

# **MOBILE DEVICES**

**Into the Breach - Will the  
Data Breach Laws Save You  
in a Massive Attack?**

**RMIMA**

**August 19, 2011**

**Lucy Thomson, Esq., CSC**

**Jennifer Kurtz, Regis University**

# Mobile Devices Heightened Risk of Data Breaches?

“Smartphones have overtaken laptops as the mobile device of choice for large businesses, while security remains a key issue for IT managers.

According to a survey of 100 UK companies by Good Technology, the number of consumer devices entering the workplace has doubled in six months, while 42 per cent of IT managers claim to have seen to [sic] unauthorized consumer devices cause data breaches.”

-- SC Magazine      August 03, 2011

# Top Threats 2011

## Mark Underwood/Tech Republic

1. Insider Threats
2. Tool Bloat Backlash
3. **Mobile Device Security**
4. Low Tech Threats
5. Risk Management Prioritizing
6. SLA Litigation – Promises, promises
7. Treacheries of Scale – All eggs in one cloudy basket

# Top Risks 2011 – Higher Ed Schuman/Franklin and Marshall College

- 1. So many mobile devices, so much risk**
2. Viruses spreading through social media
3. Virtualization--from desktops to servers
- 4. Embedded devices become the norm**
- 5. Consumerization of IT**

SOURCE: <http://campustechnology.com/Articles/2011/01/12/Higher-Education-Top-Five-Network-Security-Threats-for-2011.aspx?Page=1>

See: VIDEO FOR HW TROJANS EMBEDDED <http://koresecure.com/>

# Top Threats 2011

## Stonesoft/Tech Journal

- 1. An Apple OS targeted virus**
2. Increased malware attacks for social media
3. Political cyber warfare
4. Social engineering against the enterprise
5. Stuxnet-like attack proliferation
- 6. Smartphone takes center stage**
7. Viruses become more sophisticated
8. Advanced evasion techniques will grow if ignored by the network security vendor community

SOURCE: <http://www.techjournalssouth.com/2011/01/stonesoft-identifies-top-eight-it-security-threats-for-2011/>

# Digital Risks

- Aggregated information
  - Electronic health records
  - Tax, financial, legal records
- Organizational change
  - Organizations recently involved in merger/acquisition or restructuring
- Cloud computing (e.g., Google Docs, March 2010; Sony Playstation via EC2, April 2011)
- **Mobile devices**
- P2P technology

# Data Breach Laws

- Fulfill “duty to warn” as in “hazardous to your health” statements
- Requirements differ among states
- Health Information Technology for Economic and Clinical Health (HITECH) Act passed in 2009
- Require notification – some states require security
- Legislation for national data breach notification law reintroduced to Congress in June 2011; last big push for national legislation was 2009
- White House cyber security policy letter to Congress (May 12, 2011)

# Data Breach Ambiguities

- 1 What is a “breach”?
- 2 Must the breach result in harm?
  - How do we assess harm?
- 3 When does the encryption safe harbor apply?
- 4 What encryption is sufficient?
- 5 What general security requirements are contained in some data breach laws?



# U.S. Data Breach Notification Statutory Requirements

- Data breach laws cover sensitive information likely to be used for identity theft or fraud
  - Name + one or more personal identifiers (SSN, driver's license number, financial account or credit card number, other) (vary by state)
  - HITECH – “unsecured protected health information”
- Triggering event
  - Any breach of security (some states)
  - Breach with reasonable likelihood of harm (other states)
- Obligations on breach
  - Notify persons whose information was compromised
  - Notify state enforcement agencies (some states)
  - Notify credit agencies (some states)

# Data Breach Reporting Requirements

- Who must be notified?
- When must notification be provided?
  - Likelihood of harm
  - Exemptions for encrypted data and “good faith”
- Form of notice
- Substitute notice options

# Some State Breach Laws Include Security Requirements

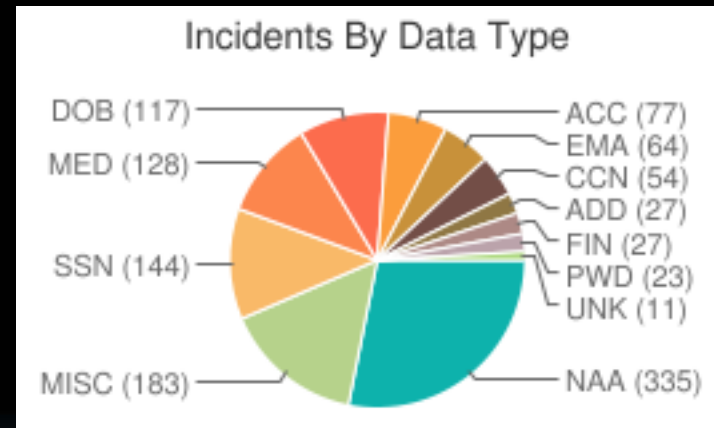
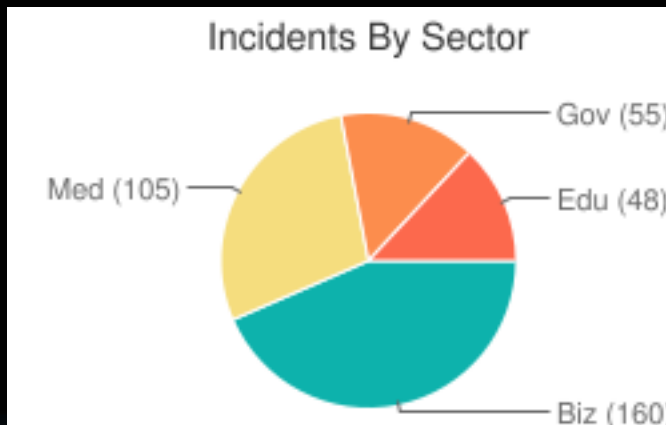
- *California* – data custodian must implement reasonable security procedures and practices
- *Massachusetts* – businesses must develop a comprehensive information security program
- *Maryland* – requires reasonable security procedures
- *New Jersey* – limits disclosure and transmission of SSN over the Internet
- *Nevada* – covers any personal customer information and requires businesses to encrypt all transmissions



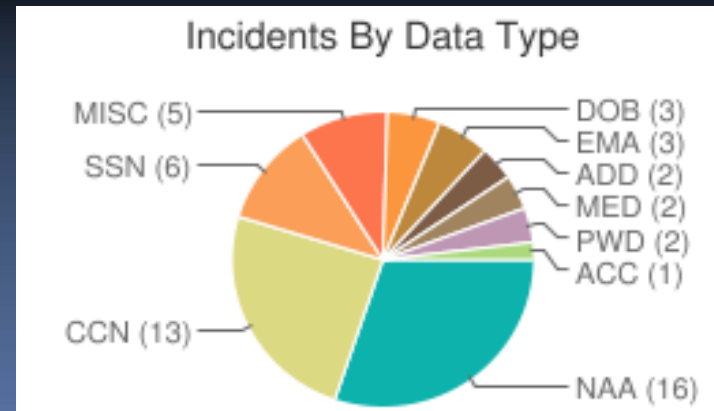
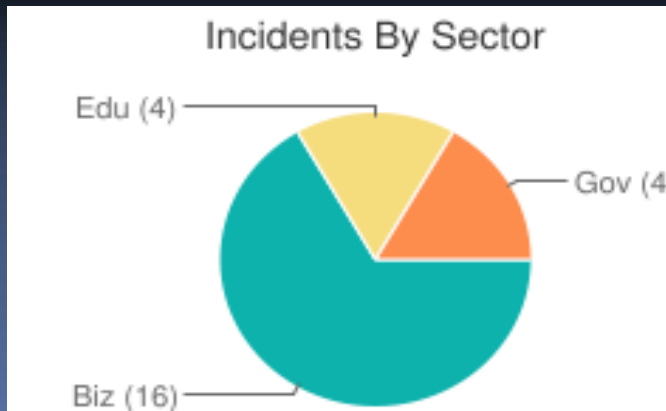
# Data Breach Trends by Sector/Data Type

369 Incidents = 126,749,634 Records vs. 22 Incidents = 232,063 Records

2011  
YTD



2001



# Out-of-Controls

Organization	Breach Announcement	Records Breached
Sony Playstation	April 2011	77,000,000+
Education Credit Management	March 2010	3,300,000
Netflix	January 2010	100,000,000
Heartland	January 2009	30,000,000
Hannaford	February 2008	4,200,000
TJX	June 2007	45,600,000
Veterans Administration	March 2006	26,500,000

# Breaches Involving Mobile Devices

Date	Company	Records Breached	Lost/ Stolen Devices
March 2010	Educational Credit Mgt. Co.	3,300,000	Portable media device stolen
February 2011	Jacobi Medical Center, Bronx NY	1,700,000	Computer backup tapes stolen
November 2009	Health Net, CT	1,500,000	Portable hard drive lost
October 2009	BlueCross BlueShield, TN	1,000,000	Hard drives missing
September 2009	Oklahoma Dept. Human Services	1,000,000	Computer stolen
October 2009	BlueCross BlueShield Association – Highmark	850,000	Laptop stolen
April 2011	Eisenhower Medical Center, CA	514,000	Computer stolen
March 2011	Cord Blood Registry	300,000	Backup tapes stolen
April 2011	Mid-State Medical Center, CT	93,500	Hard drives lost
February 2011	St. Francis Hospital, OK	84,000	Computer
September 2009	Naval Hospital Pensacola, FL	38,000	Laptop lost
January 2011	KBR Construction	many	Laptop stolen
January 2011	Tulane University	10,000	Laptop stolen

Source: Identity Theft Resource Center, <http://www.idtheftcenter.org>

# Encryption – A Safe Harbor?

- Almost 50 % of the breach notification statutes provide *no definition of encryption whatsoever*.

They simply require notice only if the stolen data is “unencrypted” or “not encrypted”

The other 50 % use *varying definitions of encryption*—

- An algorithmic process that renders the data unreadable or unusable
- An algorithmic process that results in a low probability of assigning meaning to the data
- A 128 bit or greater algorithmic process that results in a low probability of assigning meaning to the data
- Another method that renders data unreadable or unusable
- A method specified by a regulator

# Encryption in HITECH

HITECH requires notification in the event of a breach of “unsecured protected health information”

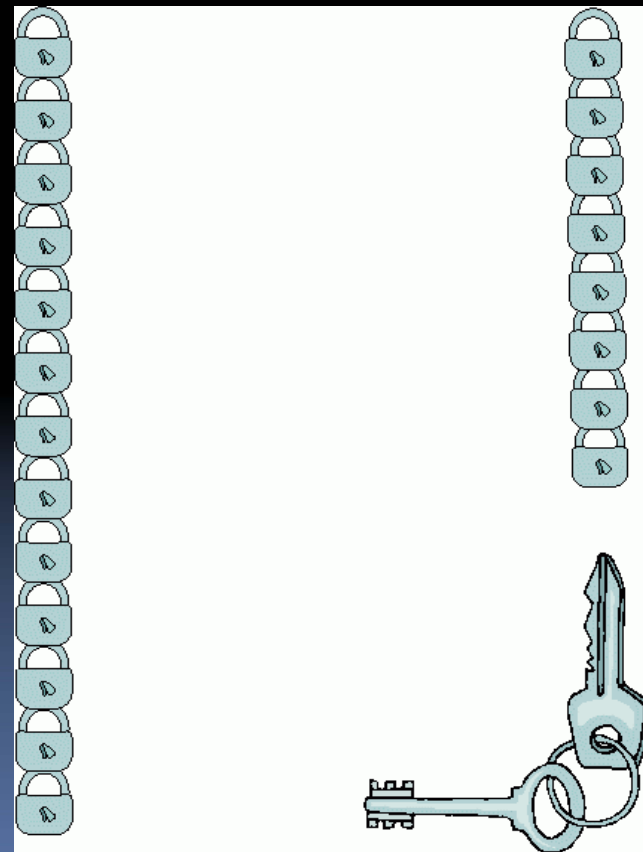
- NIST 800-111 for Data-at-Rest – Requires IT Managed Full Disk Encryption
  - Unsecured PHI is .. PHI not secured by a “technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.”

# When Is Encryption Not a Safe Harbor?

- **Encryption Keys**

If the encryption key is compromised the protection is lost

- **Security Lapses**



# Porous Network Boundaries – E-mail

- E-mail remains the number one source of leaks of proprietary or confidential information in the enterprise
- 48 % of companies surveyed perform regular audits of outbound email content
- 36 % of companies surveyed reported business impact due to exposure of sensitive or embarrassing information in the last 12 months
- 22 % of companies surveyed investigated information exposure via lost or stolen mobile devices
- 50 % of companies surveyed disciplined an employee for violating e-mail policies
- Employee e-mail was subpoenaed in 20 % of the companies surveyed, especially larger companies
- 54 % of reporting companies with more than 20,000 employees were ordered to produce employee e-mail

# Porous Network Boundaries – Social Networking and Employee Churn

- Results show increasing concern and investigations of data leaks through blogs and social networking sites among companies interviewed
- Approximately 25 % increase from 2009 survey in number of companies interviewed that are “highly concerned” about Web-based short messaging (e.g., Twitter)
- Budget constraints and increasing number of layoffs in surveyed companies have caused more concern about the risk of data leakage
- More companies investigated suspect leak or theft of confidential or proprietary information associated with employee leaving, whether voluntarily or not

# Encrypted Records

## Recent Breaches

### Sony PlayStation

#### Breach 1 – Mid-April, 2011

- What happened? Attack on the PlayStation Network
- Records breached – Personal information of 24.6 million account holders
- Encryption? Customer credit card numbers database
- Unencrypted PII? Database with payment card numbers and expiration dates

#### Breach 2 – Late April, 2011

- What happened? Sony said hackers exploited a “known security vulnerability.” Hacker group Lutzsec said it accessed SonyPictures.com with an SQL injection
- Records breached – Lots of personal information in 77 million accounts
- Users exposed to ID theft; phishing attacks; hijacked e-mail
- Letter to State AGs – State law violations?
- Indirect costs – Banks replaced 100 million payment cards

# Federal Trade Commission

- Twitter investigations (2009-2010, 2011)
  - 2009, 2010, 2011 hacking attacks
  - Compromised user account control
  - President Obama
  - Fox News
  - Published password exploits, false news, defaced PayPal UK ...

## FTC findings

- Misled users about privacy protection policy
- Barred from doing it again for 20 years (?)
- Submit to audit every two years for 10 years
- Antitrust practices – active investigation

# Federal Trade Commission

- Google investigations (2010, 2011)
  - Default Gmail account information sharing with GoogleBuzz
  - Formal complaints from Electronic Privacy Information Center (EPIC) in 2010
  - Antitrust practices – active investigation

## FTC findings

- Submit to privacy audit every two years for 20 years
- Adopt stringent privacy rules
- Facebook investigations
  - Privacy violations – sharing Facebook IDs with advertisers through apps (e.g., Farmville, Angry Birds)
- Should users be forced to connect securely?

# Performance Improvements

- Fix known vulnerabilities
- Monitor and protect storage media
- Restraint personally identifiable data collection and retention
- Dispose and destroy storage media responsibly
- Observe aberrant precursor behavior among high-risk and highly privileged insiders
- Inform data users about social engineering tactics

# Data Governance Policy Components

- Objectives, roles, responsibilities
- Scope with respect to users (staff, contractors, third parties)
- Treatment: labeling (classification), retrieval, ensured availability (i.e., sensitivity to media or application obsolescence), backup and recovery, transmittal, distribution, disposal, destruction
- Incident response
  - Policies and procedures, objectives, roles and responsibilities, training, testing
  - Handling, monitoring, reporting, investigation and analysis, corrective action

# Portable Media/Device Policy – HITECH Today

1. Inventory use of portable devices/media across All areas
2. Examine ALL avenues of product acquisition, use, disposal
3. Understand the data flow on/off each device type
4. Develop an audit plan and gather stats re amount and type of data devices being used within organization
5. Develop a policy
6. Educate ALL users on policy and organizational expectations

# Portable Media/Device Policy(cont'd)

7. Layer security controls
  - Hard disk encryption – whole disk or selective?
  - HW- or SW-based encryption?
  - SW-based USB drives may require user administrative rights. Location security implications?
8. Investigate end-point security controls
  - Restrict computer USB ports to white-listed devices
9. Educate workforce on secure device acquisition and compliance enforcement
10. With end-point controls in audit mode, monitor USB device activity

# Data Protection Considerations

- Choices for hiding information
  - Stored securely (isolated, offline, physical protection)
  - Hidden entirely or disguised as something else
  - Encrypted
- Hardware vs. software encryption
- Weak links
  - Inconsistent security policies, rules, and procedures among different organizations, environments, interfaces
  - Programming shortcuts, as in RSA's SecurId (a random number used consistently is an oxymoron)

# Extrusion Prevention Strategies

- Approximately 33 % of responding companies employ staff to review outbound email
- Almost one-half of companies perform regular audits of outbound email content
- Technology-based solutions to screen email for healthcare, identity, or financial info are increasing
- Other potential data loss channels (e.g., FTP sites, mobile devices, storage media, P2P networks) are also receiving increased attention

# Extrusion Prevention Strategies (cont'd)

- Technology-based
  - Content-aware and policy-based encryption
  - 65 % of responding companies have deployed technology to detect spam or malware in outbound messages overall, with 85 % of large companies (20,000+ employees) using such technology
- Policy-based
  - Over 79 % reported audit vulnerability scanning policy
  - Majority surveyed explicitly prohibit P2P file-sharing sites
  - ~ 50 % explicitly prohibit use of social networking, media sharing, short messaging services
  - >33 % of responding companies prohibit personal use of corporate email, web, and personal email

# Performance Improvements Action Plan

1. Conduct a risk assessment
2. Develop comprehensive information security plan
3. Develop data retention and destruction plan
4. Protect all data in all data modes
5. Match the encryption solution to the risk
6. Use data classification to minimize overprotection and under-protection
7. Validate encryption capabilities for compliance
8. Implement key management best practices
9. Analyze audit logs regularly for high-level anomalies

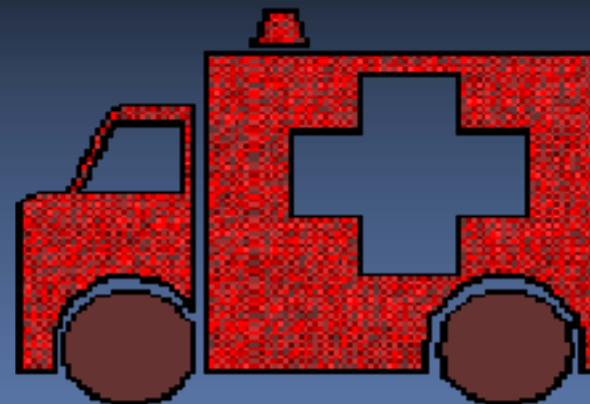
# HITECH – HHS Guidance Relies on NIST

HHS HITECH April 2009 Guidance provides:

“Encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard:

(i) Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices.*”

[more]



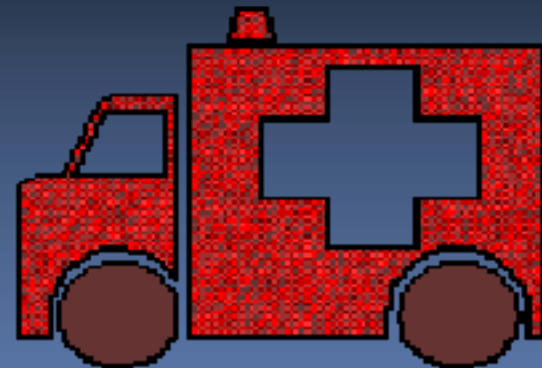
# HITECH – HHS Guidance Relies on NIST

HHS HITECH April 2009 Guidance provides:

“Encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard:

(i) Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices.*”

[more]



# HITECH Guidance Focuses on More NIST Standards

HHS HITECH April 2009 Guidance provides:

“(ii) Valid encryption processes for data-in-motion are those that comply, as appropriate, with:

- NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*
- 800-77, *Guide to IPsecVPNs*
- 800-113, *Guide to SSL VPNs*
- others which are Federal Information Processing Standards (FIPS) 140-2 ‘validated.’”

✧ Note: NIST changed these encryption requirements – see NIST SP 800-131 (January 2010)