



# Protecting UH Sensitive Information (yes, this means **YOU!**)

Jodi Ito

Information Security Officer, ITS

[jodi@hawaii.edu](mailto:jodi@hawaii.edu)

956-2400



a.k.a.  
“Preventing a Data Breach”

# UH Warrior football program invited to join MWC

[WATCH NOW](#) 

University of Hawaii president M.R.C. Greenwood announced Thursday night that the school has been...

Updated 12 minutes ago



# 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

8 retweet

f Share

41

44 Comments



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.

[http://www.staradvertiser.com/news/20101118\\_Data\\_breaches\\_earn\\_UH\\_an\\_F.html](http://www.staradvertiser.com/news/20101118_Data_breaches_earn_UH_an_F.html)

# Report cites UH in security breaches of online information

By Star-Advertiser Staff

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

2   Share  9 0 Comments

-- ADVERTISEMENT --

## **Volunteer in Cambodia**

Ethical and Affordable Volunteer Opportunities in Cambodia  
[www.globalteer.org](http://www.globalteer.org)

## **Int'l Volunteer Programs**

Volunteer overseas with Peace Corps

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."

<http://www.staradvertiser.com/news/breaking/108760734.html>



# Class-action suit filed against UH over data breaches

By Gene Park

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

14 retweet  Share 46 34 Comments

-- ADVERTISEMENT --



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.

<http://www.staradvertiser.com/news/breaking/109051759.html>

# Report on Hawaii Personal Information Breaches: Part 1

---



*November 17, 2010*

*By Aaron Titus, Information Privacy Director  
Liberty Coalition*

*Compiled at the Request of:*

Senator Mike Gabbard, Member, Committee on Judiciary & Labor



# **State of Information Security at UH**

**Code RED!**




# What is a Data Breach?

- Occurs when sensitive information is involved in:
  - Unauthorized Disclosure (either intentionally or unintentionally)
  - Theft/Loss (laptop/mobile device/storage device)
  - Penetration (unauthorized access to computer systems)



# HRS 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;



# Definition of UH Sensitive Information

- Personally Identifiable Information (PII)
  - Name, Address, SSN, DOB, etc.
- Examples of Sensitive Information at UH:
  - Student Records (FERPA)
  - Health Information (HIPAA)
  - Personal Financial Information
  - Answers to “secret” questions
  - Confidential information & more...
- Executive Policy E2.214:  
Security and Protection of Sensitive Information  
<http://www.hawaii.edu/apis/ep/e2/e2214.pdf>



# UH Breaches Recap

- 2009 April: Kapiolani CC
  - 2010 March: Honolulu CC
  - 2010 July: UH Manoa
  - 2010 October (now!)
- 
- **OVER 100,000 exposed records!**
  - **ALL BECAUSE POLICY NOT FOLLOWED**



# Breach Notification

- Determined that pursuant to HRS 487N, UH required to do a “Breach Notification”:
  - Written notification to all affected individuals
  - Legislative Report due 20 days after discovery of breach
  - Press Release/website

# Personal Information Protection POC



UNIVERSITY  
of HAWAII\*  
SYSTEM

M.R.C. Greenwood, Ph.D.  
President

July 13, 2010

## MEMORANDUM

TO: Vice Presidents  
Chancellors  
Associate Vice Presidents

FROM: M.R.C. Greenwood *MRC Greenwood*  
President

SUBJECT: Improving Protection of Sensitive Information




# Key Elements

- Campus designee: “Personal Information Protection” Point of Contact
- Limiting storage and retention of personal information to what is absolutely essential and required by law
- Review and strengthen internal controls over personal information



2. For all the information systems under your purview, the storage and retention of personal information should be limited to what is absolutely essential and permissible under the law. UH has not used Social Security Numbers (SSNs) as either an employee or student ID since 2004, so SSNs should be purged from all systems and databases where it is not absolutely required for purposes such as federal and state tax reporting, financial aid, payroll, and other personnel related matters. Similarly, credit card information should not be stored or retained. Manual and electronic credit card processing must take place in accord with applicable university and industry procedures and standards in accord with applicable UH administrative procedures (A8.710 and A8.711). The best way to protect personal information is to not store it at all.



# Annual Personal Information Survey

- Information Privacy & Security Council
- Started in 2009
- Just completed 2010
- **ALL** systems (electronic or paper) needs to be reported
- <http://www.hawaii.edu/its/information/survey>



# Hawaii Revised Statutes (HRS)

- HRS 487J - SSN Protection

[http://www.capitol.hawaii.gov/hrscurrent/Vol11\\_Ch0476-0490/HRS0487J/](http://www.capitol.hawaii.gov/hrscurrent/Vol11_Ch0476-0490/HRS0487J/)

- HRS 487N - Breach Disclosure

[http://www.capitol.hawaii.gov/hrscurrent/Vol11\\_Ch0476-0490/HRS0487N/](http://www.capitol.hawaii.gov/hrscurrent/Vol11_Ch0476-0490/HRS0487N/)

(UH Personal Information System Survey:  
<http://www.hawaii.edu/its/information/survey> )


- HRS 487R - Destruction of PI Records

[http://www.capitol.hawaii.gov/hrscurrent/Vol11\\_Ch0476-0490/HRS0487R/](http://www.capitol.hawaii.gov/hrscurrent/Vol11_Ch0476-0490/HRS0487R/)



# UH Policies

- UH Form 92:  
UH General Confidentiality Notice  
<http://www.hawaii.edu/ohr/docs/forms/uh92.pdf>
- System-wide Student Conduct Code  
<http://www.hawaii.edu/apis/ep/e7/e7208.pdf>



# E2.214: Security and Protection of Sensitive Information

(currently being reviewed/revised)

- <http://www.hawaii.edu/apis/ep/e2/e2214.pdf>
- Provides governance of sensitive information at UH:
  - Classification
  - Ownership & Responsibilities
  - Protection of sensitive data
    - Access
    - Transmission
    - Storage
    - Destruction



# Questions to ASK!

- Is sensitive information stored locally?
- Is SSN really required?
- If so, ***WHY?!***
  
- Printed report, report saved as a .pdf document, email...?



# Security for Sensitive Information

- Computers must comply with basic security standards
- Sensitive information must be protected:
  - At rest
  - In transit
  - When destroyed
- <http://www.hawaii.edu/askus/729>



# Protecting Computers with Sensitive Information

- Computers must comply with basic security standards:
  - OS and application updates applied in a timely manner
  - Anti-virus & anti-spyware software installed **AND** updated frequently
  - User accounts & password controls
  - Password guidelines: <http://www.hawaii.edu/askus/705>
  - Basic computer security: <http://www.hawaii.edu/askus/593>



# Protecting Files w/ Sensitive Information

- Sensitive information must be protected at rest:
  - Encryption
    - Windows: <http://www.hawaii.edu/itsdocs/win/gswindowsencryption.pdf>
    - Mac: <http://www.hawaii.edu/askus/676>
  - If not encrypted, then the computer system must be in a secure and controlled environment

# Transmission of Sensitive Information

- Don't send sensitive data "in the clear" including email
- Use the UH Filedrop:  
<http://www.hawaii.edu/filedrop/>
  - Information is encrypted in transit to the filedrop server and on the filedrop server
  - Information must either be encrypted or deleted after being received
  - Recipient can be required to authenticate
  - 800 MB per upload session
  - More detailed information:  
<http://www.hawaii.edu/askus/673>





# Destruction of Sensitive Information

- Paper must be shredded
- Electronic data must be securely erased or the media destroyed such that the data is unrecoverable
  - <http://www.hawaii.edu/askus/706>
- Personal Electronic Devices: PDAs, smart cell phones (Treos, Blackberry, iPhone, etc.)
  - Check w/ the manufacturer
  - Cell phones:
    - [http://www.recellular.com/recycling/data\\_eraser/default.asp](http://www.recellular.com/recycling/data_eraser/default.asp)



# Tools to Search for SSNs

ITS has just licensed Identity Finder - will announce deployment later

*NOTE: These tools are not supported by ITS!*

*They are presented here for your information.*

- Find\_SSN:

[http://security.vt.edu/Find\\_SSNs/index.html](http://security.vt.edu/Find_SSNs/index.html)

- Spider:

<http://www.cit.cornell.edu/services/spider/howto/index.cfm>

- SENF:

<https://senf.security.utexas.edu/wiki/>



# Laptop & Mobile Devices

- Use accounts & strong passwords
- Use encryption
- Backup your data
- Watch your laptop at all times in public
  - Keep your laptop in your possession at all times
  - Don't leave it out in your hotel room
  - Consider laptop recovery services



# This Cyber “stuff” ...

- ***Affects us all!***
- Each unprotected/unpatched computer is a threat:
  - Infected worm/virus/bot
  - Could be used in a concerted attack against a critical infrastructure
- Computers, servers, mobile storage devices with any sensitive information represent a vulnerability



# What Do We Do?

- Practice safe computing
  - Keep your software up-to-date with all patches
  - Install and maintain anti-virus software
  - Don't open unknown emails & attachments
  - Use good passwords and protect your password(s)
  - Only login to servers for the duration needed - disconnect when done
  - Don't let others use your computer irresponsibly
  - <http://www.hawaii.edu/askus/729>
- Know the policy E2.214
- Educate those around you



# ***BE AWARE!***



STOP | THINK | CONNECT™

DHS/Whitehouse campaign:

<http://www.dhs.gov/files/events/stop-think-connect.shtm>



# Questions?

Jodi Ito

[jodi@hawaii.edu](mailto:jodi@hawaii.edu)

(808) 956-2400