Digital Security: Policies & The Law Curtis E.A. Karnow ckarnow@sonnenschein.com <u>www.sonnenschein.com</u> Sonnenschein Nath & Rosenthal, LLP

Outline

- Topology
- •Vulnerabilities & Attacks
- •Legal Exposures
- •Direct

Indirect

•Remedies: Policies & Audits

The Facts of Life

•The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it. -Gene Stafford, Director, Computer Operations, Audit, and Security Technology (COAST) Project

Legal Liability/technical interface – mediated by policies

- •Breaches will occur
- •Policies are part of defense in depth
- •Policies rest on risk assessment- & this is *legal* risk assessment

Boundless Topology: Risks Without Borders

- •multiple parties- each may have outsourced to ASPs-
- •ASPs outsourced to others
- •multiple jurisdictions
- •bound by multiple agreements
- •linked with varied nets: internet, VPN, Extranet, intranet, direct, wireless

Example- Wireless: new topology issues (http://www.securityfocus.com/infocus/1732)

Topology: Who's interested in-- and affects -- our security:

- ●Contractual
- •Employees, independent contractors
- •Shareholders
- •Partners, customers & clients- and *their* employees and contractors
- •Insurance company
- •Users
- •Non-contractual
- •The rest of world- affected by
- 'negligence'

Increasing number of vulnerabilities: A random day in August... http://www.securityfocus.com/bid/vendor/

2003-08-05: Valve Software Half-Life Dedicated Server Malformed Parameter Loop Denial Of Service Vulnerability 2003-08-05: Webware WebKit Cookie String Command Execution Vulnerability 2003-08-05: gURLChecker HTML Parser Denial Of Service Vulnerability 2003-08-05: TightVNC Win32 Server QueryAllowNoPass Access Control Bypass Vulnerability 2003-08-05: Valve Software Half-Life Server Multiplayer Request Buffer Overflow Vulnerability 2003-08-05: FreezingCold Software aspBoard URL HTML Injection Vulnerability 2003-08-05: IBM DB2 Shared Library Injection Vulnerability 2003-08-05: IBM DB2 db2job File Overwrite Vulnerability 2003-08-05: EveryBuddy Long Message Denial Of Service Vulnerability 2003-08-05: Pine From: Field Heap Corruption Vulnerability 2003-08-05: Ethereal DCERPC Dissector Memory Allocation Vulnerability 2003-08-05: Ethereal OSI Dissector Buffer Overflow Vulnerability 2003-08-05: Ethereal SPNEGO Dissector Denial Of Service Vulnerability 2003-08-05: Ethereal TVB GET NSTRINGZ0() Memory Handling Vulnerability 2003-08-05: Ethereal Multiple Dissector String Handling Vulnerabilities 2003-08-05: Multiple Linux 2.4 Kernel Vulnerabilities 2003-08-05: Multiple Vendor C Library realpath() Off-By-One Buffer Overflow Vulnerability 2003-08-05: Linux 2.4 Kernel execve() System Call Race Condition Vulnerability 2003-08-05: Man-db DEFINE Arbitrary Command Execution Vulnerability 2003-08-05: Multiple ManDB Utility Local Buffer Overflow Vulnerabilities

Types of attacks

- •stolen access- I.d. theft, passwords, login I.d., IP addresses
- •viruses, worms & Trojan horses
- •sniffers eavesdrop on traffic (passwords etc.)
- •denial of service
- •Unauthorized install of P2P file sharing s/w, e.g. KaZaA

Increased Sophistication of Attacks

•Russia, China, Leningrad extortion attacks, senior intelligence & security officers

•Over 20 countries with information warfare strategies targeting military *and private sector networks*

•Crucial vulnerability -- the insider

CERT Incidences- Tracks growth of Internet

- ●1988: 6
- •2002: 82,094
- •_ 2003: 114,855

New Trend?

- •FBI 2002 report decrease (50% in dollars)- Does self reporting work?
- •Single Slammer loss preliminary estimate > \$1 billion
- •As always- viruses and insider abuse (>80%)

New Reports

•PWC UK Report re 2001: 44% hit; average cost £30,000

•Deloitte Touche 2003 survey: >1/3 world top financial services have major security problems

•Not enough money

•No executive assigned exclusively to security

 $\bullet No$ account for recent legislation, US and EU

Rapid Technology change = rapid shifts in

- •Partners, affiliates, ASPs
- •New applications, tools
- •Attack methods & profiles
- •Network speed- DSL 'always on'
- •Vulnerabilities

Rapid Technology, rapid shifts in

- •OS updates and service pacs
- •Patches, solutions [overwhelming #]
- •Automated? Automatic download of Trojans and security flaws!

Speed of attacks

- •Vulnerability discovery _ Attack
- •1-2 yrs
- •Now: Slammer, Nimda, Slapper: 1-6 months
- http://www.westcoast.com/securecomputing/2003_07/cover/
- •Attack speed- automated:
- •Slammer: 90% vulnerable hosts in 10 minutes, 55 million scans w/in 3 minutes

Security Failures _ Liability Outline

- •Non legal liability
- •Direct legal liability
- •Indirect legal liability

Non Legal Liabilities

- •Business interruption /destruction
- •Extortion from crackers
- •P.R.: consumer confidence, investors and partners
- •Insurance coverage issues

Direct Legal Liability

- •Trade secrets (civil & criminal)
- •Liability for disclosure
- •Lack of protection > loss of TS status
- •Breach of contract (confidentiality)
- •Computer Fraud & Abuse Act
- •"unauthorized" access to computers and files

Direct Legal Liability: Sarbanes-Oxley

- Public companies
- •Internal control reports/data affecting financial statements

Direct Legal Liability

- •E SIG: online contracts- enforceable?
- •Losing the company crown jewels & the effect on shareholder related liabilities
- •COPPA and kids

Direct Legal Liability: Privacy

•E.U. and other privacy laws - access, enabling changes to personal data, security & sharing personal information

•Gramm Leach Bliley (financial institutions)

•State privacy laws

Privacy- ECPA

Electronic Communications Privacy Act (interception of communication) - civil & criminal

•Web site data collected without *express* consent

•Honeypots may violate

•Banner/consent

•Statutory exceptions: consent; provider protecting own network (<u>Fraser</u>: Dec. 2003 (3d Cir) IT dept. reading all employee email)

An aside for lawyers...

•Theofel v. Farey-Jones (9th Cir Aug 28, 2003)

•Stored Communications Act (18 USC 2701); Computer Fraud & Abuse Act (18 USC 1030)

•Patently overbroad subpoena to ISP- emails handed over. Lawyers may be liable

Privacy: FTC

•Failure to comply with published privacy policy

- •Policy re: site or all data collected?
- •Must be accurate
- •Actions against e.g.
- •Guess ("encrypted at all times")

•Microsoft (Passport) (credit card data protected; better security; does not collect undisclosed data)

•Eli Lilly, Ziff Davis, etc.

Privacy: FTC? JetBlue

• <u>privacy policy</u> (tickets bought online): "financial and personal information collected on this site is not shared with any third parties"

•September 2003: <u>JetBlue</u> secretly turned over PII (~ 5 million passengers) to private contractor – administration data-mining project (merge w/ <u>Acxiom</u> data)

Privacy: Other enforcement

- •NY Atty General
- •Netscape spyware "none of this information is saved"
- •Victoria's Secrets (!) \$50k
- •Cable Act (telecommunication providers)-
- •massive class action
- •disclosure PII to 3rd parties w/out informing subscribers (*Parker* 2d Cir.)

Privacy: HIPAA-Covered entities: e.g.

•Health Plans, plan that provide or pay for medical care

•Transmits data electronically (e.g. employers)

•Furnishes, bills or is paid for health care in the normal course of business

Indirect Legal Liability Boundless as the 'net: Recall topography

- •Basic Theories:
- •Negligence
- •Agency
- •Partnership
- •Indemnities
- •contributory; vicarious
- •Aider & abettor: knowing assist others' illegality
- Indirect Legal Liability: Vicarious Liability
- Financial interest in activity +
- •Right & ability to *supervise*

Policies alone may *not* be defense

Negligence: the catch-all

- •Targets: Universities, employers, parents; ISPs
- •40% internet connected computer have open ports (Symantec)
- •What's "negligence"? Perhaps-
- •Bad patch management
- •No intrusion detection system <<
- •Easily accessible unencrypted PII
- •No test of firewall from *inside* (ports 80, 21)
- •No quick follow-up on employees' departure

Types of Indirect Liability

•Virus & DDOS: liable for unintended attack of other downstream targets (CI Host)

•Note: 99% of reported intrusions result from exploitation of **known** vulnerabilities or configuration errors

Types of Indirect Liability

•Verizon failure to deploy anti-Slammer patch not reasonable, not entitled to [regulatory] exceptions from penalties

- •MSFT had previously issued 'critical' security bulletins
- •New suit against Microsoft- insecure software

Types of Indirect Liability

- •Copyright (e.g., music)
- •Child pornography
- •Napster standard ensuring 100% compliance by others?

New SB 1386- anti-ID theft ["Kick me"]

•Effective July 1, 2003

•If reasonably believe

•unencrypted computer data may have been acquired

•By "unauthorized" person (not re unauthorized *conduct* of e.g. employee)

•Data e.g. name +: SS#, drivers license, account, credit card ##

•Data of California residents (no matter where servers or company)

SB 1368

•Must issue notice: 'most expedient time possible'

•Pending: Illinois, Utah, NM; federal {S.1350}

•Class action potential

•Oct.'03: Cal. Office of Privacy Protection: best practices recommendations

•Do this: audits; incident response plans; review 3rd party contracts to require encryption

The Regulatory Future

More laws and regulations likely

• 'Terrorism,' i.d. theft, publicity re viruses, expensive Windows server vulnerabilities

•Agencies, legislatures and attorneys general: looking for high visibility and being 'responsive'

Law Outside US Affecting US Action

•Japan, EU, India, etc all enacting privacy regulation & asserting personal jurisdiction •EU has 15 data protection laws- strict: Spain, Portugal, Denmark

•EU: cookies, JavaScript on EU residents drives implicates EU law

•Asia-Pacific Economic Cooperation- aware that data protection laws encourage trade/development

•China, Russia, considering privacy law

Remedies: Outline

Technical

- ●Legal
- Contracts
- Insurance
- E Policies

Remedies: Technical

- •Multi-layered, defense in depth
- •Regular audits, penetration testing, white hat
- Patch management
- •firewalls & authentication
- ●encryption
- •*Physical* security

Remedies: Legal: Review Contracts

- ●Indemnity
- •Use of subcontractors
- •Who are authorized third parties
- •Required security audits
- •Minimum security requirements
- •Restrictions on use/distribution of personal data
- •Unrealistic caps on liability

Other Legal Remedies

- •Cyber insurance
- •Adequate policies & *compliance*

Preview: Policies & Legal Risk

- •Not having one. E.g.
- •Inadvertent destruction of evidence
- •No 'unauthorized' use standard
- •Breach of contract
- •Conflicts among policies or not following policy. E.g.
- •SB 1368
- •FTC
- •Privacy
- •Spoilation

Policies: Where & What are they?

- •Formal distributed policies
- •Employee manuals
- •Employment agreements, letters
- •Emails to staff
- •Informal practices
- •Alerts, banners, TOS, web "privacy policy"
- •*Are they consistent?*

Policies: Rationale In Avoiding liability

- Copyright
- •Distance from rogue employee
- •Spoliation: Destruction of evidence (+ re: *potential* litigation)
- •Routine destruction
- •Immediate preservation on claim notice
- •Back up, archive

Policies: Rationales: Employer-employee

- •Regulate employee behavior = #1 exposure
- •Basis for employee discipline
- •Employee policies: *consent* to monitoring, interception of email

Policies: Rationales

- •Incident response
- •Ability to work with law enforcement
- •Public Key Infrastructure- required among users, certificate authorities etc.
- •Preservation of evidence
- •Email, IM
- •An alert to employees that it's all preserved!

Policies: Rationales

- •Disaster recovery
- •Monitoring communications without violating ECPA (obtaining permission)
- •Honey pots & banner warnings
- •Parameters and approvals for penetration testing, white hat, etc. SATAN problems

Privacy Policies- Key issues

- •Web policy governs all data collection by default (FTC)
- •Frankenstein creations
- •Unconnected to practice & out of date
- •Survey: more than _ believe any policy means data not sold or traded

Policies' Use in Creating Confidential Material

- •Post incident, data collection under counsel supervision
- •Privileges:
- •Attorney client
- •Attorney work product
- •Avoiding waiver

Policies Are Contracts

- •Enforce them- consistently
- •Audits- Ensuring policies are enforced
- •Make sure you can live with policies reflects culture and way business is really done

Policies As Contracts

- •Set *your* terms
- •Not others'; override statutes
- •Set expectations and permissions/ authorizations, e.g.:
- •Use of laptops + other access
- •Privacy expectations
- •ECPA
- •Civil and criminal liability predicate

Policies: implementation

•Consider standards e.g. ISO 17799

•Regular review and updating

•No legalese, but not ambiguous

•Distributed and taught to all

Policies Implementation: Funding & Backing

•CEO endorsed

•Comply with complex laws and regulation- but `Best practices' -- at what cost?

•NSA guidelines to lockdown Win2000- 1000 pages

•1/3 companies would loose critical data or operational capability due to lack of funding (Gartner 2003)

•Security always trade off: risk, expenses, functionality

Incident Response- Policy & Practice

Do you want to call the Government?

YES

Powerful message to would-be predators - we will report you Cost-effective Government has powerful tools - Search Warrants, Grand Jury – v. production of documents in civil discovery Get mandatory restitution for low investment Low likelihood of civil recovery Bad publicity from lawsuit Call Government?

NO

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

Incident Response Practice Pointers

•Failure to properly characterize incident. Don't confuse an intrusion with a fishing expedition

•Failing to follow response plan or review 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 (preservation)

•Failure to involve counsel's office at the early stages

Legal Liability/technical interface – mediated by policies

•Breaches will occur

•Policies are part of defense in depth

Resources

•I.d.. theft: FTC Guidance, www.ftc.gov/bcp/credit/idtheft.htm

•FTC privacy actions against Eli Lilly and others, www.ft.gov

•Collection of resources from ComputerWorld

(http://www.computerworld.com/securitytopics/security/report/)

•What the US Govt. is up to: <u>http://csrc.nist.gov/publications/drafts/sp800-37-</u>

<u>Draftver2.pdf</u> (draft security standards and guidelines being developed by NIST's Computer Security Division in response to the Federal Information Security Management Act of 2002)

•SATAN: Improving Security of Your Site By Breaking Into It

(<u>http://www.fish.com/satan/admin-guide-to-cracking.html</u>; http://www.fish.com/satan/) Resources: Policies

http://www.iso-17799.com/

•http://www.information-security-policies.com

•http://www.yourwindow.to/security-policies

•http://www.sans.org/resources/policies/

•<u>http://www.searchalot.com/Top/Computers/Security/Policy/</u>

•http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/default.asp

SANS Policies

Acceptable Encryption Policy - Defines requirements for encryption algorithms used within the organization.

Acceptable Use Policy - Defines acceptable use of equipment and computing services, and the appropriate employee security measures to protect the organization's corporate resources and proprietary information.

Analog/ISDN Line Policy - Defines standards for use of analog/ISDN lines for Fax sending and receiving, and for connection to computers.

Anti-Virus Process - Defines guidelines for effectively reducing the threat of computer viruses on the organization's network.

Application Service Provider Policy - Defines minimum security criteria that an ASP must execute in order to be considered for use on a project by the organization.

Application Service Provider Standards - Outlines the minimum security standards for the ASP. This policy is referenced in the ASP Policy above.

Acquisition Assessment Policy - Defines responsibilities regarding corporate acquisitions, and defines the minimum requirements of an acquisition assessment to be completed by the information security group.

Audit Policy - Defines the requirements and provides the authority for the information security team to conduct audits and risk assessments to ensure integrity of

information/resources, to investigate incidents, to ensure conformance to security policies, or to monitor user/system activity where appropriate.

Automatically Forwarded Email Policy - Documents the requirement that no email will be automatically forwarded to an external destination without prior approval from the appropriate manager or director.

Database Credentials Coding Policy - Defines requirements for securely storing and retrieving database usernames and passwords.

.Dial-in Access Policy - Defines appropriate dial-in access and its use by authorized personnel.

DMZ Lab Security Policy - Defines standards for all networks and equipment deployed in labs located in the "Demilitarized Zone" or external network segments.

E-mail Retention - The Email Retention Policy is intended to help employees determine what information sent or received by email should be retained and for how long.

Ethics Policy - Defines the means to establish a culture of openness, trust and integrity in business practices.

Extranet Policy - Defines the requirement that third party organizations requiring access to the organization's networks must sign a third-party connection agreement.

Information Sensitivity Policy - Defines the requirements for classifying and securing the organization's information in a manner appropriate to its sensitivity level.

Internal Lab Security Policy - Defines requirements for internal labs to ensure that confidential information and technologies are not compromised, and that production services and interests of the organization are protected from lab activities.

Internet DMZ Equipment Policy - Defines the standards to be met by all equipment owned and/or operated by the organization that is located outside the organization's Internet firewalls (the demilitarized zone or DMZ)).

Lab Anti-Virus Policy - Defines requirements which must be met by all computers connected to the organization's lab networks to ensure effective virus detection and prevention.

Password Protection Policy - Defines standards for creating, protecting, and changing strong passwords.

Remote Access Policy - Defines standards for connecting to the organization's network from any host or network external to the organization.

Risk Assessment Policy - Defines the requirements and provides the authority for the information security team to identify, assess, and remediate risks to the organization's information infrastructure associated with conducting business.

Router Security Policy - Defines standards for minimal security configuration for routers and switches inside a production network, or used in a production capacity.

Server Security Policy - Defines standards for minimal security configuration for servers inside the organization's production network, or used in a production capacity.

The Third Party Network Connection Agreement - Defines the standards and requirements, including legal requirements, needed in order to interconnect a third party organization's network to the production network. This agreement must be signed by both parties.

VPN Security Policy - Defines the requirements for

Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the organization's network.

Wireless Communication Policy

Speaker CV

Curtis Karnow, partner Sonnenschein, Nath & Rosenthal, LLP, and a member of the firm's e-commerce, security and privacy, and intellectual property groups. He is the author of Future Codes: Essays In Advanced Computer Technology & The Law (Artech House, 1997), and represents Sun Microsystems in the landmark antitrust case, Sun Microsystems v. Microsoft. His clients have also included Yahoo!, Excite@Home, Charles Schwab & Co., Inc., Cisco, Sony Computer Entertainment of America (Playstation), and PGP (Pretty Good Privacy). Among other areas, Mr. Karnow counsels on software licensing, public key infrastructure policies, electronic contracting, and digital signatures. Formerly Assistant U.S. Attorney in the Criminal Division, Mr. Karnow's responsibilities included prosecution of all federal crimes, including complex white-collar fraud, from investigation and indictment through jury verdict and appeal. Since then, Mr. Karnow has represented defendants indicted for unauthorized access to federal interest computers; defended against a criminal grand jury investigation into high tech (encryption) export actions; represented clients before federal grand juries investigating alleged antitrust conspiracies and securities violations; brought legal actions against internet-mediated attacks on client networks, and in a state criminal investigation represented a computer professional framed by a colleague in a complex computer sabotage. He has also advised on jurisdictional issues arising out of a federal criminal Internet-related indictment, and advises on liability and policy issues, including interfacing with law enforcement authorities, arising from computer security breaches and Internet privacy matters. He occasionally sits as a temporary judge in the California state court system. He also serves with a committee of the California Judicial Council, which operates the state's court system.

Curt Karnow can be reached at ckarnow@sonnenschein.com