Preventing a Data Privacy Breach: Securing Protected Health Information

Recent Incidents Reported by the Media, Impact, and Prevention

April 11, 2006

The Twelfth National HIPAA Summit™

The Leading Forum on Healthcare EDI, Privacy, Confidentiality, Data Security and HIPAA Compliance

perotsystems®

perotsystems®

Recent Incidents Reported by the Media

Which types of privacy and security incidents are being reported?

Which types of incidents are most common (likely)?

What is the impact of a privacy or security breach to a Healthcare organization?

perotsystems®

Recent Incidents (reported by the media)

Illegal Disclosure (insider)

- 2 plead no contest in South Bay patients' identity thefts
  - Reported by: *Daily Breeze, By Denise Nix; Mar 10, 2006*
  - Organization: Kaiser Permanente South Bay Medical Center
  - Incident:
    - **stealing information from patients' records, which they used to get fake credit cards and run up thousands of dollars in charges**
    - **The two [former employees of photocopying company Quest Nine Inc.], were hired to make copies of patient records**
  - Data compromised:
    - **patient records from the surgery and emergency room departments**
  - Impact (thus far; in addition to the negative publicity):
    - **will spend a year in jail for identity theft and grand theft**
    - **agreed to pay the victims back**

Link to article: http://www.ihealthbeat.org/index.cfm?Action=dspItem&itemID=118820

perotsystems®

Recent Incidents (reported by the media)

Inappropriate Disclosure (insider)

- IT Contractor Steals Names, Social Security Numbers From Insurer
  - Reported by: *iHealthBeat; Florida Times-Union; Feb. 17, 2006*
  - Organization: Blue Cross and Blue Shield of Florida
  - Incident:
    - **stolen by an information technology contractor who e-mailed the data to a home computer**
  - Data compromised:
    - **names and Social Security numbers of about 27,000 of its employees, contractors and vendors**
  - Impact (thus far):
    - **notifying the affected individuals and will offer them a year of credit monitoring at no cost; (note: average cost of credit monitoring services is $120 per year/person)**

Link to article: http://www.ihealthbeat.org/index.cfm?Action=dspItem&itemID=118820

perotsystems®

Recent Incidents (reported by the media)

Inappropriate Disclosure (insider)

- Boston Hospital Mistakenly Sends Bank Private Patient Data
  - Reported by: *Boston Herald; Feb. 07, 2006*
  - Organization: Brigham and Women's Hospital
  - Incident:
    - **mistakenly faxing confidential patient information**
  - Data compromised:
    - **"… 30 patients, including Social Security numbers, birth dates, home addresses, hospital room numbers, health insurance data, blood types, religious beliefs, occupations, and hospital discharge data. The records are from women who had just given birth, and included information about the infants and whether the mothers and infants tested positive or negative for diseases such as …"**
  - Impact (thus far):
    - **Local news coverage:** http://cbs4boston.com/topstories/local_story_038100017.html

perotsystems®

Recent Incidents (reported by the media)

Stolen Laptop/PC/ Back Up Tapes

- Health System Faces Class Action Lawsuit After Records Theft
  - Reported by: *Oregonian; Feb. 01, 2006*
  - Organization: Providence Health System
  - Incident:
    - **records were stolen from an employee's car**
  - Data compromised:
    - **365,000 people - home services medical records**
  - Impact (thus far):
    - **Former patient filed a class action suit against Providence**
    - **arrange and finance ongoing credit monitoring and to pay for any damaged credit ratings**
    - **security-breach bill in the Oregon Legislature**
    - **Some current and former Providence patients and employees are outraged**

Link to article: http://www.oregonlive.com/news/oregonian/index.ssf?/base/business/1138771538256400.xml&coll=7

perotsystems®

Recent Incidents (reported by the media)

Inappropriate Disclosure (insider)

- U.S. Settles With Company on Leak of Consumers' Data
  - Reported by: NY Times, by *Tom Zeller Jr.; Jan. 27, 2006*
  - Organization: ChoicePoint Inc.
  - Incident:
    - **"thieves had duped the company into turning over private data"**
    - **"… its handling of consumer data and its inadequate security procedures amounted to violations of consumer privacy rights and federal law"**
  - Data compromised:
    - **private data on more than 145,000 people**
  - Impact (thus far):
    - **FTC settlement includes $10 million in fines as well as $5 million in consumer compensation**
    - **new state laws on data security as well as several bills in Congress**

Link to article:
http://www.nytimes.com/2006/01/27/business/27choice.html?ex=1296018000&en=cc97b3dede67dd56&ei=5090&partner=rssuserland&emc=rss

perotsystems®

Recent Incidents (reported by the media)

Stolen Laptop/PC/ Back Up Tapes

- Ameriprise Says Stolen Laptop Had Data on 230,000 People
  - Reported by: *NY Times; January 26, 2006*
  - Organization: Ameriprise Financial
  - Incident:
    - **company laptop was stolen from an employee's parked car**
    - **data was being stored unencrypted [password protected] in violation of company rules**
  - Data compromised:
    - **names and Social Security numbers of about 70,000 current and former financial advisers and the names and internal account numbers of about 158,000 customers**
  - Impact (thus far):
    - **"… notifying the customers and the advisers"**

Link to article:
http://www.nytimes.com/2006/01/26/business/26data.html?ei=5090&en=683c419a10f58ef2&ex=1295931600&adxnnl=1&partner=rssuserland&emc=rss&adxnnlx=1142456762-IfyihCDKajyJgP2aSRdJ5g

perotsystems®

Recent Incidents (reported by the media)

Inappropriate Disclosure (insider)

- Kaiser Fined $200,000 for Patient Data Privacy Violation
  - Reported by: *San Francisco Chronicle; June 21, 2006*
  - Organization: Kaiser Permanente of Northern California
  - Incident:
    - **storing personal patient information on a publicly accessible Web site**
    - **did not have the patients' consent - a violation of both state law and Kaiser's privacy policy**
  - Data compromised:
    - **Identity and medical information for about 150 patients**
  - Impact (thus far):
    - **California Department of Managed Health Care fined Kaiser Permanente of Northern California $200,000**

Link to article: http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/06/21/BAG7ADBRPJ1.DTL&hw=kaiser+security+breach&sn=001&sc=1000

perotsystems®

Recent Incidents (reported by the media)

Stolen Laptop/PC/ Back Up Tapes

- Strict liability for data breaches?
  - Reported by: *SecurityFocus.com; Rasch,"A recent court case"; Jan. 22, '06*
  - Organization: Brazos Higher Education Service Corporation
  - Incident:
    - **the analyst's house was burglarized, and the unencrypted files were stolen**
  - Data compromised:
    - **files related to as many as 550,000 loans**
  - Impact (thus far):
    - **notified all 550,000 customers**
    - **free 90 day security alert on their credit files**
    - **established a call center to track ID theft**
    - **[patient] decided to sue Brazos for breach of contract, breach of fiduciary duty and negligence**

Link to article: http://www.theregister.co.uk/2006/02/22/data_breach_liaibility/
Related Court Case: http://www.nysd.uscourts.gov/courtweb/pdf/D08MNXC/06-00529.PDF

perotsystems®

Recap of Recent Incidents (grouped by type

Headline	Category	Organization	No. Records	Cost Actual/ Estimate	Notes re Cost
Stolen Laptop Includes HIV Patients' Health Records	**Stolen Laptop/PC/ Back Ups**	**CARES Clinc - UC Davis**	1,764	$211,680	Est. for CR monitoring services (***)
Stolen laptop puts patients' info at risk	Stolen Laptop/PC/ Back Ups	**M.D. Anderson**	4,000	$480,000	
Health System Faces Class Action Lawsuit After Records Theft	Stolen Laptop/PC/ Back Ups	**Providence Health System**	365,000	$43,800,000	Class Action Law suit for CR monitoring
Ameriprise Says Stolen Laptop Had Data on 230,000 People	Stolen Laptop/PC/ Back Ups	**Ameriprise**	230,000	$27,600,000	***
Medical Records Stolen From California Children's Clinic	Stolen Laptop/PC/ Back Ups	**Children's Health Council**	5,700	$684,000	***
Mo. Hospital Reports Two Stolen Computers	Stolen Laptop/PC/ Back Ups	**St. John's Regional Medical Center**	27,000	$3,240,000	***
Medical Files for 57,000 Ariz. Residents Stolen	Stolen Laptop/PC/ Back Ups	**Biodyne; BCBS AZ**	57,000	$6,840,000	***
Stolen Laptop Contains Information on Medi-Cal Beneficiaries	Stolen Laptop/PC/ Back Ups	**Medi-Cal**	21,600	$2,592,000	***
Theft exposes data of medical patients	Stolen Laptop/PC/ Back Ups	**San Jose Medical Group**	185,000	$22,200,000	***
Break-In At SAIC Risks ID Theft	Stolen Laptop/PC/ Back Ups	**SAIC**	10,000	$1,200,000	***
U.S. Settles With Company on Leak of Consumers' Data	**Inappropriate/Illegal Disclosure (by an insider)**	**Choice Point**	145,000	**$15,000,000**	FTC settlement
Boston Hospital Mistakenly Sends Bank Private Patient Data	Inappropriate/Illegal Disclosure (by an insider)	**Brigham and Women's Hospital**	30		Sensitive diagnosis information
Human error' exposes patients' Social Security numbers in N.C.	Inappropriate/Illegal Disclosure (by an insider)	**BCBS North Carolina**	600	$72,000	***
Confidential List of HIV/AIDS Patients E-mailed To Health Workers	Inappropriate/Illegal Disclosure (by an insider)	**Florida Health Dept.**	6,500		AIDS and HIV patients
Kaiser Fined $200,000 for Patient Data Privacy Violation	Inappropriate/Illegal Disclosure (by an insider)	**Kaiser Permanente of Northern California**	150	**$200,000**	Fine imposed by CA Dept. of Managed HC
IT Contractor Steals Names, Social Security Numbers From Insurer	Inappropriate/Illegal Disclosure (by an insider)	**BCBS Florida**	27,000	**$3,240,000**	Actual for CR monitoring services
Hacker Had Access to Health System's Computers for 18 Months	**Hacking by an outsider**	**Univ. of Washington School of Medicine**	2,000,000		
40 million credit card holders may be at risk	Hacking by an outsider	**Mastercard; Card System Solutions**	68,000	$8,160,000	***
Duke Health System's Web Sites Hacked	Hacking by an outsider	**Duke Health System**		$0	
FBI Probes Computer Breach at Stanford	Hacking by an outsider	**Stanford Univ. Career Dev. Center**	9,900	$1,188,000	***
Health Plan Alleges Former Employees Stole Data	Hacking by an outsider (former employee)	**Medica Health Plans**		$0	
***Sun* exposes UK ID theft racket at Indian call centre**	**Media Exposes Security Weakness**	**Indian call centre**	n/a		
Security flaw exposes CVS purchase data	Media Exposes Security Weakness	**CVS Corp.**	n/a	50M cards	
Personal Data for 3.9 Million Lost in Transit	**Data lost in transit**	**CitiFinancial of CitiGroup (UPS)**	3,900,000		

perotsystems®

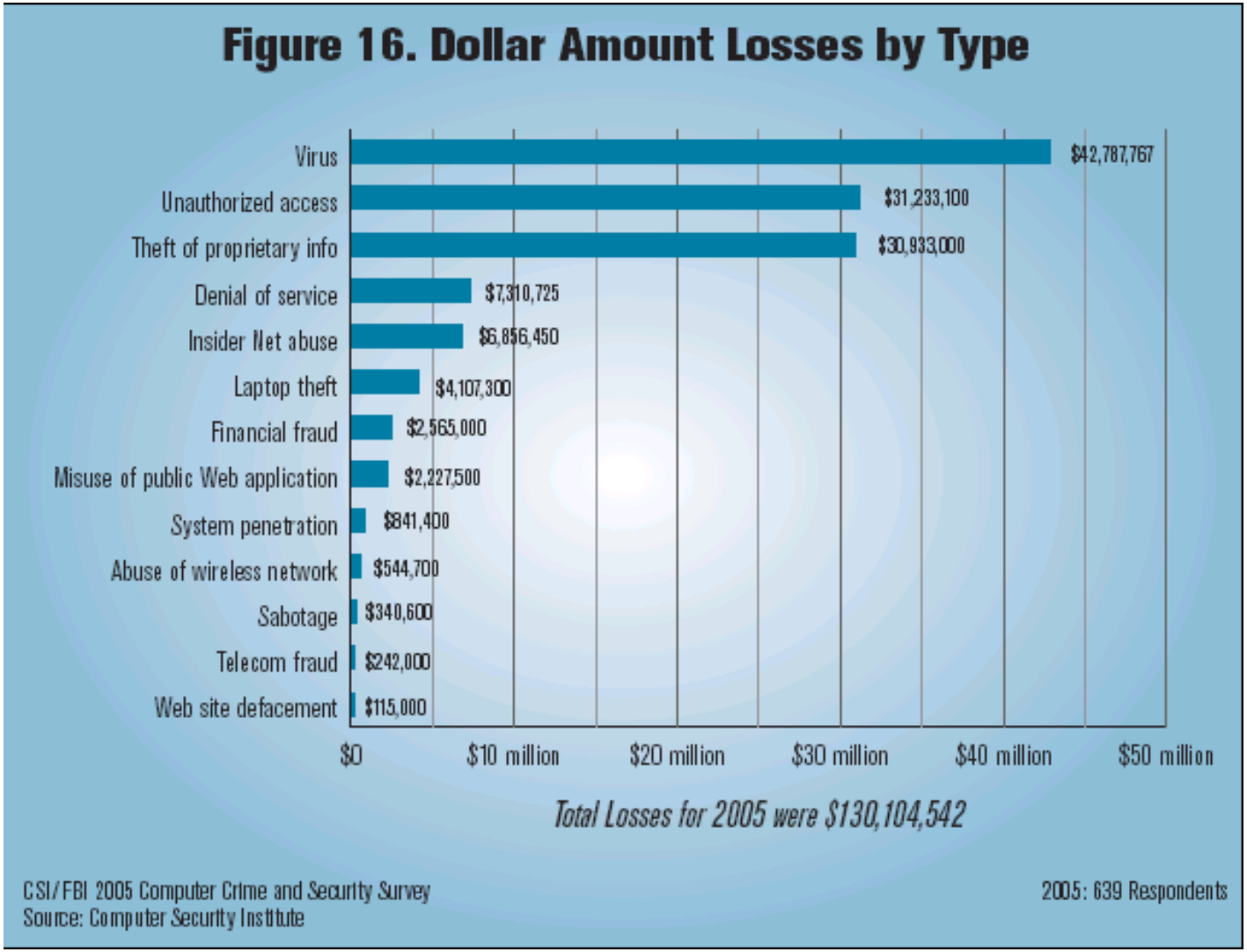
Alarming Trends

- Identity Theft is putting HIPAA PHI at considerable risk
- Patient/member notification has become necessary (and a precedent) because of potential credit fraud and new legislation
  - Notification leads to angry customers and negative publicity
- A *privacy-rights-oriented* press is not only reporting these incidents, but is proactively looking for and exposing weaknesses in enterprise safeguards
- Recent settlements are based on "fiduciary duty" and negligence
  - A lack of "reasonable and appropriate" technical safeguards (e.g., data encryption)
  - Ineffective and non-compliant human processes and a failure to enforce policies
- Significant financial penalties have become a reality
  - Recovery/resolution cost is significant - $120/individual (min.) for 1 year of credit monitoring service; now expected by individuals; a new precedent
  - Federal and state enforcement with substantial penalties
  - Civil/Class Action Lawsuit
- Negative publicity & penalties are prompting Healthcare to be compliant & spend $
- Encryption sharply reduces risk, impact and liability
- Spending on security has been for the external threat; needs to shift to internal risks

perotsystems®

Alarming Trends

Recovery/resolution cost is significant (and increasing)



CSI/FBI Computer Crime and Security Survey

perotsystems®

Alarming Trends

Recovery/resolution cost is significant (and increasing)

ACTIVITY	DIRECT COST	INDIRECT COST	LOST CUSTOMER COST	TOTAL COST
Detection & Escalation				
• Internal investigation	$19,000	$488,000	N/A	$507,000
• Legal, audit, consulting	$463,000	$51,000	N/A	$514,000
Notification				
• Letters	$547,000	$193,000	N/A	$740,000
• E-mails	$5,000	N/A	N/A	$5,000
• Telephone	$913,000	$105,000	N/A	$1,018,000
• Published media	$48,000	N/A	N/A	$48,000
• Web site	$3,000	N/A	N/A	$3,000
Ex-Post Response				
• Mail	$4,000	$3,000	N/A	$7,000
• E-mails	$1,000	$1,000	N/A	$2,000
• Internal call center	$287,000	$479,000	N/A	$766,000
• Outsourced call center	$27,000	N/A	N/A	$27,000
• Public or investor relations	$289,000	$14,000	N/A	$303,000
• Legal defense services	$1,288,000	N/A	N/A	$1,288,000
• Free or discounted services	$810,000	N/A	N/A	$810,000
• Criminal investigations	$286,000	$13,000	N/A	$299,000
Lost Business				
• Lost existing customers	N/A	N/A	$6,728,000	$6,728,000
• Lost new customers	N/A	N/A	$730,000	$730,000
Average Cost Per Company	**$4,990,000**	**$1,347,000**	**$7,458,000**	**$13,795,000**
Per Lost Record Cost	**$50**	**$14**	**$75**	**$138**

Ponemon Institute, LLC
October 2005

Note: the approximate cost of credit monitoring services per individual for one year is $120.

perotsystems®

Alarming Trends

- New Notification laws and legislation; status:
  - As of July 2005, 18 more states and Congress had proposed legislation similar to California's SB 1386
  - *Enacted State security breach notification laws:*
    - Arkansas, California, Connecticut, Delaware, Florida, Georgia (data brokers only), Illinois, Indiana (state agencies only), Louisiana, Maine (Information brokers only), Minnesota, Montana, Nevada, New Jersey, New York, North Carolina , North Dakota, Ohio, Pennsylvania, Rhode Island , Tennessee, Washington
    - source: http://www.pirg.org/consumer/credit/statelaws.htm#breach
    - Texas SB 122 IDENTITY THEFT ENFORCEMENT & PROTECTION ACT
      - "Relating to the prevention and punishment of identity theft and the rights of certain victims of identity theft; providing penalties"; effective on 9/1/05
- Federal Legislation; proposed bills
  - S.1408 Identity Theft Protection Act; FTC will have jurisdiction
  - Barton/Stearns draft legislation

perotsystems®

Prevention Strategy

- HIPAA Security calls for …
  - A comprehensive security program
    - Administrative, Physical and Technical Safeguards
  - An initial Risk Analysis
    - Assess vulnerabilities to an outside attack (e.g., vulnerability scanning)
    - Assess employee/insider policy compliance and current (PHI) disclosures
    - Identify PCs and systems that store or transmit Protected Health Information
  - Prioritize remediation efforts for each Risk/Threat by *Likelihood* and *Impact*
  - Spending levels on technical safeguards should be "reasonable and appropriate" but must be influenced by technology availability, cost and de facto standards
  - Evaluation – ensure effectiveness of safeguards (e.g., Will a policy be enough?)
  - Follow on Risk Analysis:
    - Monitor internal and external incidents, assess new threats and risks, modify strategy accordingly

Prevention Strategy

Most *Likely* Types of Incidents:	Prevention Strategy
– Stolen laptops/PCs/back-ups	☞ Data Encryption - disk & media; centralize PHI ☞ Secure elec. transfer of data/back-ups (e.g., secure FTP); secure email
– Illegal theft and disclosure (for gain) of confidential/protected data (by an insider) via email, http, IM – Inadvertent disclosures by negligent/non-compliant employee	☞ Training; policies with consequences ☞ Outbound Content Filtering: ☞ *Basic*: email – manual flagging & encryption; then, automated detection of PHI and individual identities ☞ *Advanced*: Automated monitoring/detection ☞ Automate (enforce) policies, i.e., encrypt, Block/Quarantine (route for approval) ☞ Multi channel TCP/IP (add IM, http, FTP, electronic faxing) ☞ Multiple lexicons for different data types (e.g., PHI, IP, confidential) ; accuracy is critical
– Hacking, intrusion, web site attack, data theft (by an outsider)	☞ Immediate termination of passwords ☞ Encrypt data at rest including IDs & passwords ☞ Intrusion Detection/Prevention Systems

perotsystems®

Prevention Strategy

Collaboration …

- Gartner Recommendations; June 2005:
  - *Centrally managed disk encryption* storage for all PCs that store sensitive information
  - *Outbound content filtering and blocking software* that can prevent the electronic communication of sensitive information outside the enterprise
  - Host-based *intrusion prevention* software that includes behavior-based detection to block the execution of unknown executables, as well as signature-based antivirus and anti-spyware tools

Source: “Israeli Attack Represents a Dangerous New Breed of Spyware”; Gartner, June 2, 2005

perotsystems®

Prevention Strategy

Risk/threat: Stolen laptop/PC/backups

Strategy: Data Encryption

Perot Systems response – safeguards:

- Disk encryption (laptops that store confidential data, PCs in high risk areas)
  - Disk encryption – whole disk or partial disk based on needs
  - Centralized encryption-key backup and recovery
  - Secure data deletion (file shred, disk wipe)
  - Near future: encrypt data stored on web facing servers
- Additionally, leveraging encryption solution for secure email
  - Installed at the gateway
  - Initially, manual flagging (by end user) - PHI and other confidential information
- Secure FTP

Risk/threat: Inappropriate Disclosures

Strategy: Outbound Contenting Filtering

Perot Systems response – safeguards:

- Finalizing internal product evaluation; leveraging industry studies such as Gartner
- Negotiating with leading vendors
- Implementation Plan:
  - Initially, outbound email (SMTP); then, add channels: IM, http, FTP
  - Policy automation:
    - Block/prevent and/or route for approval - high risk/impact disclosures, 1st
    - Automate encryption decision, i.e., detect PHI and individual identity information, route to encryption engine

perotsystems®

People | Processes | Technology | Results.

Thank you.

Contact Information:
Greg Cislo
Plano, Texas
972 577-7821
Greg.Cislo@ps.net
Perot Systems Healthcare
HIPAA Compliance Program Manager