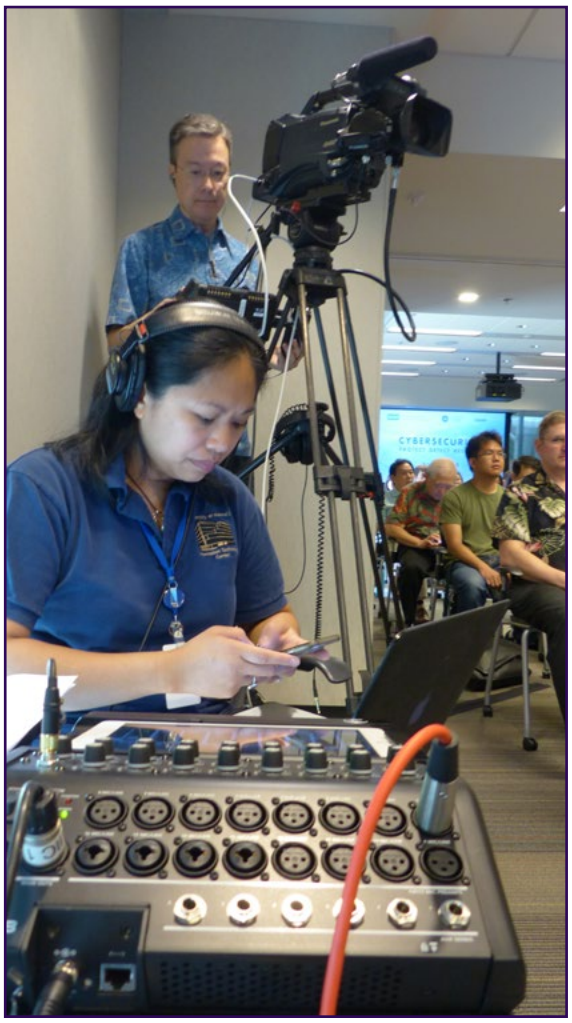
Espionage
> Nation-state actors conduct computer intrusions to steal sensitive state secrets and proprietary information

Terrorism
> Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid

Warfare
> Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

PROGRESSION OF A HACK

Recon > Initial compromise > Establish foothold > Escalate privileges > Internal recon > Move laterally > Expand presence > Exfiltrate data > Maintain presence



Al Vincent and Erica Aloang Aquino of UH's Information Technology Services Department filmed and monitored the forum's live stream. This marked the first time RCUH offered the option to live-stream, which allowed for higher participation across all islands.

Who is targeted:

- those with access to email
- those who work on a computer
- those who have a cell phone

Everyone is a potential target. It doesn't matter what your role is.

Cybercrime is a global crime. The FBI works with everyone it can. It has great relationships with foreign law enforcement. If/when a subject is identified, he/she can be tracked, arrested, and extradited no matter how long it takes.

Everyone is important in preventing and controlling cybercrime, so please continue to practice good cyber hygiene.

10 LARGEST HACKS

Count Ventures
(now Experian) 200 million accounts breached

NASDQ
161 million card numbers stolen; est. cost $300 million

eBay
145 million accounts compromised, $200 million in lawsuits

Equifax
143 million accounts breached

Target
30 million in 2013, 70—110 million accounts in 2014 impacted

Heartland Payment Systems
108 million debit/credit cards affected; est. cost $110 million

Sony
100 million accounts breached; class-action lawsuits totaling $171 million to $1.5 billion

Marshalls/TJ Maxx
94 million accounts hacked; est. cost $256 million

JP Morgan Chase
83 million personal and small-business accounts hacked

Home Depot
56 million customers affected

GARRET YOSHIMI

VP for Information Technology/CIO, UH Systems

About 10-15 years ago the security focus around campus was primarily on digital media/ copyright violations, like illegal music sharing. Fast-forward to today: the threat is now data breaches. These are becoming routine because they are showing up so often. So, if you expect your information to be private, it's not anymore. That's the reality of the world we live in today.

Public breaches: Odds are that almost all of us are affected. For example, Equifax and other organizations (e.g., Facebook, Boeing, presidential campaigns) that we trust with our valuable information have been breached.

Email compromises: There are many instances of phishing activities on campus caused by the front door or the back door being left open. For example, someone accidently clicks on a link providing your credentials to someone you thought was your buddy or was legitimate. The phishing email links take you to places that are sponsored by bad people who will attempt to capture your information or the links may contain a document that has a virus or malware embedded within it. If you receive an email from someone you don't recognize or are not expecting, it's probably not a good idea to click on the links in the email or to open the attachments that are part of the email—even if there is a promise you will win $100 million.

Highly targeted campaigns are spear phishing: they use more specific information tailored to your situation to get you to click on a link. They use tactics like these:

- Appear to be from someone you know (e.g., a supervisor, friend, UH president, etc.).
- Leverage your relationships to convince you to give up very specific information.
- Ask for bank account information.
- Conduct reconnaissance which can lead to a targeted attack.

TOP 10 SECURITY PRACTICES

1. Recognize that you, your devices, and your information are targets; know the threats.

2. Practice good password management.

3. Apply operating system and application updates frequently and regularly.

4. Install/update protective software, such as an anti-virus program.

5. Back up your data regularly and protect sensitive/regulated information by encrypting the data.

6. Use a secure network for sensitive transactions, not the coffee shop wi-fi or hotel computer.

7. Never leave your devices logged in and unattended; control access to your machines.

8. Use email and the internet safely; be careful when clicking an attachment or link in emails.

9. Monitor your accounts for suspicious activity.

10. Be careful what you share online and on social media; know your digital footprint.

Here's a recent example. The UH Financial Management Office received a legitimate-looking email supposedly from President Lassner which requested that a certain amount of money be wired to an account immediately for a critical purpose. This type of situation now happens all the time and it applies not only to UH matters but to personal accounts as well. It's imperative to practice good cyber hygiene.

These are the best ways to protect yourself:

- Use multi-factor authentication and strong passwords and password management.
- Do not use old, unsupported operating systems (e.g., Windows XP, Windows Server 2003).

Pay attention to common sense stuff: how you use your technology, computers, smartphones, and other devices. When you're looking at email on your smartphone, notice how it displays as compared to what appears on your computer. It is much harder to detect a phishing email from the phone, so use caution and don't click on those links too quickly. Same for text messages: be cautious of links within text messages. UH has had a number of security events. Not all of them are related to automated systems:

- There was a "paper breach" of 1099 information (which contained personally identifiable information) left in an unsecure and unattended area.
- Printers have been compromised: the default setting should be changed after purchase, but most people don't do it, which means that anyone can use your printer.
- A bomb threat came through a breached printer.
- Raspberry Pis[i] used for a research project were not configured properly which allowed for break-ins. The internet of things[ii] (IoT) is wonderful, but if not set up properly can cause tremendous vulnerabilities. AI and voice recognition are advancing by leaps and bounds, but the bad thing is if you don't use them properly, anyone can be following everything you are doing.

UH has a fairly robust security program that includes a number of first responders:

- ITS Help Desk: provides client services and an operations center that's now available 24/7
- ITS security office
- ITS SWAT teams
- UH CISO (Chief Information Security Officer)

"In this community and in this day and age, collaboration is very critical because the bad guys have more people, they have more resources, this is all they do."

We are here to help, identify issues, and remediate. We have excellent relationships with the three-letter agencies, and we conduct community and training/education events. We also have the ability to bring together key players.

There are other layers of protection besides our enterprise infrastructure:

- Gmail is an enterprise email; the full G-suite is available to the UH. UH conducts heavy monitoring of the network and servers that support the UH community.
- Distributed operations: IT is pretty spread out so there are folks at all

Panelist Garret Yoshimi discusses the ongoing investigation at the University of Hawai'i regarding a recent phishing scheme that impacted 2,400 individuals.

the different campuses.

- We have strong collaborative relationships that are critical to ensure we can adequately respond going forward.

A look toward the future: A number of Big-10 universities are working on automated and shared cybersecurity information among participating institutions. The "OmniSOC" represents collaboration within higher education to bring threat intelligence and threat response together in both automated fashion and with real people. The automation allows the collection of tons and tons of data on potential threats.

With machine learning and AI, you can raise the level of a small number of things that are critical threats and have the smart folks look at them to vet them properly and generate a proper response. UH is taking a close look at this as well as other similar efforts going on regionally. This is all about collaborating with peers to make sure we can actively respond to the large armies that are constantly attacking us. UH is also working closely with corporate partners, because everybody has to work together.

OTHER RESOURCES

> **University of Hawai'i Information Technology Services**

> **Federal Bureau of Investigation — Cyber Crime**

> **State of Hawaii — Office of Homeland Security**

> **Department of Homeland Security — Stop. Think. Connect.**

> **Microsoft Cybersecurity**

[i] *A Raspberry Pi is a very low-cost, credit card-sized computerized device originally created to teach programming/computer science to students. Its small size and affordability make it attractive to electronics enthusiasts, as its uses are immense: gaming, robots, weather stations, drones, etc.*

[ii] *A network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, etc., which enables these objects to connect and exchange data.*