

# SANS Institute presents:

## Legal Liability For Information Security: Ask the Experts

---

- Webcast Sponsored by **netIQ**
- Speakers
  - Charles Wood, netIQ
  - Marc Zwillinger, Sonnenschein Nath and Rosenthal
  - Greg Schaffer, Pricewaterhouse Coopers
  - Orin Kerr, Professor of Law George Washington U
  - Hal Pomeranz, Deer Run Associates
  - Q/A session with today's speakers
  - Send questions to 'q@sans.org'

# Clarifying Responsibility For Information Security

- Charles Cresson Wood, CISA, CISSP
- Independent InfoSecurity Consultant
- On behalf of NetIQ Corporation
- (c) Copyright, All Rights Reserved 2003

# Bush's Response To 9/11 Attacks (1)

- Established Office Of Homeland Security Headed By Former Pennsylvania Governor Tom Ridge (Headed By Influential Leader)
- Objective: Coordinate Private & Public Efforts To Prevent, Detect, & Respond To Terrorism Across The Board (Integrated & Centralized Approach)

# Bush's Response To 9/11 Attacks (2)

- Established Advisory Executive Council (Similar To InfoSecurity Management Committee)
- Appointed And Officially Announced By 9/21 (Visible Management Support Critical To InfoSecurity Efforts)
- Executive Order For New Office Issued 10/8 (Integrated With Org Structure)

# Responsibility Definitions (1)

- Laws & Regulations
- Case Law Precedents
- Job Descriptions
- Mission Statements
- Reporting Relationship (Wire) Diagrams
- Performance Reviews

# Responsibility Definitions (2)

- Signed Compliance Agreements
- Policies & Procedures
- Internal & External Codes of Conduct
- Information Security Manuals
- User Training Manuals
- Job Specific & Periodic Training
- InfoSecurity Intranet Sites

# Responsibility Definitions (3)

- Owner, Custodian, User Roles
- Data Sensitivity Classification Systems
- Data Criticality Ranking Systems
- Systems Development Methodologies
- Risk Acceptance Memos
- Written Statements By Developers

# Liability for Unsecured Systems

Marc J. Zwillinger

Sonnenschein Nath & Rosenthal

[mzwillinger@sonnenschein.com](mailto:mzwillinger@sonnenschein.com)

**Sonnenschein**

# Information Security Practice 2000-2003

- Immediate legal response to cyber attacks, including external penetrations and internal investigations.
- Draft and review information security policies and procedures.
- Respond to criminal and administrative investigations involving customers and subscribers of client companies.
- Advise clients on laws and regulations governing the storage and exchange of electronic data over computer networks and disclosure of electronic data..
- Represent vendors of Network Security Products and Services.

# Information Security Regulation is Here

## Source of U.S. Information Security Regulation (de jure)

- Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191, 110 Stat. 1936, “HIPAA”)
- Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (Pub. L. 106-102, “GLBA”)

## Source of U.S. Information Security regulation (de facto)

- ***Threat of Downstream/Shareholder Liability***
- AG Settlements
- Insurance Coverage Requirements

# Basic Types of Liability: Law 101

- Violating a Federal or State Law
  - Criminal Penalties
  - Civil Cause of Action
- Breaching a Contract
  - Liquidated Damages
  - Breach of Contract Damages, including special damages, consequential, exemplary (punitive)
- Committing A Tort
  - Intentional Wrongful Act
  - Negligence (Duty, Breach, Cause, Harm)
  - Strict Liability (No Wrongful or Negligent Act)

# Violating a Federal/State Law

- **Computer Fraud and Abuse Act (18 USC 1030)**
  - Intrusion + (Fraud, Damage, Obtaining Information)
  - Encompasses all denial of service attacks, viruses, logic bombs, ping floods, etc.
- **Electronic Communications Privacy Act (18 USC 2701)**
  - Hacking into e-mail server
- **Wiretap Act (18 USC 2511) /State Wiretap Law**
  - Running a sniffer
- **Spam Statutes**
  - Sending non-complying unsolicited e-mail

# Breaching a Contract

- **Contract = Agreement between two parties to do, or not do, a particular thing.**
- **Obligations imposed by negotiation**
- **Contracts in the online environment?**
  - Employment agreements
  - Terms of Service / Acceptable Use policies
  - ASP Provider / ISP Contracts
  - Consultant contracts for securing networks

# Most Cases = Contract Theory

- Most computer-security related cases are based on breach of contract
  - Specific standard of conduct against which to measure
  - Damages are usually monetary (tort theories do not compensate for economic losses)
  - In absence of contract, hard to articulate a duty
  - Intervening criminal act usually breaks the chain of causation
    - Not in cases where clear duty - see landlord cases
- Problem: Contract claims are generally limited to those with privity of contract (must be party to the contract).

# Principles of Tort Law

- Intentional Computer Misconduct is a tort by the perpetrator
- Negligent failure to secure computer systems would require:
  - A duty to secure the system
  - Breach of duty (failure to live up to standard of care)
  - Breach is the proximate (foreseeable) cause of the harm
  - Victim suffers harm/damages
- Economic Analysis - Who is the lowest cost avoider?
  - Is Cost greater or less than probability of harm \* likely loss
- Economic Loss doctrine traditional bars recovery of economic loss unless there has been damage to people or property

# Alternatives

**Does holding only perpetrator liable deter wrongful acts, compensate injured parties, promote better Internet security?**

## Alternatives

- **Owners of systems used for attacks are also liable if owners did not take adequate precautions to secure systems.**
- **ISPs carrying traffic on systems used to launch attacks could be liable if ISPs did not help owners secure systems.**
- **Vendor's failure to ship a system in a state known to be secure.**

## Legal Analysis

- **A duty to secure the system (LIMITED UNIVERSE - NOW)**
- **Breach of duty (failure to meet standard of care)**
- **Breach is the proximate (foreseeable) cause of the harm**
- **Victim suffers harm/damages as a result of the breach**

Handwritten: COPY

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF TEXAS  
FORT WORTH DIVISION

FILED  
U.S. DISTRICT COURT  
NORTHERN DISTRICT OF TX  
FT WORTH DIVISION  
FEB 15 2001  
CLERK OF COURT

CI HOST, INC.,

Plaintiff,

vs.

DEVX.COM, INC.,  
EXODUS COMMUNICATIONS, INC.,  
COMMUNICATIONS, INC., JOHN DOE  
209.14.250, INFOASIS, INC.,  
WINTELCOM, INC.,  
JOHN DOE/IP 209.1.26.235, AND  
JOHN DOE/IP 209.1.153.51,

Defendants.

401 - CV - 0150 - A  
CAUSE NO.

EXEMPLARY DAMAGES

19. The acts of John Doe/IP 209.1.14.250, and/or DevX in assailing CI Host with a DoS attack was done with the intent and under the circumstances which render these Defendants liable for exemplary damages. Defendants' motive was malicious, wanton and for no reason other than an evil purpose. Further, the actions of Exodus in failing to carefully monitor and police its collocation customers, even after such DoS attack was underway, constitutes gross negligence, and accordingly, renders them liable for exemplary damages. Plaintiff is entitled to recover exemplary damages from any and/or all of the Defendants.

# Problems with Intermediary Liability

**Is there a basis to distinguish between corporate owners of networks and others?**

Home user liability?

Universities/Non-Profits (Perception of burden)

**If not, how does imposing liability on some owners and not others accomplish goal in a network environment?**

Increase computer security?

Deter wrongful conduct?

Compensate injured parties?

# What Does the Future Hold?

- Increased litigation based on security breaches due to erosion of “reciprocity is hell” limiting factor
- Application of security standards to non-regulated entities
- Application of security standards as a prerequisite to obtaining cyber-insurance
- Application of security standards in contractual relationships / outsourcing
- *More scrutiny on incident handling and incident response*
- Less damage attributable to computer misconduct, may be outweighed by greater liability for security deficiencies
- Cost and risk-shifting of an unknown and unquantifiable variety

---

# Are Baseline Security Standards the Answer?

---

Hal Pomeranz

Center for Internet Security

*<http://www.CISecurity.org/>*

# What's the Question?

---

*How can the Internet community stop being victims of well-known exploits?*

Contributing factors:

- Millions of new systems being connected
- Systems shipped in "default open" config
- SysAdmins lack time/resources/training

# What's a Baseline/Benchmark?

---

- "Minimum due care" security standards
- The consensus of many commercial, government, and academic groups
- Meets our "three criteria":
  - ✓ "Easily applicable"
  - ✓ "Do no harm"
  - ✓ "Can be tested/scored"

# How Are Benchmarks Created?

---

- Scour the 'net for existing guidelines
- Get input/resources from members
- Lock really smart people in a room until they produce an initial document
- Bring more and more groups into the "consensus circle"
- Continuously update documents

# What's the Output?

---

- Step-by-step documents for improving host/application security
- Testing tools for checking compliance and reporting improvement

*Everything is freely available at  
<http://www.CISecurity.org...>*

# Does it Work?

---

- Testing the CIS W2K configuration with commercial vulnerability detection tools:
  - 90% reduction in overall vulnerabilities
  - 95% reduction in "high priority" issues
- CIS configuration also eliminates 83% of vulnerabilities listed in CVE database

# Where are We At?

---

- Benchmarks and Tools ready now:
  - Solaris, Linux, and HP-UX
  - WinNT, Win2K (Level I & II)
  - Cisco IOS
- Coming soon
  - IIS and Apache
  - SQL Server and Oracle
  - Windows XP
- "On the radar": AIX, BIND, Checkpoint...

# What Can You Do?

---

- Download our benchmarks and testers and give us your feedback!
- Tell your friends!
- Become a member!
- Volunteer your time and expertise!

<http://www.CISecurity.org/>