IT All-Campus Workshop 2017

# ACW Breakout Session: HIPAA + Security

Jodi Ito
Chief Information Security Officer
jodi@hawaii.edu

IT All-Campus Workshop 2017

# Thank You!!

***YOU*** *are the keys to protecting & securing UH information!*

IT All-Campus Workshop 2017

# LANDSCAPE & CURRENT THREATS

IT All-Campus Workshop 2017

# “Shift Happens” - 2016

- Jose Esteves, IU
- https://www.youtube.com/watch?v=uqZiIO0YI7Y

# 821,000 user records exposed due to misconfigured MongoDB for smart stuffed toys

The MongoDB for CloudPets was not protected with a password; it's unknown how many hackers gobbled the data, but the database was deleted and replaced with ransom demands at least three times.

Network World | FEB 28, 2017 7:22 AM PT


*Credit: CloudPets*

**RELATED**


Hacker wiping unprotected MongoDB installs and holding data for ransom


Witcher dev, XBOX 360 ISO & PSP ISO forums hacked: Over 4.4 million accounts...


Cool Yule Tools 2016: Digital disruption at Santa's Workshop


VIDEO
Bruce Schneier and the call for "public service technologists"

http://www.networkworld.com/article/3175508/security/821-000-user-records-exposed-due-to-misconfigured-mongodb-for-smart-stuffed-toys.html

IT All-Campus Workshop 2017

# University Hackers Attacked 5,000 IoT Devices on Campus

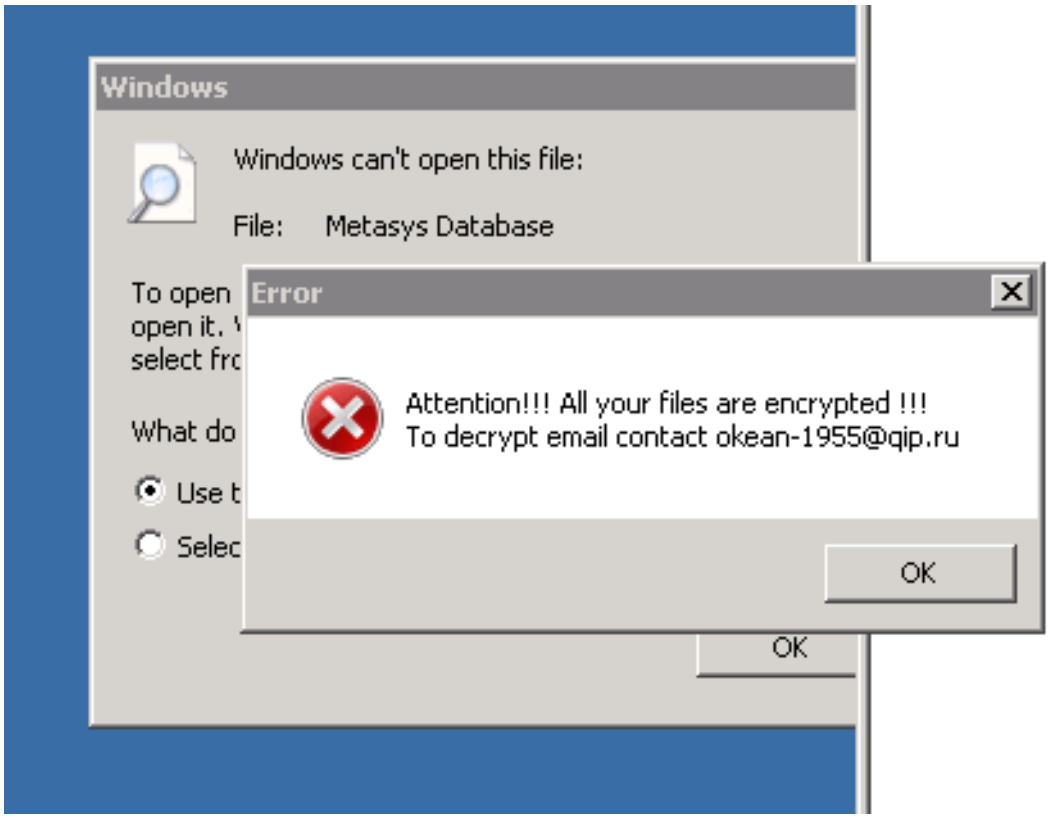
https://campustechnology.com/articles/2017/02/13/university-hackers-attacked-5000-iot-devices-on-campus.aspx

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?

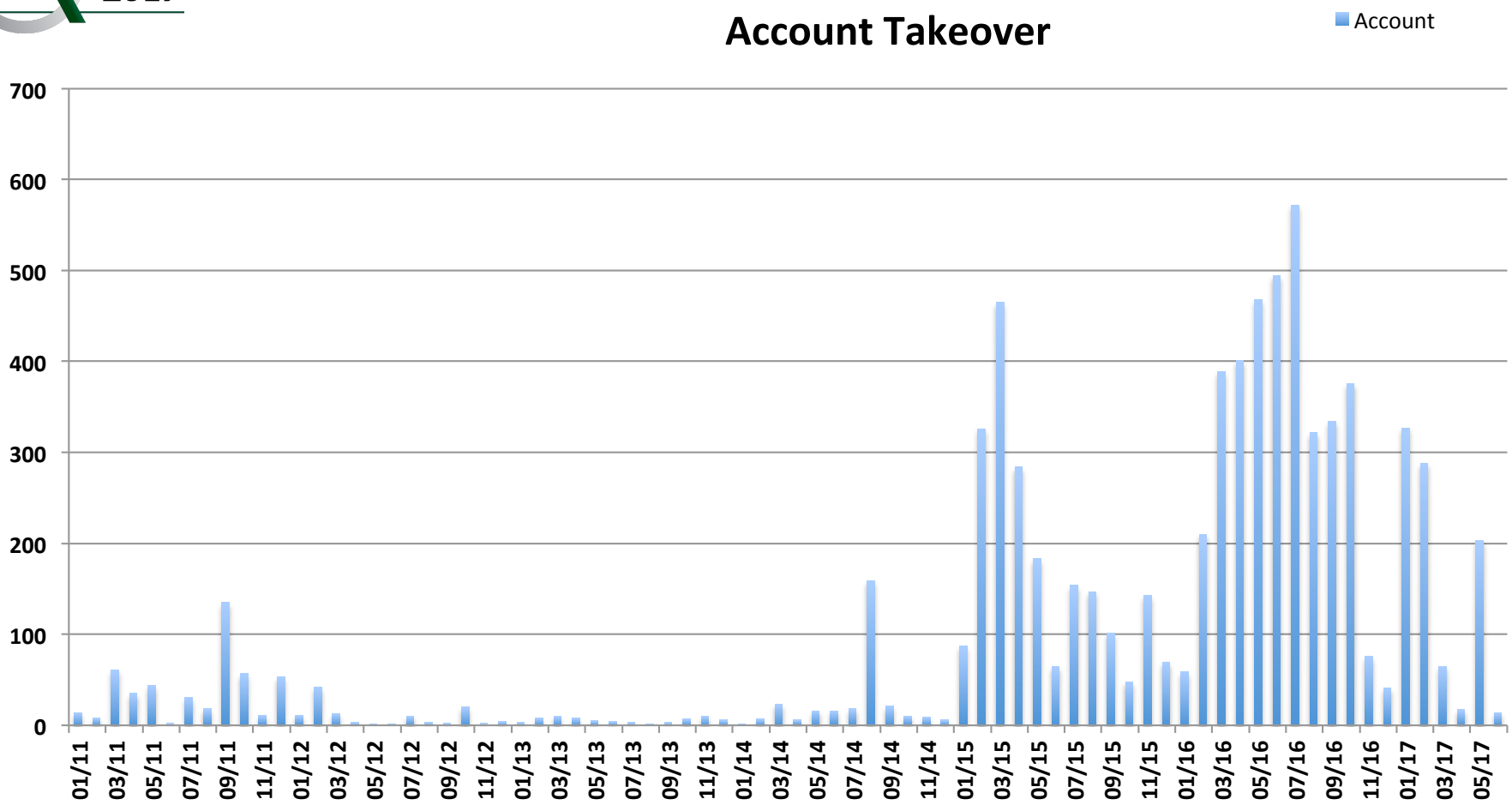


IT All-Campus Workshop 2017

# Who's Responsible?

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

IT All-Campus Workshop 2017



IT All-Campus Workshop 2017

# 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.

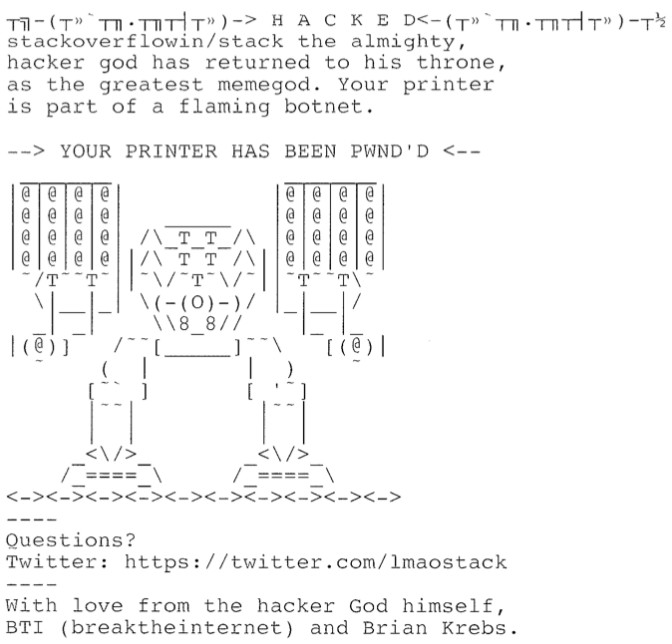
---

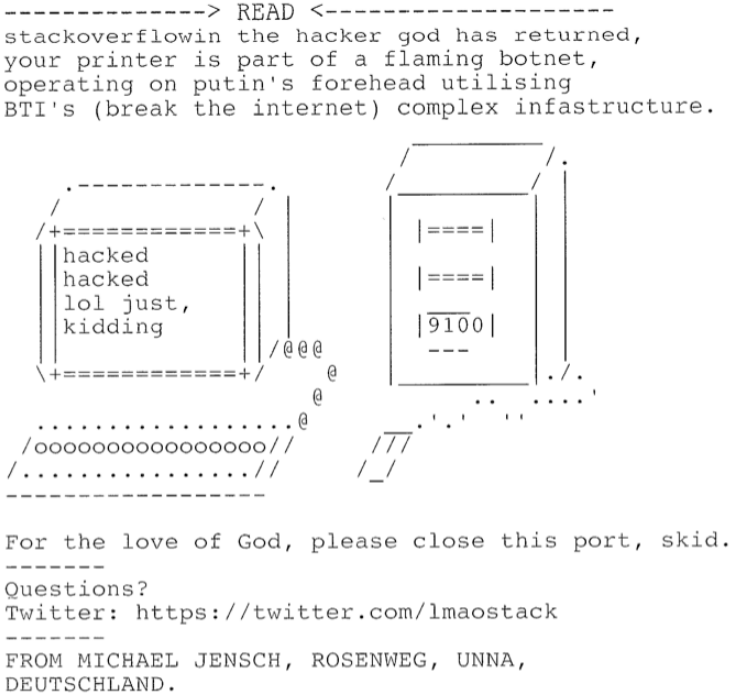
Susan Lin | Director of Financial Management and Controller | **University of Hawaii System Financial Management Office**
1406 Lower Campus Road, Room 41 | Honolulu, HI 96822

IT All-Campus Workshop 2017

# Compromised Printers

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



IT All-Campus Workshop 2017

# 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.

IT All-Campus Workshop 2017

# Other Compromises

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

IT All-Campus Workshop 2017

# Analysis of a Compromise

- Multiple systems involved
- Able to acquire images of machines which provided more insight into the event
- Able to see that attackers tried to move laterally within the network

IT All-Campus Workshop 2017

# Highlights

- May 17: Computer compromised with ransomware
- Found exploit code related to EternalBlue & DoublePulsar (NSA toolkit leaked 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)

IT All-Campus Workshop 2017

# HoneyPot Project

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

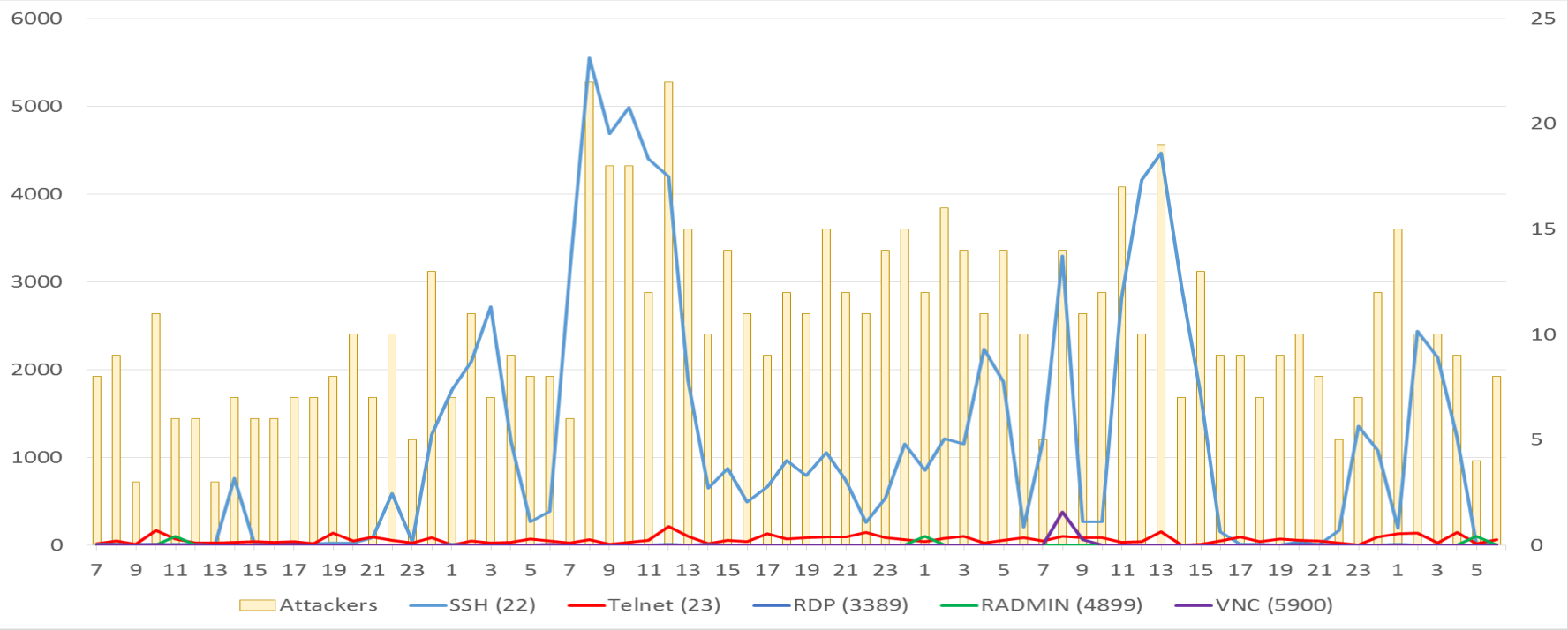
**Monitored Services:**

- 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)

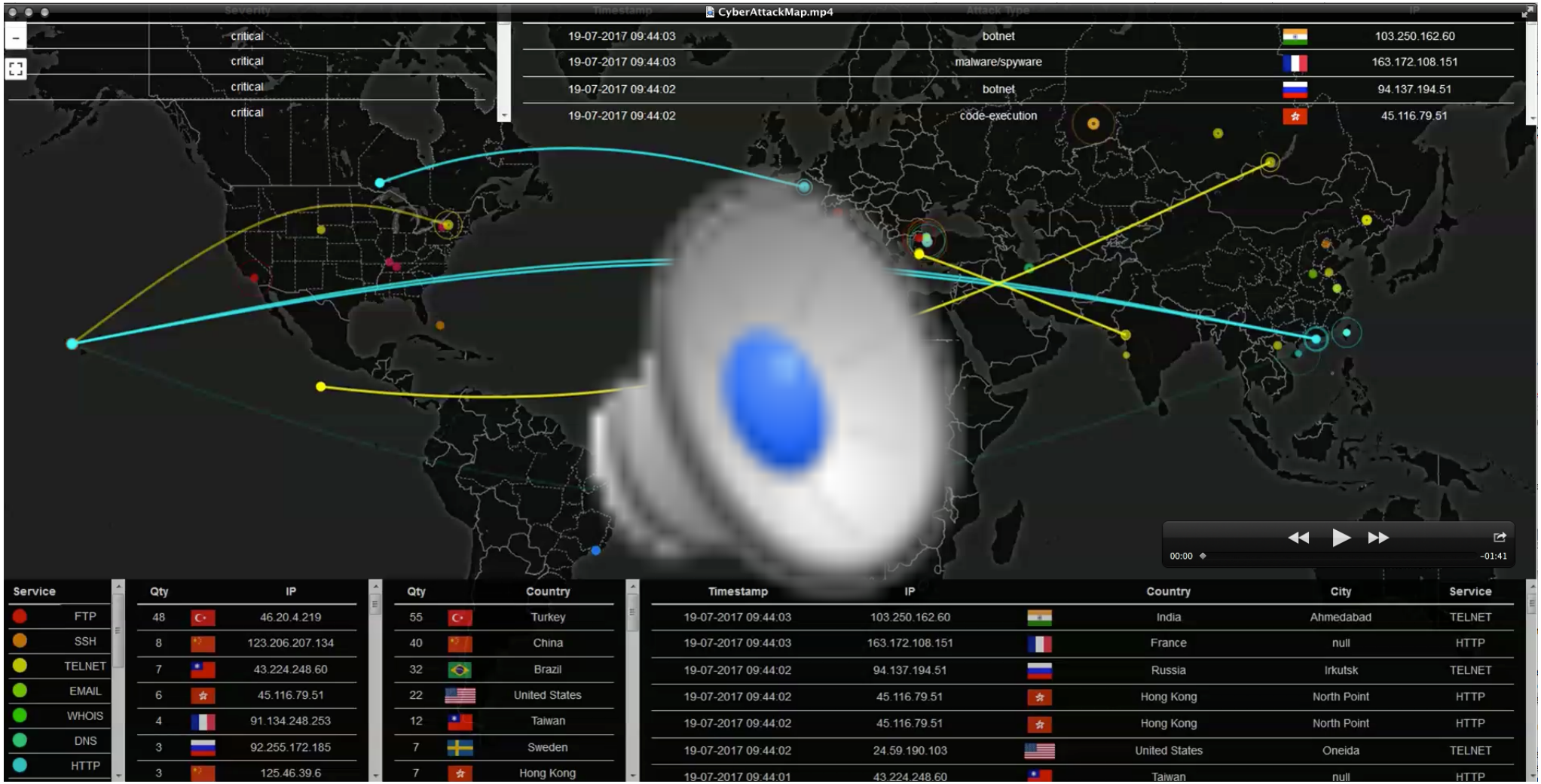
**Attacked Services:** SSH, Telnet, RDP, RAdmin, VNC

IT All-Campus Workshop 2017

# 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




| 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 |

IT All-Campus Workshop 2017

# USB Malware

- Plug-in USB drive and/or open the drive
- Automatically infected
- DEMO

IT All-Campus Workshop 2017

# POLICY UPDATES

IT All-Campus Workshop 2017

# UH HIPAA Policy: New!

- Health Insurance Portability & Accountability Act
- EP 2.217
- UH is a Hybrid Entity
- Covered Components are listed on HIPAA website
- www.hawaii.edu/infosec/hipaa

IT All-Campus Workshop 2017

# Highlights

- Covered Components fall under HIPAA
- Each Covered Component must designate a Unit HIPAA Coordinator
- Unit's workforce must complete HIPAA training
- Unit must complete a Risk Assessment
- Unit must provide and post a Notice of Privacy Practices (NOPP)

IT All-Campus Workshop 2017

# What is a Covered Component?

- http://www.hawaii.edu/infosec/docs/HIPAA-UH-Basics-r2.pptx.pdf

https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html

IT All-Campus Workshop 2017

# Essential Definitions

- Individually Identifiable Health Information (IIHI)
  - Includes demographic info 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
  - **UH Data Classification Categories define IIHI as "regulated"**
- Protected Health Information (PHI)
  - All of the above but EXCLUDES
    - IIHI in education records covered by FERPA
    - IIHI in employment records in the unit's role as an EMPLOYER

IT All-Campus Workshop 2017

# Civil Money Penalties (CMP)

| HIPAA Violation | Minimum Penalty | Maximum Penalty |
|---|---|---|
| Unknowing | $100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation) | $50,000 per violation, with an annual maximum of $1.5 million |
| Reasonable Cause | $1,000 per violation, with an annual maximum of $100,000 for repeat violations | $50,000 per violation, with an annual maximum of $1.5 million |
| Willful neglect but violation is corrected within the required time period | $10,000 per violation, with an annual maximum of $250,000 for repeat violations | $50,000 per violation, with an annual maximum of $1.5 million |
| Willful neglect and is not corrected within required time period | $50,000 per violation, with an annual maximum of $1.5 million | $50,000 per violation, with an annual maximum of $1.5 million |

IT All-Campus Workshop 2017

# Introducing our new UH HIPAA Compliance Officer:

# ***J.T. Ash***

IT All-Campus Workshop 2017

# UH Policy Revisions

- EP 2.214:  Institutional Data Classification Categories & Security Guidelines
- EP 2.215:  Institutional Data Governance
- New AP:  Mandatory Training & Continuing Education Requirements for Data Users
- Undergoing union consultation

IT All-Campus Workshop 2017

# Manoa SEC comments

- Will there actually be pro-active tech support on call? It isn't clear we will have the logistic support at the individual computer level to follow all this or to know if we are in compliance.  One of the requirements was that we must use secure networks when accessing these data. That is their responsibility to utilize HTTPS with valid certificates, etc. A faculty member cannot be expected to secure the Hilton wifi in their room when on travel. A university is an open, ad-hoc system. They should secure the information on their side and limit access accordingly. We should be expected to follow common sense. Many of us, work, from time to time, at remote sites or travel for work.  Will we be limited access to data while we are off campus?  Or do we have to provides means to further encrypt data while we're at remote sites? Will we have to add devices in advance so that we can use them in the field?  These things should be worked out in advance not after the fact.

IT All-Campus Workshop 2017

# Additional Comments

- UH has no responsibility for safe, new hardware? Ransomware like WannaCry went after older machines and un-updated software. How many of these legacy machines are lurking in faculty offices because faculty can't afford new machines? We know that backdoor attacks on whole systems come through such machines.

IT All-Campus Workshop 2017

www.hawaii.edu/infosec/techguidelines/



# E2.214: Institutional Data Classification Categories and Technical Guidelines

## Overview

UH Executive Policy E2.214: Institutional Data Classification Categories and Technical Guidelines provides specific provisions for handling of sensitive information. This document provides technical guidance for compliance with E2.214.

## General Information Security Practices

- Access to Sensitive Information
- Transmission of Sensitive Information
- Use and Storage of Sensitive Information
- Disposal of Media Containing Sensitive Data
- Multi-Function Printers, Copiers, Scanners and Fax Machines
- Data Classification Examples (Attachment 1)

## Technical Guidelines Table

Click Here to view the table in PDF form.

Key

| | |
|---|---|
| n/a | Does not apply |
| Optional | Not officially recommended but may be implemented |
| Recommended | Implementation should be done though not required |
| Required | Implementation must be done |

* Hover over the table cell or text to display additional information.

Click on entries in the first column to receive more resources/information.

| Classification: | Public | Restricted | Sensitive | Regulated |
|---|---|---|---|---|

IT All-Campus Workshop 2017

# Federal Requirements

- Export Control
- NISPOM (DoD)
- Controlled Unclassified Information (CUI) NIST 800-171
- Federal Information Security Management Act (FISMA) NIST 800-53

IT All-Campus Workshop 2017

# INFORMATION SECURITY PROGRAM UPDATE

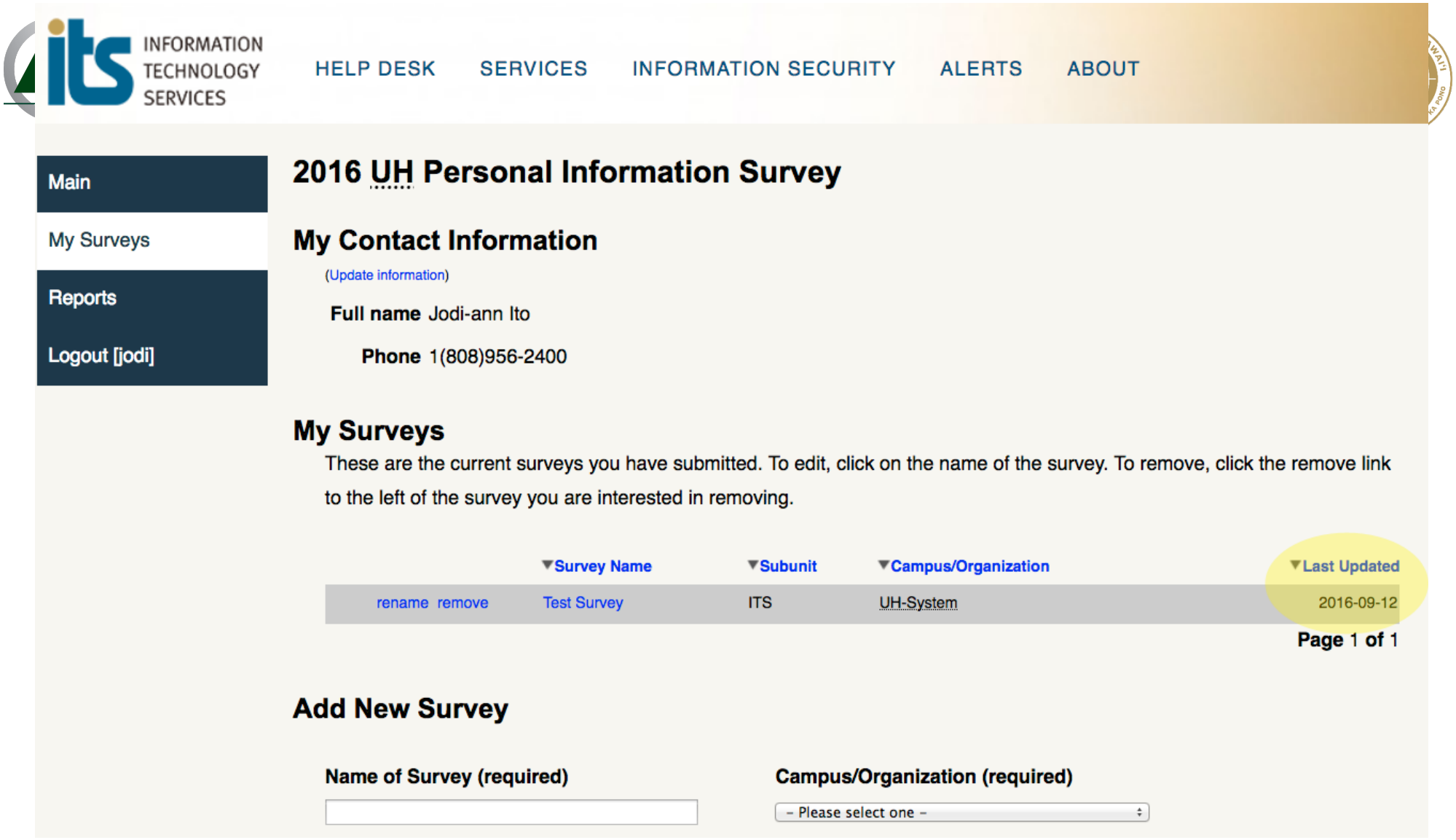
# Personal Information Survey & Server Registration

- Stats from last year
  - Personal Information Survey:
    - Total 773; Updated in 2016:  503
  - Server Registration:
    - Total Active Servers 905; Scanned/Remediated in 2016: 656

# 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 respositories
- 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

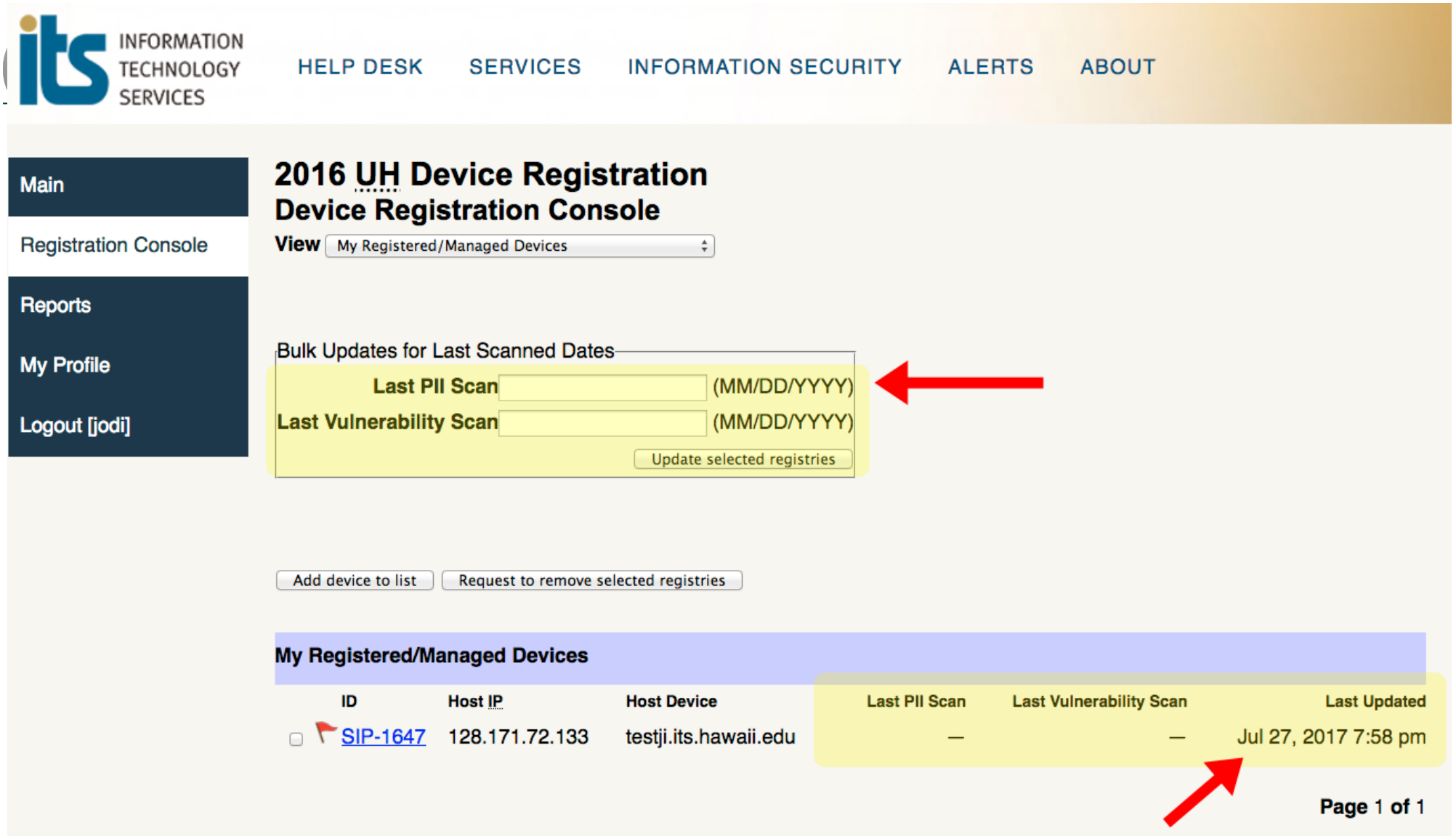

INFORMATION TECHNOLOGY SERVICES
HELP DESK
SERVICES
INFORMATION SECURITY
ALERTS
ABOUT
Main
My Surveys
Reports
Logout [jodi]
2016 UH Personal Information Survey
My Contact Information
(Update information)
Full name Jodi-ann Ito
Phone 1(808)956-2400
My Surveys
These are the current surveys you have submitted. To edit, click on the name of the survey. To remove, click the remove link to the left of the survey you are interested in removing.
Survey Name
Subunit
Campus/Organization
Last Updated
rename remove
Test Survey
ITS
UH-System
2016-09-12
Page 1 of 1
Add New Survey
Name of Survey (required)
Campus/Organization (required)
- Please select one -

IT All-Campus Workshop 2017

# Server Registraion

- Required by UH E2.214
- Any server running on UH Network must be registered
- Yearly PII Scans (to identify type of data on server) using IdentityFinder/Spirion
- Yearly vulnerability scanning using OpenVAS
- Failure to comply could result in server being blocked on network

http://www.hawaii.edu/its/server/registration/


INFORMATION TECHNOLOGY SERVICES
HELP DESK
SERVICES
INFORMATION SECURITY
ALERTS
ABOUT
Main
Registration Console
Reports
My Profile
Logout [jodi]
2016 UH Device Registration
Device Registration Console
View
My Registered/Managed Devices
Bulk Updates for Last Scanned Dates
Last PII Scan
(MM/DD/YYYY)
Last Vulnerability Scan
(MM/DD/YYYY)
Update selected registries
Add device to list
Request to remove selected registries
My Registered/Managed Devices
ID
Host IP
Host Device
Last PII Scan
Last Vulnerability Scan
Last Updated
SIP-1647
128.171.72.133
testji.its.hawaii.edu
—
—
Jul 27, 2017 7:58 pm
Page 1 of 1

# 2017 PI Survey & Server Registration Deadline

- Update Period: **NOW** until Sept. 15, 2017
- Reminder emails will be sent out by Aug. 7
- START NOW!

IT All-Campus Workshop 2017

# Training Opportunities

- Hawaii Cyber Challenge (1/2 day CTF)
  - Thursday, Aug. 3 @ Honolulu CC PCATT
  - Register: http://go.hawaii.edu/jHx
- UH Challenge-Based Training Framework for Incident Response training:
  - http://go.hawaii.edu/ktj

IT All-Campus Workshop 2017

# Description

- A hands-on workshop that is designed for IT professionals who want to develop relevant cybersecurity skills necessary to respond to a variety of security incidents
- Security incidents are based on real-world PC infections using actual methods and malware used by cybercriminals today
- Each section consists of a set of challenges designed to help you learn the tools and techniques required to perform incident response in a live system challenge.

IT All-Campus Workshop 2017

# Description – cont.

- Participants will need to find a flag in order to successfully complete each challenge; flags can be found when performing incident handling tasks in the live system.
- This workshop incorporates training gamification which provides instant, positive feedback and promotes engagement, memory retention, and personal satisfaction.
- Everything is done within a safe, and sandboxed environment and contains everything you need to complete the challenges

IT All-Campus Workshop 2017

- UH Challenge-Based Training Framework for Incident Response training:
  - http://go.hawaii.edu/ktj
- Hawaii Annual Code Challenge:
  - http://hacc.hawaii.gov/

IT All-Campus Workshop 2017

# CyberHawai‘i

- 501(c)3
- Membership organization
- Affiliated with CyberUSA
- Purpose:  coordinate and support cyber activities related to readiness and resilience, education and workforce development, economic development and innovation throughout the state
- Information Sharing and Analysis Organization (ISAO) of Hawaii
- More information will be forthcoming in October

IT All-Campus Workshop 2017

# Questions?