

Data Breach Debrief

Jodi Ito
Information Security Officer, ITS
jodi@hawaii.edu
956-2400

Agenda for Today

- Background Information
- Incident Overview & Response
- State Laws & UH Policies
- Mitigation Strategies
- Security Awareness

What is Data Leakage?

- 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 Personal Information

- Individual's first name or first initial 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;

What is 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...

Data Breaches

- Privacy Rights Clearinghouse
<http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP>
- Over 240 millions records containing sensitive information are involved in security breaches
- Educational Security Incidents:
<http://www.adamdodge.com/esi/>
Sept. 2008: 44,697

Booming Cyber Crime Industry

- Botnets: Rent-a-botnet
- SPAM generators
- \$\$\$ - Stolen sensitive information
- Organized crime involved
- TJX Data Breach: 45 million credit/debit cards stolen
- August 2008: Hacker ring charged with conspiracy, computer intrusion, fraud, & identity theft:
http://www.consumeraffairs.com/news04/2008/08/hacker_ring.html

Agenda for Today

- Background Information
- **Incident Overview & Response**
 - <http://kcc.hawaii.edu/object/idalerts.html>
- State Laws & UH Policies
- Mitigation Strategies
- Security Awareness

What happened?

- Compromised computer
- Did NOT store sensitive information
- BUT computer was used to access a server that contained sensitive information
- One particular malware's signature: searched for sensitive information and sent it to the Russian domain

Why it happened...

- Antivirus not active and not up-to-date
- Opened all email and attachments regardless of subject or legitimacy
- Connected to the server at the start of the work day without regard to need
- Stayed connected all day

What did we have to do?

- Investigation of the incident
 - Determine nature and scope of incident
- Breach notification
 - Notify all affected individuals
 - Setup website for public notification
 - Press release
- Report to Legislature
- Within 20 days of discovery!

Agenda for Today

- Background Information
- Incident Overview & Response
- **State Laws & UH Policies**
- Mitigation Strategies
- Security Awareness

Hawaii Revised Statutes (HRS)

- HRS 487J - SSN Protection
http://www.capitol.hawaii.gov/hrscurrent/Vol11_Ch0476-0490/HRS0487J/
- HRS 487N - Breach Disclosure
http://www.capitol.hawaii.gov/hrscurrent/Vol11_Ch0476-0490/HRS0487N/
- HRS 487R - Destruction of PI Records
http://www.capitol.hawaii.gov/hrscurrent/Vol11_Ch0476-0490/HRS0487R/

E2.214: Security and Protection of Sensitive Information

- <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

Data Handling @ UH

- Who has access to sensitive information?
 - Trustworthiness of individual?
 - UH General Confidentiality Notice - anyone handling sensitive information should sign (including RCUH employees, student employees, vendors, etc.)
(<http://www.hawaii.edu/ohr/docs/forms/uh92.pdf>)
- Who monitors access to sensitive information?

Data Handling - continued

- What controls are in place?
 - Are accounts being shared?
 - Are passwords secure?
(<http://www.hawaii.edu/askus/705>)
 - Are accounts left logged-in when you walk away from your computer?
 - When an employee leaves UH?
- Is sensitive information stored locally? And WHY?
 - Printed report, report saved as a .pdf document, email...?

Security for 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>
- Sensitive information must be protected
 - Encryption
 - Windows: <http://www.hawaii.edu/itsdocs/win/gswwindowsencryption.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 (Treas, Blackberry, iPhone, etc.)
 - Check w/ the manufacturer
 - Cell phones:
http://www.recellular.com/recycling/data_eraser/default.asp

Tools to Search for SSNs



*NOTE: These tools are not supported by ITS!
They are presented here for your information.*

- Cornell's Spider:
<http://www.cit.cornell.edu/security/tools/>
- UT Austin's SENS:
<http://www.utexas.edu/its/products/senf/>
- Virginia Tech's Find_SSN:
http://security.vt.edu/Find_SSNs/
- Will return false positives

Other Resources



- McAfee EPO - E-Policy Orchestrator
- Malware scanners (not validated by ITS - use with caution, results are not guaranteed, you may need to use other tools not listed here)
 - Combofix:
<http://www.bleepingcomputer.com/combobox/how-to-use-combox>
 - Ccleaner: <http://www.ccleaner.com/>
 - Malwarebytes: <http://www.malwarebytes.org/>
 - sdfix: <http://www.bleepingcomputer.com/files/sdfix.php>
 - (Note: AVAST! was mentioned during the session as being able to clean off Vundo: <http://www.avast.com>)

Laptop & Mobile Devices



- Use accounts & strong passwords
 - Check your password strength:
 - <http://www.securitystats.com/tools/password.php>
 - <http://www.microsoft.com/protect/yourself/password/checker.aspx>
- 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

Cyber "stuff" and YOU



- 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?



- Be aware!
- Practice safe computing
- Protect your computers & information:
 - 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
- Know the policy E2.214
- Educate those around you

Questions?

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

