Financial Management Office

Fiscal Administrator's Meeting

Wednesday, March 21, 2018
Topics

• Welcome
  - Susan Lin, Director of Financial Management and Controller

• Bank of Hawai’i Merchant Services
  - Richard Pernice, Relationship Officer

• Data Governance & Information Security
  - Jodi Ito, Security Officer

• eTravel Compliance Enhancements
  - James Kashiwamura, Director of Disbursing and Payroll

• Personal Tax 101
  - Ken Lum, Manager of Tax Services
About Us

Bank of Hawaii Merchant Services enables merchants to accept any form of non-cash payment from their customers/vendors

- Credit cards (Visa, MasterCard, Discover, JCB)
- EMV/Chip Card, debit or “check” cards
- Purchasing cards
Bank of Hawaii’s processing platform for over 22 years
Payment Solutions

- Stand-Alone Terminals (Dial and IP)
- Wireless Terminals
- Virtual Terminal (Web-based)
- Integration with Point-of Sale (POS) software
- E-Commerce processing
Transaction Process Flow

Authorizations
Transaction Process Flow

Settlement
Best Practices
When Charging a Customer’s Card:

• **ALWAYS** insert the EMV chip cards
  – Do not remove the card until prompted
• Confirm customer’s ID
• **ALWAYS** have the customer sign the sales draft (receipt).
  – Keep sales drafts for your records
    • Visa = 12months, MC = 18months, Discover = 3 years
Best Practices

To Avoid Chargebacks

- Utilize the EMV chip reader and have customer sign sales draft to validate the card was present.
- Obtain an authorization code for the full amount of the transaction.
  - If you receive a decline, ask for another form of payment.
- Clearly disclose your store return and exchange policy at all points of sale.
Best Practices

Equipment and Statement Validation

• Periodically examine equipment to insure it is intact and un-tampered with.
  – Check EMV slot and card-swipe for any devices that could record card information.

• Validate your merchant statement every month to make sure amounts and activity match your records.
Chargeback Items

Procedures

• Bank of Hawaii Merchant Services will receive notice via reporting and notify UH Treasury Dept.

• UH Treasury Dept. will notify location.

• Location will also receive notification from card issuer.

• Beginning April, 10 days to respond.
Invoicing Procedures

Remit Billing Account

- BOH unable to directly debit or credit UH bank account.
- For debits or credits due, invoices or memos will be generated.
- For Chargebacks, the monies are automatically debited, BOH credits the account back and issues a credit memo for the amount.
Debit Suspense Items

Procedures

• Debit Suspense occurs when auth files are received but not the settlement files.
• Items held in reserve for 5 business days as a result.
• Bank of Hawaii to notify UH Treasury Dept. of items in suspense.
Offline Procedures
What to do if processing goes down

• In the event of a power outage or loss of processing abilities, contact Richard or the Merchant services general line.
  – Contact info provided on next slide

• If after hours, contact 24 hour help desk
  – Contact info provided on next slide

• Default to manual imprinter- Record customer phone numbers.
Contacts – BOH Sales and Service

Sales Officer
Kimie Lau 694-6616

Service Team: Michael Shimote: Service & Operations Manager 694-7308

- Services Team 694-7300
- Richard Pernice, Merchant Services Relationship Officer.
  - Tel: 694-7317, email: Richard.Pernice@boh.com, Cell: 861-6653
- Edie Tanicala, Merchant Services Relationship Officer.
  - Tel: 694-7316, email: Edie.Tanicala@boh.com

- Denise Corpuz, POS Service and Tech Rep
  - Tel: 694-7315, email: Denise.Corpuz@boh.com
Other Contacts – 24 Hours

- Customer Service 800-279-4195
- Authorization (automated) 800-532-9002
- POS Terminal 24hr Help Desk 800-279-4215
Mahalo!
Data Governance & Information Security @ UH

Spring 2018
FA Town Hall Meeting

www.hawaii.edu/uhdatagov
www.hawaii.edu/infosec

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.
Giant Equifax data breach: 143 million people could be affected

by Sara Ashley O'Brien  @saraashleyo

September 8, 2017: 9:23 AM ET

Equifax says a giant cybersecurity breach compromised the personal information of as many as 143 million Americans — almost half the country.
<table>
<thead>
<tr>
<th>Year</th>
<th>Breach</th>
<th>Accounts Compromised</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>Equifax</td>
<td>143 m</td>
</tr>
<tr>
<td>2016</td>
<td>Adult Friend Finder</td>
<td>412.2 m</td>
</tr>
<tr>
<td>2015</td>
<td>Anthem</td>
<td>78.8 m</td>
</tr>
<tr>
<td>2014</td>
<td>eBay</td>
<td>145 m</td>
</tr>
<tr>
<td>2013</td>
<td>Yahoo</td>
<td>3B</td>
</tr>
<tr>
<td></td>
<td>Target Stores</td>
<td>110 m</td>
</tr>
<tr>
<td></td>
<td>Adobe</td>
<td>38 m</td>
</tr>
<tr>
<td>2012</td>
<td>US Office of Personnel</td>
<td>22 m</td>
</tr>
<tr>
<td></td>
<td>Management (OPM)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sony's PlayStation Network</td>
<td>77 m</td>
</tr>
<tr>
<td></td>
<td>RSA Security</td>
<td>40 m</td>
</tr>
<tr>
<td>2009</td>
<td>Heartland Payment Systems</td>
<td>134 m</td>
</tr>
<tr>
<td>2006</td>
<td>TJX Companies, Inc.</td>
<td>94 m</td>
</tr>
</tbody>
</table>

SOURCE: C3O
HAWAI'I 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
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).
Security Landscape & Current Threats at UH
# HoneyPot Project

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

<table>
<thead>
<tr>
<th>Monitored Services</th>
<th>Attacked Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP (21)</td>
<td>SSH, Telnet, RDP, RAdmin, VNC</td>
</tr>
<tr>
<td>SSH (22)</td>
<td>MSSQL (1433)</td>
</tr>
<tr>
<td>Telnet (23)</td>
<td>RDP (3389)</td>
</tr>
<tr>
<td>HTTP (80)</td>
<td>RAdmin (4899)</td>
</tr>
<tr>
<td>HTTPS (443)</td>
<td>VNC (5900)</td>
</tr>
<tr>
<td>POP3 (110)</td>
<td></td>
</tr>
<tr>
<td>POP3S (995)</td>
<td></td>
</tr>
<tr>
<td>IMAP (143)</td>
<td></td>
</tr>
<tr>
<td>IMAPS (993)</td>
<td></td>
</tr>
</tbody>
</table>
• Hours (HST) at the bottom
• Unique attackers (IP addresses) are on the secondary axis
• Brute force attacks began 4 minutes after the honeypot started
Email Compromises

- 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

- Send you malware via infected attachments or links to malware infected sites
From: John Daniel <amyg@hawaii.edu>  
Date: Thu, Feb 15, 2018 at 10:55 AM  
Subject: Assignment Schedule  
To:

Secured PDF Document


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

- **Stop. Examine. Ask. Report.**
- [www.hawaii.edu/infosec/phishing](http://www.hawaii.edu/infosec/phishing)
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
Best Way for Individuals to Protect Themselves

- Use multi-factor authentication (DUO) 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)
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
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
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)
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 April 14; Exploit used on April 18
Recent Security Events @ UH

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”

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

Questions?
Twitter: https://twitter.com/lmaostack

With love from the hacker God himself, BTI (breaktheinternet) and Brian Krebs.

For the love of God, please close this port, skid.

Questions?
Twitter: https://twitter.com/lmaostack

FROM MICHAEL JENSCH, ROSENWEG, UNNA, DEUTSCHLAND.
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

• 2018: External reports of compromised UH websites being used to attack other organizations (5+)
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
<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
<th>Penalty</th>
</tr>
</thead>
</table>
| 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)

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
<th>Penalty</th>
</tr>
</thead>
</table>
| Health Insurance Portability and Accountability Act (HIPAA) | • Federal law that protects the privacy of individually identifiable health information  
• UH’s HIPAA policy: EP2.217 | 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 | If data is intentionally revealed that should not be, could be convicted of a misdemeanor unless a greater penalty is provided for by law. |

Data subject to regulation:  
• Health  

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, etc.)
## Key Regulations and Penalties (3)

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Card Industry Data Security Standard (PCI-DSS) information</td>
<td>• A widely accepted set of policies / procedures that protects cardholders’ credit/debit/cash card transactions</td>
<td>Financial fines; also requires a breach notification in accordance with HRS §487N</td>
</tr>
<tr>
<td></td>
<td>Data subject to regulation:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Credit Card</td>
<td></td>
</tr>
<tr>
<td>Hawai‘i Revised Statutes (HRS) §487N</td>
<td>• State law that defines the breach notification to the legislature</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Written report to the legislature within 20 days after the discovery of a data breach</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data subject to regulation:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• First Name or First Initial/Last Name combined with:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Social Security Number (SSN)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Driver license or state ID #</td>
<td></td>
</tr>
<tr>
<td>Regulation</td>
<td>Description</td>
<td>Penalty</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| 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)

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Description</th>
<th>Penalty</th>
</tr>
</thead>
</table>
| 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 120-149 |         |
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
<table>
<thead>
<tr>
<th>Executive Policies</th>
<th>Administrative Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Institutional Data Governance EP2.215</strong></td>
<td><strong>FERPA AP7.022</strong></td>
</tr>
<tr>
<td>Use and Management of Information Technology Resources EP2.210 (to be updated)</td>
<td><strong>Data System Authorizations (TBD)</strong></td>
</tr>
<tr>
<td>System and Campus Wide Electronic Channels for Communicating with Students EP2.213</td>
<td><strong>Mandatory Training &amp; Continuing Education Requirements AP2.215</strong></td>
</tr>
<tr>
<td><strong>Data Classification Categories &amp; Info Security Guidelines EP2.214</strong></td>
<td><strong>Open Records Requests (TBD)</strong></td>
</tr>
<tr>
<td><strong>Institutional Records Management and Electronic Approvals / Signatures EP2.216 (to be updated)</strong></td>
<td><strong>Data Sharing Request Process (in progress)</strong></td>
</tr>
<tr>
<td><strong>HIPAA EP2.217</strong></td>
<td><strong>Specialized Purchasing AP8.265</strong></td>
</tr>
<tr>
<td>Online Approvals of Internal University Transactions EP2.218</td>
<td><strong>Records Retention Schedule (in progress)</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Credit Card Program AP8.710</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Data Breaches (coming soon)</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Electronic Payments via University Websites AP8.711</strong></td>
</tr>
</tbody>
</table>
## EP2.214, Data Classification Categories

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

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

---

59
Technical Guidelines
http://www.hawaii.edu/infosec/techguidelines/

## Awareness
- 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

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

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

*Unless otherwise noted, all security requirements are required.
AP2.215, Mandatory Training and Continuing Education Requirements for Data Users

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Renewal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Awareness Training (ISAT)</td>
<td>Every 2 years</td>
</tr>
<tr>
<td>General Confidentiality Notice (GCN) acknowledgment</td>
<td>Annually</td>
</tr>
</tbody>
</table>

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)
Prevent Data Breaches

- Know what sensitive and regulated data you have & use
- Get rid of what you don’t need
- Protect what you need to keep (encrypt!)
- Keep your machines and applications updated (patch!)
- Be aware of spear phishing and malicious attachments
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
eTravel Compliance Enhancements

James Kashiwamura, Director of Disbursing and Payroll
Internal Audit Observations

• 8 of 12 travel requests for non-advance travel did not include all necessary approvals in eTravel prior to travel departure date.
• Instances of noncompliance with respect to travelers receiving additional advances when deemed not eligible.
• Significant late repayments from excess travel advances.
Changes to AP 8.851

• Section III, E to:

• All travel must be approved in writing. Any travel expense that is not approved in advance is at the risk of the traveler and may become the traveler’s personal expense. Individual departments are allowed to use their discretion in the establishment of internal control requirements.
Change to eTravel

• AP 8.851 requires that travel completion must be submitted within 21 calendar days from the travelers’ return date. That means document status must be “Routing for approval”.
  • System modification to enforce the 21 day completion deadline.

| Traveler Departure Date | Traveler Return Date | 21 days from return date: Travel Submission Deadline | Business Office Review & Approval |

Travel Completion must be submitted **Within 21 calendar days** from travelers return date
Travel Completion

- If the traveler wants to create a new travel request but has an outstanding travel completion that is more than 21 calendar days past the return date, an error message will appear. The system will disallow new travel request.

<table>
<thead>
<tr>
<th>CREATE NEW TRAVEL REQUEST</th>
<th>STEP 1: ALL FIELDS ARE REQUIRED AS IT DRIVES THE FORM IN STEP 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TRAVELER INFO</strong></td>
<td></td>
</tr>
<tr>
<td>Traveler</td>
<td>Sample: A new request cannot be created for this traveler. See the delinquent traveler report for a listing of outstanding travel completions.</td>
</tr>
<tr>
<td></td>
<td>• Includes Travelers you may prepare travel for - as the Traveler's Preparer or as the Business Office of the Traveler's home department.</td>
</tr>
<tr>
<td></td>
<td>• Currently the system only accommodates UH employees in Peoplesoft.</td>
</tr>
<tr>
<td>Position</td>
<td>Pulls a traveler's appointments from PeopleSoft.</td>
</tr>
<tr>
<td>Bargaining Unit</td>
<td>• Defaults to the Traveler's Bargaining Unit in Peoplesoft, but may be changed if the data is not current.</td>
</tr>
<tr>
<td></td>
<td>• Determines travel reimbursement rules and rates.</td>
</tr>
<tr>
<td><strong>TRIP INFO</strong></td>
<td></td>
</tr>
<tr>
<td>Travel Dates</td>
<td>• Determines Per Diem rates in effect, i.e. which bargaining unit contract applies.</td>
</tr>
<tr>
<td></td>
<td>• If typing dates input all numeric, i.e. 010109 automatically formats to 01/01/2009.</td>
</tr>
<tr>
<td>Destination (where costs incurred)</td>
<td>• Destinations determine travel expense object codes, i.e. there's a different set of object codes for Intra-State travel, U.S. travel, and Foreign travel. Therefore, select &quot;Mixed Destination&quot; only when travel costs are incurred at two or more different destinations, i.e. combination of Intra-State, U.S., Foreign.</td>
</tr>
<tr>
<td>Itinerary Type</td>
<td>• Determines number of destination legs in the itinerary.</td>
</tr>
<tr>
<td></td>
<td>• The itemized itinerary allows entering all connecting stops, which may help locate travelers during remote emergencies.</td>
</tr>
</tbody>
</table>
Travel Advance

- If a traveler requests a new travel advance but has an outstanding travel advance that is more than 30 calendar days past the return date, an error message will appear.

- Modification to enforce the eligibility of travel advances.
Travel Advance

• Travelers with advances that are not in “FINAL” status within 30 days of their return date will not be able to request another advance.

• Traveler will still be able to create new travel requests.

Travel Completion must be in FINAL status 30 calendar days from travelers return date
Advance Deposit Field

• An Advance Deposits field has been added for the eDoc number associated with repayment of the advance.
• If traveler’s advance exceeds their reimbursable expenses, the advance deposit field is required.
Questions
Personal Tax 101 – Ken Lum

Purpose:
To gain basic knowledge of U.S. Individual Tax reporting and pertinent impacts of the Tax Cuts and Jobs Act on individual tax reporting
Basic Knowledge of individual taxes in United States

1. Each person is responsible for their own tax reporting.
2. Depending on which state you are living in, besides federal tax reporting, you may be subject to state and county taxes. (i.e. New York)
3. Underreporting (or forgetting to report) of income will be easily detected for wages, interest income, dividend, and capital gains from selling stocks, as IRS already has copy of same tax form from the responsible reporting entity.
4. Income for individuals is on “cash basis”. i.e. pay check for Dec. 31, 2017 is 2018 income as it was paid on January 5, 2018.
5. Tax Cuts and Jobs Act signed by President Trump on Dec. 22, 2017 changes individual taxes significantly for the next 8 years. (thru Dec. 31, 2025)
## Changes in Individual Income Tax Rates

<table>
<thead>
<tr>
<th>2017 Individual Income Tax Rates</th>
<th>2018 Individual Income Tax Rates</th>
</tr>
</thead>
<tbody>
<tr>
<td>10%</td>
<td>10%</td>
</tr>
<tr>
<td>15%</td>
<td>12%</td>
</tr>
<tr>
<td>25%</td>
<td>22%</td>
</tr>
<tr>
<td>28%</td>
<td>24%</td>
</tr>
<tr>
<td>33%</td>
<td>32%</td>
</tr>
<tr>
<td>35%</td>
<td>35%</td>
</tr>
<tr>
<td>39.6%</td>
<td>37%</td>
</tr>
</tbody>
</table>
### Changes in Individual Income Tax Rates (cont’d)

<table>
<thead>
<tr>
<th>Tax Rate</th>
<th>2017</th>
<th>Tax Rate</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>10%</td>
<td>$1 to $9,325</td>
<td>10%</td>
<td>$1 to $9,525</td>
</tr>
<tr>
<td>15%</td>
<td>$9,326 to $37,950</td>
<td>12%</td>
<td>$9,526 to $38,700</td>
</tr>
<tr>
<td>25%</td>
<td>$37,951 to $91,900</td>
<td>22%</td>
<td>$38,701 to $82,500</td>
</tr>
<tr>
<td>28%</td>
<td>$91,901 to $191,650</td>
<td>24%</td>
<td>$82,501 to $157,500</td>
</tr>
<tr>
<td>33%</td>
<td>$191,651 to $416,700</td>
<td>32%</td>
<td>$157,501 to $200,000</td>
</tr>
<tr>
<td>35%</td>
<td>$416,701 to $418,400</td>
<td>35%</td>
<td>$200,001 to $500,000</td>
</tr>
<tr>
<td>39.60%</td>
<td>over $418,400</td>
<td>37.00%</td>
<td>over $500,000</td>
</tr>
</tbody>
</table>
## Changes in Individual Income Tax Rates (cont’d)

<table>
<thead>
<tr>
<th>Tax Rate</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>10%</td>
<td>$1 to $18,650</td>
<td>$1 to $19,050</td>
</tr>
<tr>
<td>15%</td>
<td>$18,651 to $75,900</td>
<td>$19,051 to $77,400</td>
</tr>
<tr>
<td>25%</td>
<td>$75,901 to $153,100</td>
<td>$77,401 to $165,000</td>
</tr>
<tr>
<td>28%</td>
<td>$153,101 to $233,350</td>
<td>$165,001 to $315,000</td>
</tr>
<tr>
<td>33%</td>
<td>$233,351 to $416,700</td>
<td>$315,001 to $400,000</td>
</tr>
<tr>
<td>35%</td>
<td>$416,701 to $470,700</td>
<td>$400,001 to $600,000</td>
</tr>
<tr>
<td>39.60%</td>
<td>over $470,700</td>
<td>over $600,000</td>
</tr>
</tbody>
</table>
Key changes from Tax Cuts & Job Act (TCJA)

<table>
<thead>
<tr>
<th></th>
<th>Prior Law</th>
<th>TCJA (2018 to 2025)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Child Tax Credit</strong></td>
<td>$1,000 (refundable up to $1,000)</td>
<td>$2,000 (refundable up to $1,400)</td>
</tr>
<tr>
<td><strong>Standard Deduction</strong></td>
<td>s: 6,350 MFJ: $12,700</td>
<td>s: 12,000 MFJ: $24,000</td>
</tr>
<tr>
<td><strong>Personal Exemption</strong></td>
<td>$4,050</td>
<td>Repealed</td>
</tr>
<tr>
<td><strong>State and local Taxes</strong></td>
<td>Deductible</td>
<td>Maximum $10,000 Deduction</td>
</tr>
<tr>
<td><strong>Mortgage Interest</strong></td>
<td>$1,000,000 Limit</td>
<td>$750,000 Limit</td>
</tr>
</tbody>
</table>
Key changes to itemized deductions

<table>
<thead>
<tr>
<th>Other Changes in tax law for itemized deductions</th>
<th>Prior Law</th>
<th>TCJA (2018 to 2025)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Charitable Contributions</td>
<td>Up to 50% of Adjusted Gross Income</td>
<td>Up to 60% of Adjusted Gross Income</td>
</tr>
<tr>
<td>Medical expenses</td>
<td>Exceed 7.5% of adjusted gross income (2017 and 2018)</td>
<td>Exceed 10% of adjusted gross income (2019 to 2025)</td>
</tr>
<tr>
<td>Miscellaneous Deductions (investment and consulting fees, tax preparers fees, unreimbursed employee expenses etc.)</td>
<td>Exceed 2% of adjusted gross income</td>
<td>Repealed</td>
</tr>
</tbody>
</table>
# Comparing taxes using prior law vs. TCJA law

<table>
<thead>
<tr>
<th>Prior Law</th>
<th>TCJA Law</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Facts:</strong> UH employee, filing single, wages of $45,000, State tax withheld $7,000, no mortgage interest, no property tax</td>
<td><strong>Facts:</strong> UH employee, filing single, wages of $45,000, State tax $7,000, no mortgage interest, no property tax</td>
</tr>
<tr>
<td>Wages</td>
<td>Wages $45,000</td>
</tr>
<tr>
<td>Deductions: Itemized Deduct:</td>
<td>Deductions: $12,000</td>
</tr>
<tr>
<td>Personal Exemptions</td>
<td>Personal Exemptions $ -</td>
</tr>
<tr>
<td>Taxable Income</td>
<td>Taxable Income $33,000</td>
</tr>
<tr>
<td>Tax amount</td>
<td>Tax amount $3,770</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Prior Law</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wages</td>
<td>$45,000</td>
</tr>
<tr>
<td>Deductions: Itemized Deduct:</td>
<td>$7,000</td>
</tr>
<tr>
<td>Personal Exemptions</td>
<td>$4,050</td>
</tr>
<tr>
<td>Taxable Income</td>
<td>$33,950</td>
</tr>
<tr>
<td>Tax amount</td>
<td>$3,884.</td>
</tr>
</tbody>
</table>
In closing:

- TCJA tax law for individuals may or may not be beneficial to you, depending on your income and deductions, and filing status.
- IRS has “withholding calculator” on website to assist you in analyzing whether current federal taxes withheld is adequate for you. https://www.irs.gov/individuals/irs-withholding-calculator
Disclaimer

• This presentation is intended to provide general information on preparing a U.S. tax return.
• The University of Hawaii does not provide personal assistance with individual tax return preparation.
• Please consult with your tax advisor if you need further assistance
Financial Management Office

Thank You for attending the Fiscal Administrator Meeting

Susan Lin’s Contact Information:
Email: slin@hawaii.edu
Phone: 808-956-5445