Session 3.04
Planning for Failure: Developing an Effective Incident Response Plan for HIPAA Compliance

HIPAA Summit VII
September 16, 2003

Marne E. Gordan

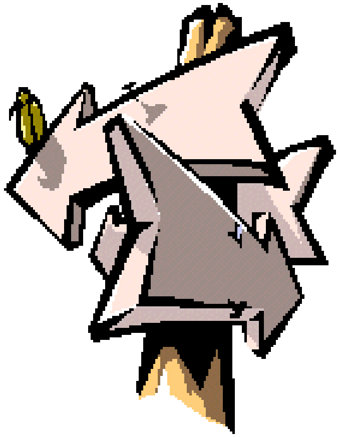
Director, Regulatory Affairs

TruSecure

Agenda

- **HIPAA Overview**
  - Protecting Patient Data (PHI)
  - HIPAA Incident Response Requirements
- **State of the Internet**
- **8 Common Mistakes in Incident Response**
- **Object Lessons Straight from the Headlines**
  - Then and now
  - Why health care organizations
- **Investigative Response**
  - Fix, Prosecute, or Notify ??
- **Q&A**

HIPAA Overview



HIPAA Overview

- **Affected health care organizations are expected to *protect* Protected Health Information (PHI) from breach or compromise**
- **A key element in protecting PHI will be your organization's plans and procedures for responding to an information security incident**
- **The security standard currently requires that affected organizations have in place**
  - Reporting procedures
  - Response procedures

  for dealing with breaches of information security

HIPAA Overview

- **§164.308(a)(6)(i) Standard: Security incident procedures**.
  - Implement policies and procedures to address security incidents
- **§164.308(a)(6)(ii) Implementation specification: Response and Reporting (Required).**
  - Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.
- **NOT specifically required by HIPAA**
  - Development and maintenance of an IR plan
    - "Key man" identification
    - Notification and escalation procedures
    - Training of all personnel identified by job function within the plan
    - Routine review and updating of the plan
    - Annual testing of the plan

HIPAA Overview

- **Health care organizations have to prepare for HIPAA compliance and real world threats**
- **Health care organizations are a target for hackers and thieves because**
  - they process and store PHI
  - they contain attractive corporate assets
- **HIPAA focuses on harm to the patient**
  - Embarrassment
  - Identity Theft
- **Security and Privacy protections overlap**
  - It is often a security breach that leads to a privacy violation

State of the Global eBusiness Environment

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 procedures

Examples of Incidents

- Trusted insider copies and removes a large amount of proprietary data from a financial institution
- Unknown entity accesses and removes customer data from a retail industry client, and publishes it
- Administrator observed accessing sensitive government data without specific authorization, however, the individual needs administrative access rights and privileges to those machines
- Financial services provider receives questionable threat from unknown source about proposed hacking activity
- Manufacturer receives credible threat that a known group may try to interrupt a industry-sponsored Internet event

Slammed on All Sides

Viruses

Employee Error

Rogue Insiders

Software Bugs

Corporate Spies

Script Kiddies

Web Defacements

Password Crackers

Network vulnerabilities

Denial of Service

"SneakerNet"

War Drivers

Backdoors

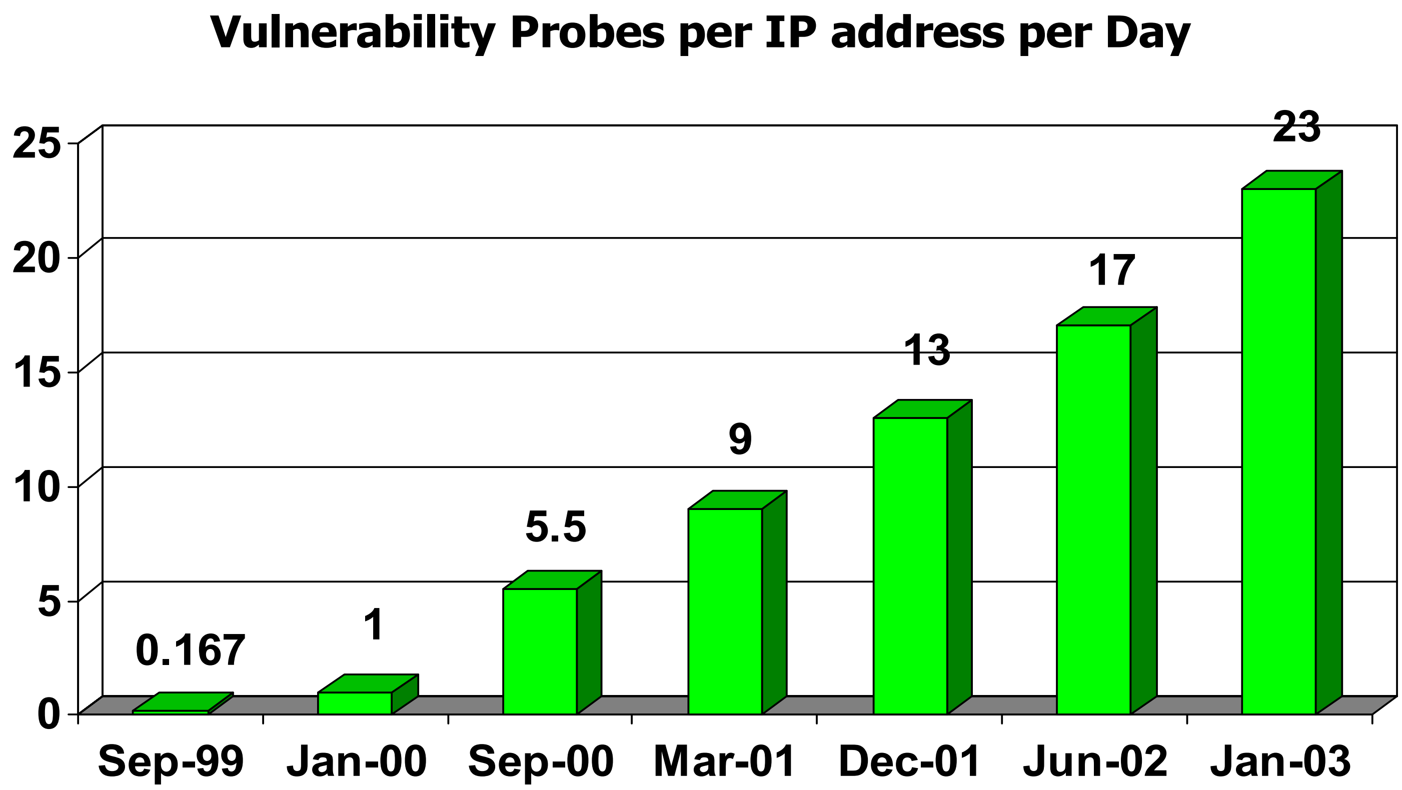
Worms

Trojans

Buffer Overflows

"Blended Threats"

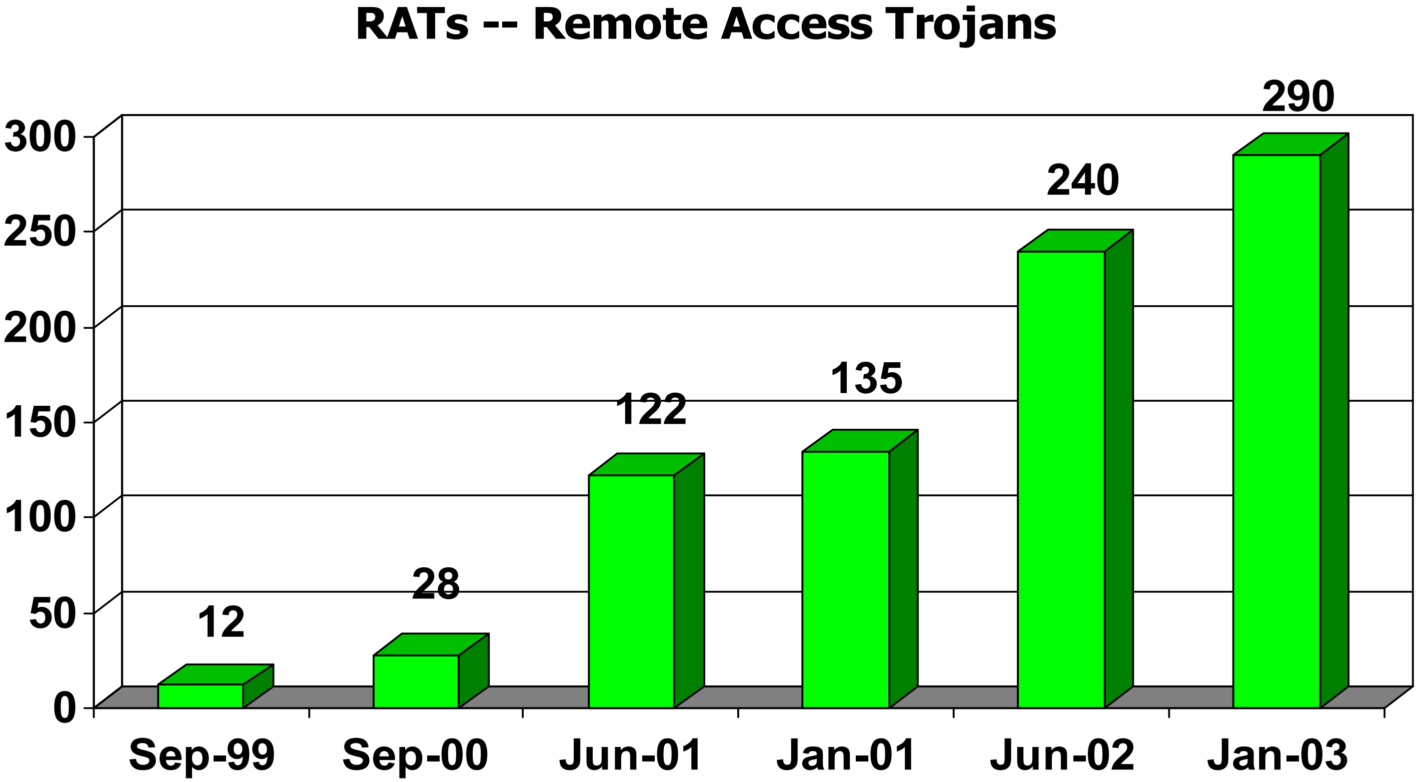
Daily Vulnerability Probes



Source: Statistics provided by ICSA Labs

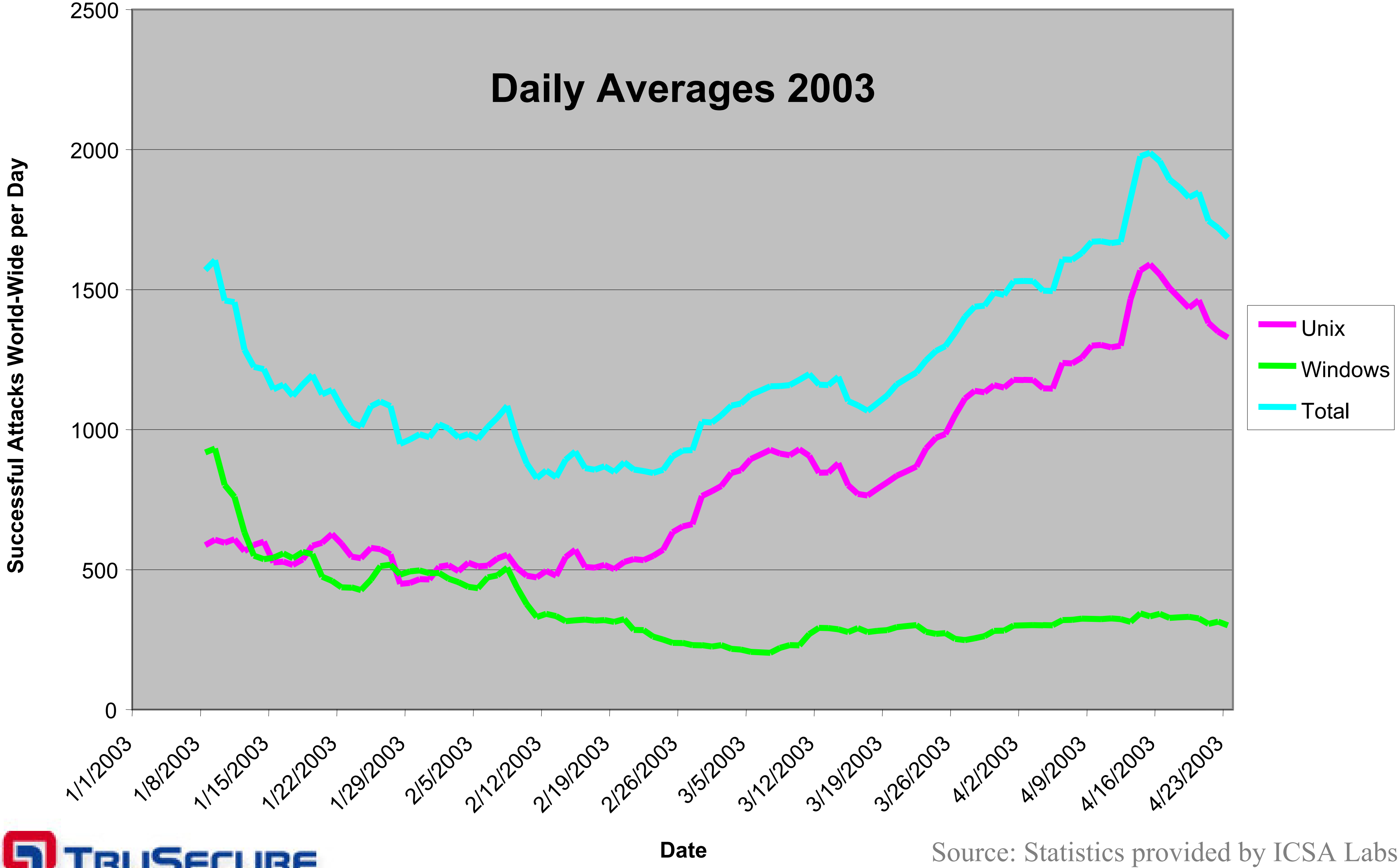
Remote Access Trojans Planted Daily

Each leads to perhaps 10-10,000 compromised PCs



Source: Statistics provided by ICSA Labs

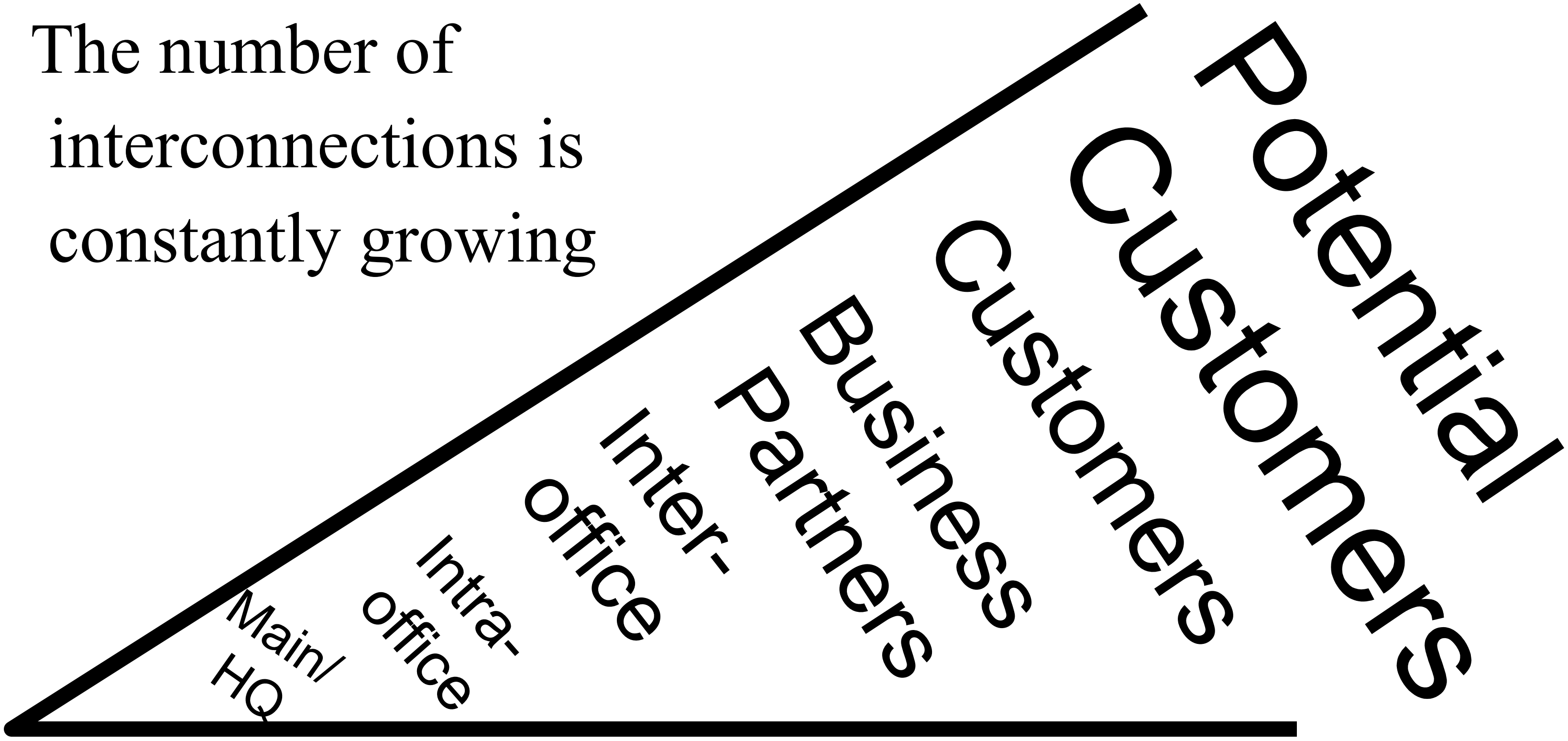
Successful Web Site Attacks:



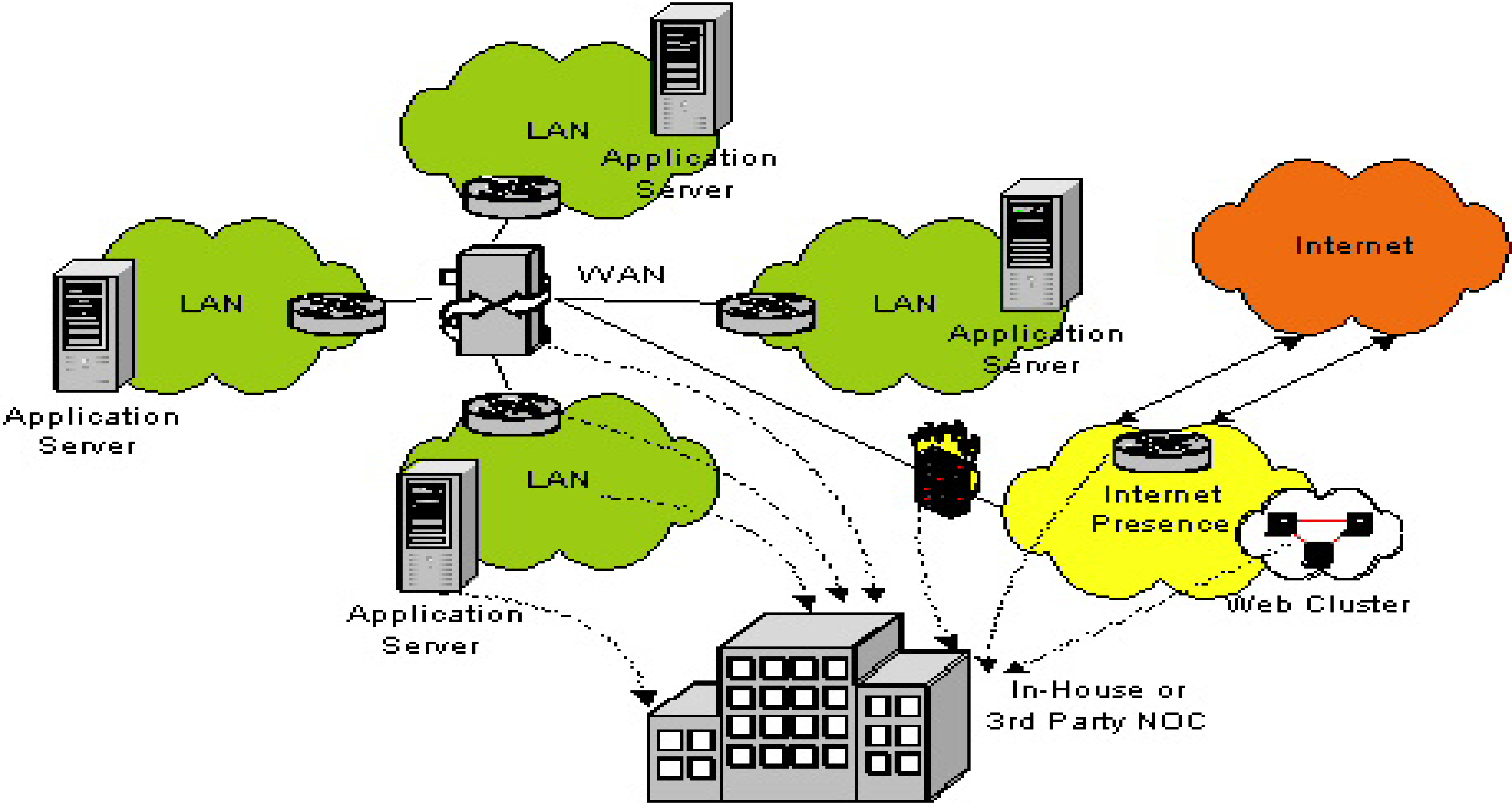
Source: Statistics provided by ICSA Labs

Connectivity Scenario Increasingly Complex

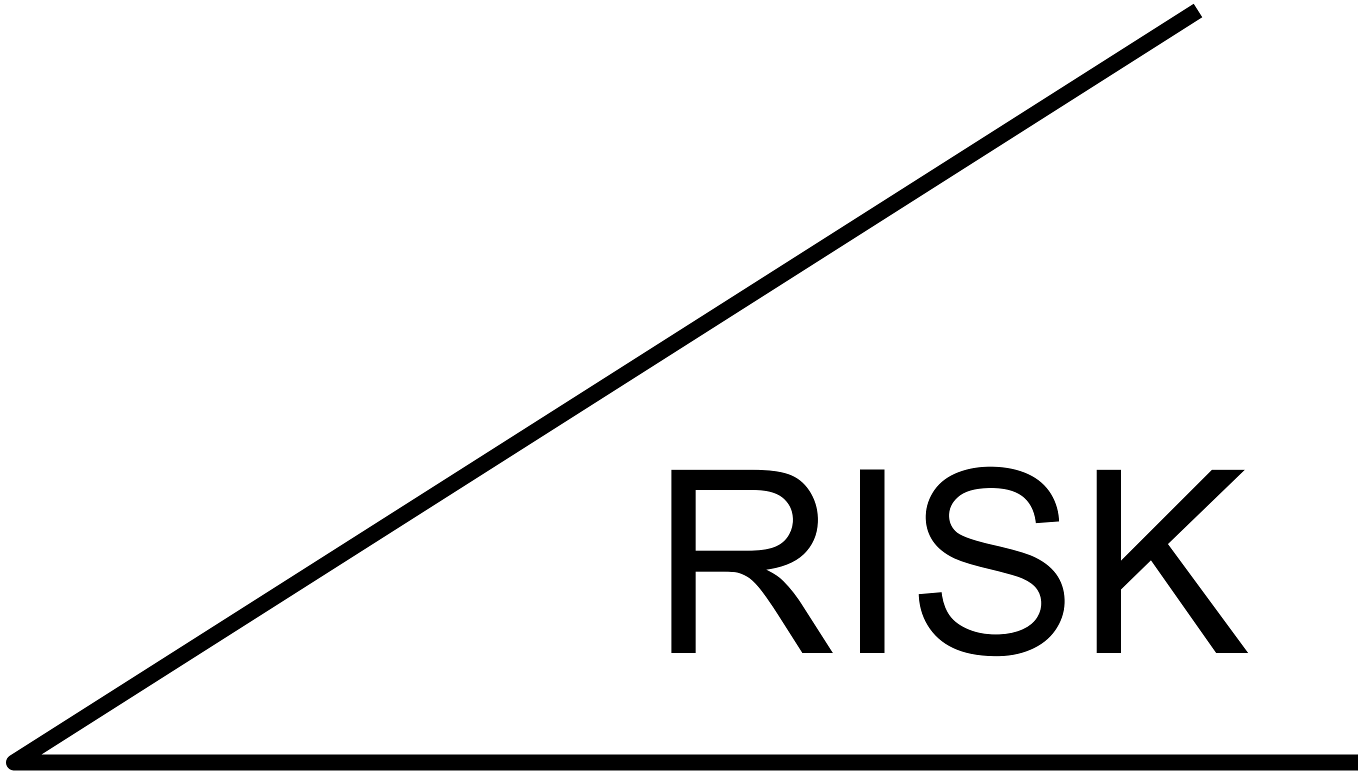
The number of interconnections is constantly growing



Connectivity Scenario



Increased Connectivity = Increased Risk



RISK

Network Size, Services, Connections

“Get Security”

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 14 times per day for known vulnerabilities.
- About a dozen computers somewhere in your organization encountered a computer virus.
- 17 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 six 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 one person 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 65% likelihood that the next security breach your staff deals with will come from an insider.

Statistics provided by ICSA Labs

The odds are good that you will experience some sort of breach ….

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

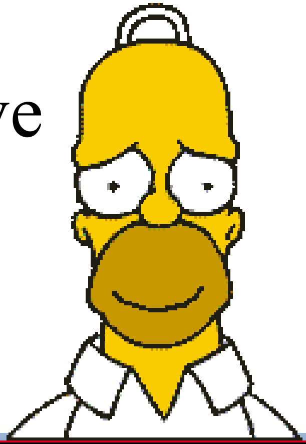
Incident Response: 8 Common Mistakes

#8: Failure to Address the Risk

- **Organizations fail to close or shut down attack vector while “fire fighting”**
- **Isolate the attack and halt the spread**
  - Disconnect the system from all network connections
  - Don’t underestimate the scope of the event
  - Unless there is clear and compelling reason to permit a continuation of the breach, stop the attack!

#7: Failure to Learn from the Past

- **The organization's security training does not include learning from past events, or the maintenance of performance trends**
- **"Those who fail to learn from the past…"**
  - Conduct an "after action"
    - Review the incident
    - Review the response
  - Refine the plan according to the most effective response measures



#6: Failure to Invoke Escalation Policy

- **Staff fail to notify appropriate personnel and follow IR procedures**
- **It is imperative that the organization develop and implement escalation procedures.   Staff should understand when and how to:**
  - Identify an incident
  - Notify IR Coordinator
  - Triage the incident
    - Do no harm
    - Protect life, data, infrastructure, operations
    - Develop and execute a course of action
  - Implement a "need to know" classification
  - Establish "out-of-band" communications channels – PGP, pre-established phone bridge

#5: Failure to Keep Good Backups

- **When original data is compromised or lost, the organization cannot recover or restore it.**
- **The organization must maintain secure backups and forensically sound media images**
  - Surprisingly, backups are often ignored or forgotten.
  - System compromise is often discovered months after the event; backups should be maintained for several months
  - Creating backups on a regular basis and label media clearly
  - Don't assume that backups are always good; test periodically
  - Periodically verify the correctness and completeness of backups
  - *The best backup scheme in the world is useless if you cannot also do a recover.*

Source: RFC 2196, “Site Security Handbook,” September 1997.

#4: Failure to Document

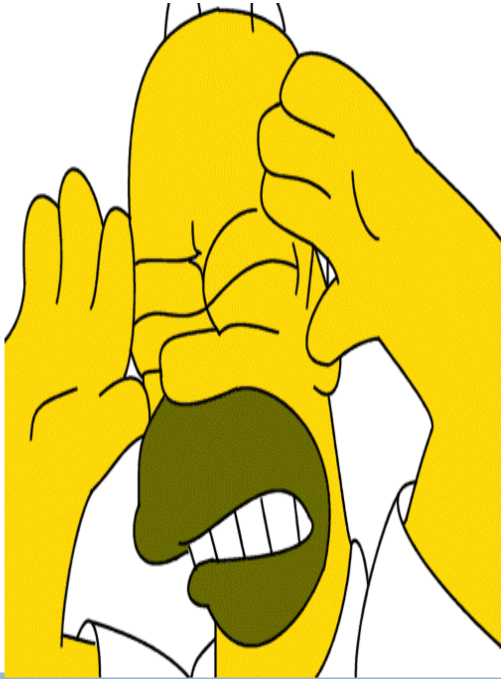
- **If the organization needs to involve law enforcement to investigate, or chooses to prosecute, complete documentation of the incident is required.**
- **Take Good Notes**
  - Invest the time
    - If it isn't written down, it didn't happen
    - Documentation of incidents is required by HIPAA
  - Use Old Fashioned Pen and Composition Book
    - Harder to alter than electronic files
    - Some jurisdictions view hard copies and paper files as the official records
  - Notes should be Clear, Concise, and to-the-point
    - They may be your only fall-back in court!

#3: Failure to Protect Potential Evidence

- **During recovery, staff may inadvertently destroy critical evidence, limiting the ability to prosecute**
- **Create and Maintain Secure Copies**
  - Protect it from alteration -- Lock it, document it, limit access to it
  - Make non-invasive copies (bit image)
  - Analysis work from copies of copies - ONLY
  - Protect the "chain-of-custody"
  - Ensure no one touches the system and possible evidence until IRT has gathered and cataloged the evidence.
  - Ensure that no one does the **Wrong Thing**, thinking it is the Right Thing.
    - **Wrong Things** would include
      - Taking a backup, using system backup software
      - Editing the log files for ease of readability or to remove company confidential information

#2: Failure to Communicate

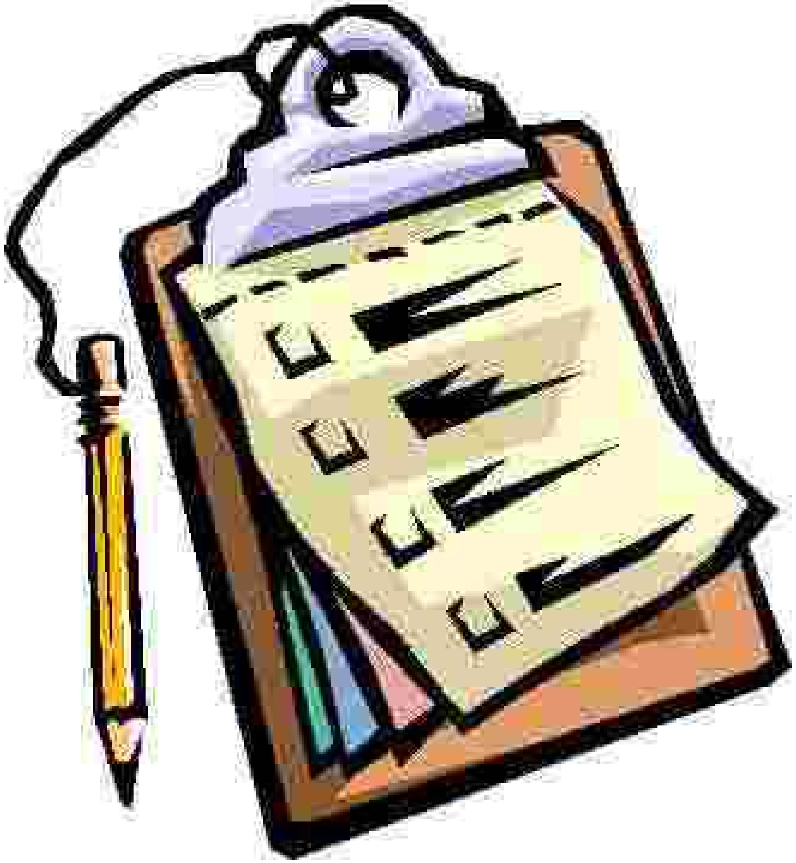
- Internal Communications Breakdown
- It is imperative that staff are trained on Incident Response procedures, and that changes and updates to procedures are communicated on a regular basis. Staff should understand:
  - Defining an “incident”
  - Declaring it an “incident”
  - Invoking the response plan
  - Having common understanding of terms
  - Tracking what has been done and what needs to be done (and documenting it!)



#1: Failure to Prepare

- **Insufficient, untested, or non-existent IR procedures**
  - No reliable audit trail
  - No accountability
  - Untrusted installation media
  - Untested backup and recovery
  - Disorganized, incomplete, inaccurate, or non-existent logs
  - No physical or electronic access records
  - No working incident response plan
- **Incidents can't be predicted, but preparation is critical**

Incident Response: Important To-Dos



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, and Tested
- **Staff must be**
  - Trained on security and IR
  - Offered refresher information on a regular basis
  - Provided with information on updates to policies and procedures

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

Performs electronic testing

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

Reviews Network Architecture

- Segmentation
- Critical Devices
- User rights and permission

A Sound Security Program

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

Issues to Consider

- 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

Learn from the 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

Lessons Learned

A Look at 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

Are You a Target ??

- Health care organizations
  - not typically viewed as hacking targets
  - Not as obvious as banks, e-retailers, etc.
- But
  - Process and store huge amounts non-public personal consumer information
    - SSN, insurance information, payment information, etc.
  - Payment and insurance information is a target for fraud
  - SSN is the key to identity theft

Case A

Hacker Accesses Patient Records

By Robert O'Harrow Jr.
Washington Post Staff Writer

Saturday, December 9, 2000; Page E01

“A hacker gained access to confidential medical information at the University of [ABC] Medical Center, using the Internet to download thousands of files containing patient names, conditions, home addresses and Social Security numbers, hospital officials said yesterday. “

The Highlights

- In this case, a hacker specifically targeted the hospital
  - Because of the PHI
  - Because of the perceived security weakness
  - Executed a relatively simple exploit
  - "To make a point"
- Hacker had unrestricted access for over six months
- Hospital KNEW there was an intruder in the network, didn't realize that data was compromised
- Patients PHI publicly disclosed

Then and Now

- **Incident occurred in December 2000**
  - Health care industry viewed it as an object lesson
  - Pointed to security and privacy issues
  - "No harm done"
- **A similar incident in 2003??**
  - Plaintiffs attorneys are circling…..
  - Consumer privacy advocacy
  - Identity theft awareness
  - There is going to be a push to establish case law/ precedent
  - "Good Faith Effort", following well documented procedures, and other "proactive measures" will be an organization's best defense in court

Case B

Tiny Nevada hospital attacked by Russian hacker

USA Today Online

April 7, 2003

RENO (AP) — A hacker who invaded the computer system at [Case C]Hospital in Ely has been traced to the former Soviet Union, authorities said.

The Highlights

- **Hacker**
  - Did not specifically target the hospital
  - Used the Al-Jazeera website as an attack conduit
  - Did not access PHI
  - Did access employee SSN and payment records
- **Hospital response**

"It was just after 6 a.m. and I saw an active connection from outside, on a path through the emergency room to the payroll computer, but I knew no one was in the payroll office." He ran to the affected computer and pulled the plug.

  - Informed FBI – performed forensics
  - Took immediate corrective action – Revised end-user policies

Case in Point

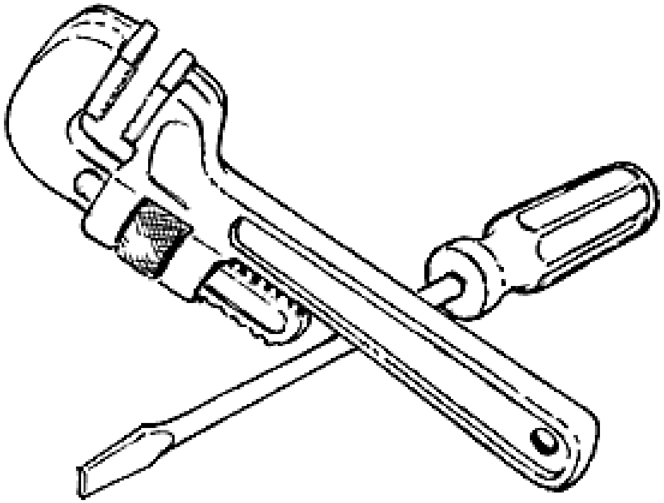
- **There's no telling what will attract some hackers . . . .**
  - **"Capture the flag"** – greater glory and personal bests (traditional and almost old-fashioned)
  - **"altruistic"** – making statements and proving points (Deceptive Duo, S4t4n1c_S0uls, and The Bugz)
  - **"scorched earth" attackers** – 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 C]**
  - More than half the UK workforce* would be prepared to seek revenge on former employers by exploiting continued access to corporate systems if they were unhappy at losing their 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

Fix, Prosecute or Notify??



When to Notify ??

- **Now required in California**
  - **CA SB 1386**
    - 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
- **National legislation proposed**
  - Dianne Fienstein (D-CA) proposed similar legislation in the Senate
  - Will California courts establish privacy case law?

Investigative Response

- One step beyond incident response
  - There is no requirement under the HIPAA Security Standard to investigate or prosecute
  - 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 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

When to Prosecute ??

- **Also at the discretion of the organization**
  - **Typically associated with more complex attacks**
    - Malicious intent
  - **Civil or criminal activity**
    - PHI or corporate data clearly accessed, stolen, altered
    - Intellectual property accessed, stolen, or altered
    - Damage to systems, services, devices, or data
    - Evidence of an external intruder
  - **In cases of a PHI breach or privacy violation, furtherance of the organization’s good faith effort**
    - Hard to prove negligence

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**

Summing up . . . .

- **Plan for failure** –
  - **Develop policies and procedures** – for responding to security incidents across the organization, and include all appropriate personnel
  - **Maintain the plan** – keep it current and test it annually
  - **Learn from the common mistakes** – yours and others
  - **Think outside of HIPAA** – there are resources in your organization outside of PHI that may be targeted
  - **When possible, spend in parallel** – if HIPAA controls make sense for other areas of the organization, take the opportunity to implement
  - **Make decisions now** – not during an actual emergency

Q & A

Contact Information:
Marne E. Gordan
TruSecure Corporation
703/480-8727
mgordan@trusecure.com