

Session #59

Protecting Students' Information from Unauthorized Access

Danny Harris, PhD
U.S. Department of Education



START HERE
GO FURTHER
FEDERAL STUDENT AID®

Defining the Terms

- **Data Breach** – Includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, access for an unauthorized purpose, or other unauthorized access to data, whether physical or electronic
- **Personally Identifiable Information (PII)**
 - Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
 - OMB Memorandum 06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, dated July 12, 2006

Data Breaches in the News...



“Sony Pictures breach confirmed to be authentic; Sony launches investigation”

-A Sony website was breached allowing access to personal information belonging to over 1 million Sony customers.

– *June 2011, October 2011*



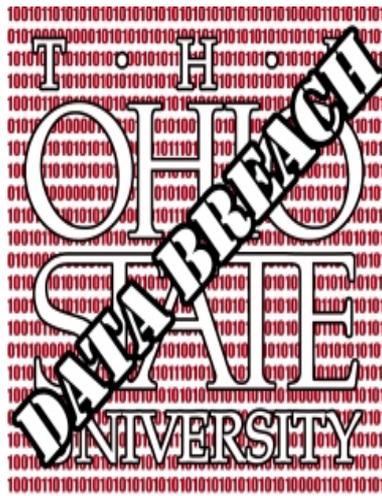
“Gmail Accounts Compromised by Chinese Hackers, Google Says”

- Chinese hackers have infiltrated Google's Gmail system and broken into hundreds of accounts, including those of senior government officials, military personnel and political activists, the company said.

– *June 2011*



...In Education



“Hacked: Data breach costly for Ohio State, victims of compromised info - Breach affects 760,000 people, expected to cost university \$4 million.”

-December 2010



Personal information exposed in a data security breach where a hacker was able to access the Huskydirect.com customer database affecting +18K records.

-January 2011



Private financial information belonging to as many as 5,000 college students was open for viewing on a federal government student loan website in recent weeks, according to a senior Department of Education staff member.

- October 2011



START HERE
GO FURTHER
FEDERAL STUDENT AID

Breaches by Educational Institutions

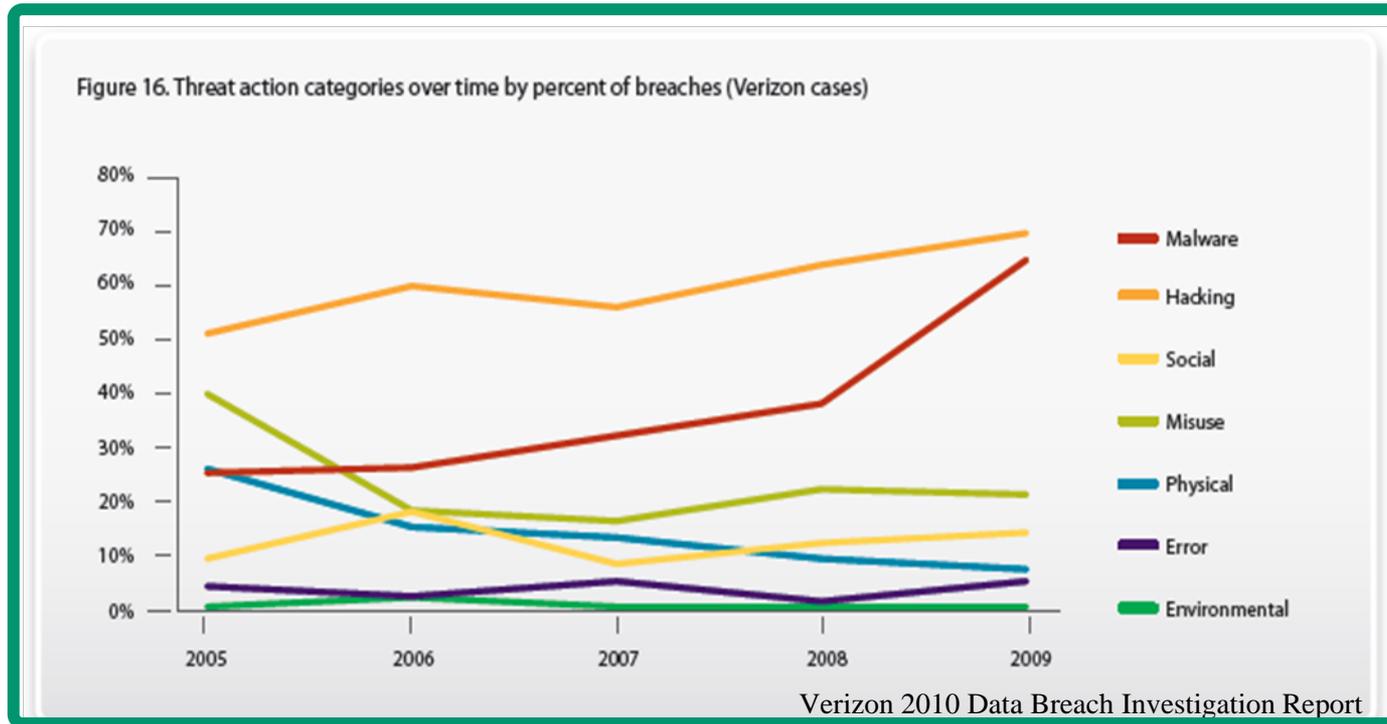
All varieties: hacking, loss of portable device, unintentional, insider breach, etc.

Year	Number of Breaches	Number of Records
2005	64	1,886,841
2006	102	2,016,119
2007	107	791,938
2008	103	1,107,001
2009	71	1,062,275
2010	73	1,588,698
2011 estimated	50	388,515



Source: Privacy Rights Clearinghouse, July 2011.

Facts About Intrusions



WHO IS BEHIND DATA BREACHES?

- 48% were caused by insiders
- 11% implicated business partners

WHAT COMMONALITIES EXIST?

- 85% of attacks were not considered highly difficult
- 61% were discovered by a third party
- 86% of victims had evidence of the breach in their log files
- 96% of breaches were avoidable through simple or intermediate controls



What's at Risk?

- **Identity theft**
 - The FTC estimates that as many as 9 million Americans have their identities stolen each year
 - Victims can spend hundreds of dollars and significant time to repair their good name and credit record
- **Business and financial security**
 - Trust and confidence in the market place and U.S. companies
 - Data breaches are hemorrhaging U.S. research which has given us an economic and military advantage in the past
- **Social interactions and norms**
 - Adults and children are willing to share information with people they don't know
 - Not all social media sites protect information and privacy with the same sincerity
 - 49% of teens who use social networking websites use it to make friends with people they don't know
 - 32% of teens have experienced some type of harassment online
- **Cyber stalking - a technologically-based "attack" on one person who has been targeted specifically for that attack for reasons of anger, revenge, or control. It can take many forms, including:**
 - Harassment, embarrassment, and humiliation of the victim
 - Emptying bank accounts or other economic control such as ruining the victim's credit score
 - Harassing family, friends, and employers to isolate the victim
 - Scare tactics to instill fear and more



What are we Doing?

Office of the Chief Information Officer Privacy Support Initiatives

Current:

- Hired a New Chief Information Security Officer
- Established Robust multi-factor authentication for internal and external authentication
- Enhanced continuous monitoring program enabling real-time automated auditing
- Deployed full disk encryption for mobile devices
- Significantly enhanced our Cyber Security Awareness Program
- Partnered with the Chief Privacy Officer and Privacy Technical Assistance Center to make Security Program more holistic

Planned:

- Improve systems engineering processes to build security into the system at design
- Implement data loss prevention tools to enforce information sharing policies and prevent inadvertent disclosure
- Establish a Mobile Device Management Strategy

What Can You Do?

The Joy of Tech™

by Nitrozac & Snaggy



©2007 Geek Culture

joyoftech.com

Signs of the social networking times.



STAIR HERE
GO FURTHER
FEDERAL STUDENT AID

Implement– Multi-Factor Authentication (MFA)



1. If you have remote access users, MFA should be a high priority capability
2. MFA should support web applications and should not require client-side software
3. When interfacing with federal agencies ensure identification and authentication mechanisms are compliant with NIST, FIPS, and other federal standards
4. Support the National Strategy for Trusted Identities in Cyberspace



START HERE
GO FURTHER
FEDERAL STUDENT AID®



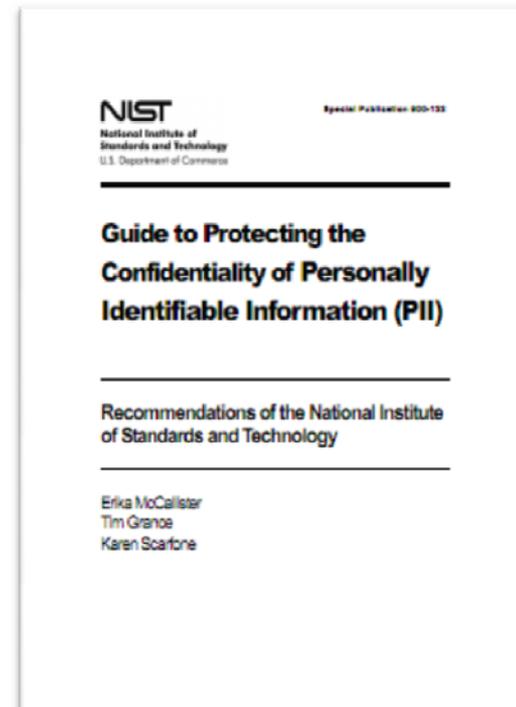
Deploy Best Practices – Network & System Security

- **Use a firewall.** A well configured firewall keeps criminals out and sensitive data in
- **Install and maintain anti-virus software.** Computer viruses can steal and corrupt your privacy data. Install good anti-virus software on all your computers, and make sure it stays up-to-date
- **Install and maintain anti-spyware software.** Like viruses, spyware can compromise privacy data. If kept up to date, a good anti-spyware program will protect you from most of it
- **Use spam filters.** Spam can carry malicious software and phishing scams, some aimed directly at a state agency or school. A good spam filter will block most of it and will make your email system safer and easier to use
- **Set your software to auto-update, or make sure to download and install the updates yourself regularly.** Updates to your operating system and custom software often close serious security gaps
- **Build Security In.** Developers should use emerging tools, rules, guidelines and security practitioners to build security into software in every phase of its development



Employ Best Practices – NIST Selected PII Security Controls

- Access Enforcement (ACLs, RBACs, encryption)
- Separation of Duties
- **Least Privilege** (read, write, edit)
- Remote Access (limit or deny)
- Access Control for Mobile Devices (deny or limit)
- **Auditable events and Audit Reviews (policy that monitors certain events)**
- Identification and Authentication
- Media Access, Marking, Storage, Transport, and Sanitization.
- Transmission Confidentiality (encryption)
- **Protection of Information at Rest**
- Information System Monitoring (automated tools to detect suspicious transfers)



**NIST Special Pub 800-122
Guide to Protecting the
Confidentiality of Personally
Identifiable Information,**

Contact Information

We appreciate your feedback & comments.

Danny Harris, PhD
Chief Information Officer

- E-mail: Danny.Harris@ed.gov



START HERE
GO FURTHER
FEDERAL STUDENT AID®

Session # 59

Protecting Student's Information From Unauthorized Access

Sheila Colclasure
Global Public Policy & Privacy Officer
Axiom Corporation



START HERE
GO FURTHER
FEDERAL STUDENT AID®

Data is Gold



The News!

“...vast data gathering...used to discriminate in the services that companies offer customers or government agencies offer citizens.”

“the wall has been breached’ between what users share under their real identity online and what information they provide under the cover of anonymity.”

“...growing concern on Capitol Hill about the ability of organizations to keep data secure.”

"It is technically impossible for Yahoo! to be aware of all software or files that may be installed on a user's computer when they visit our site," Anne Toth, Yahoo's vice president of global policy and head of privacy, wrote to U.S. Reps. Edward Markey (D-Mass.) and Joe Barton (R-Texas)."

“Mr. Markey said he wasn't satisfied that "consumers are able to effectively shield their personal Internet habits and private information from the prying eyes of online data gatherers.”

“...the analytical skill of data handlers...is transforming the Internet into a place where people are becoming anonymous in name only.”



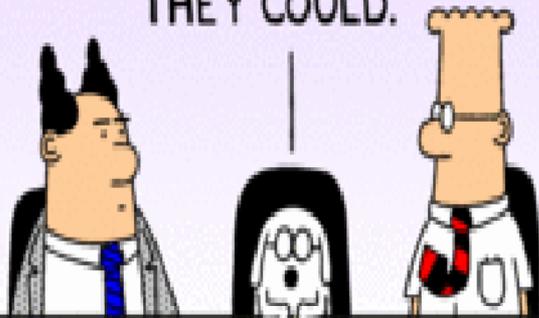
DOGBERT CONSULTS

CUSTOMER DATA
IS AN ASSET THAT
YOU CAN SELL.



Dilbert.com DilbertCartoonist@gmail.com

IT'S TOTALLY
ETHICAL BECAUSE
OUR CUSTOMERS
WOULD DO THE SAME
THING TO US IF
THEY COULD.



10-13-10 © 2010 Scott Adams, Inc./Dist. by UFS, Inc.

IN PHASE
SOUNDS FAIR. ONE, WE'LL
DEHUMANIZE
THE ENEMY BY
CALLING THEM
"DATA."



OVER-ARCHING CONCERN...CONSUMER ATTITUDES

- Privacy is an emotionally charged issue
 - Being watched, monitored, taken advantage of
- Consumers feel like they are losing control
- Consumers don't understand our information based economy
 - Information technology is part of our economic infrastructure
 - Benefits are not fully understood by consumers or law makers
 - Technology used often “unappreciated” by consumers



Drivers and Trends

- Riskier World
 - Scams (Phishing & Fraud)
 - **Identity Theft**
- New Data Intensive Technologies
 - Collecting Too Much Data
 - Data Collection Not Obvious to Consumer
 - Blurring of Anonymous versus Personal
 - Too Much is Unregulated
- Surveillance Society
 - Private Sector
 - Government
 - Very Aggressive



Awareness

• Privacy & American Business Survey

- 64% decided not to use a site because they weren't sure how data would be used
- 67% decided not to register or shop at a website because they found their privacy policy too complicated or unclear
- **20% responded yes when asked if they have personally been a victim of ID fraud or theft**
- 87% of consumers have read or heard about personal data being stolen
- 78% of consumers feel they have lost all control over how personal information is collected and used
- 50% believe government does not handle personal information in a proper way
- **34% of consumers are Privacy Fundamentalists**

Surveillance Society...

Placefulness

Apps

Collecting even "private" data, little governance, little enforcement...lots of secondary commercialization

Device Fingerprint

Capture device data points, formulates "fingerprint," spoofable, not "categorized" as pii...yet used that way

The Internet of Things...

Precise GeoLocation

Multiplied by time; checking in

eHealth & HITECH

Relies on the Cloud, devices monitor, report back

HTML5

Offers even more tracking & collection, utilizes the Cloud

Meters

Ride the pipes, capturing and closing the loop on every data point- digital dust, digital exhaust related to digital device

Sniffers and Listeners

Sit on networks, watch traffic, sniff out brands and..."listen"

DOGBERT CONSULTS

YOUR CUSTOMER
DATA IS WORTH
A FORTUNE.



Dilbert.com DilbertCartoonist@gmail.com

I'LL FIND
YOU SOME
BUYERS IF
YOU GIVE
ME 25%.

WHAT
ABOUT
PRIVACY?



10-12-10 © 2010 Scott Adams, Inc./Dist. by UFS, Inc.

THAT'S NOT A
PROBLEM. I NEVER
USE MY REAL
NAME.



Protecting Data - Common Misconceptions

It's only about hackers and external intrusion

Truth: It is about all types of breaches, not just external intrusion – hackers are only a part of the problem

It's all about identity theft

Truth: Most breaches don't result in identity theft

This is just an IT security issue

Truth: System security is necessary, but not sufficient

This is just a legal issue

Truth: It's much, much broader and affects every division of the organization

More Common Misconceptions

I'm probably OK not having a Data Breach Response Plan

Truth: If you wait until you need one, it's too late and can cost you tens of millions of dollars; not knowing does not equal OK

I don't have Social Security or credit card numbers, so I am probably ok

Truth: ** It's about ANY data that identifies an individual**

It's all changing, I'll just wait until it is clear

Truth: Law and public opinion are formed and getting more punitive today (actions today may result in long-term consequences)

This will go away

Truth: The problem for organizations is escalating as data dependency and collection increase

Costs

- Direct and Indirect impact on Organizations: stock price, notification costs, fines, lawsuits, customers, broken trust, damaged brand image
 - TJX Breach (parent company of T.J. Maxx, Marshalls, HomeGoods) absorbed **\$168 million** charge related to their massive security breach (Source: Erik Shuman, Store Front Back Talk, August 15, 2007)
 - ChoicePoint FTC Consent Decree – spent \$43 million to get Consent Decree inked (\$15mm fine/negotiations)
 - Eli Lilly spent 3 record in violation – spent \$18 million to ink Consent Decree
- Average cost of **\$210 per record breached**

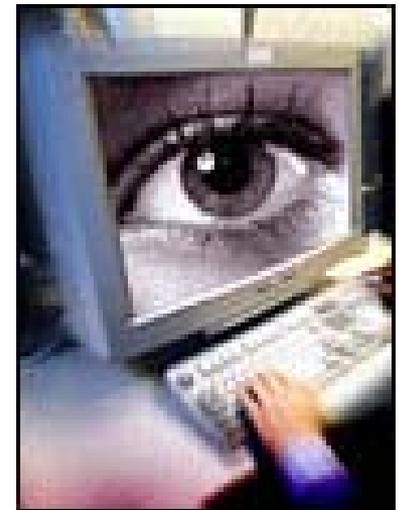
Case Studies

- **TJX Breach**
 - Laptop computer intercepted and decoded data streaming between hand-held price-checking devices, cash registers and the store's computers. Little or no firewalls.
 - USB drives, loaded with software, were physically installed onto “Work Application Kiosks” to tap into their network.
- **POS Payment Systems**
 - No touch/contact-less payment systems probed wirelessly for payment tag in close proximity, then use that info to crack secret cryptographic key on tag and charge purchases to the tag owner's account.
- **Certegy Check Services**
 - Inside job: A Senior Database administrator removed the information from Certegy's facility via physical processes: not electronic transmission.
- **Call center audio file security**
 - Outsourced companies that review tapes for customer service purposes can access credit card information, SSN, home address, etc to be resold to identity thieves
- **Boston Globe**
 - Used old paper account docs to label bundles for distribution pickup

Identity Theft

Identity theft is a crime of stealing key pieces of someone's identifying information, such as:

- Name/address,
- Social Security Number
- Date of Birth
- Mother's Maiden
- Driver's License #
- Other.....!!!



How Identity Theft Occurs

Identity thieves...

- Social Engineering: pose fraudulently as someone else to get information
- steal business or personnel records at workplace
- **buy personal info from “inside sources”**
- Key Stroke Logging
- “shoulder surf” at ATMs and telephones.
- steal wallets and purses containing ID/ steal mail
- complete false “change of address” forms
- rummage through trash (“dumpster diving”)
- *Getting more creative every day!*



How Identity Thieves Use Information

- Change mailing addresses on credit card accounts
- Open new credit card accounts
- Establish phone or wireless service in victims name
- Open new bank accounts and write bad checks
- File for bankruptcy under victims' name
- Counterfeit checks or debit cards
- Buy and take out car loans in victims name
- Get Arrested under victims' name
- Receive medical care under victim's name



Protecting Student Information = Business Culture

Protecting Student Information is not just for IT folks to worry about

Protecting Student Information is a requirement for a trusted relationship with your stakeholders

A way to minimize reputation risk and protect your brand

A component of your business culture

Security risks evolve over time – if your practices aren't changing you aren't keeping up with new risks

Make your employees aware of risks, responsibilities, consequences

Sensitize employees to watch for bad behavior

To Do's

Have an effective Data Governance Plan

- Assess needs and purposes
- The more you collect, the greater your fiduciary duty
- Don't keep what you don't need
- Regularly monitor compliance

Have an effective Security Incident Response Plan

- Question of "when," not "if"
- Assess technical, physical & administrative vulnerabilities
- Address them
- Understand your obligations in the event of a breach
- Have it in writing and keep it up to date



Seven Rules to Live By

1. You have more sensitive information than you think you have.
2. Data in transit is data at risk: digital, paper, tape, disc
3. Employees are your greatest risk
4. Vendors are your second greatest risk
5. Over-react if you have a security breach
6. Be helpful to stakeholders if you have to give them notice of a breach
7. Learn from the marketplace



Building Trust Into Your Brand



Contact Information

We appreciate your feedback & comments.

Sheila Colclasure

Global Public Policy & Privacy Officer

- E-mail: Sheila.Colclasure@acxiom.com