How the #@%! Did This Happen ?!?!?!

Marne E. Gordan

Director, Regulatory Affairs

Session 7.03
HIPAA Summit XIII
September 2006
Washington, DC

Cybertrust

The Global Information Security Specialist

- The outcome of the 2004 merger of BeTrusted, TruSecure, and Ubizen
- Parent corporation of ICSA Labs
- Product and vendor-neutral
- Global presence
- Offices in more than 30 countries
- Earned the trust of more than 4,000 customers worldwide
- 15 years of proven excellence

TruSecure

has merged with

Betrusted.
Providing Trust Worldwide

ubizen

A CYBERTRUST COMPANY

ICSA labs
CERTIFIED
www.ICSALabs.com

The expertise and experience of a pure play vendor with the global reach and objectivity of a systems integrator.

Today’s Agenda

- **When Bad Things Happen to Virtual People**
- **It’s a Jungle Out There**
  - **Events vs. Incidents**
  - **The eBusiness Environment**
  - **How Vulnerable are You?**
- **Case(s) in Point**
  - **Lessons from the Headlines**
- **Fix, Prosecute or Notify ?**
- **Summary**
- **Q&A**

When Bad Things Happen to Virtual People

The Exponential Rise in ID Theft

At the Seattle Cancer Care Alliance

Patient Eric Drew’s identity stolen by phlebotomist Richard Gibson

- Gibson had access to patient record
- Obtained Drew’s SSN, date of birth, and primary address
- Used this information to open lines of credit
- Ran up over $9k in debt
  - Clothing
  - Jewelry
  - X-Box
  - Porcelain figurines

http://www.msnbc.msn.com/id/10549098/

Drew Began Receiving Unsolicited Mail/Collection Notices

Contacted major credit bureaus

- Placed fraud warnings on legitimate credit cards
- Begged major issuers not to issue any new cards
- Contacted local law enforcement

Nothing happened, until

- Local reporter Chris Daniels at KING-5 NBC TV reported the story
- Daniels and Drew continued the investigation
- Forensic trail led to Gibson

Gibson plead guilty

- 16 months in jail, plus restitution
- First documented “HIPAA conviction”
- **Convicted of unlawful use of IIHI**

It’s a Jungle Out There . . . .

Defining Events and Incidents

Millions of Threats Out There . . .

- Events
- Incidents

Defining Events

- Typically non-malicious
- Typically random
  - Global – ISP outages, fiber cuts, power spikes
  - Regional – Earthquake, tornado, flood, etc.
  - Local – Fire, storm damage, pipes burst
- Typically non-intrusive
- Typically not intelligence-driven
- Organizations respond to these events through disaster recovery

Defining Events and Incidents

Defining Incidents

- Intelligence-driven attacks
  - Malicious code – Virus, Trojan, DoS, etc.
  - Hacker
- Typically focused
  - Target is identified for whatever reason(s)
  - Agenda drives the attack
    - Virus or web defacement for damage
    - Hacking for theft
- Typically malicious
- Always intrusive
- Organizations require incident response plans

Remember those Cisco commercials??

It's a very destructive worm, but the network caught it. How did it even get in here??

Daddy, I just downloaded a new game, and it's SOOO cool !!!

Examples of Incidents

- Trusted insider copies and removes a large number of patient billing records from data warehouse
- Unknown entity accesses and removes customer data from a hospital, and publishes it
- Administrator observed accessing sensitive government data without specific authorization, however, the individual needs administrative access rights and privileges to those machines
- A large insurance company receives questionable threat from unknown source about proposed hacking activity
- A large application service provider (ASP) receives credible threat that a known group may try to interrupt a industry-sponsored Internet event

From the Federal Trade Commission

2005 Consumer Sentinel Survey

- 686,683 complaints re: consumer fraud
- 255,565 complaints re: ID Theft
- ID Theft the largest category of complaint (37%)
- 46% of ID Theft activity is Internet related
  - Internet auctions 12%; Internet services 5%
- 55% of consumers surveyed indicated that fraud was perpetrated through the Internet
  - Websites; Emails
- Total fraud reported was $680m; median loss $350
- Internet related fraud was $335m; median loss $345

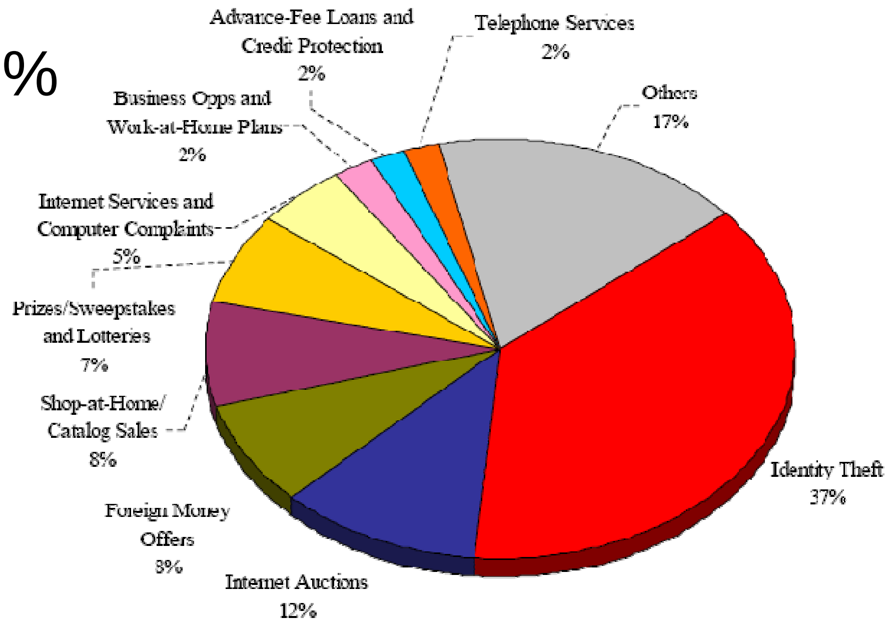
Available at http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf

More from the Federal Trade Commission

Types of Fraudulent Activity

- SSN not specifically compromised
  - Credit Card Theft 26%
- SSN compromised
  - Phone and Utility Fraud 18%
  - Bank Fraud 17%
  - Employment Fraud 12%
  - Government Benefits 9%
  - Loans 5%

Sentinel Top Complaint Categories[1]
January 1 – December 31, 2005

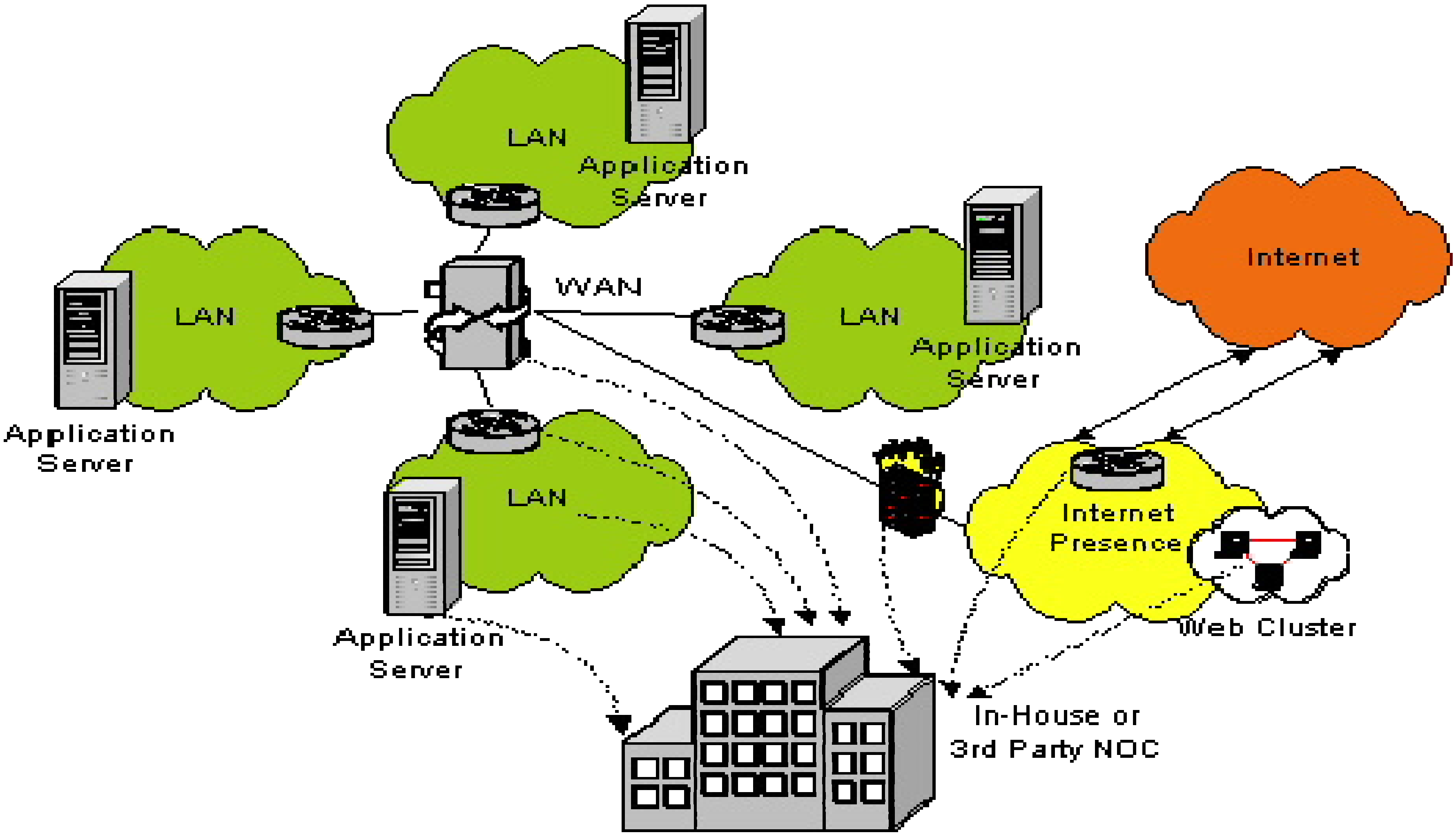


Available at http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf

A Paradigm Shift

For many regulated industries, the world changed in 1999.   Ownership of consumer’s personal information was “given back” to the consumer.   It is now considered personal property, rather than a corporate asset.   The organization may own the database, but they serve as the primary custodian of the personal information, rather than the owner.   In effect, this extends the duty of care that many businesses and organizations owe to customers and consumers.   They must now proactively protect personal information, in addition to providing goods or rendering services.

eBusiness Connectivity Scenario



Slammed on All Sides

Rogue Insiders

Employee Error

VIRUSES

Software Bugs

Corporate Spies

Script Kiddies

Web Defacements

Password Crackers

Network vulnerabilities

Trojans

“SneakerNet”

War Drivers

Backdoors

Worms

Denial of Service

Buffer Overflows

“Blended Threats”

How Vulnerable Are You?

If yours is an average U.S. corporation here’s what your network experienced in the last week . . .

- Every Internet connected devices was "probed" about 26 times per day for known vulnerabilities.
- About 13 computers somewhere in your organization encountered a computer virus.
- 16 already logged-in desktop computers were inappropriately used by another employee in your company to access information.
- Three people scrounged through desks and drawers looking for someone else’s password. One of them succeeded and used it.

Statistics provided by ICSA Labs

How Vulnerable Are You?

If yours is an average U.S. corporation here's what your network experienced in the last week . . . .

- On average 16 sexually explicit graphics were mailed or shared among some of your users. There is a 50-50 chance that some of these are stored on your network.
- At least two people experimented with a "hacking" tool or technique on the general computers, servers, and databases inside your network in the past month.
- Despite all the press and focus on hacking and viruses, there is a 72% likelihood that the next security breach your staff deals with will come from an insider.

2005: Year of the Data Breach

Tufts University

Polo Ralph Lauren

CA FasTrack

CA Dept of Health

DSW Shoes

Ameritrade

Carnegie Mellon

Michigan State

CSJ Hospital

Georgia Southern

Wachovia

Oklahoma State

Time Warner

ChoicePoint

Air Force

University of North Texas

PayMaxx

Hinsdale High

Westborough Bank

Jackson CC

LexisNexis

U CA Berkeley

Boston College

Nevada DMV

Northwestern

UNLV

Cal State Chico

U CA SF

Georgia DMV

Bank of America

University of Colorado

Cisco.com

DOJ

Stanford Univ

Valdosta State

CardSystems

Duke Univ

Cleveland State

Merlin Data Services

Motorola

CitiFinancial

FDIC

MCI

SJ Medical

CO Dept of Health

Purdue Univ.

USC, Michigan, Southern California State

Sonoma State University

Source: http://www.privacyrights.org/ar/ChronDataBreaches.htm

2006: The Good Times Just Keep Coming . . .

UPMC Squirrel Hill Family Medicine
H&R Block
Atlantis Hotel - Kerzner Int'l
People's Bank
City of San Diego, Water & Sewer Dept.
Univ. Place Conference Center & Hotel Indiana Univ.
California Army National Guard
Univ. of Notre Dame
Univ. of WA Medical Center
Providence Home Services (OR)
State of RI web site
Boston Globe
The Worcester Telegram & Gazette
BCBS of North Carolina
FedEx
Honeywell International
Ernst & Young (UK)
Dept. of Agriculture
Old Dominion Univ.
BCBS of Florida
Calif. Dept. of Corrections, Pelican Bay
Mount St. Mary's Hospital (Lewiston, NY)

Deloitte & Touche (McAfee employee information)
Medco Health Solutions
OH Secretary of State's Office
Olympic Funding (Chicago, IL)
Los Angeles Cty. Dept. of Social Services
Hamilton County Clerk of Courts
Metropolitan State College
Georgetown Univ.
Verizon Communications
iBill (Deerfield Beach, FL)
CA Dept. of Consumer Affairs
General Motors (Detroit, MI)
Buffalo Bisons and Choice One Online
Ernst & Young (UK)
Bananas.com
Fidelity Investments
CA State Employment Development Division
Vermont State Colleges
Georgia Technology Authority
Conn. Technical High School System
Progressive Casualty Insurance
DiscountDomain Registry.com

University of Medicine and Dentistry of New Jersey
Ross-Simons
Univ. of South Carolina
University of Alaska, Fairbanks
Ohio University Innovation Center University of Texas‘ McCombs School of Business
Univ. of Northern Iowa
Purdue University
Aetna -- health insurance records for employees of 2 members, including Omni Hotels and the Dept. of Defense NAF
MasterCard (Potentially UK only)
Long Island Rail Road
Ohio's Secretary of State
Dept. of Defense
Georgia State Government
Idaho Power Co.
Ohio University Hudson Health Center
Dept. of Veteran Affairs
Wells Fargo
Mercantile Potomac Bank
American Institute of Certified Public Accountants (AICPA)

Source: http://www.privacyrights.org/ar/ChronDataBreaches.htm

2006: And Coming . . .

Univ. of Delaware
M&T Bank
Sacred Heart Univ.
American Red Cross, St. Louis Chapter
Vystar Credit Union
Texas Guaranteed Student Loan Corp.
Florida Int'l Univ.
Miami University
Univ. of Kentucky
Buckeye Community Health Plan
Ahold USA
YMCA
Humana
Internal Revenue Service
Univ. of Texas
Univ. of Michigan Credit Union
Denver Election Commission
U.S. Dept. of Energy
Minn. State Auditor
Oregon Dept. of Revenue
U.S. Dept of Energy, Hanford Nuclear Reservation
American Insurance Group (AIG)

NY State Controller's Office
ING
Univ. of Kentucky
Automatic Data Processing (ADP)
CA Dept. of Health Services (CDHS)
Equifax
Univ. of Alabama
U.S. Dept. of Agriculture (USDA)
Cape Fear Valley Health System
Fed. Trade Comm. (FTC)
San Francisco State Univ.
U.S. Navy
CA Dept. of Health Services (CDHS)
Catawba County Schools
King County Records, Elections, and Licensing Services Division
Gov't Accountability Office (GAO)
AAAAA Rent-A-Space
AllState Insurance Huntsville branch
Nebraska Treasurer's Office
Minnesota Dept. of Revenue
Nat'l Institutes of Health Federal Credit Union NIH
American Red Cross, Farmers Branch
Bisys Group Inc.
Automated Data Processing (ADP)

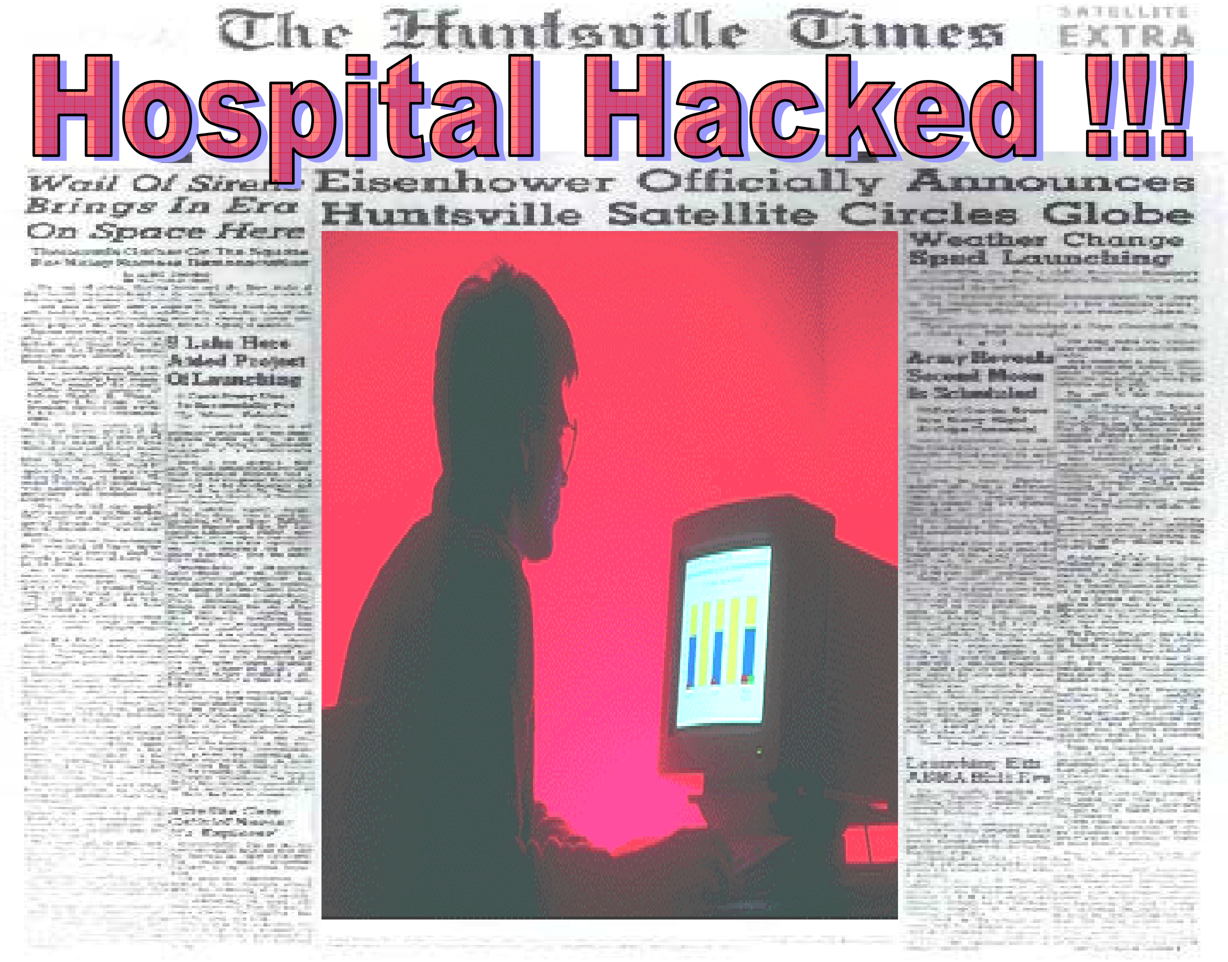
University of Tennessee
Nat'l Association of Securities Dealers (NASD)
Naval Safety Center
Montana Public Health and Human Services Dept.
Moraine Park Technical College
Northwestern Univ.
University of Iowa
Treasurer's computer in Circuit Court Clerk's office
Nelnet Inc.
CS Stars, subsidiary of insurance company Marsh Inc.
U.S. Dept. of Agriculture
New York City Dept. of Homeless Services
Armstrong World Industries
Georgetown University Hospital
Old Mutual Capital Inc.
Cablevision systems
U. S. Navy recruitment offices
Kaiser Permanente Northern Calif. Office
Los Angeles County, Community Development Commission (CDC)
Los Angeles County, Adult Protective Services
Western Illinios Univ

Source: http://www.privacyrights.org/ar/ChronDataBreaches.htm

. . . . So what will you do ???

Case(s) In Point

Lessons from the Headlines . . . .


The Huntsville Times
SATELLITE EXTRA
Hospital Hacked !!!
Wail Of Sirens Brings In Era On Space Here
Eisenhower Officially Announces Huntsville Satellite Circles Globe
Weather Change Sped Launching
Army Reveals Second Moon Is Scheduled

The Northwest Hospital Incident (Case A)

Botnet attack hits hospital systems

One day last year, things started going haywire at Northwest Hospital and Medical Center. Key cards would no longer open the operating-room doors; computers in the intensive-care unit shut down; doctors' pagers wouldn't work. This might have been just another computer-virus attack, a common and malicious scheme that sometimes is done for little more than bragging rights. But federal officials say it was something far more insidious.

The hospital's computer network is alleged to have been disrupted by the botnet infection.

The Highlights

Northwest Hospital and Medical Center in Seattle experienced system problems

- 150 out of ~1,100 computers were infected over the course of 3 days.
  - Medical records were not accessible electronically
  - Pagers went off-line
  - Key cards were disabled
  - Computers in the ICU shut down
- They contacted law enforcement
  - The FBI found that approximately 50,000 computers nationwide were infected
  - The forensic trail led to compromised computers at the University of Michigan, Cal State Northridge and UCLA
  - The trail ultimately led to 20 year-old hacker Christopher Maxwell in Vacaville, CA
  - He launched a bot-net attack against random computers *TO INSTALL ADWARE*

The Highlights

Northwest Hospital was not specifically targeted for this attack

- Hacking for Profit
  - Maxwell and two teenage accomplices [allegedly] created the botnets
  - They worked for a mainstream adware company, which paid them commission per download of the adware
  - The [unidentified] company claims it had no idea that adware was downloaded without the permission of the system owners
  - Maxwell made over $100K in 2005 through this exploit
- Blunt-force attack
  - Similar to virus in terms of exploit
  - Bot-nets send out messages looking for computers to compromise
  - Repeated messages tie up systems and often shut them down
  - Once installed on a system, they wait for instructions from a “bot-herder”
  - In this case, the instructions were to install adware on all infected systems
  - In many cases, such DOS attacks are used for extortion

Where Were the Controls ??

Who knows ??

- No comment on controls in place
  - Point(s) of failure?
- Northwest immediately resorted to backup systems
  - They went low-tech
  - Paper records and files were used for patients
  - Personal cell phones in place of pagers
  - Physical ID inspection by security guards in place of key card
- Northwest appears not to have been proactive
  - But, admittedly, this type of attack is very difficult to anticipate and prevent

What Would Have Helped ??

Controls in place

- BotNet infections can be treated as viruses and other malcode
- Anti-Virus
  - Deployed across the enterprise: servers, desktops, and portables
  - Signatures updates on a frequent basis (once per week or more)
  - Regular checking of AV installation and configuration
  - Quick response to AV alerts through temporary preventive measures
- Patching
  - Rapid patch identification, testing, and deployment cycle
  - Use of centralized patching services and automatic updates
- Electronic Monitoring
  - Detecting and responding to malcode at the perimeter
  - Integrity checks of critical servers
- Policy and Procedure
  - Acceptable Use Policy
    - Acceptable software
    - Connecting non-corporate devices to the corporate network
  - End-User Training

What Does HIPAA Say ??

Security Standard

- **Administrative Safeguards 164.308(a)**
  - **(1)(ii)(D)** Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
  - **(5)(2)(B)**Protection from malicious software (Addressable).
  - Procedures for guarding against, detecting, and reporting malicious software.
- **Technical Safeguards 164.312 (a)**
  - **(2)(iv)(b)** Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Ultimately . . . .

Northwest was lucky

- Failover systems worked
- No patients were harmed
- There was no permanent damage to critical systems
- The attack was contained
- Law enforcement identified the source of the attack
- Prosecution is pending
- No evidence of a HIPAA Security/Privacy violation
  - No PHI damaged or exposed
- All things considered – Well Done !!

The San Jose Medical Center Incident (Case B)

SUSPECT IN SJ MEDICAL DATA THEFT TO BE IN COURT MONDAY

A California medical group is telling nearly 185,000 current and former patients that their financial and medical records may have been exposed following the theft of computers containing personal data. Given the number of people affected, the theft from the San Jose Medical Group ranks among the largest in the nation. It follows a rash of other breaches that have raised concerns about the security of sensitive information.

The Highlights

Burglars stole two Dell laptops from SJ Medical offices

- The incident took place only days after thousands of patient records were backed up from secured servers onto the laptops
  - SJ Medical was also in the middle of a patient data encryption project
  - It was originally believed that the hardware was the target
  - The data, some of which was encrypted, was part of a patient billing project and also part of the medical group's 2004 year-end audit
  - A CD containing patient data including names, addresses, SSNs, DoBs, insurance data, bill records and detailed medical histories was also stolen
- 185,000 patients affected
  - SJ Medical contacted the FBI
  - The trail led almost immediately to former McKee Branch manager Joseph Harris

The Highlights

SJ Medical was specifically targeted for this attack

- Former Employee/Trusted Insider
  - Harris had been asked to resign several month prior to the breach
  - He was suspected of involvement in several incidents of theft of money and medications
  - He acknowledged having a side business of selling used computers
  - There were six burglaries at three SJ Medical Group offices after his resignation
  - He had previously worked at Silicon Valley Children's Fund
  - He was dismissed for conducting his personal business on company time
  - Shortly after his dismissal, two computers were stolen from SVCF's offices
- Smash and grab
  - Harris was aware of the IT projects
  - He targeted both hardware and data
  - [allegedly] listed the hardware for sale on www.Craigslist.com
  - The removable media was [allegedly] found in his car
  - He also confessed

Where Were the Controls ??

Who knows ??

- No comment on controls in place
  - Point(s) of failure?
- SJ Medical immediately
  - Contacted law enforcement
- SJ Medical appears to have been somewhat proactive
  - "We started to encrypt things this year because of (medical regulations), ID theft reports and security regulations," SJM reported
  - As a security measure, the medical group has historically stored its information only on the secured servers, where employees have only limited access to the computers and the information can only be accessed via the network.
  - They are now improving security controls, starting with the deployment of surveillance cameras.

What Would Have Helped ??

Controls in place

- Alarms to detect the break-in
- Laptops secured
- Removable media secured
- Data encrypted?
  - In storage
  - On removable media
- Policy and Procedure
  - Background Checks
  - Hiring, Retention, and Termination Policy

What Does HIPAA Say ??

Security Standard

- **Physical Safeguards 164.310(a)(2)(ii)**
- Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
- **Administrative Safeguards 164.308 (a)(3)(ii)**
- (B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
- (C) Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

Ultimately . . . .

SJ Medical's performance was so-so in this case

- The suspect was found relatively quickly
- No reports to date of patients' personal or financial information being misused
  - Yet
- Evidence of a HIPAA security/privacy violation?
  - Preventative measures did not perform
  - Incident response was good
  - Remediation efforts are also good
- All things considered – ???
  - They did notify affected individuals as required by California SB 1386
  - Notification took nine days
  - Delay not attributed to law enforcement, but because it took time "to gather the necessary information for notices and distribute it to thousands of affected individuals"

UCSF's October Surprise (Case C)

Excerpt from a letter sent to UCSF medical center

"Your patient records are out in the open to be exposed, so you better track that person and make him pay my dues or otherwise I will expose all the voice files and patient records of UCSF Parnassus and Mt. Zion campuses on the Internet."

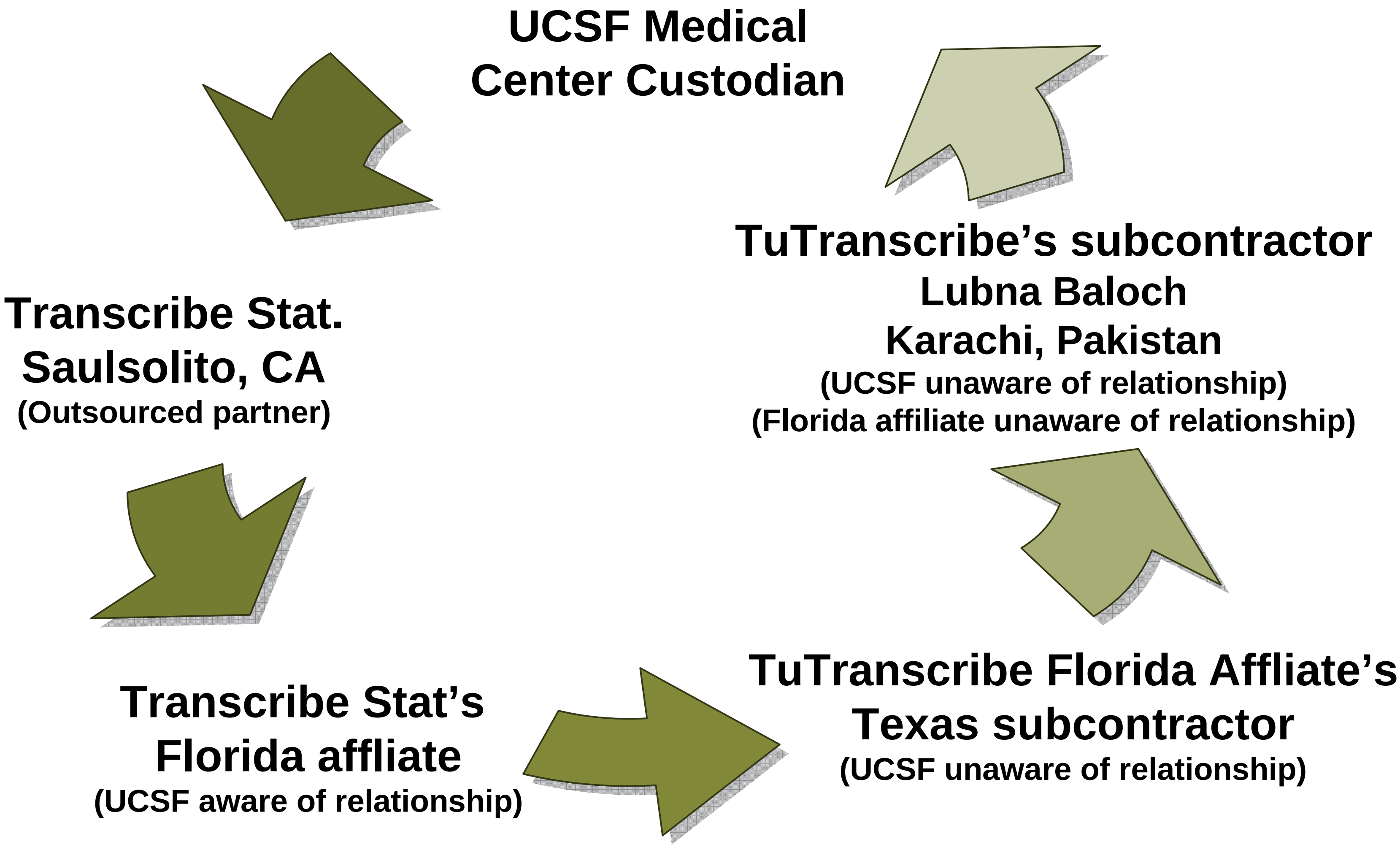
The Highlights

In October 2003, UCSF Medical Center was contacted by Lubna Baloch, demanding payment for transcription services.

- She threatened to expose patient information if she were not paid immediately
- She also sent an email containing patient data, to prove that she was serious
- UCSF had no prior contact with Baloch – she was not their employee, consultant or contractor
- UCSF has outsourced for over 20 years to Transcription Stat., a firm that maintains a network of 15 independent contractors
- One of the network participants in Florida then subcontracted to TuTranscribe in Texas, which maintains a network of cut-rate independent contractors overseas

Baloch was in this network

Clarifying the Chain



UCSF Medical Center Custodian

Transcribe Stat.
Saulsolito, CA
(Outsourced partner)

Transcribe Stat's
Florida affliate
(UCSF aware of relationship)

TuTranscribe Florida Affliate's
Texas subcontractor
(UCSF unaware of relationship)

TuTranscribe's subcontractor
Lubna Baloch
Karachi, Pakistan
(UCSF unaware of relationship)
(Florida affiliate unaware of relationship)

The Highlights

UCSF was unaware of some outsourcing, and had assumed the work was done directly by Transcription Stat.'s affiliate network

- TS was aware that it's Florida affiliate often subcontracted work, but was unaware of the offshore network maintained by the Texas subcontractor
- Baloch went to UCSF when the Texas subcontractor refused to pay
- She was ultimately made whole by the Florida contractor
- Baloch then contacted UCSF, retracting her threat
- UCSF has no evidence, however, that their data has been securely destroyed

The amount in question was $500.

Where Were the Controls ??

In this case, UCSF had a long-term trusted relationship with Transcribe Stat, and were aware that TS outsourced

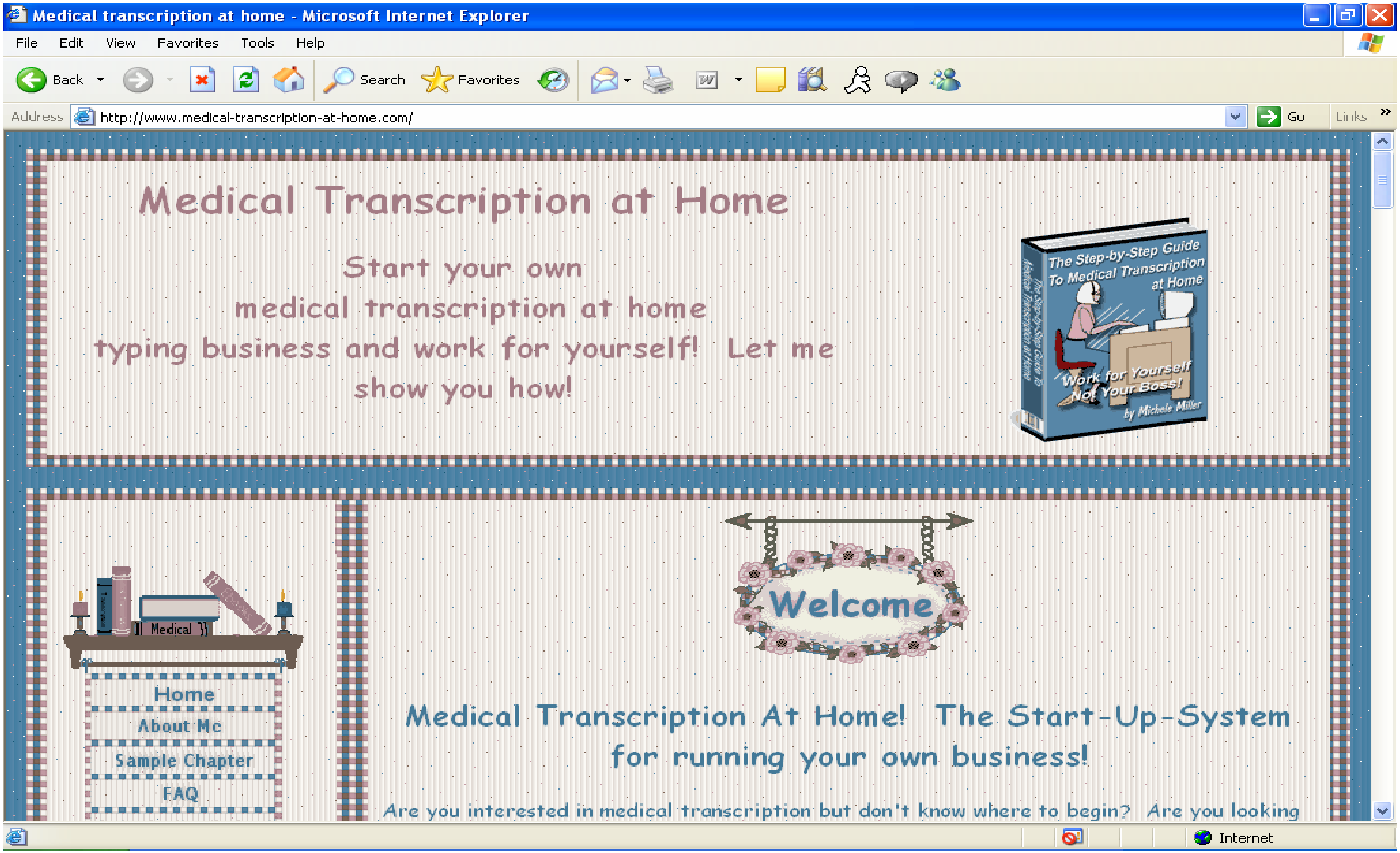
- UCSF admittedly did not investigate outsourcing further
- Clearly insufficient management of the chain of custody
- The only control in evidence in this situation is *trust*

What Would Have Helped ??

Controls in place

- **Appropriate contract management**
  - SLA documenting level of security responsibility and liability for client and primary contractor
- **Due Diligence**
  - Due diligence on primary contractor should have revealed
    - Length of outsourcing chain
    - Security controls in place in each outsourced environment
    - The manner in which residual data is (securely!) destroyed
    - Each participant’s acknowledgement of security responsibility and liability
  - Legal Representation
    - When sensitive data is outsource, the primary client should retain in-country legal representation to mediate disputes
- **Technical and Physical Controls not applicable**
- **Administrative Controls must be applied**
  - Policy and enforcement
  - Documentation

Could This be Your Worst Enemy?


Medical transcription at home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
Home
About Me
Sample Chapter
FAQ
Internet
The Step-by-Step Guide To Medical Transcription at Home
Work for Yourself Not Your Boss!
by Michele Miller
Medical

http://www.medical-transcription-at-home.com/

Medical Transcription at Home

Start your own medical transcription at home typing business and work for yourself! Let me show you how!

Welcome

Medical Transcription At Home! The Start-Up-System for running your own business!

Are you interested in medical transcription but don't know where to begin? Are you looking

What Does HIPAA Say ??

Security Standard

- Administrative Safeguards 164.308(b)(1)
- **Standard: Business associate contracts and other arrangements.**
- **A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information.**
- Organizational Requirements 164.314 (a)
- ***[The covered entity must ensure through contract that each organization with which it shares electronic PHI must implement appropriate technical, physical and administrative safeguards to protect its proprietary environment, secure communication channels, and report any security incidents or breaches back to the covered entity.   Failure to do so can result in a material breach of the contract, and may be considered a HIPAA compliance violation if corrective action is not immediately taken.]***

Ultimately . . . .

UCSF was lucky

- The patient data was not made public
- Patients unharmed
- Contractor was satisfied and retracted the threat
- It was a wake up call
- BUT
  - UCSF still has no concrete assurance that the data was securely destroyed
  - Technically, that data, and those patients, are still at risk

Are You a Target ??

Health care organizations

- Not a traditional target
- Process and store a wealth of personal information
  - Social Security Numbers
  - Payment information
  - Insurance account information
  - Medicare/Medicaid
  - Medical information

Don’t forget non-traditional targets

- Employee non-public personal information
- Organizational records

Who Knows ….

There's no telling what will attract some hackers . .

- **"Capture the flag" –** greater glory and personal bests (traditional and almost old-fashioned)
- **"Altruistic" –** making statements and proving points (**Deceptive Duo, S4t4n1c_S0uls, and The Bugz**)
- **"Scorched earth" attackers –** setting off logic bombs and self-replicating worms simply to destroy as much data as possible
- **Thieves –** credit card fraud, insurance fraud, ID theft (fun and profit)

And don’t forget . . .

The disgruntled employee !!!

Recent Novell research indicates [Case D]

- More than half the UK workforce* would be prepared to seek revenge on former employers by exploiting continued access to corporate systems if they lost a job
- 55% would continue to use their company laptop if it were not taken back; 58% would continue use of company mobile phones.
- 6% said that they would delete important files
- 4% would let a virus loose in the corporate email system
- 67% would be prepared to steal sensitive information that would help in their next job
- 38% said that they would steal company leads

*article did not indicate how large the polling group was, nor if it were a scientific poll

Learn from Common Mistakes

Incidents can’t be predicted

Preparation is critical

- Implement and maintain a reliable audit trail for accountability
- Maintain baseline systems with known Hash values
- Maintain trusted installation media
- Securely maintain validated backup and recovery
- Maintain logs – where, what, how old, and review
- Generate reports – log reports may qualify as “business records” – admissible as evidence
- Maintain physical and electronic access records

Implementing the Basics

The organization must maintain a formal Incident Response Policy and clearly documented procedures for dealing with breaches of security.

The policy must include:

- Key contacts and contact information;
- Notification/Escalation;
- Recovery;
- Disciplinary Procedures

Procedures must be routinely

- Reviewed
- Updated
- Tested

Issues to Consider

Staff must be

- Trained on security and IR
- Offered refresher information on a regular basis
- Provided with information on updates to policies and procedures

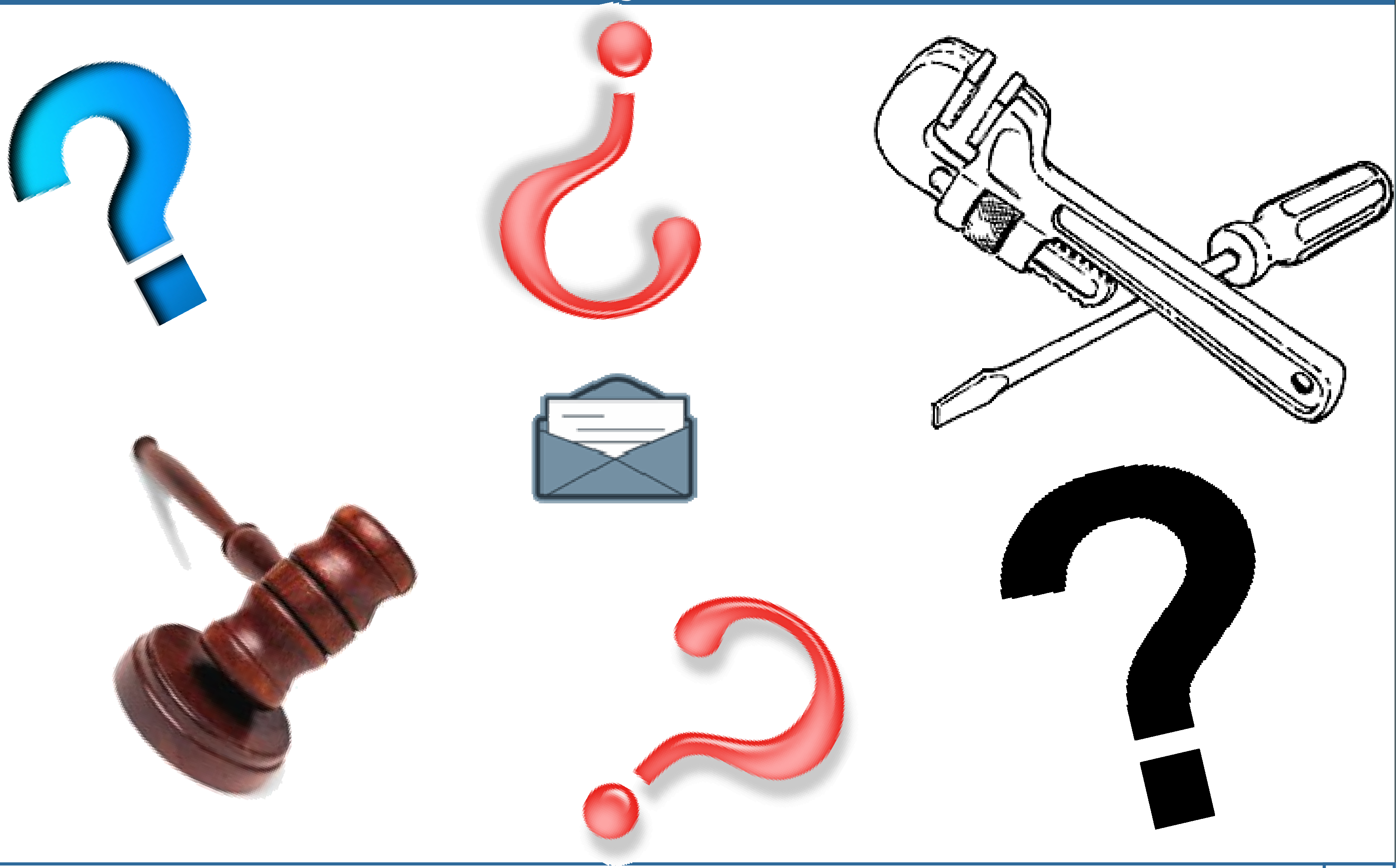
Extend IR Plan across the enterprise

- Just like the organization’s security program, the IR Plan must become part of the corporate culture
- Incident Response Plan must be supported in-house
- Include HR, PR, Legal, Administration, and Senior Management

Fix, Prosecute, or Notify ??

What Should a Covered Entity Do?

Fix, Prosecute or Notify??



When to Notify ??

Now required in 23 states

- **12 more pending**
- **Also required for retail banks**
- **Dozens of national laws proposed in the House and Senate**
- **CA SB 1386 (the first of the state laws)**
  - Affects organizations that do business in, have customers in, or have employees in California
  - Must provide appropriate notification to said individuals if systems are compromised and personal data is exposed
- **The organization must contact the individual**
  - In writing or through email
  - Publicly, if private conduit fails
- **The organization must inform the individual that their personal information was or may have been compromised**

When to Notify ??

- **Exceptions**
  - Does not apply to organizations that do not store personal customer information or personal employee information on computers
  - If the data was encrypted in storage at the time of the breach
- **Common interpretation**
  - As long as the organization encrypts data in storage, they do not have to notify
- **But, ask yourself**
  - Was the data in storage at the time of the attack ??
- **Rule of thumb for encryption**
  - **In all cases of breach, notify, unless there is evidence to suggest reasonable assurance that the data was encrypted at the point of attack.**
  - **Look for the courts to establish this as precedent**

When to Fix ??

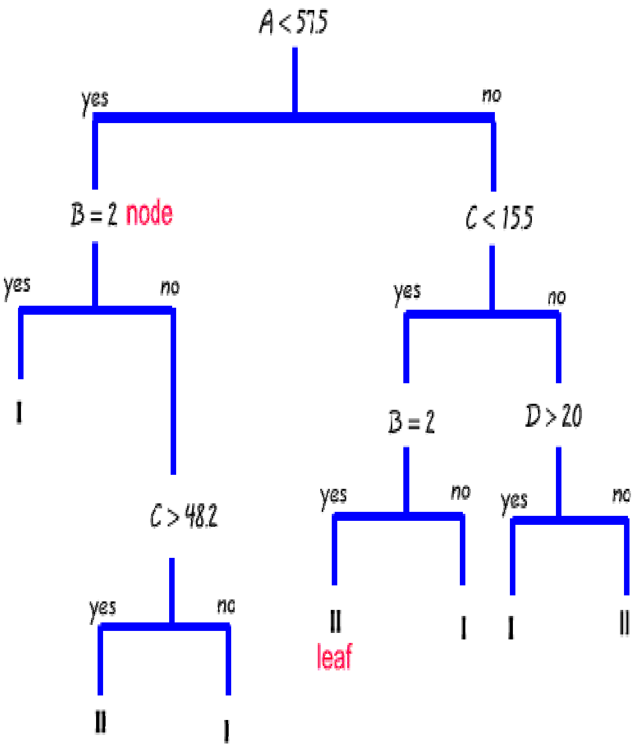
Resolution of incidents is at the discretion of the organization

- **Typically, fixing is associated with simple mistakes**
  - Blunders
  - Misuse of privilege
  - Well-intentioned employees
- **Administrative matters**
  - No evidence of criminal intent
  - No harm done
  - May involve disciplinary measures for the employee
  - Formal documentation of the incident is sufficient
- **Notify ??**
  - Look to specifics of state law

Investigative Response

Neither Federal regulation nor state law currently require investigation or prosecution

- **Not a decision that the organization can reasonably make during an incident**
- **Create a decision tree**
  - Establish parameters – when to fix, if and when to investigate
  - Fixing and investigating can sometimes be mutually exclusive
  - Organization needs to understand the impact of investigation and prosecution
  - Incorporate these decisions and procedures into the Incident Response Plan



When to Prosecute ??

Also at the discretion of the organization

- **Typically associated with complex attacks**
  - Malicious intent
- **Civil or criminal activity**
  - Sensitive data clearly accessed, stolen, altered
  - Damage to systems, services, devices, or data
  - Evidence of an external intruder
- **Furtherance of the organization's good faith effort**
  - Hard to prove negligence
  - Satisfies common law liability

Brace for Impact

In either case, the organization must be prepared

- **Freeze systems as long as it takes to establish the forensic trail**
  - Isolate affected systems
  - Invoke business continuity plan to maintain operations
- **Submit to the authorities**
  - Local law enforcement search
  - Federal law enforcement search and seizure of equipment and data
  - Provide resources for the duration of the investigation
- **Prosecution takes time and resources**
- **In cases of organized crime, revenge is an issue**
  - Be prepared for retaliatory attacks on systems and data
- **Investigation and prosecution may delay notification**

But this is all after the fact

- Affected organizations should set up a security program to mitigate risk, and protect from breaches to the extent reasonably possible
- At minimum
  - Identify systems containing PHI and consider intrusion detection.
  - Encrypt personal information. (maybe)
  - Ensure that third-party contracts involving the creation, transmission, storage and destruction of PHI include information security provisions.

A Sound Information Security Program

A Sound Security Program

Reviews HR & Management Issues

- Hiring and retention policies for IT/security staff & end-users
- Adequate staffing, authority, responsibility, succession
- “Key Man” and training policies
- Termination

“Institutionalize” InfoSec

- IT in Corporate Governance
- Management Philosophy
- Corporate Culture
- Periodic training and review for all personnel

Reviews Network Architecture

- Segmentation
- Critical Devices
- User rights and permission

Inspects Physical Security

- Door locks and alarms
- Security cameras and monitoring
- Visitor access logs
- HVAC, fire suppression, etc.
- Racks and cabling

Reviews Business Policies & Procedures

- Backup and failover contingency
- Redundancy, disaster recovery, and business continuity planning
- Current equipment inventory
- Third-party provider SLAs & liability
- User rights and permissions
- End-user computing policies

Performs electronic testing

- Firewall(s) & Routers
- Devices visible to the Internet
- Network segmentation
- Active/Inactive modems
- OS levels & patches
- Anti-virus software

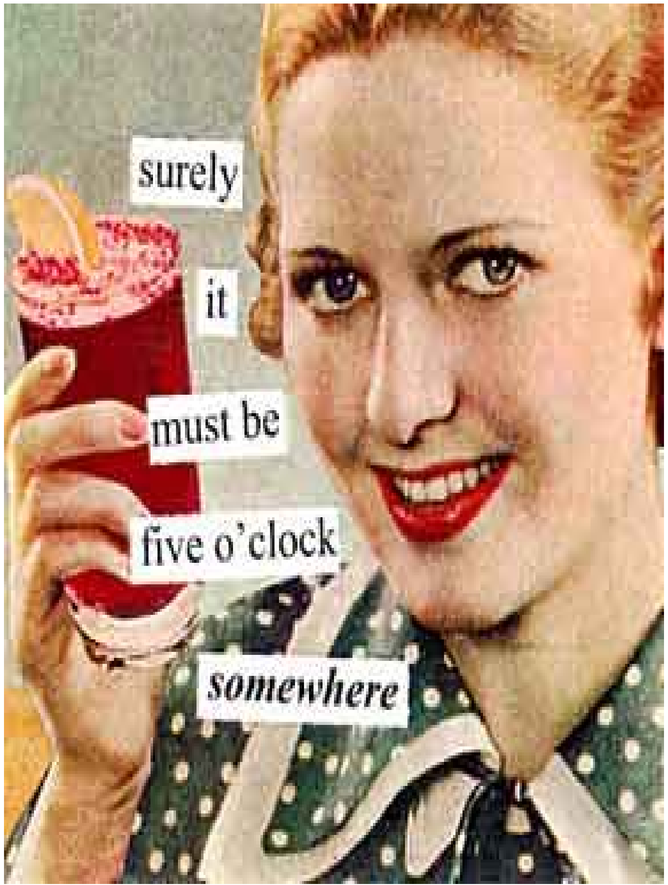
That being said

- Accept that there are no 100% guarantees with information security
- Establish a level of risk tolerance based upon a thorough, document risk assessment
- If not directly affected by state law, consider making notification a part of your incident response plan and your disaster recovery plan
- Federal notification law is inevitable !!!!

Summing Up . . .

In the event of a security breach

- Invoke the incident response plan immediately
- Restore to the point of being made whole
- Make notification a part of the incident response plan
- Learn from the mistakes of others (or your own)



- But most importantly
  - Have an infosec program in place so that you don't have to worry
- HIPAA compliance means never having to say you're sorry…..

Questions? Comments? More Info?

- Security Portal -- www.cybertrust.com
  - White papers
  - Webinars (live and archived)
  - Hype or hot

- Contact Info

Marne E. Gordan
Director, Regulatory Affairs
marne.gordan@cybertrust.com
703/480-8727