HIPAA Security and Cybercrime:

The View from the Trenches

The Seventh National HIPAA Summit
September 16, 2003

Sonnenschein®
SONNENSCHEIN NATH & ROSENTHAL LLP

Presenters

W. Reece Hirsch, Partner
Sonnenschein Nath & Rosenthal LLP
San Francisco, California

Michael Falzano
Senior Director/Chief Healthcare Compliance Officer
The TriZetto Group
Albany, New York

Christian S. Genetski, Partner
Sonnenschein Nath & Rosenthal LLP
Washington, D. C.

The Factual Background

- In 2002, PharmCo hired 5 new drug interaction specialists to conduct patient trials on a potential breakthrough drug
- The employees were hired during a period of high turnover in PharmCo's R&D department
- Rushed process to get new employees laptops and RIM devices

More Facts

- 3 of the 5 employees get laptops containing data from former employees resident on drives, including PHI
- 2 of the 5 employees elect to use their own RIM devices rather than PharmCo supplied devices

One Year Later

- 3 of the 5 employees leave to join a new, competing company
- Laptops are confiscated upon their departure
- After a few months, word begins to spread via Internet message boards that the competing company will be announcing new drug and results of extensive patient trials (same type as PharmCo is developing and set to announce)

PharmCo Suspicions

- CEO of PharmCo wants to know who is posting the message, and whether former employees stole confidential data and/or are being assisted by 2 remaining employees
- He wants investigation, and demands it be fast, thorough and quiet

Investigation

- External
  - Pre-litigation discovery options
- Internal
  - Have IS staff check audit logs for big file transfers, max out firewall rule sets
  - Review exchange servers for e-mail
  - Forensic review of employee (and former) laptops

Investigative Issues

- Do policies permit necessary searching and monitoring?
- Does company culture pose obstacles to investigation?
- Were sufficient logging and forensic capabilities performed?

Results of Investigation

- Audit logs show large FTP file transfers shortly before former employees left (late at night)
  - Match file sizes to current patient trial data files
- Laptops show both transfers of data to removable storage devices and deletions (no wiping software though)

Results of Investigation

- Forensic review shows entire drive of laptop appears to have been copied by former employee who had laptop containing PHI files
- Additionally, data from current patient trials, which also includes PHI, appears to have been stolen

HIPAA

- PharmCo is a HIPAA health care provider covered entity because it is directly conducting clinical trials.
- PharmCo is also a PBM acting as a business associate of health plans.
- Theft of data implicates both Privacy and Security Rules.
  - The "little Security Rule": Section 164.530(c)

Security Rule: The Four Commandments

- Section 164.306(a) provides four general requirements, which give rise to more specific standards and implementation specifications.
- A covered entity must:
  - (1) Ensure the confidentiality, integrity and availability of all electronic PHI the CE creates, receives, maintains or transmits.
    - Did PharmCo "ensure confidentiality?"

Security Rule Commandments

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI.

- Could the data theft have been "reasonably anticipated"?
- Risk analysis (164.308(a)(1)(ii)(A))
- Risk management (164.308(a)(1)(ii)(B))
- Workforce clearance procedure (164.308(a)(3)(ii)(B))

Security Rule Commandments

(3) Protect against any reasonably anticipated threats or hazards that are not permitted or required under Privacy Rule.

- Disclosure by employees would violate Privacy Rule
- But could the actions have been "reasonably anticipated"?
- Information system activity review (164.308(a)(1)(ii)(D))
- Workforce authorization and/or supervision (164.308(a)(3)(ii)(A))

Security Rule Commandments

(4) Ensure compliance with Security Rule by workforce.

- Sanction policy (164.308(a)(1)(ii)(C))
- How far is a covered entity expected to go to "ensure" compliance?

Reasonable and Appropriate

- For addressable implementation specifications, CE must determine whether the measure is "reasonable and appropriate," taking into account:
  - CE's size, complexity and capabilities
  - CE's technical infrastructure, hardware and software capabilities
  - Cost
  - Probability and criticality of potential risks

California Civil Code Section 1798.82

- First-of-its-kind California security breach reporting law, requiring:
  - any person or business conducting business in California
  - must report any breach of security
  - resulting in disclosure to an unauthorized person
  - of personal information in electronic form

Contracting Issues

- PharmCo's obligation to report incident under business associate agreement
  - Has PharmCo agreed to "security incident" reporting?
  - Coordinating notification process under Cal. Civ. Code Section 1798.82

Class Action Lawsuits

- Remedies under Cal. Civ. Code Section 1798.82
  - an invitation to class action lawsuits
- HIPAA Security Rule as a standard of care in civil litigation

HIPAA Security and Cybercrime

Michael A. Falzano, Chief Compliance Officer

The TriZetto Group, Inc.

Agenda

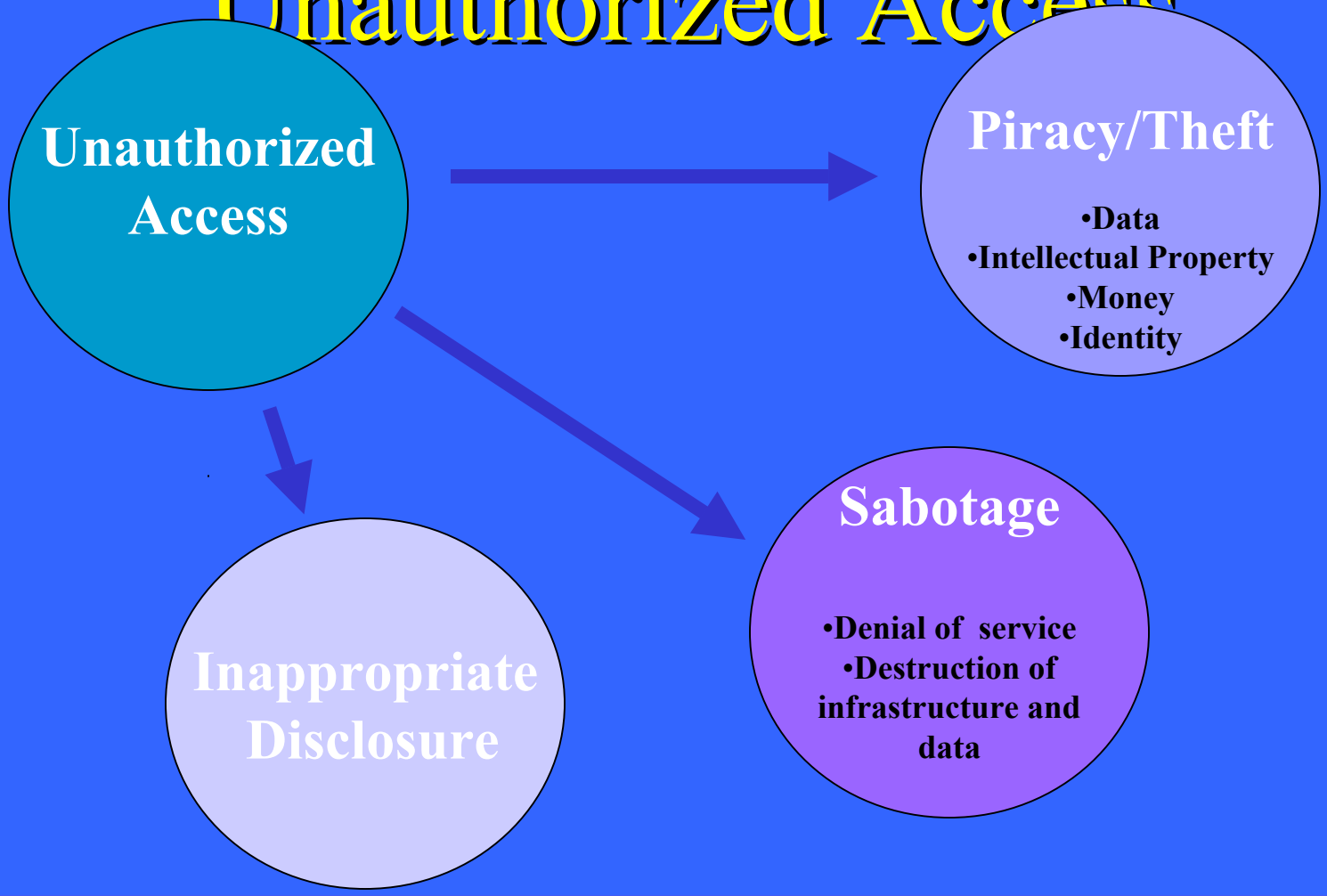
WELCOME!

- ✓ Cybercrime '101'
- ✓ HIPAA security risk framework
- ✓ Elements of an effective compliance program

Cybercrime

- Cybercrime is unlawful activity that involves the use of computers and related technologies
  - Some examples:
    - Unauthorized access
      - Theft/piracy
      - Inappropriate disclosure
      - Sabotage
    - Fraud
    - Stalking

Unauthorized Access



Computer Crime and Security Survey

- CSI/FBI jointly conduct annual survey - available at www.gocsi.com
- Over 500 security professionals surveyed
- Highlights of Survey 2003
  - Risk of cybercrime remains high
  - Even the most "secure" entities can incur losses
  - Information theft caused greatest financial loss, followed by denial of

Cost of Cybercrime

- Industries are quantifying cost of cybercrime
- Increased awareness will improve reporting
- Information to date is incomplete due to:
  - Lack of uniform reporting
  - Some cybercrimes can't be easily costed out
    - i.e., what is real cost of a security breach

Psychosocial Factors in Cybercrime

- Anger
- Revenge
- Greed
- Curiosity
- Recognition/infamy
- Beliefs, religion, politics, ideology etc.
- Control
- Obsession

Who Commits Cybercrimes?

- Employees*
- Terrorists
- Organized crime members
- Students
- Competitors
- Anyone can (‘8 – 80’ years old)

* Some studies show that over 75% of computer crimes are committed by employees. Others show less stunning, but still significant

Computers and Cybercrime

"Perpetrator"

"Victim"

"Witness"

What's In Your Computer System ?

Assets

- **Hardware/software**
- **Intellectual property**
- **Business and financial plans**
- **Prospect/customer lists**
- **Your customer's data**
- **Individual-specific information**
  - **Protected Health Information (PHI/HIPAA)**

What To Focus On?

Look at your company from all sides

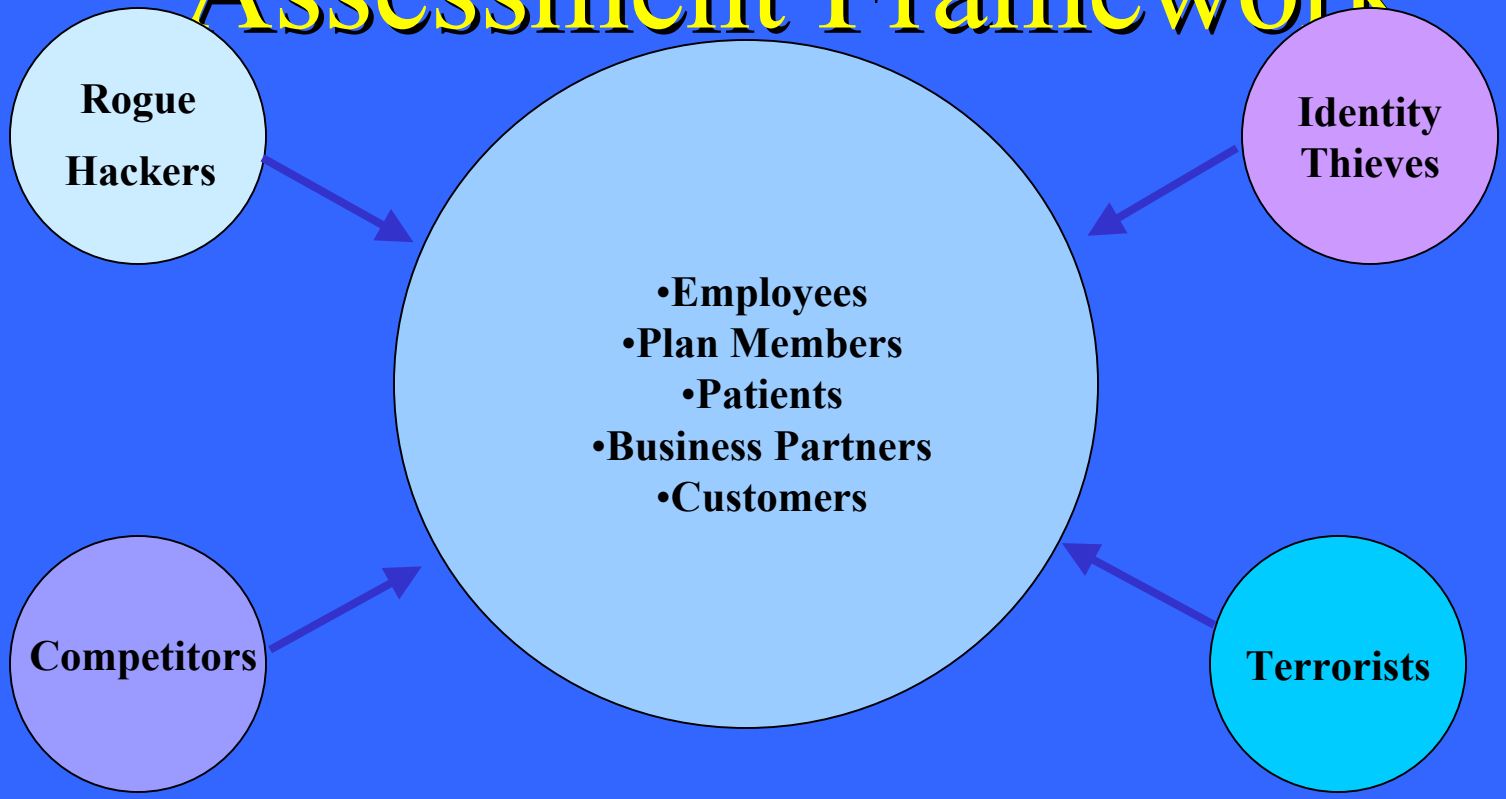
- **Internal threats from disgruntled current or former:**
  - **Employees**
  - **Customers**
  - **Plan members or patients**
- **External threats**
  - **Business competitors**
  - **Individuals looking for targets to prove they can find a vulnerability**

HIPAA Security – High Level

- **Ensure CIA of electronic PHI**
  - Confidentiality
  - Integrity
  - Availability
- **Protect "against reasonably" anticipated threats/hazards**
- **Protect "against reasonably" anticipated uses/disclosures**
- **Ensure compliance by workforce**

HIPAA Security Risk Assessment Framework

Think inside and outside your circle!



HIPAA Security Risk Assessment Framework

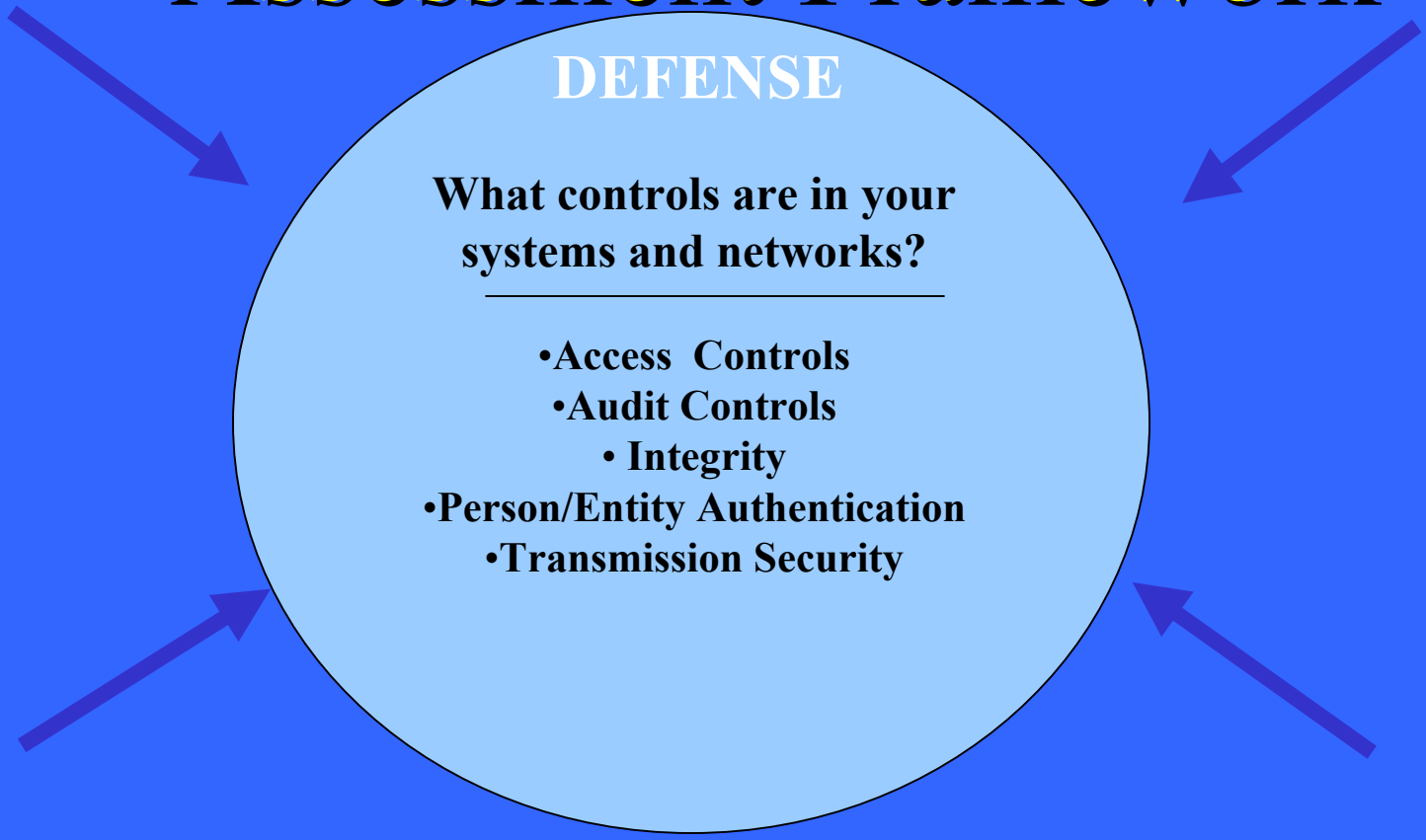
Identify and assess your administrative safeguards/vulnerabilities!

HIPAA Security Risk Assessment Framework

Identify and assess your physical safeguards/vulnerabilities!

HIPAA Security Risk Assessment Framework

Identify and assess your technological safeguards/vulnerabilities!



Access Control is Key to HIP rity

Access Controls

STOP

- **Administrative Safeguards**
- **Technical Safeguards**
- **Physical Safeguards**

Inappropriate Disclosure

Piracy/Theft

- **Data**
- **Intellectual Property**
- **Money**
- **Identity**

Sabotage

- **Denial of service**
- **Destruction of infrastructure and data**

A Word About Regulatory Enforcement

- Per Interim Final Enforcement Rule
  - OCR and CMS want to promote voluntary compliance
    - Guidance and technical assistance
    - Plan to adopt Office of Inspector General (OIG) approach as "platform"
- Having an effective security compliance program is evidence of voluntary compliance

Effective Compliance Program

Excerpt from Federal Sentencing Guidelines

"An effective compliance program means a program that has been **reasonably** designed, implemented and enforced so that it **generally** will be effective in preventing and detecting criminal conduct. Failure to prevent or detect the instant offense, by itself, does not mean that the program was not effective. The hallmark of an effective program is that the organization **exercises due diligence in seeking to prevent and detect** criminal conduct by its employees and other agents."

Compliance Program Basics

Federal Sentencing Guidelines is industry standard

- **Focus on criminal conduct but generally applicable**
- **Corporate "good citizenship" model**
- **Does not offer precise details**
- **One size does not fit all**
- **Go to http://www. ussc.gov for detailed explanation (Chapter 8)**

Compliance Program Elements

1. Standards, policies and procedures
2. Executive oversight
3. "Due care" in delegating authority
4. Communication and training plans/programs
5. Monitoring/auditing program
6. Consistent enforcement of standards
7. Reasonable approach to incident response and prevention

Closing Points

- Security enables privacy
- Don't wait until security rule compliance deadline to act
- HIPAA security standards nicely mirror elements of an effective compliance program
- Build a security risk management and compliance program that is:
  - Customized
  - Dynamic

Incident Response Planning

- Response cannot be ad hoc
- Response team should be: Security, Legal, Forensic, Press Relations, Insurance
- Designate key personnel and regularity of meetings
- Identify anticipated issues, sensitive systems - think about mergers and acquisitions and integration
- Determine reporting posture and obligations
- Plan Trigger - What sets the plan into motion
- Identify Outside Support - forensic and legal

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Division of Financial Practices

[redacted], 2003

[redacted]
Chief Privacy Officer
[redacted]

Dear [redacted]

As we discussed, the staff of the Federal Trade Commission ("FTC") is conducting a non-public inquiry into certain information practices by [redacted] connection with personal information that it maintains. According to a recent news report, client data maintained by [redacted] on an FTP server was stolen by the former employee [redacted] Section 5 of the FTC Act prohibits deceptive or unfair practices, including misrepresentations about security practices and unfair practices that cause substantial injury to consumers. Accordingly, we are seeking to determine whether [redacted] or its clients' representations and practices regarding the handling of consumer information raise any issues under Section 5.

Unless otherwise stated, the scope of the inquiry is from January 1, 2003, to the present. Please provide the following:[2]

1. The complete legal name of [redacted] and all other names under which [redacted] has done business; the corporate mailing address; and the date and state of incorporation.

2. Copies of all policies describing the privacy and security practices employed by [redacted] at the time of the incident referred to above.

3. All documents containing or relating to representations [redacted] has made to clients and/or consumers regarding [redacted] safeguarding of consumer personal information in its possession, custody, or control.

4. All information and/or documents related to the security of the FTP server from which information was stolen or improperly accessed; the security measures in place to protect data posted on the server; policies governing the proper use of the server; persons with access to the server; and all logging, monitoring or backup procedures for the server.

5. All information and/or documents regarding the files that were stolen by or potentially accessible to unauthorized individuals, including:

Designating Personnel

- Create team from IT Security Staff, Counsel's Office, Press or Investor relations. Meet in peacetime. A crisis is no time for introductions or background briefing!
- Issues to know:
  - Who has access to the network?
  - Extent of authorizations?
  - What types of logs or backup copies are available?
  - What types of preventive forensics have we done?
  - What range of options do our internal policies permit?

Issues for Counsel

Does incident create potential liability to customers, shareholders, downstream sources?

What level of due diligence is required to avoid liability if the incident escalates?

If Internal Investigation - should it be under supervision of counsel's office?

Any internal investigation must be in compliance with corporate policies and applicable laws

Will litigation be necessary to find out who is responsible? John Doe suits? Should a criminal referral be made?

Are there reporting obligations? To whom?

Most Cybercrime Cases

- Should we call law enforcement?
  - How will the government's involvement help us?
  - How will the government's involvement hurt us?
- When should we call?
  - What do we know about the conduct?
  - How would we want to investigate the conduct?
  - What's the actual or potential value of the loss?
  - Are our own remedies inadequate?
- What should we say?
  - Not the 911 model
  - Do we want civil investigation/lawsuit to continue?

Do you want to call the Government?

YES

- Sends powerful message to would-be predators - we will report you
- Cost-effective
- Government has powerful tools - Search Warrants, Grand Jury - versus voluntary production of documents in discovery
- Get mandatory restitution for low investment (MVRA)
- Low likelihood of civil recovery
- Bad publicity from lawsuit
- It's a crime, it's the right thing to do.

NO

- Government may move slowly
- Exposing internal workings/information
- Potential bad publicity
- Lose control over matter
- Disruption of our business
- Potential unclean hands
- Coordination/ Interference Issues

Incident Response Practice Pointers

- Overreacting
- Failure to be very specific (tech staff-lawyer miscommunication)
  - Scanned, probed, attack, denial of service, back doors, trojans
  - Don't confuse an intrusion with a fishing scheme
- Failing to follow response plan, if one exists
- Failing to look at text of policies
- Failing to keep track of response actions
- Premature notifications - cannot unring the bell
  - Proof of specifics and scope of illegal conduct
  - Understanding of loss issues
- Failure to follow forensic procedures
- Failure to involve counsel's office at the early stages

Mistakes - Criminal Referrals

- Calling Law Enforcement too soon
  - Proof of specifics and scope of illegal conduct
  - Understanding of loss issues
  - Proof of urgency
- Cold calling
- Focusing on only one law enforcement entity
  - Many federal agencies
  - Hi-Tech crime task forces
  - Call the right person, get a champion
- Failing to identify the evidence that needs to preserved.
- Waiting for government response
- Failing to coordinate ALL subsequent activity

Mistakes - Civil Investigations

- Assuming you have civil powers you do not have
  - Federal discovery is not immediate
  - Some states are much better than others for pre-litigation and post-litigation discovery
- Not understanding ISP notification policy
  - ISPs will not notify subscriber based on government request
  - ISPs WILL notify subscriber in response to civil subpoena
- Not thinking creatively
  - Many lawful and helpful solutions
    - Investigative solutions - web-bugs, cookies
    - Consent
- Internal Cases need external assistance

Contacts

W. Reece Hirsch
(415) 882-5040
rhirsch@sonnenschein.com

Michael Falzano
(518) 862-3477
Mike.Falzano@trizetto.com

Christian S. Genetski
(202) 408-6463
cgenetski@sonnenschein.com


Sonnenschein®
SONNENSCHEIN NATH & ROSENTHAL LLP