Session #58

Computer Data-
Cracks and Leaks

Michele Iversen

U.S. Department of Education

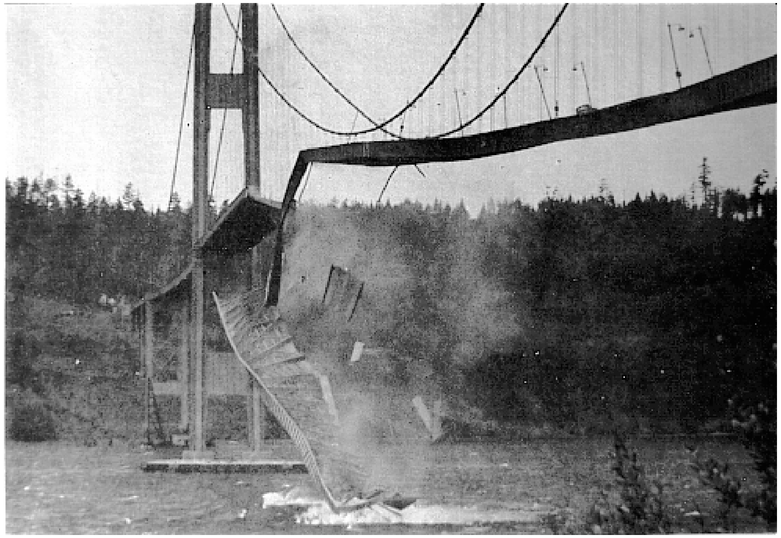
START HERE
GO FURTHER
FEDERAL STUDENT AID®

Cyber Security Landscape

- Networks upon networks
- Hierarchies of virtual and physical networks
- Range from tiny to large
- Many smart, small devices
- Highly interconnected
- Hybrid systems pervasive
- Sensor and control

Enormous Complexity

Engineering Challenges and Dangers

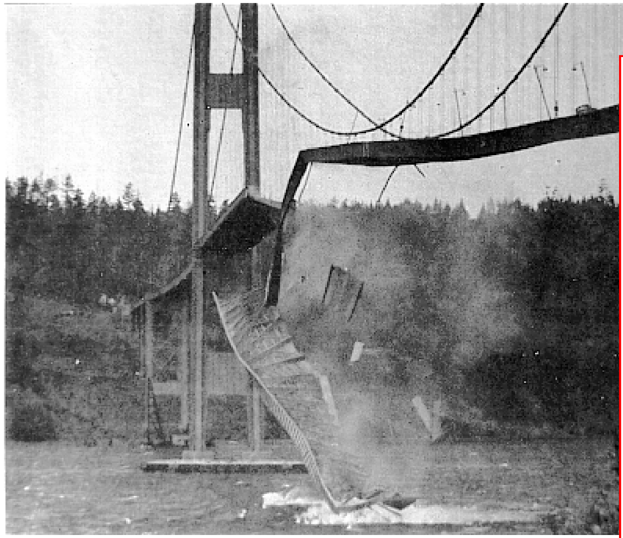


Many of the problems exhibited in today’s bridges are due to a lack of adequate pre-construction engineering—a combination of naivete among owners regarding design challenges and an unwillingness to provide the necessary financial resources.

Three days after the disaster a structural engineer discovered a significant change of the original design of the walkways. This design change would prove fatal.

Investigators concluded that the basic problem was a lack of proper communication. The architect failed to review the initial design thoroughly, and accepted the developer’s proposed plan without performing basic calculations that would have revealed its serious intrinsic flaws.

Engineering Challenges and Dangers



While it's unclear whether principal (
Leon Moisseiff, was aware of the pro
plaguing other new bridges, he argu
cost-cutting adjustments to the orig
design and against initiatives that w
detract from the bridge's appearanc

Many of the problems exhibited in to
bridges due to a lack of adequate pre-
constructio
naivete am
challenges and an unwillingness to provide
the necessary financial resources.

s after the disaster a structural
discovered a significant change of the
esign of the walkways. This design
ould prove fatal.

ors concluded that the basic problem
k of proper communication. In
the drawings prepared by the
architects were only preliminary sketches but
d
initial design thoroughly, and accepted the
developer's proposed plan without performing
basic calculations that would have revealed its
serious intrinsic flaws.

A single flaw can topple the entire system.

IT System Engineering Challenges and Dangers

- A broad spectrum of critical applications and infrastructure, from process control systems to commercial application products, depend on secure, reliable software

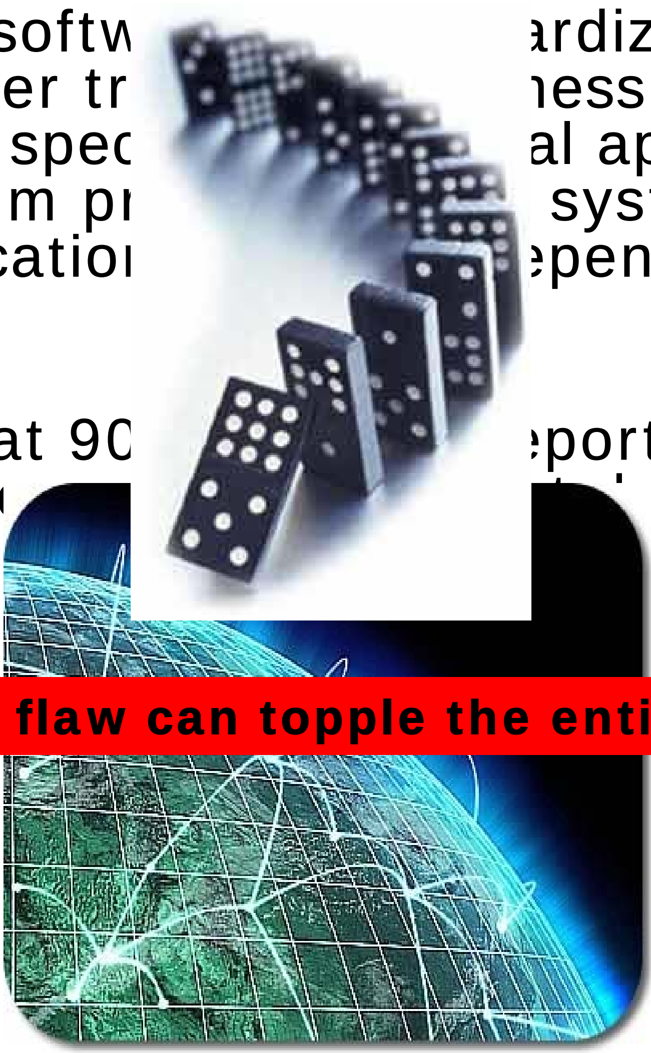
- Vulnerabilities in software can jeopardize intellectual property, consumer trust, and business operations and services

- It is estimated that 90 percent of reported security incidents result from exploits against defects in the design or code of software

IT System Engineering Challenges and Dangers

- Vulnerabilities in softw ardize intellectual property, consumer tr ness operations and services. A broad spec al applications and infrastructure, from pr systems to commercial applicatio epend on secure, reliable software.

- It is estimated that 90 eported security incidents result fr fects in the design or code of



A single flaw can topple the entire system.

Building Security Into the System

- **Information Systems Security Engineering must be an integral part of the System Engineering Lifecycle**
  - In the same manner that structural, safety and other types of specialties are utilized
  - To ensure Security Requirements are developed, maintained and achieved alongside other requirements, not as separate, parallel or follow on process
  - Failure to incorporate security requirements will result in marginalization of their importance or removal resulting in a less secure system
  - Implementing security controls at later stages is not as simple as ‘adding’ them to the architecture
  - Implementing security controls at later stages increase costs and risks

Where Do We Start?

- Improved Software Engineering Practices
  - CWE/SANS Top 25 Most Dangerous Software Errors - http://cwe.mitre.org/top25/#Listing
    - SQL injection is the means to steal the keys to the kingdom from data-rich software applications
    - OS command injection, is where the application interacts with the operating system
    - The classic buffer overflow still harmful after all these decades
    - Cross-site scripting is the bane of web applications
    - Missing Authentication for critical functionality
  - **Open Web Application Security Project – https://www.owasp.org/index.php/Main_Page**

Develop Resilient & Survivable Systems

- Systems must:
  - Degrade gracefully
  - Maintain security under attack
  - Recover securely from fall-back mode
  - In worst case: fail secure

Continuously Monitor for Vulnerabilities and Threat Activity

- Continuous monitoring is a risk management approach that maintains an accurate picture of an organization’s risk posture, provides visibility into assets, and leverages the use of automated feeds to quantify risk, ensure effectiveness of security controls, and implement prioritized remedies
  - Know what is on your network
  - Identify your sensitive data or the “crown jewels” and where it resides in the system
  - Conduct real-time automated monitoring and analysis through implementation of tools that use Security Content Automation Protocols
- Develop a robust threat analysis and awareness program

Through Integrated System Security Engineering We Can Build Safer Systems

...and minimize data cracks and leaks in the future.

Contact Information

We appreciate your feedback & comments.

Michele Iversen
Chief Information Security Officer

- Phone: 202-245-8287
- E-mail: Michele.Iversen@ed.gov

FSA 2011: Computer Data: Cracks & Leaks

Jodi Ito

Information Security Officer
Information Technology Services
jodi@hawaii.edu
(808) 956-2400

START HERE
GO FURTHER
FEDERAL STUDENT AID

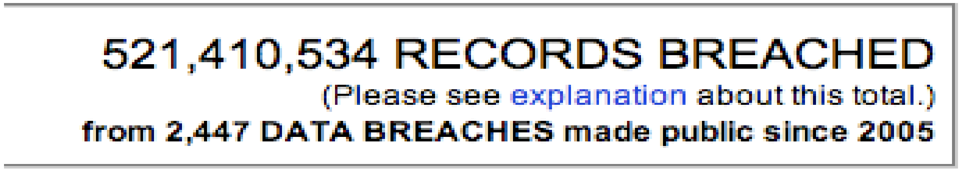
What happens after a data breach?

Today's Discussions

- Data Breach Background Information
- Mitigation Strategies
- Resources

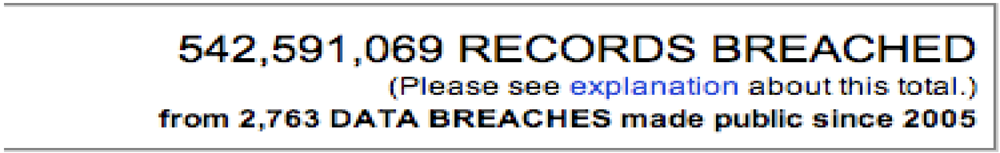
Data Breaches

- Privacy Rights Clearinghouse
  http://www.privacyrights.org/data-breach



521,410,534 RECORDS BREACHED
(Please see explanation about this total.)
from 2,447 DATA BREACHES made public since 2005

March 2011

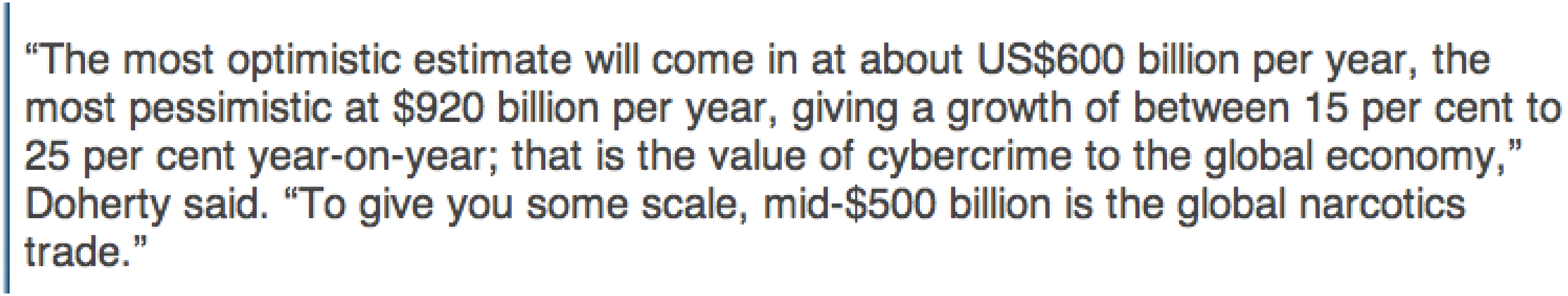


542,591,069 RECORDS BREACHED
(Please see explanation about this total.)
from 2,763 DATA BREACHES made public since 2005

Nov. 2011

- Educational Security Incidents:
  http://www.adamdodge.com/esi/

Cyber Crime Industry

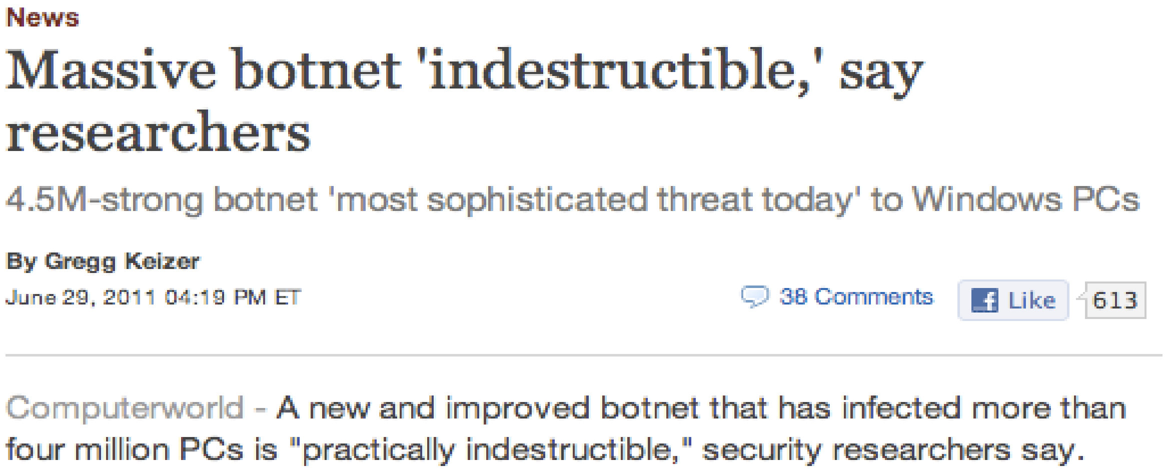


> "The most optimistic estimate will come in at about US$600 billion per year, the most pessimistic at $920 billion per year, giving a growth of between 15 per cent to 25 per cent year-on-year; that is the value of cybercrime to the global economy," Doherty said. "To give you some scale, mid-$500 billion is the global narcotics trade."

- Reported 2/2011
- http://www.itworldcanada.com/news/the-cybercrime-game-has-changed-symantec/142570

What do they do?

- Botnets: Rent-a-botnet



News

Massive botnet 'indestructible,' say researchers

4.5M-strong botnet 'most sophisticated threat today' to Windows PCs

By Gregg Keizer

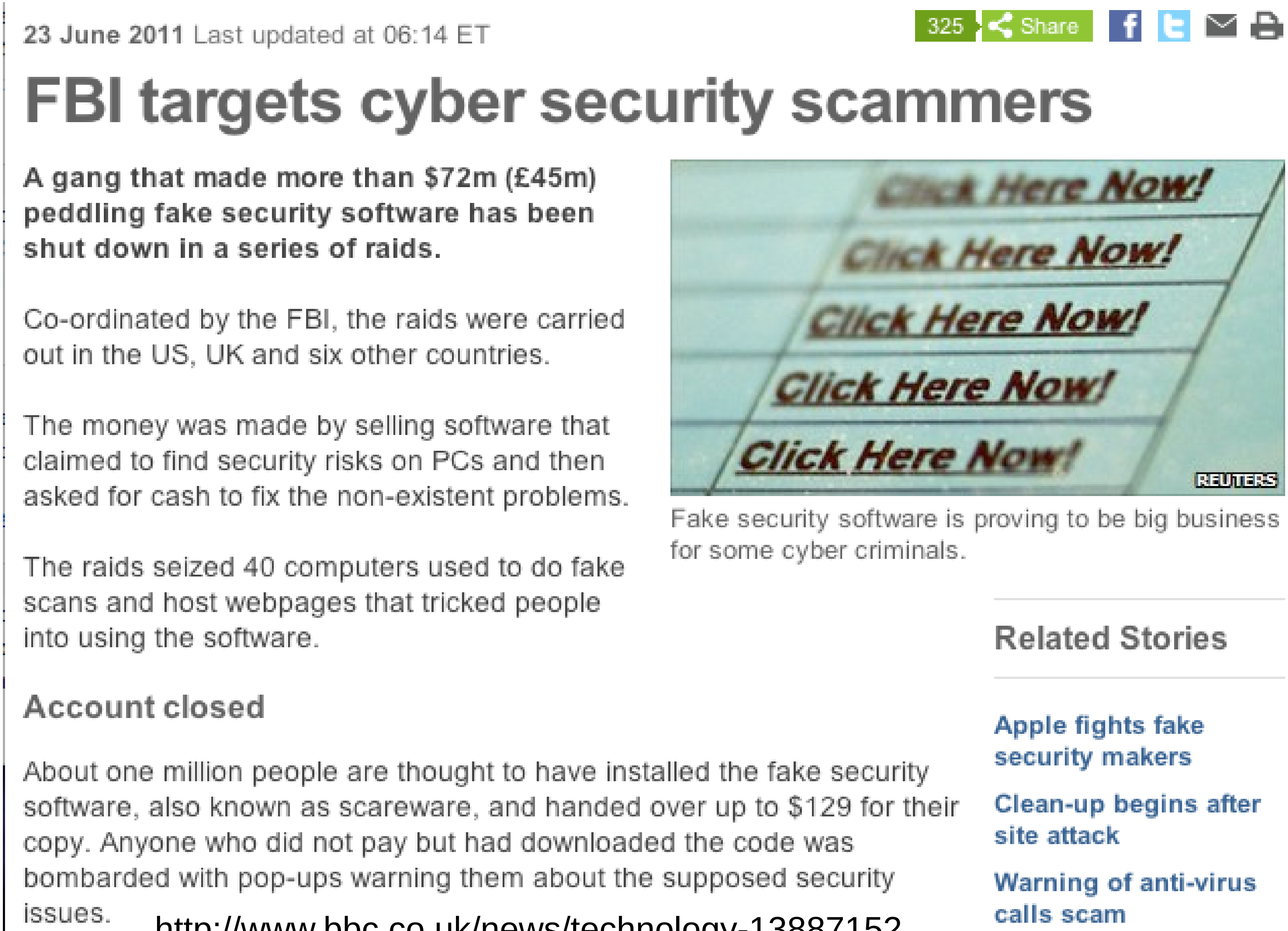
June 29, 2011 04:19 PM ET

Computerworld - A new and improved botnet that has infected more than four million PCs is "practically indestructible," security researchers say.

- SPAM generators (steal email accounts and passwords)
- $$$ - Stolen sensitive information

Underground Economy

- 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



23 June 2011 Last updated at 06:14 ET

FBI targets cyber security scammers

A gang that made more than $72m (£45m) peddling fake security software has been shut down in a series of raids.

Co-ordinated by the FBI, the raids were carried out in the US, UK and six other countries.

The money was made by selling software that claimed to find security risks on PCs and then asked for cash to fix the non-existent problems.

The raids seized 40 computers used to do fake scans and host webpages that tricked people into using the software.

Fake security software is proving to be big business for some cyber criminals.

Account closed

About one million people are thought to have installed the fake security software, also known as scareware, and handed over up to $129 for their copy. Anyone who did not pay but had downloaded the code was bombarded with pop-ups warning them about the supposed security issues.

Related Stories

Apple fights fake security makers

Clean-up begins after site attack

Warning of anti-virus calls scam

http://www.bbc.co.uk/news/technology-13887152

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)

State Laws & Federal Regulations

- Know what constitutes a data breach in your state
- As an example, for Hawaii:
  - 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 Sensitive Information:

- Personally Identifiable Information (PII)
  - Name, Address, SSN, DOB, etc.
- Examples of Sensitive Information:
  - Student Records (FERPA)
  - Health Information (HIPAA)
  - Personal Financial Information
  - Answers to “secret” questions
  - Confidential information & more…

If you suspect there has been a breach…..

Immediate Actions

- Notify your Information Technology Security Staff to assist with confirmation if a breach occurred
- Notify Senior Administrators & Legal Counsel
- Develop/follow data security incident response plan

Compliance with State & Federal Laws & Regulations

- Example: Hawaii Revised Statute 487N:
  - Written notification to all affected individuals
  - If a government agency, must submit a legislative report due 20 days after discovery of breach
  - If unable to notify all affected individuals, a substitute notice is required: Press Release/website

Other Actions

- For affected individuals:
  - Provide details on what happened and who was affected
  - Provide phone number for questions
  - Provide advice on how to protect themselves from identity theft
  - *Offer credit monitoring to affected individuals (individual institution’s decision)*

Remediation

- Work with IT staff to correct the problem and prevent it from happening again
- Ensure data is classified appropriately
- Ensure data is handled properly
- Educate faculty, staff, students on applicable policies & procedures
- Provide cyber security awareness training for everyone

EDUCAUSE Resources

- EDUCAUSE: http://www.educause.edu
- Higher Education Information Security Council: http://www.educause.edu/heisc
- Information Security Guide: https://wiki.internet2.edu/confluence/display/itsg2/Home

Incident Checklist

- New! (Draft version)
- https://wiki.internet2.edu/confluence/display/itsg2/Incident+Checklist

Data Incident Notification Toolkit

- https://wiki.internet2.edu/confluence/display/itsg2/Data+Incident+Notification+Toolkit
  - Notification Templates
  - Federal & State Legal Requirements
  - Sample Policies, Procedures, & Plans
  - Other links to helpful resources

Data Classification Toolkit

- https://wiki.internet2.edu/confluence/display/itsg2/Data+Classification+Toolkit
  - Determine Need
  - Determine Roles/Responsibilities
  - Determine Classification Process
  - Determine Impact on Process/Procedures

Contact Information

We appreciate your feedback & comments.

Jodi Ito
Information Security Officer

- Phone: 808-956-2400

- E-mail: Jodi@hawaii.edu

START HERE
GO FURTHER
FEDERAL STUDENT AID