Breaches & A Lawsuit: One Institution’s Road to Recovery

Jodi Ito
Information Security Officer
University of Hawaii
jodi@hawaii.edu
(808) 956-2400
Copyright Statement

- This presentation leaves the copyright of the content to the presenter. Unless otherwise noted in the materials, uploaded content carries the Creative Commons Attribution-NonCommercial-ShareAlike license, which grants usage to the general public with stipulated criteria.
University of Hawaii System

1 - Research University
- UH Manoa: 20,000

2 - Baccalaureate Universities
- UH West Oahu: 2000
- UH Hilo: 4000

7 - Community Colleges
- Kapiolani CC: 8000
- Honolulu CC: 4000
- Leeward CC: 7200
- Windward CC: 2500
- UH Maui College: 4000
- Hawaii CC: 3200
- Kauai CC: 1300
Information Technology Services

- System Office
- Office of the Vice President of Information Technology & Chief Information Officer
- 120+ full time staff
- 4 groups: TI, AT, MIS, Admin.
- ISO direct report to VP IT & CIO
ITS Responsibilities

- System-wide information systems & services
  - Student information system
  - Personnel system
  - Financial system
  - Data warehouse / operational data store
  - Learning management system
  - Email, web, identity management/directory services, contract services, help desk, desktop support, phone, site licensing

- Overall Network Infrastructure
- Information Security
State Breach Law: HRS 487-N

- Definition of Personal Information:
  - Individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
    - Social Security Number;
    - Driver’s license number or Hawaii Identification Number;
    - Account number, credit or debit card number, access code, or password that would permit access to an individual’s financial account;
HRS Definition of Breach

- “Security breach” means an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach.
State Reporting Requirements

- Provide notice to affected individual
  - Description of incident
  - Type of personal information involved
  - Remediation and preventive actions taken
  - Contact phone number for additional information
  - Advice to affected individual

- Written report to state legislature within 20 days after discovery of security breach
Four Breaches - Facts

- **April 2009**: Kapiolani CC – 15,000
  - Desktop computer with access to sensitive information infected with malware designed to steal sensitive information

- **February 2010**: Honolulu CC – 35
  - Desktop computer with credit card numbers breached; unauthorized access was from a networked lab computer with internet access
The Continuing Saga...

- June 2010: UH Manoa – 53,000
  - Parking office
  - Compromised server discovered through a routine audit of logs
  - Both SSNs & CC#s involved but only one type per individual
July 2010: Executive Directive

- 3rd known breach since enactment of identity theft law
- Directed every executive to make it a priority to protect sensitive information because highly decentralized organization
- Identify a single individual to oversee unit’s information protection and compliance program
- Directed executive to ensure full compliance to:
  - Report PI systems (per state law)
  - Purge unnecessary SSNs; ensure credit card processing in compliance with UH policy
  - Review and strengthen internal controls around handling of sensitive information
One More...

- October 2010: UH West Oahu - 40,000
- UH System notified that sensitive information was exposed on UH WO web server
- Discovered by a watchdog organization using search engine
Report cites UH in security breaches of online information

By Star-Advertiser Staff

POSTED: 11:22 a.m. HST, Nov 17, 2010

Since 2005, at least 479,000 Hawaii records have been breached online with the University of Hawaii responsible for more than half of the security lapses, according to a Washington, D.C.-based privacy group.

In a 17-page report, the Liberty Coalition said the University of Hawaii is the biggest offender and "has a pattern of breaches and unfulfilled promises."
Data breaches earn UH an 'F'

Personal information in nearly 260,000 records has been exposed since 2005, a report says

By Gordon Y.K. Pang

POSTED: 01:30 a.m. HST, Nov 18, 2010

A national organization has given the University of Hawaii a grade of "F" for online security breaches that exposed Social Security numbers and other sensitive information in nearly 260,000 records.

The Liberty Coalition, a nonprofit civil liberties watchdog group, yesterday said more than half of the estimated 479,000 Hawaii records breached since 2005 were those mishandled by UH.
November 17, 2010
By Aaron Titus, Information Privacy Director
Liberty Coalition

Compiled at the Request of:
Senator Mike Gabbard, Member, Committee on Judiciary & Labor
Class-action suit filed against UH over data breaches

By Gene Park

POSTED: 01:35 p.m. HST, Nov 18, 2010

The University of Hawaii is now the target of a class-action lawsuit filed today, as a result of recent data breaches.

The main plaintiff in the case, Philippe Gross, was a student at the Manoa campus from 1990 through 1998. He said four other names have been attached to his social security number, and that his credit card has been used in Georgia.
“The purpose of this Act is to strengthen the safeguards for security breaches of personal information held by government agencies.”
Class Action Lawsuit: Original Complaint

- “Seeks an injunction: (a) forbidding UH from violating the constitutional rights of its students, faculty and guests, as protected by the right to privacy of the United States and Hawaii Constitutions by the unauthorized released of private information, including but not limited to SSN and (b) mandating that the University of Hawaii take appropriate measures to ensure the protection of private information within its possession.”

- “Seeks monetary damages to compensate class members for expenses including but not limited to enrollment in credit reporting monitoring program(s), time spent in monitoring credit reports, credit card and bank statements, and identity theft insurance.”
Lawsuit Timeline

- June 2011: Enforce litigation hold on all involved emails (in process: migration to Google)
- June 2011: UH filed motion to dismiss
- July 2011: One more breach – theft of paper documents containing credit card numbers – 2500 affected
- July/Aug 2011: Compiling list of ALL affected individuals (est. over 800 man hours)
Timeline (continued):

- Jan. 2012: Working on tentative settlement
- Jan. 2012: Motion for Preliminary Approval of Settlement
- Feb. 1, 2012: Court hearing on Motion for Preliminary Approval
- Feb. 15, 2012: Credit monitoring service begins mailing out notices to sign up for services; services would begin AFTER final court approval
- March 1, 2012: Public notification: joint press release, email blast to all UH faculty/staff/students, Alumni Association, posts on campus web sites, newspapers
- May 21, 2012: Final Approval Granted (no appeals received)
- 2 years of continuous credit monitoring & ID Theft Consultation and Restoration
End of 2010: State of Information Security @ UH

**CODE RED!**

- Negative media (over 2M hits)
- Battered reputation
- Legislative scrutiny
2011: State of Info Sec @ UH

- End of 2010: retained external consultant to perform an information security posture assessment
- Preliminary analyses of incidents:
  - Weak desktop computer security practices
  - Insecure operational practices
  - Information retained longer than needed
  - Cannot identify who has access or possession of UH sensitive information (including tracking IRB requests)
  - Servers: Misused or not managed appropriately
  - UH policy not followed or existence unknown
Already In Process:

- Phased out use of SSNs as primary identifiers
- Identified campus leadership for protection of sensitive information
- Identified technical leads for protection of sensitive information
- Instituted mandatory reporting of repositories of sensitive information
- Acquisition of Identity Finder for scanning for sensitive information
- Started Data Governance initiative
- In contact with “functional” groups (PO, FO, AO, managerial/executive teams, campus groups, etc.)
The University of Hawaii (UH) is committed to implementing a systemwide information security program to replace the current decentralized approach. This program must leverage best practices to maximize information security while continuing to support the principles of academic freedom and openness central to a university's culture and mission. UH believes it essential to begin with an impartial expert assessment to develop a plan for a holistic systemwide approach. This assessment will assess current policies, current practices and current campus awareness as the basis of recommendations for improvements in security policies, practices and education.
Services Provided:

- Review existing internal and external documentation including reports, policies and legislation
- Interview key stakeholders
- Identify the major IT security issues faced by UH and best practices for solutions
- Prioritize solutions for immediate action
- Provide recommendations for how UH should implement a comprehensive systemwide approach to information security
Summary of Findings:

- A significant under-investment in information security resources
- Trying to operationally manage information security as a fully de-centralized activity
Overarching Recommendation

“Develop a properly funded, strategically oriented, university-wide information security program that is centrally managed and operates in collaboration with the many decentralized units throughout the university.”
UH Information Security Program

- Took what we are already doing
- Added consultant’s specific recommendations
- Develop strategic areas:
  - Data Governance and Oversight
  - Information Security Audits & Risk Assessments
  - Information Security Policies & Procedures
  - Identity Management & Access Controls
  - Information Security Training and Awareness
Specific Projects (partial list)

- Data Governance structure & Data Sharing request procedures
- Server registration & scanning (random audits)
- Network scans for servers (map against registered servers)
- Policy review
- Automated deprovisioning via identity management
- Evaluation & implementation of additional network security technologies
- Compliance & Risk Assessments for “high risk” area
Awareness & Training

- Mandatory information security awareness training for UH employees with access to sensitive information (by function) including reporting
- Convene “outreach groups”: application, web, database developers to inform them of new policies/procedures and solicit feedback on upcoming projects
- Provide specific training for targeted groups
Develop Project Plan & Priorities

- Funding: VP IT & CIO worked with Executive Leadership (Pres/VP/Chancellors) to assess each campus – building in to funding model for other system information systems
- Staffing: added 2 additional positions
- Need ITS leadership support for “security” projects: Created ITS Security Program Leads
- Any project needs group approval before proceeding
- Projects need to be included in overall ITS priorities list
Work with Campuses

- Starting to make security a priority
- VC/Director/CIO leadership positions
- Each campus has a “security” lead
- Honolulu CC is working on campus policies
- JABSOM (School of Medicine)
- Kapiolani CC established their own campus information security lead
Kapiolani Community College

- Jason Akiyama
- akiyamaj@hawaii.edu
- (808) 734-9812
DSLC/UH IT Security Leads:
Sample Agenda

- Server registration update (including random audits); *ITS Info Sec*
- Summary of Information Security Compliance Assessments; *Internal Audit*
- Data Governance & Data Sharing Request Process Update; *Dir. Data Governance*
- FERPA Policy Update; *UH Registrar*
- Developers & Identity & Access Management (IAM) update; *ITS IAM Manager*
- Rollout of Identity Finder for desktops; *ITS Info Sec*
- External Information Security Posture Assessment; *External Consultant*
Server Registration Update

- Random Audit – Users will be contacted by 4/14
- Provide OpenVAS scan results and Identity Finder scan results
  - Few servers with PII
  - Few servers without PII
  - Few servers from campuses that reported no PII on any servers
Current Number of Registered Servers

<table>
<thead>
<tr>
<th>Campus</th>
<th>Total Registered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hilo</td>
<td>45</td>
</tr>
<tr>
<td>Manoa</td>
<td>442</td>
</tr>
<tr>
<td>West Oahu</td>
<td>6</td>
</tr>
<tr>
<td>System</td>
<td>52</td>
</tr>
<tr>
<td>Maui</td>
<td>48</td>
</tr>
<tr>
<td>KCC</td>
<td>64</td>
</tr>
<tr>
<td>Hawaii</td>
<td>28</td>
</tr>
<tr>
<td>HCC</td>
<td>24</td>
</tr>
<tr>
<td>Kauai</td>
<td>14</td>
</tr>
<tr>
<td>LCC</td>
<td>31</td>
</tr>
<tr>
<td>Windward</td>
<td>29</td>
</tr>
<tr>
<td>Other</td>
<td>78</td>
</tr>
<tr>
<td>TOTAL</td>
<td>861</td>
</tr>
</tbody>
</table>
Information Security Compliance Assessments

- General Process:
  - Contact the respective Unit to discuss scope and timing.
  - Completion of *Maintenance of Sensitive Information Survey*.
  - Conduct meeting and site visit with Unit.
  - Inform the Unit of observations / recommendations
Status

- Work Performed during January – March 2013
- Selected Departments/Schools
  - Financial Aid Services (All Campuses)
  - Community Colleges – Non-Credit Programs
  - John A. Burns School of Medicine
- Surveys completed and site visits for O‘ahu units completed.
- Memo containing observations (if any) to be circulated to all units shortly.
- Status report to the Board of Regents in progress
Common Observations

- Background Checks
- Record Retention of Sensitive Information
- Cross-Cut vs. Strip-Cut Shredder
- Securing Physical Files containing Sensitive Information
- Encrypting electronic transmission of Sensitive Information using UH File Drop
Summary

- Know your KEY players
- Be prepared: Not if a breach will occur – What will you do WHEN it occurs?
  - HEISC Information Security Guide: Data Incident Notification Toolkit
- Have a “PR” plan: Reputation Management
- Analyze the incident; develop mitigation strategy; incorporate into your Information Security Program
Your Plan?

- Do you have an incident response plan?
- Do you know who to contact? *AND* what to tell them?
- How will you communicate to the affected individuals and to the public?
Questions?

Jodi Ito, UH System  
jodi@hawaii.edu  
(808) 956-2400

Jason Akiyama, Kapiolani CC  
akiyamaj@hawaii.edu  
(808) 734-9812