Data Governance & Information Security @ UH

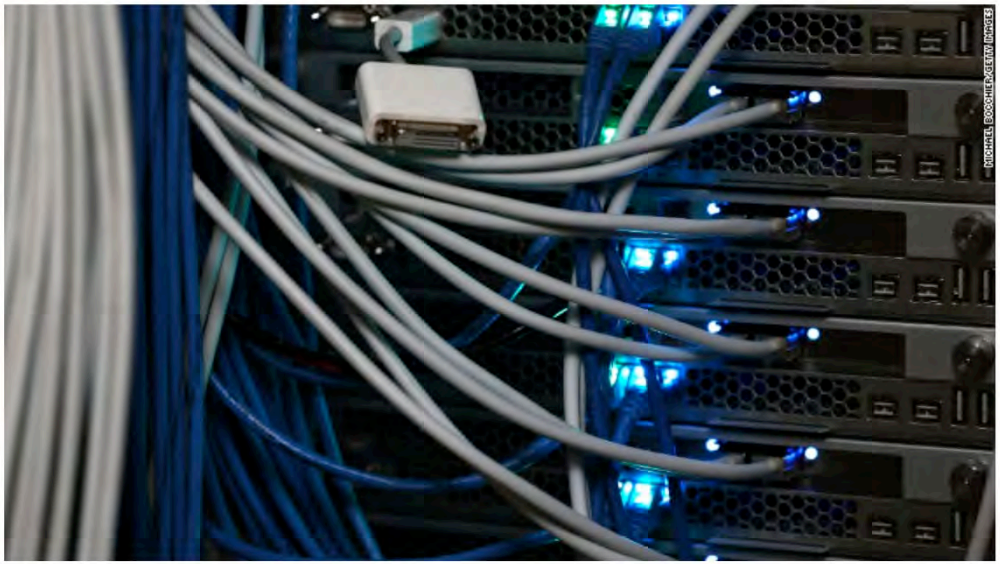
Spring 2018
Systemwide Campus Briefings

JT Ash, HIPAA Compliance Officer
Sandra Furuto, Data Governance Director
Jodi Ito, Chief Information Security Officer

2016 Presidential Campaign Hacking Fast Facts

CNN Library

Updated 1:19 PM ET, Mon February 5, 2018



(CNN) — Here's a look at hacking incidents during the 2016 presidential campaign and Russian meddling in the election. For details about investigations into hacking and efforts to interfere with the election, see 2016 Presidential Election Investigation Fast Facts.

CNN tech BUSINESS CULTURE GADGETS FUTURE STARTUPS

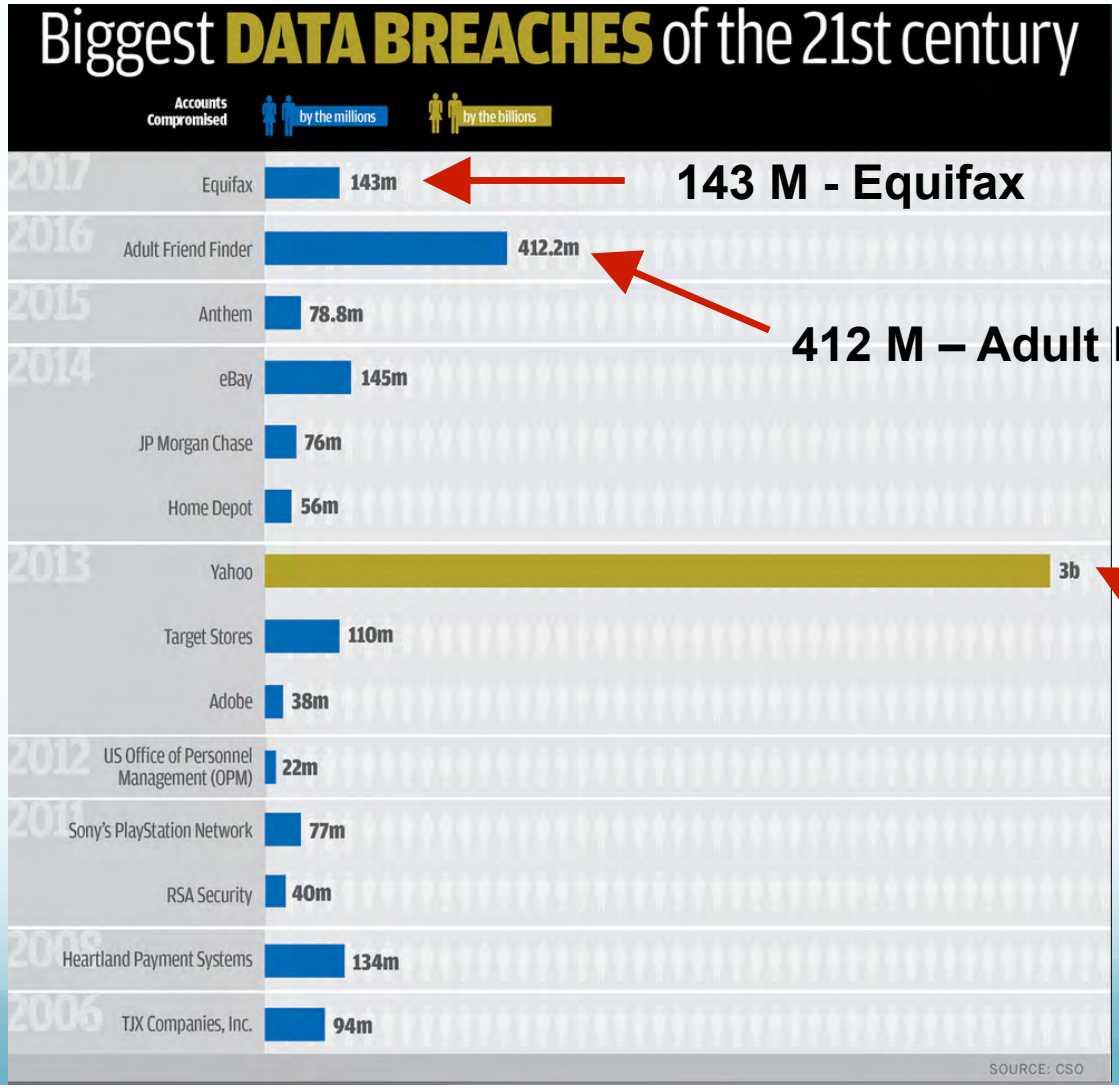
Giant Equifax data breach: 143 million people could be affected

by Sara Ashley O'Brien @saraashleyo

September 8, 2017: 9:23 AM ET

5 of the biggest data breaches ever

Equifax says a giant cybersecurity breach compromised the personal information of as many as 143 million Americans — almost half the country.



143 M - Equifax

412 M – Adult Friend Finder

3 B - Yahoo

HONOLULU Star-Advertiser

January 25, 2018 | 75° | Check Traffic

HAWAII NEWS

2,400 were exposed to phishing scheme, UH tells lawmakers

By Tyne Phillips tphillips@staradvertiser.com
Posted January 25, 2018
January 25, 2018

Updated January 25, 2018 1:03am

NOTE: some items in article are inaccurate

http://www.staradvertiser.com/2018/01/25/hawaii-news/2400-were-exposed-to-phishing-scheme-uh-tells-lawmakers/

Subject: Report to the Legislature on Data Exposure at the University of Hawaii

Discovery of Data Exposure:	October 2017
Location of Data Exposure:	University of Hawai'i
Nature of Data Exposure:	Files containing sensitive information discovered while investigating a Business Email Compromise (BEC)

Incident Description:

In October 2017, while investigating an email compromise, network devices on the University of Hawai'i (UH) network were found to contain sensitive information. At this time, UH cannot confirm that any of the sensitive information was taken or that it was misused.

It is important to note that these types of attacks are extremely difficult to detect and to protect against. The network was protected by a firewall but the attackers were able to circumvent security controls and compromise login credentials to gain access to the network.

UH is in consultation with federal law enforcement agencies and is continuing its investigation. Due to the sensitivities of the investigation, more comprehensive details will be supplied at a later date when doing so does not impede the investigations. Approximately 2400 individuals have been identified. Notification letters are being sent out and all potentially affected individuals are being provided one (1) year of credit monitoring services (Attachment A).

http://www.hawaii.edu/govrel/docs/reports/2017/hrs487n-4_2017_october-2017-breach_report.pdf


CyberAware
TECHNOLOGY
MAKES OUR LIVES EASIER AND
MORE EFFICIENT ONLY IF WE KEEP
OUR DEVICES
SAFE AND SECURE
STAYSAFEONLINE.ORG
National Cyber Security
Awareness Month
STOP | THINK | CONNECT

"Alexa, order dog food."

"Alexa, reorder paper towels."

"Alexa, turn off the lights."

Google Home

Big help is here with Google Home. It has the Google Assistant built-in, so you can ask it questions and tell it to do things. Just start with "Ok Google" to get answers from Google, play your songs, tackle your day, enjoy your entertainment and control your smart home. And when you ask for something, thanks to Voice Match, the Assistant provides information that's personalized just for you since it can distinguish your voice from others. There's plenty of help to go around.

"Cyber threats are among the gravest national security dangers to the United States. "

The White House Office of the Press Secretary For Immediate Release, February 25, 2015

"Our citizens, our private sector, and our government are increasingly confronted by a range of actors attempting to do us harm through identity theft, cyber-enabled economic espionage, politically motivated cyber attacks, and other malicious activity."

The White House Office of the Press Secretary For Immediate Release, February 25, 2015

Data Governance Update

Sandra Furuto, Data Governance Director

What is Data Governance

"...a framework that enables us to effectively manage data"

- Defines how data are collected, stored, and used
- Defines who can access data, when, and under what conditions
- Establishes decision rights
- Establishes clear lines of accountability
- Gives a voice to all appropriate parties
- Provides a mechanism for conflict resolutions involving data

UH Data Governance Goals

Protect the privacy and security of Institutional Data

(i.e., data created, received, maintained, and/or transmitted by UH in the course of meeting its administrative and academic requirements)

- Produce higher quality data for informed decision making
- Promote efficient use of resources
- Increase transparency and accountability

Key Regulations and Penalties (1)

Regulation	Description	Penalty
Family Educational Rights and Privacy Act (FERPA)	• Federal law that protects the privacy of student education records • Access to personally identifiable information (PII) is based on a legitimate educational interest • UH's FERPA policy: AP7.022 • Data subject to regulation: • All student data EXCEPT directory information (e.g., name, major, class standing, date of attendance, full- or part-time status, degrees conferred, honors and awards, height/weight of athletes, etc.)	Potential loss of federal financial aid funding
Higher Education Act (HEA)	• Federal law that protects the federal financial aid information • Much more restrictive than FERPA Data subject to regulation: • FAFSA data • PII cannot be shared even with student consent – waiting for clarification from USDOE	Potential loss of federal financial aid funding

Key Regulations and Penalties (2)

Regulation	Description	Penalty
Health Insurance Portability and Accountability Act (HIPAA)	• Federal law that protects the privacy of individually identifiable health information • UH's HIPAA policy: EP2.217 Data subject to regulation: • Health	Financial fines; also requires a breach notification to HHS & in accordance with SoH HRS §487N
Hawai'i Revised Statute (HRS) Chapter 92F	• State law also known as the Uniform Information Practices Act (UIPA) which requires open access to government records • Governs open records requests Data subject to regulation 92F-12: • Employee data that must be made available to the public (e.g., name, salary range, bargaining unit, job title, business address/ phone, employing agency, etc.)	If data is intentionally revealed that should not be, could be convicted of a misdemeanor unless a greater penalty is provided for by law.

Key Regulations and Penalties (3)

Regulation	Description	Penalty
Payment Card Industry Data Security Standard (PCI-DSS) information	• A widely accepted set of policies / procedures that protects cardholders' credit/debit/cash card transactions Data subject to regulation: • Credit Card	Financial fines; also requires a breach notification in accordance with HRS §487N

Hawai'i Revised Statutes (HRS) §487N	• State law that defines the breach notification to the legislature
	• Written report to the legislature within 20 days after the discovery of a data breach
	
	Data subject to regulation:
	• First Name or First Initial/Last Name combined with:
	  • Social Security Number (SSN)
	  • Driver license or state ID #
	  • Info to access a person's financial account (account #, access codes, passwords, etc.)
	• Health information covered by HIPAA
	• PCI-DSS information	

Key Regulations and Penalties (4)

Regulation	Description	Penalty
National Institute of Standards and Technology Special Programs (NIST SP) 800-171r1	• Dept. of Defense (DoD) Defense Federal Acquisition Regulations Supplement (DFARS) clause 252.704.2012 • To protect Controlled Unclassified Information (CUI) Data subject to regulation: • Data defined by DoD as requiring protection (primarily research project data sponsored by the DoD) • Near future: Educational data (future US Dept. of Education mandate)	
National Industrial Security Program	• DoD Directive 5220.22-M • National Industrial Security Program Operating Manual Data subject to regulation: • Classified data	

Key Regulations and Penalties (5)

Regulation	Description	Penalty
Biological Safety Program	Governs all research, teaching, and testing activities involving infectious agents and recombinant materials • Section 511 of the Antiterrorism and Effective Death Penalty Act of 1996 • Public Health Security and Bioterrorism Preparedness and Response Act of 2002 • Executive Order 13546 • 7 CFR Part 331, 9 CFR Part 121, and 42 CFR Part 73	
Export Control & International Traffic in Arms Regulations (ITAR)	• Federal regulations that impose access, dissemination or participation restrictions on the use and/or transfer of commodities, technical data, or the provision of services subject to United States (US) export controls for reasons of national security, foreign policy, anti-terrorism or non-proliferation • 22 Code of Federal Regulations (CFR) Parts 120-130 • 15 CFR Parts 730-774 • 31 CFR Parts 500-599	

Impact of Data Breaches

- Loss of federal financial aid funding (FERPA, HEA)
- Financial fines (HIPAA, PCI-DSS)
- Class action lawsuits
- Expenses, financial and human capital
- Loss of reputation / unfavorable publicity
- Additional legislative scrutiny

UH Data Related Policies and Procedures

Executive Policies

- **Institutional Data Governance EP2.215**
- Use and Management of Information Technology Resources EP2.210 (to be updated)
- System and Campus Wide Electronic Channels for Communicating with Students EP2.213
- Data Classification Categories & Info Security Guidelines EP2.214
- Institutional Records Management and Electronic Approvals / Signatures EP2.216 (to be updated)
- HIPAA EP2.217
- Online Approvals of Internal University Transactions EP2.218

Administrative Procedures

- FERPA AP7.022
- Data System Authorizations (TBD)
- Mandatory Training & Continuing Education Requirements AP2.215
- Open Records Requests (TBD)
- Data Sharing Request Process (in progress)
- Specialized Purchasing AP8.265
- Records Retention Schedule (in progress)
- Credit Card Program AP8.710
- Data Breaches (coming soon)
- Electronic Payments via University Websites AP8.711

EP2.214, Data Classification Categories

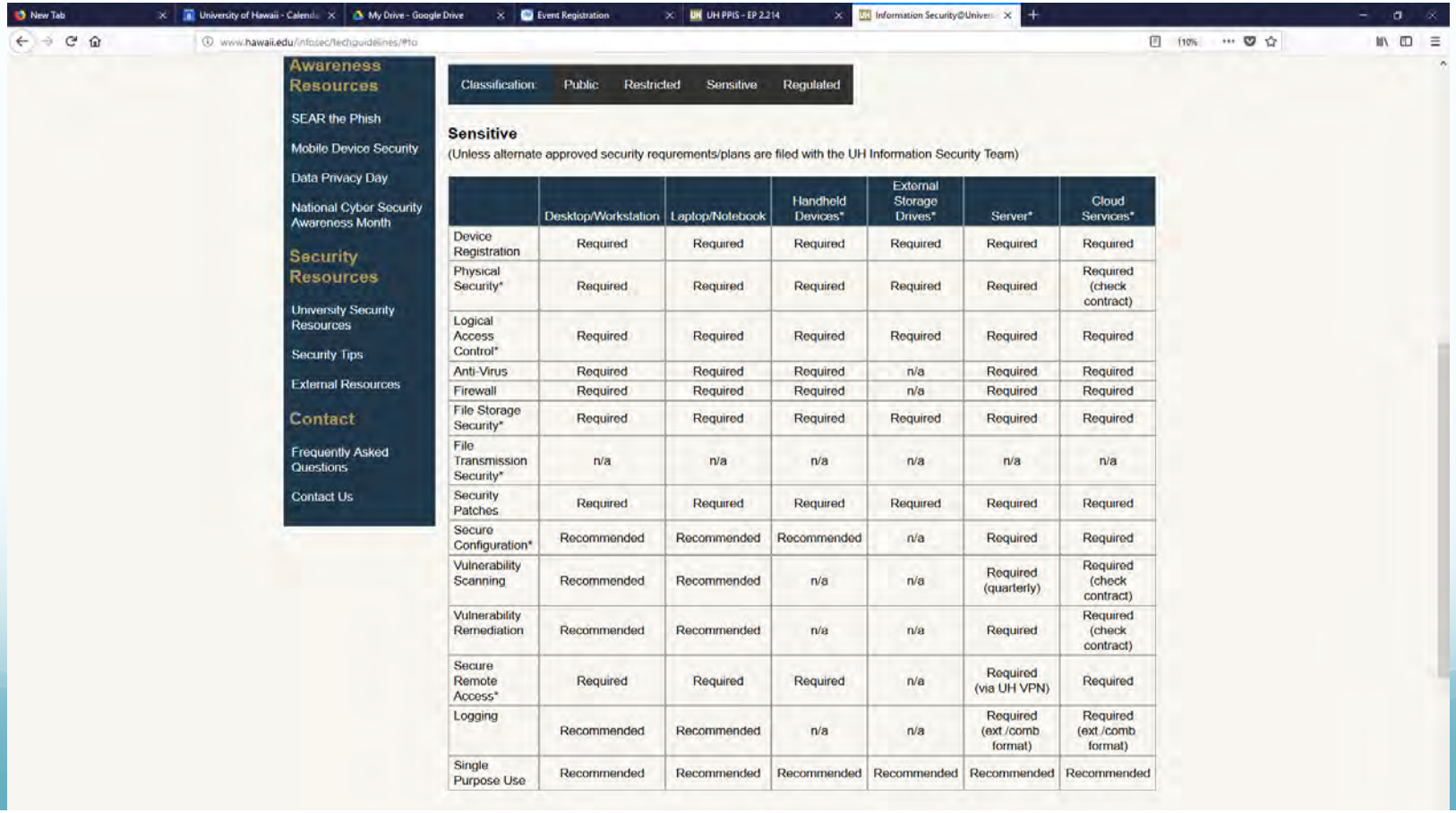
Category	Definition	Examples
Public	Access is not restricted and is subject to open records requests	Student directory information, employee's business contact info
Restricted	Used for UH business only; will not be distributed to external parties; released externally only under the terms of a written MOA or contract	Student contact information, UH ID number
Sensitive	Data subject to privacy considerations	Date of birth, job applicant records, salary/payroll information, most student information
Regulated	Inadvertent disclosure or inappropriate access requires a breach notification by law or is subject to financial fines	FN or first initial/LN in combination with SSN, driver license number, or bank information; credit card, HIPAA, or financial aid information

Examples of Data / Information by Category

Public	Restricted	Sensitive	Regulated
Student Data • Name • Major field of study • Class (i.e., freshman, sophomore, etc.) **Employee Data** • Name • Job title, description • Business address, phone number • Education and training background • Previous work experience • Dates of first and last employment • Position number, type of appointment, service computation date, occupational group or class code, bargaining unit code	**Student Data** • UH email address/ username • Address (street name and number) • Personal phone number • UH ID card photographs for University use **Student and Employee Data** • UH ID number • Banner PIDM • ODS PIDM	**Student Data** • Gender • Ethnicity • Grades • Courses taken • GPA **Employee Data** • Address (street name and number) • Personal phone number **Student and Employee Data** • Date of birth • Non-UH email address • Job applicant records (names, transcripts, etc.) • Salary and payroll information	**FN and first initial and LN with the following:** • Social Security Number • Driver's license • Hawai‘i ID card number • Financial account (checking, savings, brokerage, CD, etc.), credit card, or debit card numbers **Business/Financial Data** • Payment Card Industry Data Security Standard (PCI-DSS) information **Protected Health Information (PHI)** • Health status • Healthcare treatment • Healthcare payment **Financial Aid Data** • FAFSA data

Technical Guidelines

http://www.hawaii.edu/infosec/techguidelines/



Awareness Resources
- SEAR the Phish
- Mobile Device Security
- Data Privacy Day
- National Cyber Security Awareness Month

Security Resources
- University Security Resources
- Security Tips
- External Resources

Contact
- Frequently Asked Questions
- Contact Us

Classification: Public | Restricted | Sensitive | Regulated

Sensitive

(Unless alternate approved security requirements/plans are filed with the UH Information Security Team)

	Desktop/Workstation	Laptop/Notebook	Handheld Devices*	External Storage Drives*	Server*	Cloud Services*
Device Registration	Required	Required	Required	Required	Required	Required
Physical Security*	Required	Required	Required	Required	Required	Required (check contract)
Logical Access Control*	Required	Required	Required	Required	Required	Required
Anti-Virus	Required	Required	Required	n/a	Required	Required
Firewall	Required	Required	Required	n/a	Required	Required
File Storage Security*	Required	Required	Required	Required	Required	Required
File Transmission Security*	n/a	n/a	n/a	n/a	n/a	n/a
Security Patches	Required	Required	Required	Required	Required	Required
Secure Configuration*	Recommended	Recommended	Recommended	n/a	Required	Required
Vulnerability Scanning	Recommended	Recommended	n/a	n/a	Required (quarterly)	Required (check contract)
Vulnerability Remediation	Recommended	Recommended	n/a	n/a	Required	Required (check contract)
Secure Remote Access*	Required	Required	Required	n/a	Required (via UH VPN)	Required
Logging	Recommended	Recommended	n/a	n/a	Required (ext./comb format)	Required (ext./comb format)
Single Purpose Use	Recommended	Recommended	Recommended	Recommended	Recommended	Recommended

Institutional Data Governance Principles and Guidelines (1)

- Access to Institutional Data will be based on a need-to-know
- Minimal access will be granted whenever possible
  - i.e., the most restrictive set of permissions and privileges will be granted, and only for the duration needed
- De-identified data will be provided whenever possible
- Duplication of data is discouraged
- Data requested for a specific purpose cannot be used for another purpose, i.e., re-purposed and re-disclosed

Institutional Data Governance Principles and Guidelines (2)

- Data within a record or document will be protected based on the data element with the highest level of sensitivity
- Be aware that a data element may not be personally identifiable, but when combined with other data elements, it may become personally identifiable
- Be aware of small cell sizes in reports
- When accessing data outside of work, do not use unprotected or public wireless connections
- When data is no longer needed—redact, remove, or destroy it!

What Constitutes PII under FERPA

"…information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty."

AP2.215, Mandatory Training and Continuing Education Requirements for Data Users

Requirements	Renewal
Information Security Awareness Training (ISAT)	Every 2 years
General Confidentiality Notice (GCN) acknowledgment	Annually

Other information:

- Both requirements are located at www.hawaii.edu/its/acer
- The training modules are being updated this spring 2018
- Users will be given 2 months advance notice to complete requirements

Who needs to take the training? (1)

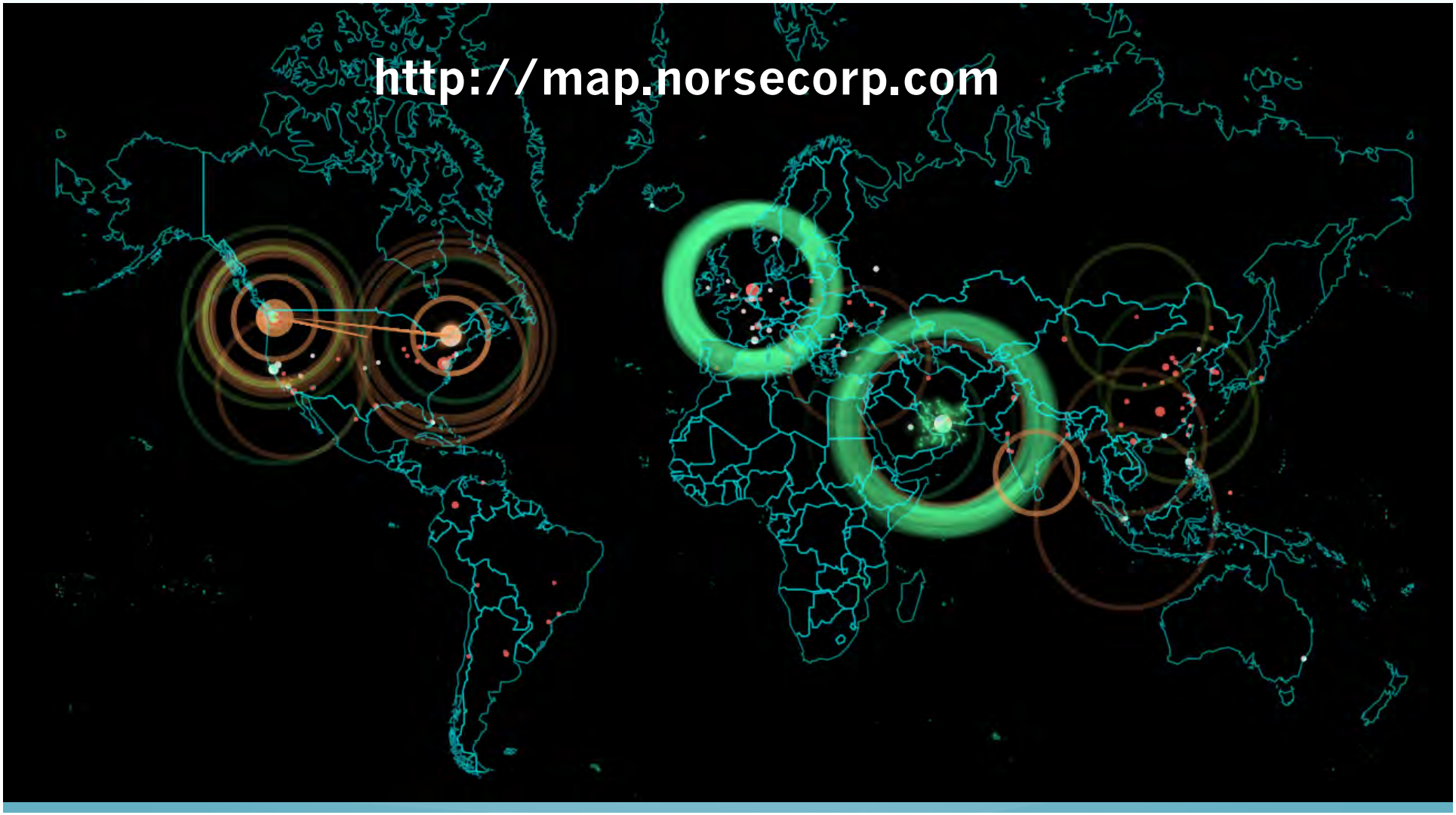
1. UH Data Users with access to
   - non-public data AND
   - multiple quantities / bulk records (accessed electronically, on paper, or through other media)

   Note individuals with electronic (view) access to a single record at a time are not required to take the training at this time
2. Those who submit a data sharing request (process where a copy of Institutional Data will be released to an individual who does not normally have access to the data or to a third party)

Who needs to take the training? (2)

- UH personnel with login privileges to Institutional Data Systems (and who have access to bulk records)
  - Examples: Banner/ODS, Peoplesoft/HR Data Mart, KFS/eThority, STAR, Laulima
- Pilot will be ODS in summer 2018
- Those who are requesting login privileges to an Institutional Data System for the first time (and who will have access to bulk records)
- New hires - incorporate training into the onboarding process (future goal)

Security Landscape & Current Threats at UH


http://map.norsecorp.com

University Hackers Attacked 5,000 IoT Devices on Campus

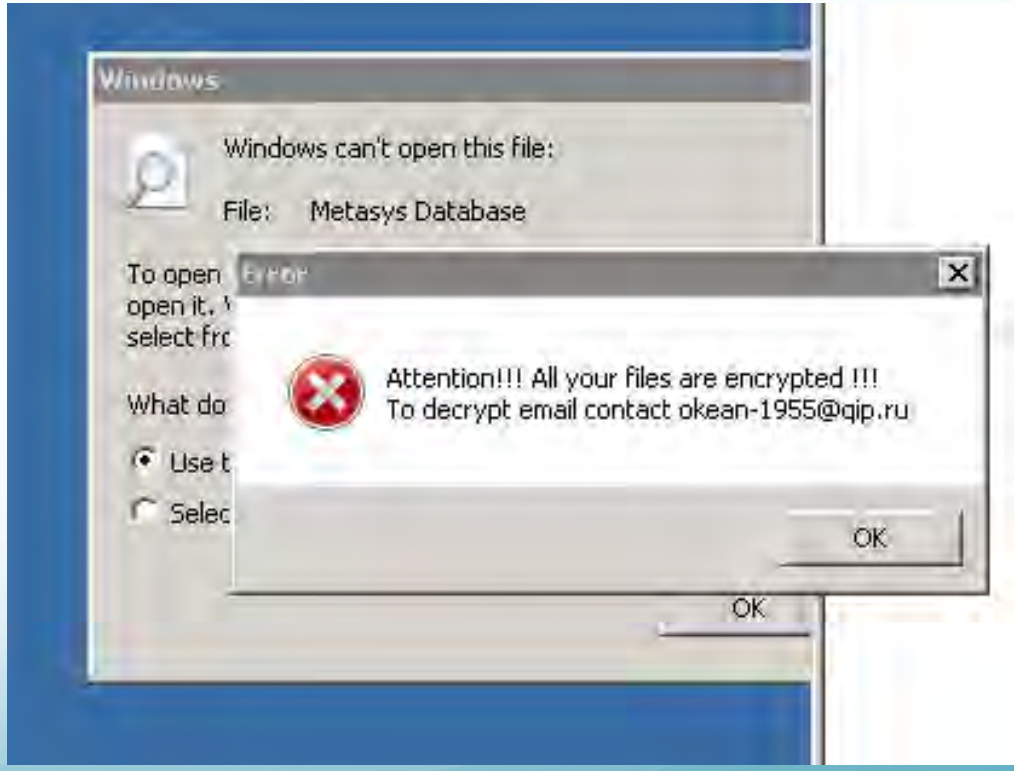
https://campustechnology.com/articles/2017/02/13/university-hackers-attacked-5000-iot-devices-on-campus.aspx

In the case of "the botnet barrage," as the case study dubbed the attack, senior members of the university's IT staff had received complaints of slow and inaccessible network connectivity on campus. Upon examination, the incident commander found that name servers "were producing high-volume alerts and showed an abnormal number of sub-domains related to seafood," according to the preview. The incident inspector contacted Verizon's RISK Team, which conducted a firewall analysis that "identified more than 5,000 discrete systems making hundreds of DNS lookups every 15 minutes."

"Of these, nearly all systems were found to be living on the segment of the network dedicated to our IT infrastructure," the incident commander said in the preview. "This was a mess. Short of replacing every soda machine and lamp post, I was at a loss for how to remediate the situation. We had known repeatable processes and procedures for replacing infrastructure and application servers, but nothing for an IoT outbreak."

Control Systems, Access Control Servers, etc.

- June 2016: HVAC control server hit w/ ransomware
- Ques. from contractor: Who is responsible for patching/maintenance?



Who's Responsible?

- State of Hawaii Dept. of Human Services (DHS) contracted with UH Community Colleges
- HiNET: provides training for SNAP eligible individuals
- DHS-owned computer on UH public network accessing DHS databases w/ PII

Business Email Compromise (BEC)

- Phishing & Spear Phishing
- Want your personal information:
  - username/password: gain access to YOUR email account, YOUR computer & information systems that you use
  - SSN, credit/bank account information, home address – financial crimes
- Will use that information for other malicious/criminal purposes

From: **John Daniel** <amyg@hawaii.edu>
Date: Thu, Feb 15, 2018 at 10:55 AM
Subject: Assignment Schedule
To:

Compromised UH email account

Secured PDF Document

View Download

https://manishy.ml/ll/doc/doc/doc/index.php

the file is secured from unnecessary access only you can open it,
it requires you to your email and password to gain access.

Highly Targeted Spear Phishing

- Appears to be from someone you know (supervisor, colleague, friend, President of the University…)
- Leveraging your relationship to attempt to get you to give up very specific information
- Email from the UH President apparently addressed to the Director of FMO/UH Controller
- Asking for bank account information
- Possible reconnaissance; leading to a targeted attack

S.E.A.R. the Phish

- **S**top. **E**xamine. **A**sk. **R**eport.
- www.hawaii.edu/infosec/phishing

http://www.hawaii.edu/infosec/spearphishing/

Home

Report Issues or Incidents

About the UH Information Security Program

Policies & Compliance

HIPAA

UH Information Security Awareness Training

Spearphishing

Information Security for

Students

Research

Faculty & Staff

System Administrators & Developers

Technical Guidelines

Awareness

Spearphishing

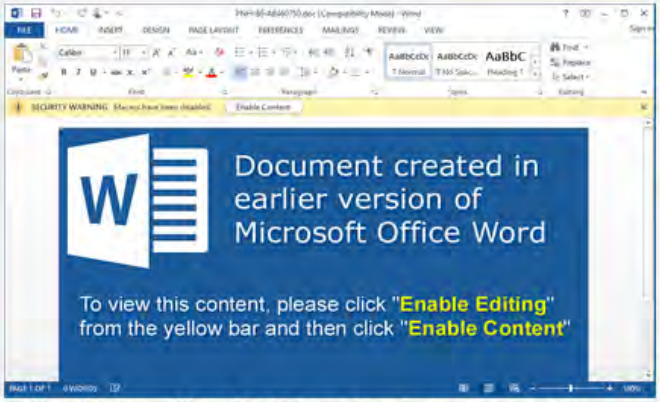
What is a Spearphish?

A malicious email that targets an individual which appears to be from a trusted sender. The spearphish will contain a link or attachment that appears to be safe to open. If the link is clicked or the attachment opened, malicious software can be silently installed on the computer. This gives the cybercriminals remote access to the computer who can then steal all of the individual's personal information, business files, and passwords stored on the hard drive and network shared folders as well as search for and compromise other computers in the organization in order to steal more data.

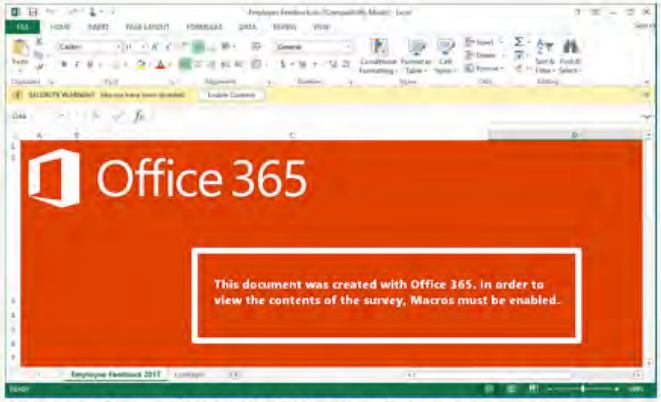
Examples of Suspicious Attachments

Note: The following are tested on Windows 10 and Office 2013 (other versions may display different messages or none at all).

Click on the images to enlarge them.



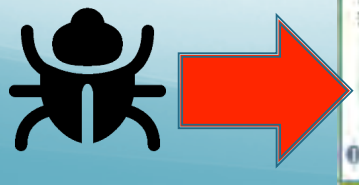
1. Word Macro - Word file (.doc, .docm) contains a script. Warning appears in yellow bar at the top.

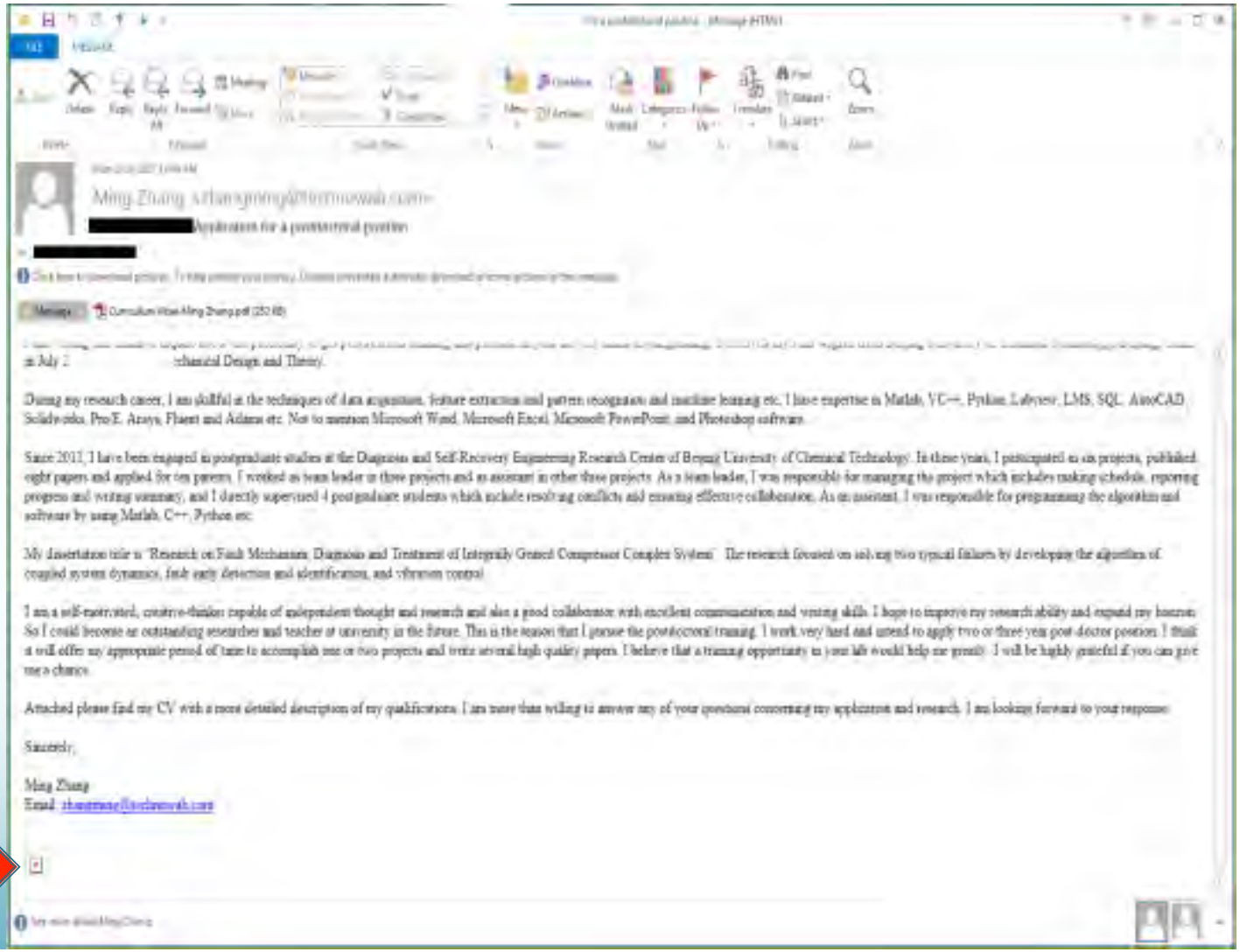


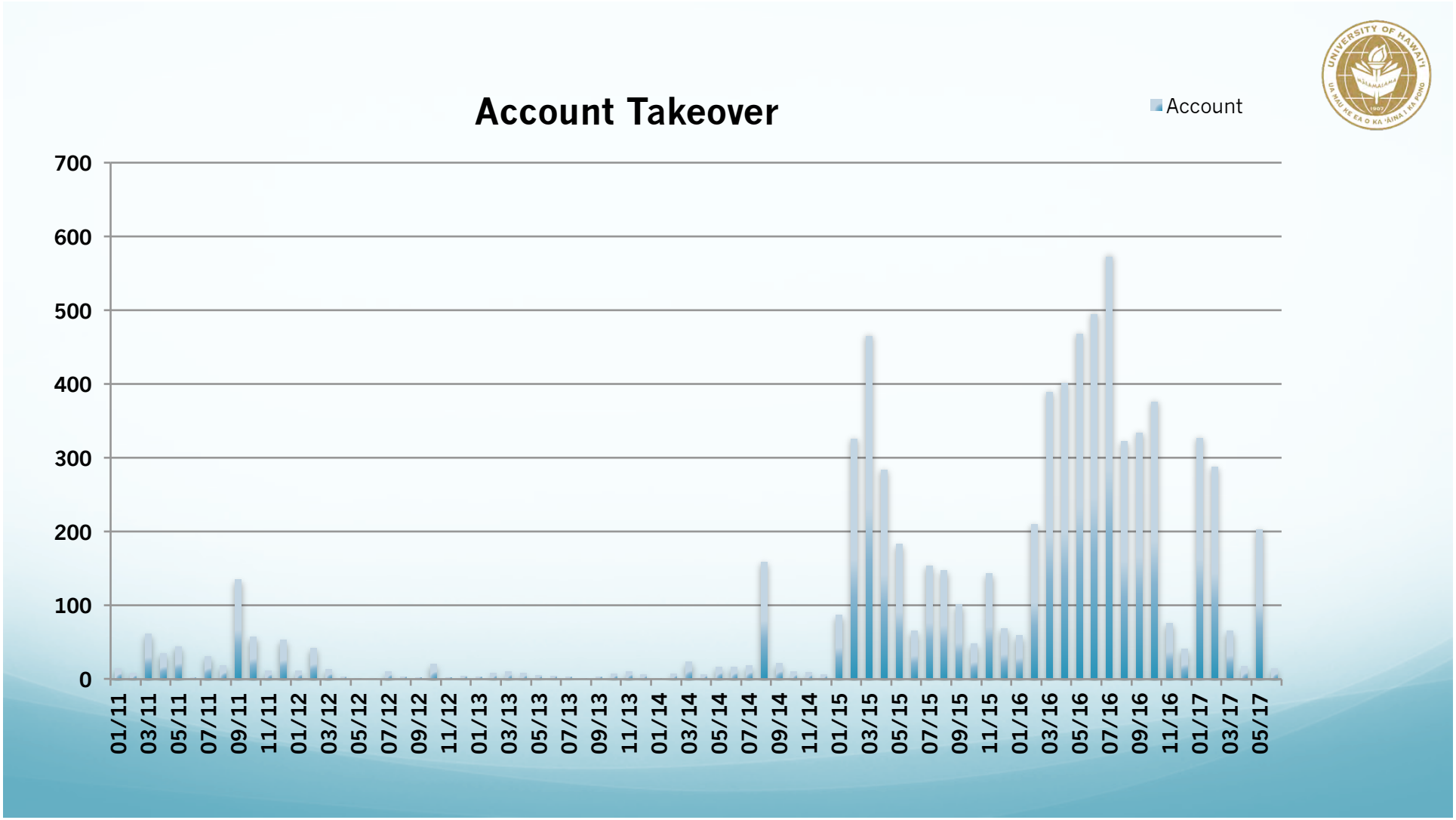
2. Excel Macro - Excel file (.xls, .xlsm) contains a script. Warning appears in yellow bar at the top.

Possible Reconnaissance

- E-mails from foreign nationals with resumes and “web bugs” in them






Account Takeover
Account
700
600
500
400
300
200
100
0
01/11
03/11
05/11
07/11
09/11
11/11
01/12
03/12
05/12
07/12
09/12
11/12
01/13
03/13
05/13
07/13
09/13
11/13
01/14
03/14
05/14
07/14
09/14
11/14
01/15
03/15
05/15
07/15
09/15
11/15
01/16
03/16
05/16
07/16
09/16
11/16
01/17
03/17
05/17

Recommendations

- Inventory computing assets and data files
- Remove / Replace old systems (sanitized or destroy hard drives before disposal)
- Close off remote login/access capabilities from the world (rdp, vnc, team viewer, etc.)
- Look for user accounts (that you didn't create)
- Use network segmentation; look for lateral movement*
- Be suspicious of resumes (or unsolicited documents) from any source (could be from a trusted colleague whose email account was compromised), don't immediately share

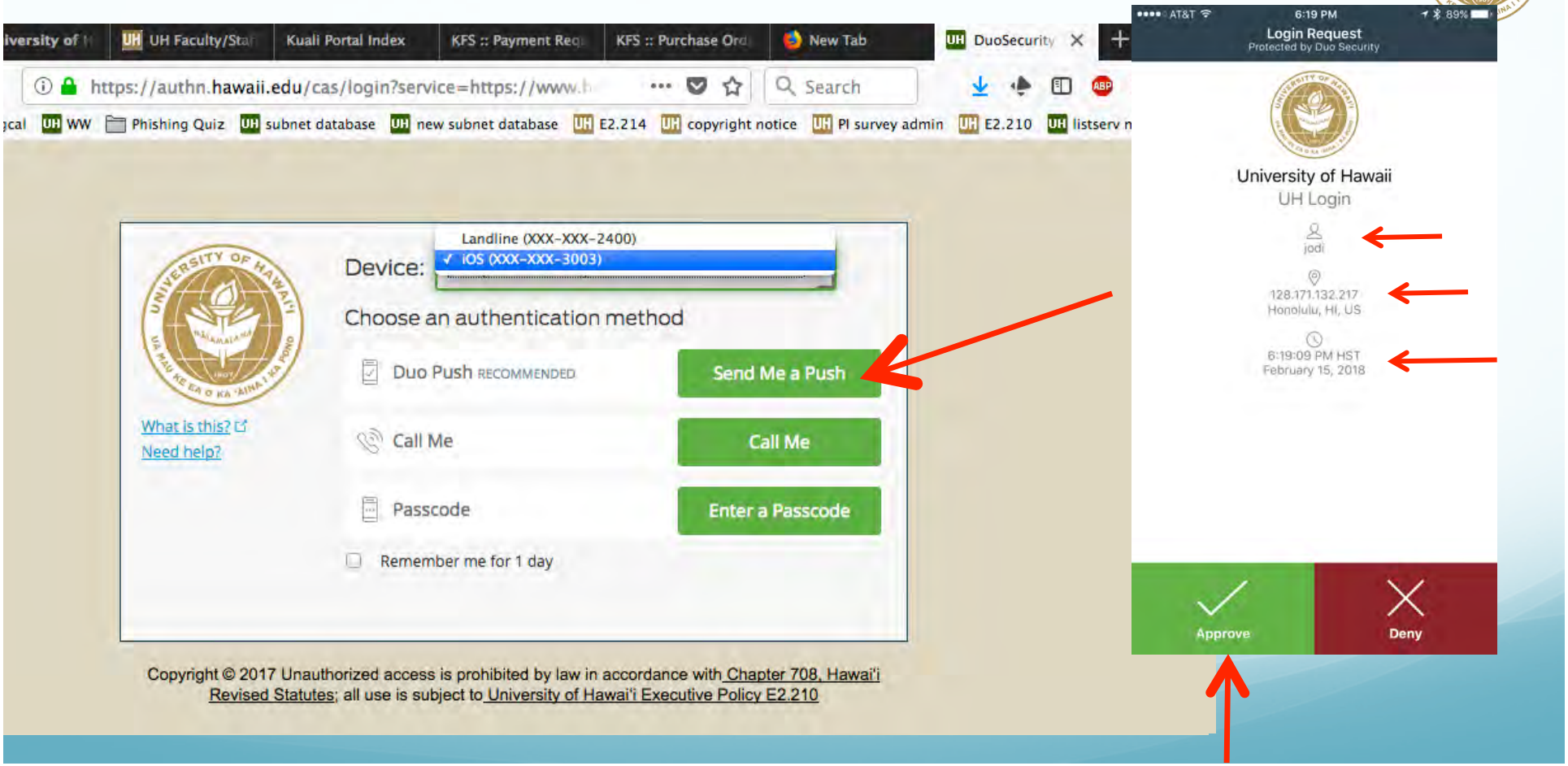
* for technical/IT support

Best Way for Individuals to Protect Themselves

- Use multi-factor AND strong passwords/password management
  - http://www.hawaii.edu/its/uhlogin/
  - DO NOT RE-USE PASSWORDS!
  - Use hard to guess passwords
  - Change passwords regularly

- If at all possible, DO NOT USE OLD/ UNSUPPORTED Operating Systems (e.g. Windows XP, Windows Server 2003)

Multi Factor Authentication at UH - DUO



Proactive Cyber Hygiene

- Be suspicious of emails – even if from people you know!
  - Does it have an attachment that you weren't expecting?
  - Does it seem "strange"? Unusual tone/vocabulary?
- EVERYONE is a TARGET!
- Patch your systems and applications as soon as a patch is released

Attackers are Persistent

- Remain VIGILANT!
- Stay up-to-date!
- Attackers are stealthy, adaptive, fast, well-organized, well-trained
  - Vulnerability announced on Sept. 12; Exploit used on Sept. 15.
  - NSA exploit code released on April14; Exploit used on April 18

Recent Security Events @ UH

Feb. 2017: Paper "Breach"

To: Administrative Officers, Fiscal Administrators, and HR Representatives:

From: Financial Management Office, University of Hawaii

Subject: Reminder – Handling UH Employee's W2 and 1095C Documents

As a reminder, the original W2 (Wage and Tax Statement) and 1095C (Employee Provided Health Insurance Offer and Coverage) documents should have been issued to respective employees no later than January 31, 2017. With the increase in identity theft, please exercise due diligence in safeguarding an employee's record containing confidential and personal information. All documents containing such confidential and personal information must be secured at all times by authorized personnel. There should be no photocopies of the W2 or 1095C documents made by the schools, colleges and departments for any purpose.

If employee requests for a duplicate copy of the W2 or 1095C, please see below:

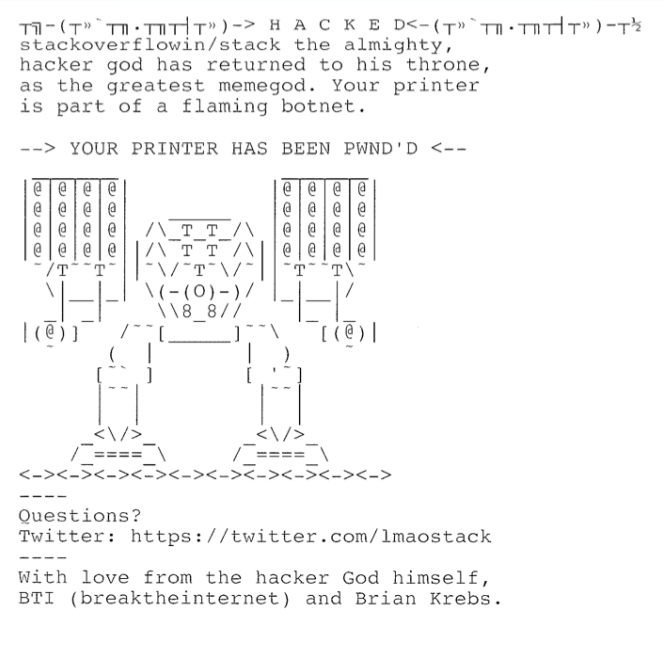
- Employee requests for duplicate W2 should be sent to the UH Payroll Office in writing. See the instructions here.
- Employee requests for duplicate 1095C should be directed to the HR representative who is able to regenerate a copy for that employee.

In addition, please return all undeliverable W-2 and 1095 C documents and the envelopes in which they were mailed in to the UH Payroll Office after April 13, 2017.

Susan Lin | Director of Financial Management and Controller | **University of Hawaii System Financial Management Office**
1406 Lower Campus Road, Room 41 | Honolulu, HI 96822

Compromised Printers

- Feb. 2017: another round of “printer spam”

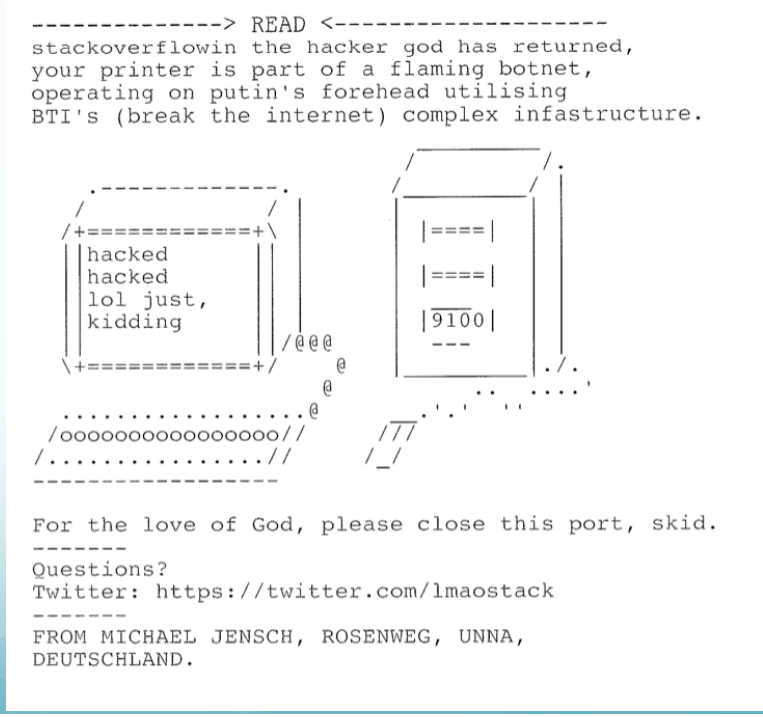


```
ᴛᴛ̄-(ᴛ»`ᴛᴛ·ᴛᴛᴛ┼ᴛ»)-> H A C K E D<-(ᴛ»`ᴛᴛ·ᴛᴛᴛ┼ᴛ»)-ᴛ½
stackoverflowin/stack the almighty,
hacker god has returned to his throne,
as the greatest memegod. Your printer
is part of a flaming botnet.

--> YOUR PRINTER HAS BEEN PWND'D <--
```



```
Questions?
Twitter: https://twitter.com/lmaostack
----
With love from the hacker God himself,
BTI (breaktheinternet) and Brian Krebs.
```



```
-------------> READ <--------------------
stackoverflowin the hacker god has returned,
your printer is part of a flaming botnet,
operating on putin's forehead utilising
BTI's (break the internet) complex infastructure.
```



```
For the love of God, please close this port, skid.
-------
Questions?
Twitter: https://twitter.com/lmaostack
-------
FROM MICHAEL JENSCH, ROSENWEG, UNNA,
DEUTSCHLAND.
```

May 2017: Bomb threats

Good Morning,

I'll be brief.

I installed several explosives in the building.

If you do not send in the amount of $ 25,000 by May 31st I will blow up this whole block.

If you try to contact the police, I'll know.

I also have access to your computers and email addresses.

Go to the nearest WesternUnion agency and send the amount to Emerson Eduardo Rodrigues Setim. The passport number is FO645170. It´s a brazilian passport. The city that the money will be withdraw is Chicago, Illinois, USA.

Do as I say and no one will get hurt.

PS: I repeat, if you try to contact the police i will known.

Other Compromises

- Raspberry Pis used for a research project
  - Tiny (credit card sized) computer
  - Within 30 minutes, Pis were compromised – all passwords changed and running 100% utilization
  - Running Linux.MulDrop.14 – mining cryptocurrency
  - Raspberry Pis used the default username and password
- New computer placed on the network; compromised overnight

Analysis of a Compromise

- May 17: Computer compromised with ransomware
- Found exploit code related to EternalBlue & DoublePulsar on the system; installed on April 18, 2017 (NSA toolkit leaked on April 14, 2017- 4 days earlier)
- System compromised in April via **RDP**
- Moved laterally trying to compromise other systems
- Not sure why attacker exposed themselves by launching ransomware
- NSA toolkit/exploit framework extremely hard to detect (runs in memory)

When to Notify UH InfoSec Team

- UH webserver is defaced
- UH server appears to be compromised
- Sensitive information may be lost, stolen, exposed, accessed by unauthorized personnel
- Computer, laptop, mobile device, portable storage, etc. containing sensitive information is compromised, lost, stolen
- Paper documents containing sensitive information is lost, stolen, exposed, or accessed by unauthorized personnel
- http://www.hawaii.edu/infosec/notification ; email: infosec@hawaii.edu; Call Jodi (808) 956-2400

Incident Response

- Assess situation & risk:
  - Does the user access/use sensitive information as part of their roles & responsibilities?
  - Could the user have sensitive information on their system?
  - If yes, to any of the above – BEFORE remediation:
    - Contact UH InfoSec for guidance
    - Contact your IT support staff
    - Take memory dump
    - Take an image of the system

HoneyPot Project

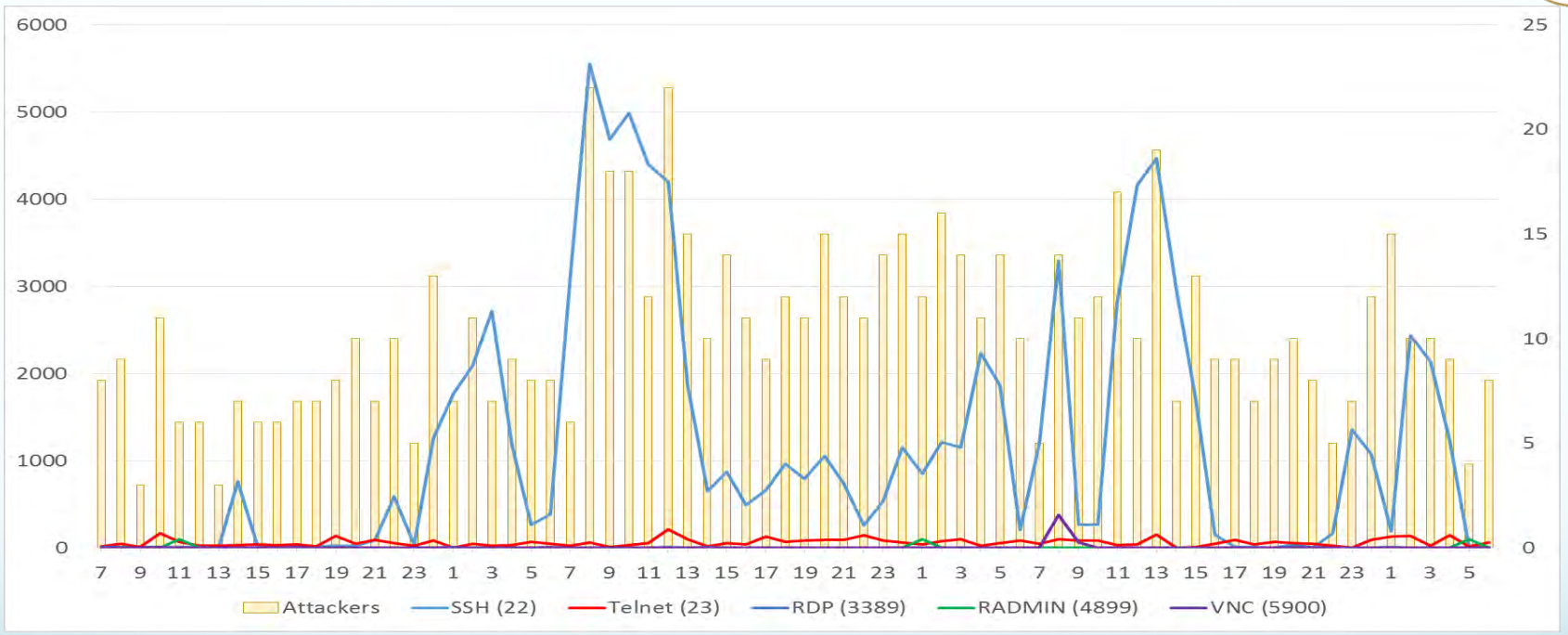
Date Span: 7/21/17 (Fri) to 7/24/17 (Mon)

Monitored Services:

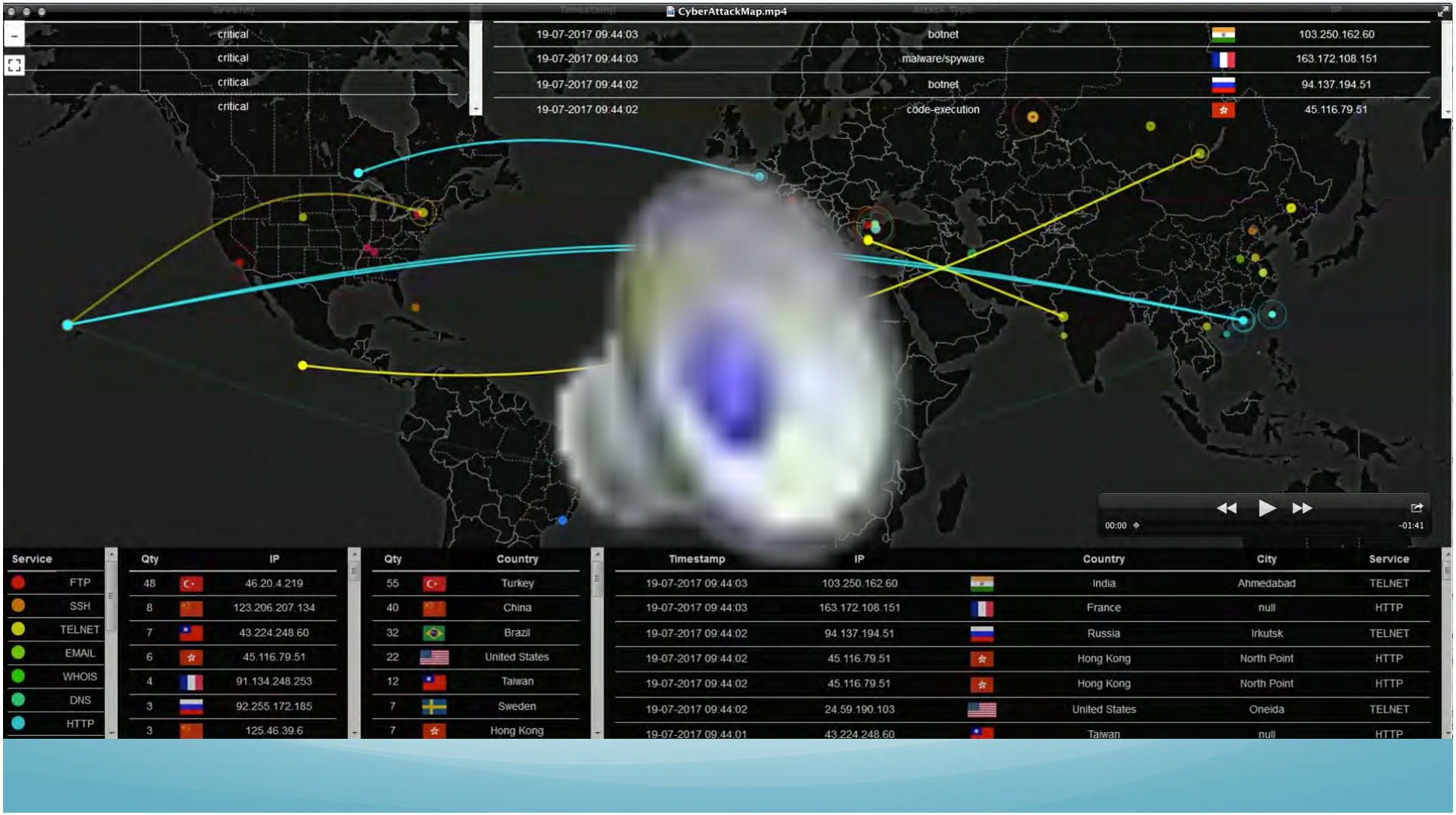
- FTP (21)
- SSH (22)
- Telnet (23)
- HTTP (80)
- HTTPS (443)
- POP3 (110)
- POP3S (995)
- IMAP (143)
- IMAPS (993)
- MSSQL (1433)
- RDP (3389)
- RAdmin (4899)
- VNC (5900)

Attacked Services: SSH, Telnet, RDP, RAdmin, VNC

UH HoneyPot Project



- Hours (HST) at the bottom
- Unique attackers (IP addresses) are on the secondary axis
- Brute force attacks began 4 minutes after the honeypot started


CyberAttackMap.mp4
critical
critical
critical
critical
19-07-2017 09:44:03 botnet 103.250.162.60
19-07-2017 09:44:03 malware/spyware 163.172.108.151
19-07-2017 09:44:02 botnet 94.137.194.51
19-07-2017 09:44:02 code-execution 45.116.79.51
00:00
-01:41
Service
FTP
SSH
TELNET
EMAIL
WHOIS
DNS
HTTP
Qty IP
48 46.20.4.219
8 123.206.207.134
7 43.224.248.60
6 45.116.79.51
4 91.134.248.253
3 92.255.172.185
3 125.46.39.6
Qty Country
55 Turkey
40 China
32 Brazil
22 United States
12 Taiwan
7 Sweden
7 Hong Kong
Timestamp IP Country City Service
19-07-2017 09:44:03 103.250.162.60 India Ahmedabad TELNET
19-07-2017 09:44:03 163.172.108.151 France null HTTP
19-07-2017 09:44:02 94.137.194.51 Russia Irkutsk TELNET
19-07-2017 09:44:02 45.116.79.51 Hong Kong North Point HTTP
19-07-2017 09:44:02 45.116.79.51 Hong Kong North Point HTTP
19-07-2017 09:44:02 24.59.190.103 United States Oneida TELNET
19-07-2017 09:44:01 43.224.248.60 Taiwan null HTTP

Information Security Program Update

Information Security Program Elements

- Data Governance and Oversight – Overarching Governance and Principles
  - Information Security Audits & Risk Assessments
    - Network & vulnerability scanning
    - Sensitive information and server registration
  - Information Security Policies & Procedures
    - Implementation of security standards as required
  - Identity Management & Access Controls
    - Stronger password requirements
    - Multifactor Authentication (DUO): http://www.hawaii.edu/its/uhlogin/
  - Information Security Training and Awareness

Personal Information Survey & Server Registration

- Stats from last year 2017
  - Personal Information Survey:
    - Total 770
  - Server Registration:
    - Total Servers Registered 927
  - Estimated number of REPORTED records with Protected Data
    - **25.2 million**

Personal Information Survey*

- Required by State Law (§487N-7); submitted annually to Information Privacy and Security Council
- Must report any repository of Personally Identifiable Information (PII)
  - Full Name (or First Initial and Last Name) in combination with either
  - Social Security Number
  - Drivers License or Hawaii ID Number
  - Account Number, Credit or Debit number, Access Code, or password that would permit access to an individuals financial account
- Includes Paper and Electronic repositories
- Must "Submit" Survey to Update. Surveys are considered complete when "last updated" date shows a date between 01/01/17 – 09/15/17
- http://www.hawaii.edu/its/information/survey

* Will be updated in 2018 to include "Sensitive" and/or "Regulated" information

Server Registration

- Required by UH E2.214
- Any server running on UH Network must be registered
- Yearly PII Scans (to identify types of data on server) using Spirion (formerly known as Identity Finder)
  - https://www.hawaii.edu/software/
- Yearly vulnerability scanning using OpenVAS
- Failure to comply could result in server being blocked on network
  - http://www.hawaii.edu/its/server/registration/

2017 PI Survey & Server Registration Deadline

- Update Period: officially concluded Sept. 15, 2017 (but you can still update your information for 2017)
- You can update your information at any time throughout the year
- START EARLY for 2018!

Best Ways to Secure Computers & Information

- Establish good “cyber hygiene” practices
- Know your assets; know where your sensitive data resides
- Scan your computer for sensitive information
- Securely delete any sensitive information that is no longer needed
- Encrypt the sensitive information that is required to be maintained for business operations purposes

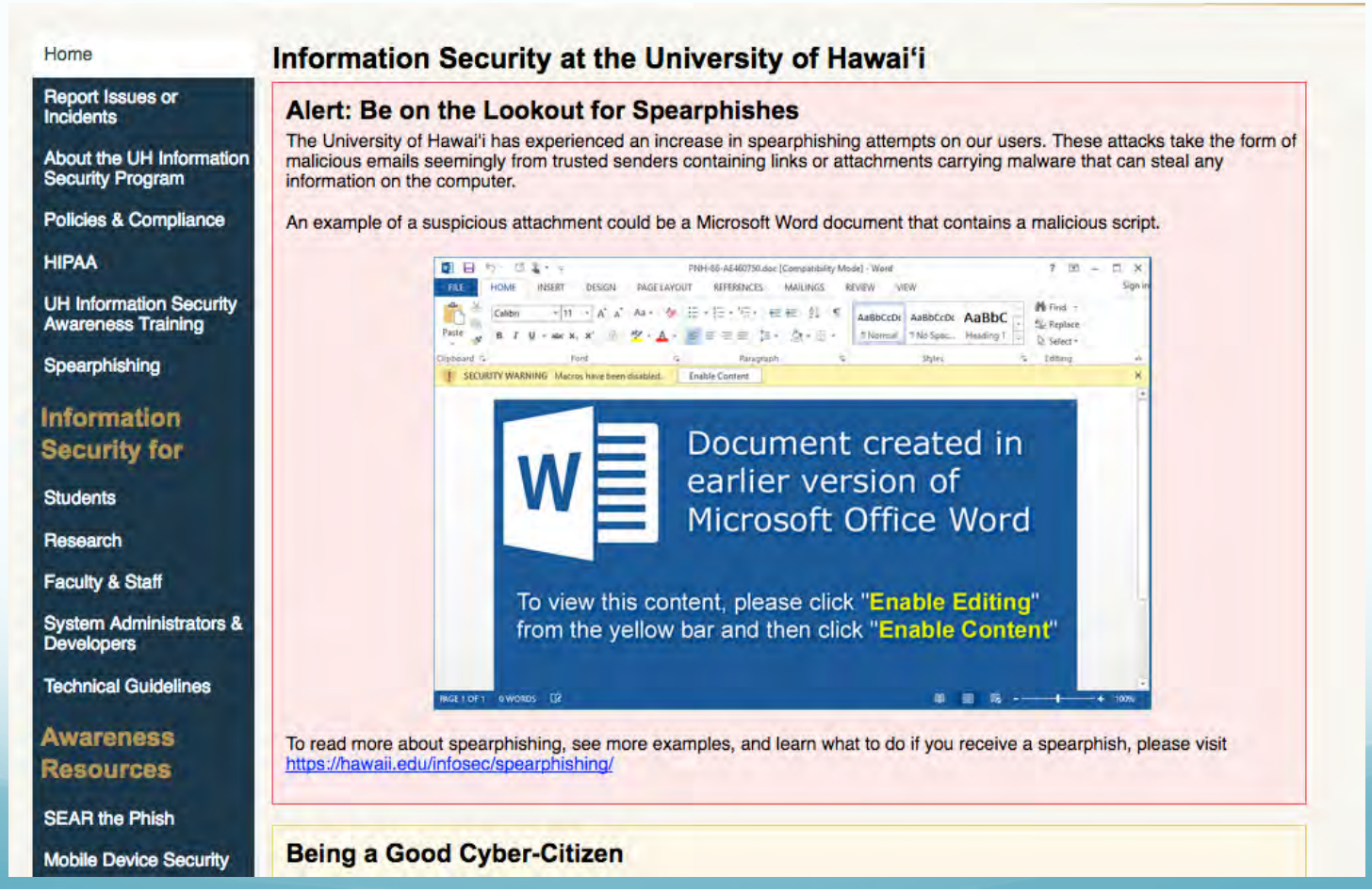
Top 10 Cyber Security Practices

1. Recognize that **YOU**, **YOUR DEVICES, and YOUR INFORMATION** are targets; know the threats
2. Practice good password management;
   a. Use multi-factor authentication (Duo at UH)
   b. Use STRONG passwords
3. Apply operating system and application updates frequently and regularly
4. Install and update protective software such as anti-virus software
5. Back up your data regularly and protect sensitive/regulated information by **encrypting** the sensitive/regulated data

Top 10 Cyber Security Practices (2)

6. Use a secure network for sensitive transactions (not the coffee shop wi-fi or hotel computer)
7. Never leave your devices logged-in & unattended; control access to your machines
8. Use email & the Internet safely; be careful when clicking on attachments or links in email
9. Monitor your accounts for suspicious activity
10. Be careful what you share online & on social media (know your digital footprint)

www.hawaii.edu/infosec/



HIPAA at the University of Hawaii

J. T. Ash
University of Hawaii System
HIPAA Compliance Officer
jtash@hawaii.edu
hipaa@hawaii.edu

Agenda

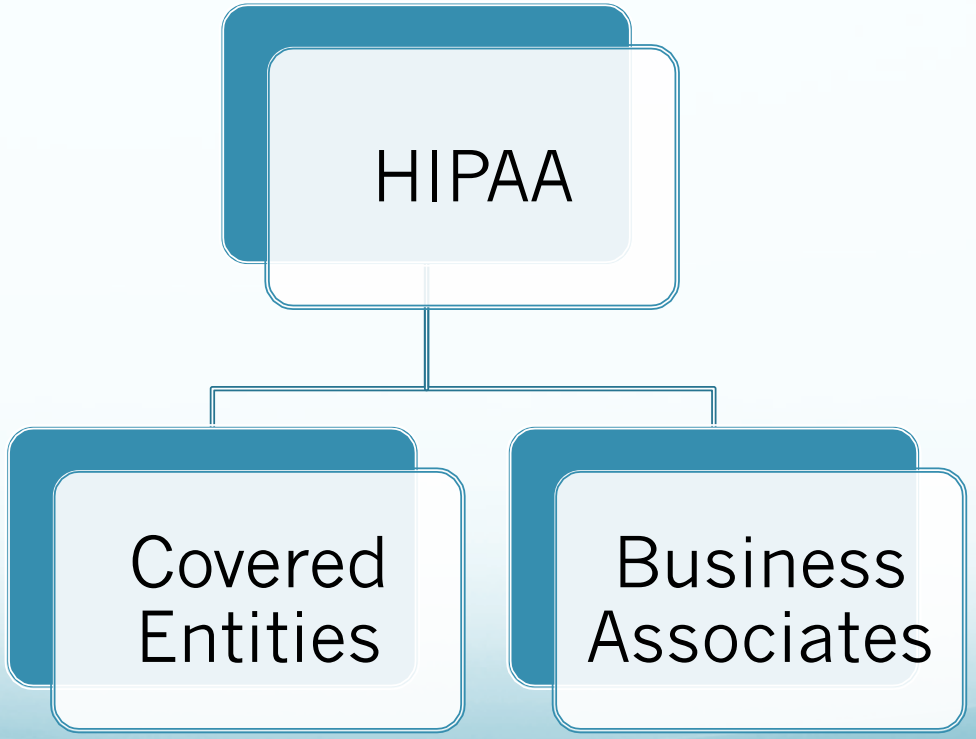
- HIPAA is a "**TEAM SPORT**" and everyone has a role in protecting protected health information (PHI).
- What has changed and how does it affect me?
- Application of HIPAA (UH & UH Covered Components)
- Individually Identifiable Health Information (IIHI) & Protected Health Information (PHI)
- Privacy Rule, Security Rule, & Breach Notification Rule
- Research Process
- Methods to Share PHI for Research (Privacy Rule)
- Breaches

What has changed and how does it affect me?

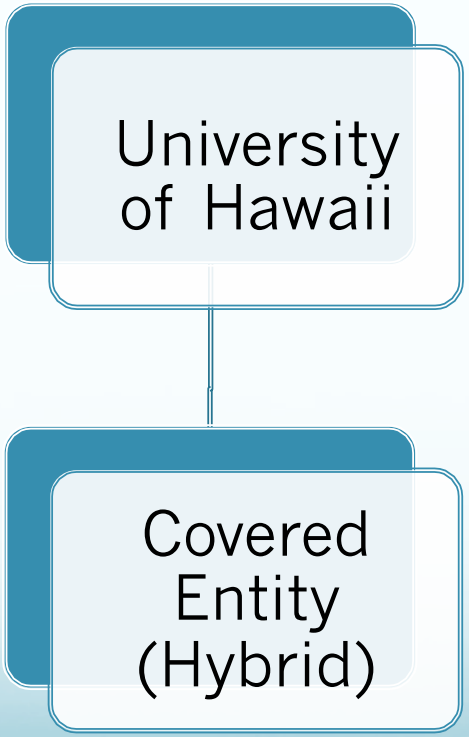
- New UH HIPAA Policy (EP 2.217) – May 2017
- Designated University of Hawaii a “Covered Entity – Hybrid”
- All designated “Covered Components” under UH must comply with HIPAA & UH HIPAA Policy
- Hired a HIPAA Compliance Officer

*** University Units that collect, use, transmit, and/or store IIHI but are not designated as UH Covered Components are still required to protect IIHI in accordance with applicable HIPAA privacy and security policies.

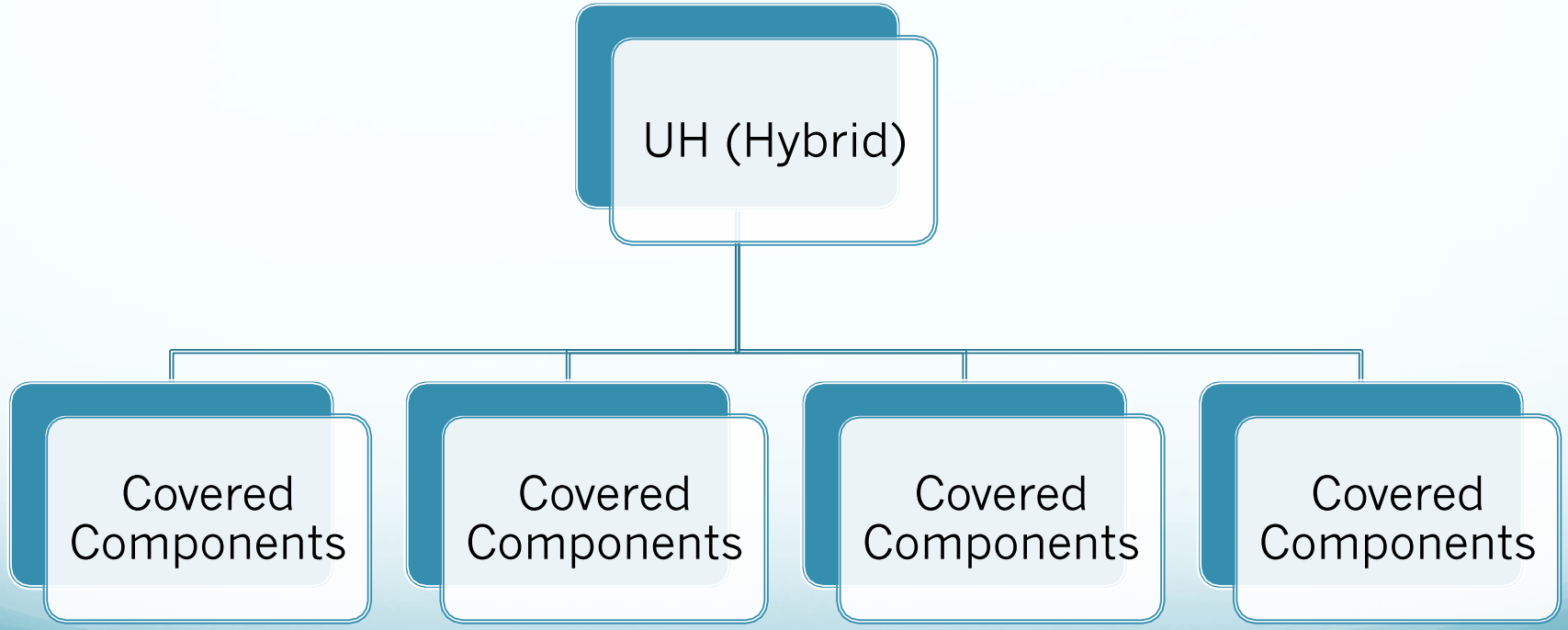
Application of HIPAA



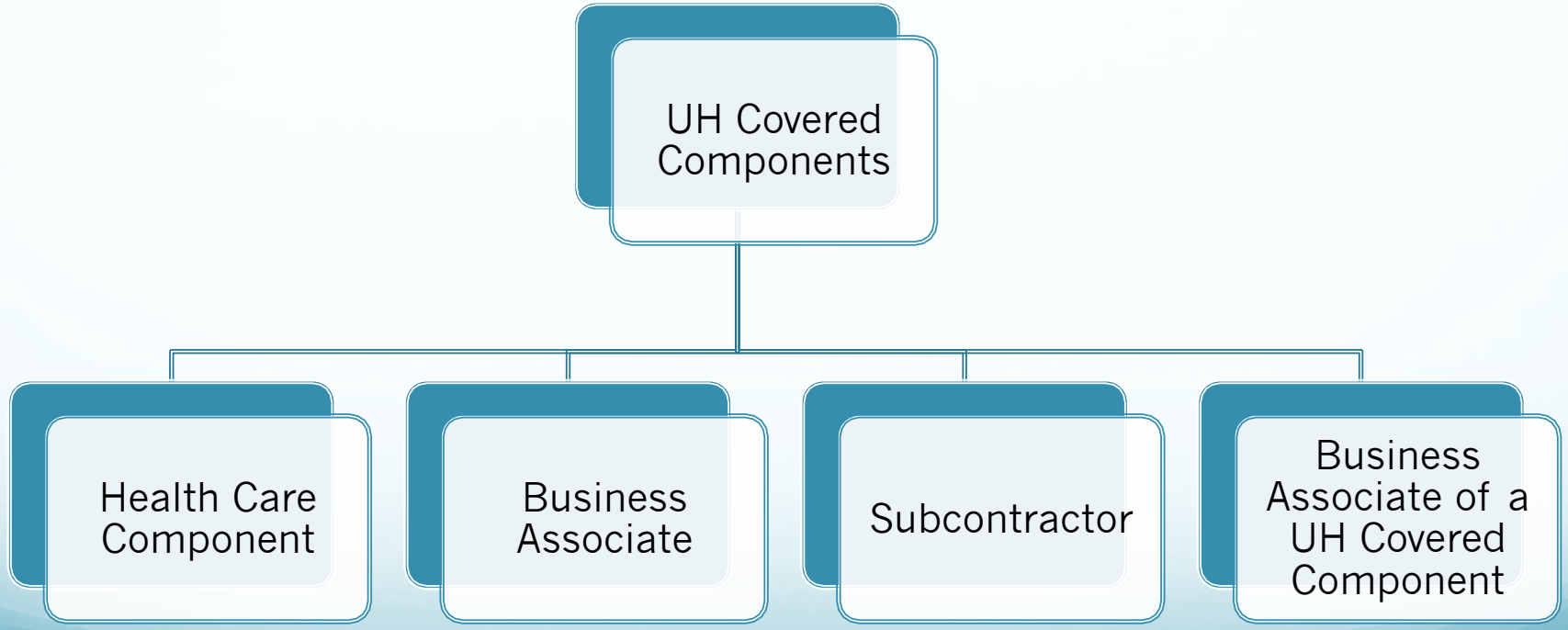
“Who” is UH?



Covered Components



“Who” is a UH Covered Component?



Essential Definitions

- Individually Identifiable Health Information (IIHI):
  - Includes demographic information that reasonably identifies an individual
  - Created or received by a health care provider/clearinghouse/plan
  - Relates to physical or mental health of an individual past, present, or future
  - Involves past, present, or future payment for the provision of health care to an individual

- Protected Health Information (PHI)
  - All of the above (that is transmitted or maintained electronically or in any other forum or medium) but EXCLUDES:
    - IIHI in education records covered by FERPA
    - IIHI in employment records in the unit's role as an EMPLOYEE

*** University Units that collect, use, transmit, and/or store IIHI but are not designated as UH Covered Components are still required to: (1) protect IIHI in accordance with applicable HIPAA privacy and security policies (EP 2.217 UH HIPAA Policy)

18 Personal Identifiers

1. Name
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers

18 Personal Identifiers

9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers/serial numbers
13. Device identifiers/serial numbers
14. Web URLs
15. IP address numbers
16. Biometric identifiers
17. Full-face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code; and the covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

HIPAA Privacy Rule

- The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.
- https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
- 45 CFR Part 160 and Subparts A and E of Part 164.

HIPAA Security Rule

- The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
- https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
- 45 CFR Part 160 and Subparts A and C of Part 164.
- Safeguards:
  - Administrative
  - Physical
  - Technical

Breach Notification Rule

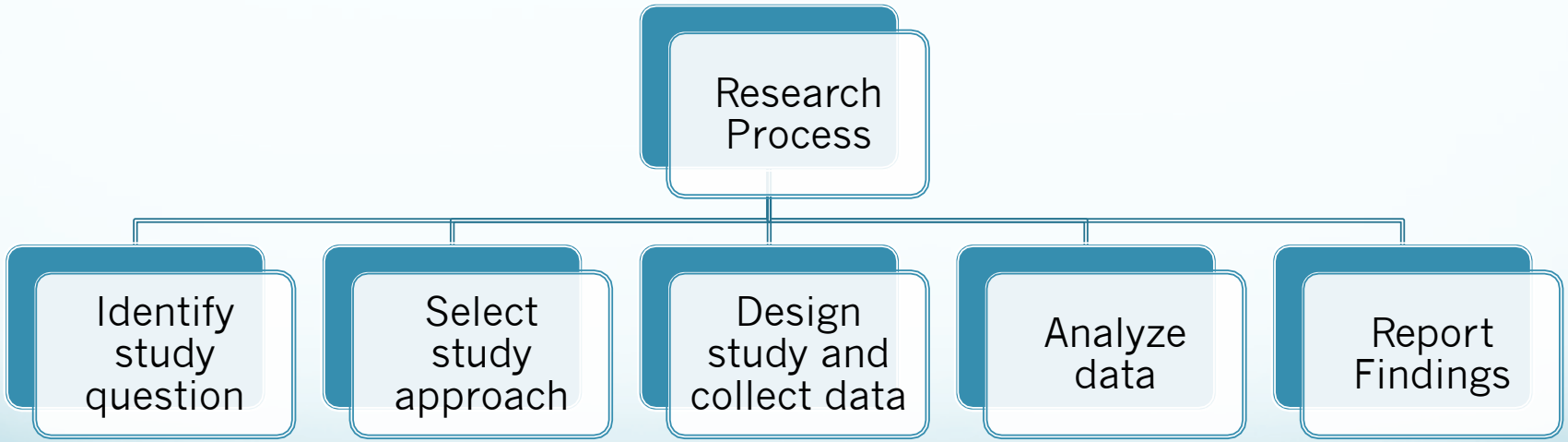
- **Notification to Individuals**: Individuals whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach must be notified without unreasonable delay and in no case later than 60 calendar days following the discovery of such breach.

- **Notification to Others**: A UH Covered Component shall also notify prominent local media outlets if the breach involves more than 500 residents of the State no later than 60 days after discovery of the breach.

- **Notification to DHHS Secretary**: A UH Covered Component shall notify the DHHS Secretary on an annual basis, in a manner specified on the DHHS Web site, and via a report due to the DHHS Secretary no later than 60 calendar days after the end of the calendar year in which breaches are discovered *if less than 500 individuals are involved*. *If more than 500 individuals are involved*, the UH Covered Component shall notify the DHHS Secretary in the manner provided by the DHHS Web site, which presently requires notice without unreasonable delay and in no case later than 60 days following a breach.

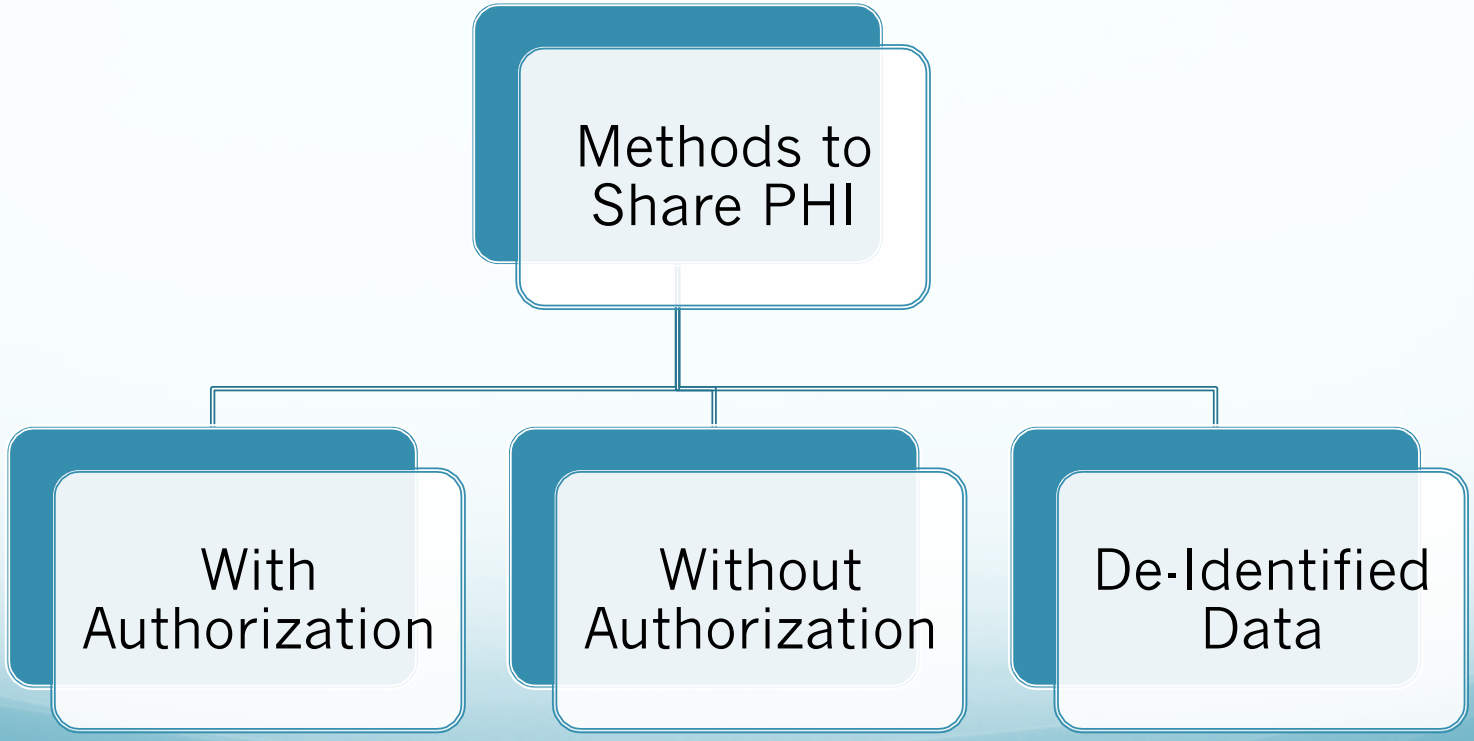
- **Notification by a Business Associate**. A Business Associate shall notify a UH Covered Component of a breach within 5 business days that the Business Associate discovered a breach occurred…

The Research Process



Methods to Share PHI for Research

(***Satisfies Privacy Rule Obligations)



With Individual Authorization

- The Privacy Rule has a general set of authorization requirements that apply to all uses and disclosures, including those for research purposes. However, several special provisions apply to research authorizations:
  - Unlike other authorizations, an authorization for a research purpose may state that the authorization does not expire, that there is no expiration date or event, or that the authorization continues until the “end of the research study;” and
  - An authorization for the use or disclosure of protected health information for research may be combined with a consent to participate in the research, or with any other legal permission related to the research study.

Without Authorization

- A Covered Entity must obtain one of the following:
  - Documented Institutional Review Board (IRB) Board Approval
  - Preparatory to Research
  - Research on Protected Health Information of Decedents
  - Limited Data Sets with a Data Use Agreement

What is De-identified Data?

- De-identified data is not considered PHI
- No obligations to the Privacy/Security/Breach Notification Rules
- May use and disclose de-identified data without restriction

Security Rule & Breach Notification

- Still need to work with your IT support to ensure they have an environment that can satisfy the obligations of the Security Rule
- Still need to work with your InfoSec support to ensure they have the policies/procedures in place to satisfy the obligations of the Breach Notification Rule

Breaches

- Idaho State University (2013)
  - $400,000 resolution payment
  - Corrective Action Plan
  - Annual submission of compliance for 2 years

Breaches

- Columbia University (2014)
  - $1,500,000 resolution payment
  - Corrective Action Plan
  - Annual submission of compliance for 3 years

Breaches

- University of Mississippi (2016)
  - $2,750,000 resolution payment
  - Corrective Action Plan
  - Annual submission of compliance for 3 years

Breaches

- Oregon Health and Science University (2016)
  - $2,700,000 resolution payment
  - Corrective Action Plan
  - Annual submission of compliance for 3 years

Breaches

- University of Massachusetts Amherst (2016)
  - $650,000 resolution payment
  - Corrective Action Plan Implementation
  - Annual submission of compliance for 2 years

Please Help Us!

Link to a quick survey:

https://goo.gl/forms/AqezMAXQz5Ao8Z8z1

Questions?

JT Ash
HIPAA Compliance Officer
Office of the Vice President for Information Technology
jtash@hawaii.edu
http://www.hawaii.edu/infosec/hipaa

Sandra Furuto
Data Governance Director
Office of the Vice President for Academic Policy and Planning
yano@hawaii.edu
http://www.hawaii.edu/uhdatagov

Jodi Ito
Chief Information Security Officer
Office of the Vice President for Information Technology
jodi@hawaii.edu
http://www.hawaii.edu/infosec