Assessing & Auditing Internet Usage Policies

Presented to the Institute of Internal Auditors 13 April 2004

M. E. Kabay, PhD, CISSP Associate Professor & Program Director, Information Assurance

Division of Business & Management, Norwich University <u>mailto:mkabay@norwich.edu</u> <u>http://www2.norwich.edu/mkabay</u>

Topics



- > Assessing vs Auditing
- > Fundamentals of Information Assurance
- > Functions of IA
- > Selected Topics in 'Net Abuse
- > Intellectual Property
- > Video from Commonwealth Films
- ➤ Wrap-up

Copyright © 2004 M. E. Kabay. All rights reser

Assessing vs Auditing



- Assessment—Evaluation: judgement about something based on an understanding of the situation.
- > Audit—Verification: judgement of extent of compliance with formal policies.
- ➤ Goals today:
 - □Facilitate both assessments and audits
 - √Provide wider context than simply compliance with formal written policies.
 - ✓ Increase awareness of issues so that auditors can engage in more productive discussion with IT and security colleagues

Copyright © 2004 M. E. Kabay. All rights reserved.

Fundamentals of IA



- > The Classic Triad
 - **□**Confidentiality
 - □Integrity
 - □Availability
- ➤ The Parkerian Hexad
 - □Possession
 - □Authenticity
 - □Utility
- ➤ Information Assurance (IA)

Copyright © 2004 M. E. Kabay. All rights reserved.

The Classic Triad C S CONCRETE SOURCE FORMER ALFORDMENDAMEN 5

Confidentiality



Restricting access to data

- Protecting against unauthorized disclosure of existence of data
 - □E.g., allowing industrial spy to deduce nature of clientele by looking at directory names
- Protecting against unauthorized disclosure of details of data
 - □E.g., allowing 13-yr old girl to examine HIV+ records in Florida clinic



Integrity



Internal consistency, validity, fitness for use

- > Avoiding physical corruption
 - □E.g., database pointers trashed or data garbled
- > Avoiding logical corruption
 - □E.g., inconsistencies between order header total sale & sum of costs of details



Availability



Timely access to data

- > Avoid delays
 - □E.g., prevent system crashes & arrange for recovery plans
- > Avoid inconvenience
 - □E.g., prevent mislabeling of files



Copyright © 2004 M. E. Kabay. All rights reserved

Problem: Missing Elements



- Which principle of the C-I-A triad has been breached when
- □A child takes bank card with password in envelope but does not open it?
 - □Someone sends threat to President using your e-mail address but not your e-mail logon?
- □Someone converts all the salary figures in your database to Iraqi Dinars?

ANSWER: NONE OF THEM – THE TRIAD IS INSUFFICIENT TO DESCRIBE SECURITY BREACHES

Copyright © 2004 M. E. Kabay. All rights reserved.

The Parkerian Hexad



otect the

atomic elements of INFOSEC:

- ➤ Confidentiality
- > Possession or control
- ➤ Integrity
- > Authenticity
- ➤ Availability
- **>** Utility

Copyright © 2004 M. E. Kabay. All rights reser-

Why "Parkerian?" Donn G. Parker Recipient of Lifetime Achievement Award from NCSC in 1993

Possession



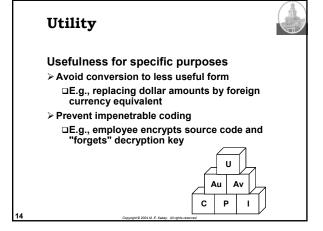
Control over information

- ➤ Preventing physical contact with data

 □E.g., case of thief who recorded ATM PINs
 by radio (but never looked at them)
- Preventing copying or unauthorized use of intellectual property
 - □E.g., violations by software pirates



Authenticity Correspondence to intended meaning > Avoiding nonsense □E.g., part number field actually contains cost > Avoiding fraud □E.g., sender's name on e-mail is changed to someone else's



Functions of IA (1)



- Avoidance: e.g., prevent vulnerabilities and exposures
- ➤ Deterrence: make attack less likely
- ➤ Detection: quickly spot attack
- > Prevention: prevent exploit
- ➤ Mitigation: reduce damage
- > Transference: shift control for resolution

Functions of IA (2)



- > Investigation: characterize incident
- ➤ Sanctions & rewards: punish guilty, encourage effective responders
- > Recovery: immediate response, repair
- ➤ Correction: never again
- Education: advance knowledge and teach others

Information Assurance (IA)

Avoid Deter

Correct Prevent

Recover Mitigate

Investigate

Abuse by Outsiders



- > Industrial espionage
- > Web defacement
- > Trojan horses
- Viruses and worms
- ▶ Bad software
- > Denial of service
- ➤ Psyops / disinformation

 □Discourage investors

 □Demoralize employees
 - □Lead to bad decisions

18

Internet Abuse by Insiders



- > Attacks on the employer
 - □Stealing property / information
 - □Damaging / vandalizing property / information
 - □Sullying reputation (of self and employer)
- > Attacks on others (leading to liability)
- > Creating hostile work environment
- > Wasting time and resources

19

Copyright © 2004 M. E. Kabay. All rights re

Essential Policies for 'Net Use



- > Appropriate use of e-mail and Web
- Protecting privacy
- > Protecting intellectual property
- ➤ Safeguarding resources

20

)

Selected Topics in 'Net Abuse



- > Selling Products and Services
- > Netiquette for Beginners
- > Marketing on the 'Net
- > Spamming the 'Net
- Market Data Collection: Ethical & Legal Issues
- ➤ Public Relations Nightmares
- ➤ Covert Ads
- > Flamewars

21

Selected Topics (cont'd)



- > Shills
- > Spoofs
- ➤ USENET Etiquette
- > Internal E-mail & the Law
- > Avoid Hostile Work Environment
- > 'Net Filters & Audit Trails
- > Intellectual Property

2

22

Selling Products and Services



Nothing inherently unethical

But problems include:

- > Immortal messages (need expiration date)
- > Inaccurate messages (need digital signature)
- > Inauthentic messages (need non-repudiation)
- > Unwanted messages (need good judgement)

23

Netiquette for Beginners



All e-mail & postings using company e-mail ID are equivalent to writing on

company letterhead

24

Copyright © 2004 M. E. Kabay. All rights

Marketing on the 'Net



- > World-Wide Web-marketing the right way
- > Legitimate mailing lists
- > NOT Junk e-mail (spam)
 - unsolicited, often fraudulent, many forged headers: is this the company you want to keep?
 - □who pays?
 - □denial of service
 - □outrage from many recipients
 - □serious business consequences

Spamming the 'Net



- ➤ Term from Monty Python skit about SPAM™
- > Sending large numbers of identical messages to many news groups or e-mail addresses
- > Many readers get several related news groups
- > Annoys members, uses bandwidth
- > Severe consequences

□hate e-mail

□mail bombing

□removal of Internet access

□deletion of all future messages

□expulsion from new groups

Spamming the 'Net: Case Studies



Anonymous executive writing in Network World (1994)

- > Posted advertising to 20 news groups
- > Thought people would be interested
- ➤ E-mail bombs
- > 800 number posted in alt.sex groups
- > Thousands of obscene phone calls
- > Receptionist quit
- > All 800 calls sent directly to his phone
- > Nearly destroyed his career

CAN-SPAM Act (2003)



- > Dictates requirements for opt-out facilities
 - □Requires identification of source
 - □Completely useless in stopping criminal spammers
 - □Fines for violation of restrictions
- > Can lead to problems for legitimate businesses whose employees are ignorant of law and Internet culture
 - □Marketing manager contracts with spammer
 - □Employee sends spam on own initiative

Market Data Collection: Ethical & Legal Issues



- > Point of sale data capture
- > Credit records (beware GLB Act)
- Medical records (beware HIPAA)
- Compilations of e-mail addresses
- > 'Net usage statistics about individuals
- Spyware
- Misleading EULAs (end-user license agreements)
- > ASK YOUR CORPORATE ATTORNEY
- > FOR ADVICE

Public Relations Nightmares



- Lack of professionalism a killer
- > Dishonesty of any kind remember the audience
- > Spamming
- > Flaming people in professional news groups
- > Copyright violations

Covert Ads



- > Forums, newsgroups may have strict standards
- > Responses should be technical and helpful
- > Do not introduce company name and product without clear benefit to recipient
- > Repeated marketing hyperbole in technical forum repels potential customers
- Beware of posting superficially-objective responses that are slanted: will be nailed

Flamewars



- > Technology insulates some people from empathy
- > Not everyone capable of writing with subtlety and sensitivity
- > Flamewars are written shouting matches
- Avoid ad hominem remarks
 - □comments on intelligence or competence
 - □imputation of motives
 - □statements claiming to know other people's thoughts
 - □outright verbal abuse

Shills



- > Employees who write as if they were customers
- > All employees should identify themselves as such if information bears on their credibility
- - □strong objections to dishonesty
 - □perpetrators locked out of forums
 - great abuse heaped on individuals and employers
 - □long term distrust

Spoofs



- > Impersonation of others
- Writing bad things about competitors
- > Can be used as industrial sabotage
- > Possibly actionable

Spoofs: Case Study



ReplyNet vs Promo: October 1995

- Promo Enterprises is mass e-mail
 - □sent junk e-mail to 171,000 recipients
 - □listed "REPLY.NET" as return address
 - □Promo has recently announced competition with ReplyNet auto-reply service
- > ReplyNet Inc. provides non-objectionable advertising on 'Net
 - □ReplyNet received 100s of complaints
 - □sent apologies but largely rejected
 - □damage to reputation as responsible service

Spoofs: Case Study (cont'd)



ReplyNet initiated lawsuit:

- > Violations of US. federal law
 - □Forgery
 - □Trademark violation
- > Damages payable to ReplyNet
 - □\$5-\$10 for each of 171,000 people
- > Refunds for on-line time to all unwilling recipients
- > May be a case of industrial sabotage ("spamotage" in John Schwartz's phrase— Washington Post)
- > Settled out of court on "generous terms"

USENET Etiquette



- > Lurk before you leap: learn specific style
- > Stick to the forum/section subject area
- > Make messages concise
- > Quote only relevant text from previous message
- > Respect copyright laws
- > Don't flame people
- > Avoid profanity, ethnic/religious slurs, etc.
- > On USENET, everything you write may be archived and available forever

Internal E-mail



- > E-mail can be used in court of law
 - utypically stored on system or e-mail backups (sometimes for years)
 - □don't send e-mail you would be ashamed of in public
 - □can be seized under subpoena

Avoid Hostile Work Environment



- > Abusive internal e-mail should be explicitly barred by corporate policy

 - □sexism
 - □harassment of all kinds
 - □Libel
- > Same applies to inappropriate Web use

'Net Filters & Audit Trails



- > Filters control what can be displayed through Web browser
 - ■Web pages
 - **□USENET** groups
- > Useful as part of pattern of parental controls
- > Also useful in workplace (contentious issue)
- > Game filters also available
 - □to purge games
 - □similar to anti-virus software

Intellectual Property I: Fundamentals



- ➤ Purpose
- **≻ HTML**
- ➤ Subject Matter
- > Linking
- ➤ What is Protected by
- > Framing
- Copyright?

- > Scumware
- > Formalities
- > Works Made for Hire
- > E-mail

- > Contractual Sale
- > Criminal Law > 1st Amendment?
- > Infringement
- > Fair Use

Property Law

Stimulate creativity for



- > Protect intellectual property
 - □Prevent loss of control or possession
- > Support gainful return on investment

Purpose of Intellectual

- □Copyright
- □Trademark
- □Patent

Copyright © 2004 M. E. Kabay

Subject Matter



- > Original works of authorship
 - □Independent product of author
 - ■Not copied
- > Exclusion □ldea
 - □Procedure
 - □Process
 - ■Method of operation
 - □Concept
 - □Principle
 - □Discoverv

What is Protected by Copyright?



- > Reproduction
- > Preparation of derivative works
- > Distribution
- > Performance
- > Display in public

Formalities



- > Original work is automatically copyrighted in the name of the author / creator
 - □Not necessary to indicate "Copyright © 2001 name-of-author. All rights reserved."
 - □Advisable to do so to strengthen legal position in case of claimed doubt.
- > May register US works with US Copyright
 - □Offers increased protection
 - □\$500-\$20,000 statutory damages
 - □Register within 3 months of publication

Works Made for Hire



- > Full-time employees generally forfeit claim to work created expressly for purpose of their job
 - □Copyright belongs to the employer
- > Employers' rights do not apply to creative work outside employment
 - √ Not created with employer facilities,
 - √ Not interfering with regular work
 - √ Created outside normal working hours
- > Problems can occur when creative outside work is directly related to job function

Contractual Sale



- > Copyright ownership may be traded or sold
- > Employers often include clause claiming copyright over all creations by employee
 - □Sometimes specify work created for any purpose and at any time
 - √E.g., children's story book
 - ■No obligation to agree to such clause
 - □But no obligation to hire employee without such agreement
- > Publishers almost always try to get all rights
- □Recent case distinguishes between paper publication and electronic publication

Writers Win a Court Battle for Control 1999-09



- > New York state court ruled in favor of **National Writers Union**
- > Against New York Times □& other major publishers
- > Affirmed right of writers to control publication if their materials in new media
- > Publishers wanted to use submissions for CD-ROMs or Web without paying additional royalties

Infringement



- > Any use without express permission of copyright holder
 - □Printing
 - □Posting on Web
 - □Using in derivative work
- > Direct infringement
 - ■Monetary profit is not an issue
 - □Distributing someone else's work for free is not a mitigating factor
- > Contributory infringement: ISPs?
- □Requires substantial or pervasive involvement

Facts?



- > Factual information cannot be copyrighted in itself; e.g.,
 - $\Box 2 + 2 = 4$
 - □Distance between Norwich and Montpelier
- > The representation of factual information can be copyrighted; e.g.,
 - □A times-table designed for children with pictures of friendly animals romping around edge of the table
 - □A map of Vermont with particular fonts, colors, and symbols

NBA vs Pagers



1997.02 — EDUPAGE

- Sports pagers receive scores in real time
- > NBA does not want pagers to broadcast games scores during games
- > NBA argues in court that this information is proprietary
- > Second U.S. Court of Appeals in New York ruled in favor of pager companies

Associated Press



- > June 2001 claim copyright protection for facts reported in news wire feeds
- > Would prevent even summarizing or abstracting articles
- > Serious doubts that this claim will be accepted if any case goes to court

HTML



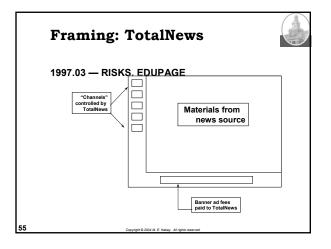
- > Does "borrowing" HTML source code constitute infringement?
 - □In theory yes
 - □In practice, no

Linking



- Does pointing to a Web site violate copyright?
 - □Depends on how it's done
 - □Putting copyrighted material in a FRAME has been argued to be infringement
 - □www.babesontheweb.com was accused of infringement

Copyright © 2004 M. E. Kabay



Framing: TotalNews (cont'd)



News organizations claimed

- Misappropriation
 - □Entire commercial value of news
 - □Reselling to others for TotalNews' profit
- > Federal trademark infringement & dilution □Diluting distinctiveness
 - □Causing confusion, deceiving customers
- > Copyright infringement
 - □Violating several exclusive rights

Framing: TotalNews (cont'd)



- > Violation of advertising laws, deceptive practices & unfair competition
 - ■Mistaken impression of affiliation
- > Tortious interference with business relationships
 - □Selling ads by making news available

Conclusion: case settled out of court

- > TotalNews would stop framing
- > Would link to news sites only with permission

See http://www.publaw.com/framing.html

Links: Ticketmaster vs Microsoft



1997.04 — Ticketmaster Group sues Microsoft

- > MS includes hot links from Microsoft Web pages to Ticketmaster Web pages
- > No formal agreement granting permission for such links
- > Ticketmaster sees MS as deriving benefit from the linkage but bypassing Ticketmaster's advertising
- > Ticketmaster programmed Web pages to lead all Sidewalk users trying to follow unauthorized links to a dead end

Links: Gary Bernstein Sues Entire Web? (1998-09)



- > Hollywood photographer Gary Bernstein □Sued several Web operators for having links to sites containing pirated copies of his
- > Included indirect links □links to site with links to sites. . . .
- > Contamination spread along Web links □from bad site to all those linked to it □presumably every Web site on planet
- > Los Angeles Federal District Court Judge Manuel A. Real dismissed indirect linkage □Bernstein withdrew entire suit

Superpose Your Own Ads on Competitor's Site? 1999-02



- > Alexa Internet company
 - □Subscribers to Alexa service got "smart links" □Pop-up information
 - √ company address
 - √ financial information
- Offered competitors opportunity to superpose their own ads on top of their competition's Web
- > Advertisements could be tailored for specific target
 - □E.g., when user clicked competitor's Web site
- > Such services became known as scumware

What is Scumware?



- > Software changes appearance and functions of Web sites without permission of Webmasters
- > Overlays advertisements with other ads
- > Adds unauthorized hyperlinks to possibly objectionable sites
- > Interferes with existing hyperlinks by adding other destinations
- Some products install themselves without warning of these functions
- > Difficult or impossible to control
- ➤ Difficult to uninstall
- > Also known as thiefware

Examples of Scumware: Surf+



Platitudes or Prophecy?

Sure, they sell. But are they serious? NEWSWEEK's religion guru opines about the new spiritual best sellers.

By Kenneth L. Woodward

Aug. 27 issue -- Sociologists tell us that the United States is experiencing a religious revival -- a third "great awakening" echoing those of the 18th and 19th centuries. But if the best-seller lists are any guide, the revival looks more like a collective leaving of the senses. The hottest books among evangelical Christians, for example, is a religious

Examples of Scumware: TopText



Dun & Bradstreet - http://www.dnb.com/

Provider of international and U.S. business credit information

Experian - http://www.experian.com

National consumer credit bureau and business credit reporting service

Equifax - http://www.equifax.com

One of three national <u>consumer credi</u>t repositories

Trans Union - http://www.www.transunion.com

National repository of consumer credit information

Credit Managers Association of California -

Business credit services

CMA Business Credit Services - http://www.creditservices.org/ Provides business credit reporting and commercial collections worldwide

Legal Issues



- ➤ Robin Gross, Attorney for Electronic Frontier Foundation (EFF) - scumware may violate

 - □US federal rules against deceptive/unfair business practices
- > Copyright:
 - □Creating unauthorized derivative work
- > Deception:
 - □Give impression that new hyperlink is endorsed by original Website owners

Legal Issues (cont'd)



- Moral Rights recognized by most countries other than USA
- > Package of intellectual property rights granted to the original creator of work
 - □Right of integrity;
 - □Right of attribution;
 - □Right of disclosure;
 - □Right to withdraw or retract;
 - □Right to reply to criticism.
- > Modifying Web pages without permission can violate all of these moral rights

Fighting Scumware



- - □Don't sign up for such software without reading and understanding terms of
 - □Remove products if unacceptable √Guides available online
- > Webmasters
 - □Test pages to see what scumware does to
 - □Use scripts to redirect visitors with infested browsers to warning pages
 - □Sign petitions, join lawsuits to protest

All rights reserved.

E-mail



- > E-mail is covered by copyright law
 - □Your e-mail message is inherently copyrighted
 - □Do not copy / post / otherwise distribute someone else's e-mail message without permission
- What about postings to public discussion groups?
 - □Posting copyrighted materials in public without permission is a violation of copyright
 - □How does permission get signified?

Copyright © 2004 M. E. Kabay. All rig

Criminal Law



- > 17 USC 506(a)
 - □stipulates criminal liability for infringing copyright "wilfully and for purposes of commercial advantage or private financial gain."
 - □Includes removal of copyright notice
 - □Use of fraudulent copyright notice
- > Felony sanctions (18 USC 3571)
 - □10 or more copies in 180 days of 1 or more works with total retail value of at least \$2500
 - □5 years in prison & \$250,000 in fines □2nd offense: 10 years

68

Copyright © 2004 M. E. Kabay. All rights reserved

1st Amendment?



- Does the 1st Amendment protect unauthorized copying of copyrighted works?
 - □Some defendants have claimed 1st
 Amendment protections when publishing
 work of public officials
- But SCOTUS* ruled that even a public official's own copyrighted materials cannot be infringed
- No ban on publishing the substance of such documents; only on publishing exact form

*SCOTUS: Supreme Court of the United States

69

Copyright © 2004 M. E. Kabay. All rights reserved.

Fair Use



- > Fuzzy doctrine
 - □No specific law with specifics
 - □Questions: more YES the fairer the use

Cc

Fair Use - Cont'd



Guidelines for determining if your use of copyrighted materials qualifies as fair use*:

- 1. Is your use noncommercial?
- 2. Is your use for purposes of criticism, comment, parody, news reporting, teaching, scholarship, or research?
- 3. Is the original work mostly fact (as opposed to mostly fiction or opinion)?
- * Larry Lessig, David Post and Eugene Volokh in Cyberspace Law for Non-Lawyers (1996):

http://www.eff.org/Government/Legislation/Legal/CyberLaw_Course/

72

Fair Use - cont'd



- 4. Has the original work been published (as opposed to sent out only to one or a few people)?
- 5. Are you copying only a small part of the original work?
- 6. Are you copying only a relatively insignificant part of the original work (as opposed to the most important part)?

Fair Use - Cont'd



- 7. Are you adding a lot new to the work (as opposed to just quoting parts of the original)?
- 8. Does your conduct leave unaffected any profits that the copyright owner can make (as opposed to displacing some potential sales OR potential licenses of reprint rights)?
- > The more YES answers there are to the above questions, the more likely it is that your use is legal. The more NO answers there are, the more likely it is that your use is illegal.

So is this use of the Fair Use text a fair use?

Intellectual Property II: Trademarks



- > Trademarks
- ➤ Domain Names
- ➤ Cybersquatting Cases
- > Federal Trademark Dilution Act of 1995
- > Anticybersquatting Consumer Protection Act
- > International Protection of Trademarks

Trademarks



- > Purpose
- ➤ Definition and Types
- > Classes of Marks
- > Application and Exceptions to Grant
- > Nature of Protection
- > Relief for Violation



Purpose of Trademarks



- Represent origin of goods or services
- > For the producer
 - □Use symbol or other designation
 - □Represent who makes goods or provides
 - □Reap financial rewards resulting from past quality
- > For the consumer
 - □Allow quick recognition of goods or services as being from same manufacturer or provider
 - □Prevent confusion and counterfeits

Examples of Marks

Definition and Types of Marks



- > Trademark
 - □ Word, name, symbol, device or combination
 - □ Used to distinguish goods from other similar goods
- Service mark
- □ Identifying and distinguishing services
- > Collective mark
 - ☐ TM or SM
 - □ Coöp, association, union, guild
- > Certification mark
 - □ Assertion of compliance with standards or origin by certifying organization

TruSecure OverWatch

TruSecure SecureWatch



CISSP



@TRUSECURE

US Legal Protection of Trademarks



> Trademark Protection Act of 1946

□= "Lanham Act" – see

http://www.bitlaw.com/source/15usc/

- □In 15 USC
- □Civil law
- > 15 USC §1114 = §32 of Lanham Act
 - □Use likely to
 - √ Cause confusion
 - √ Cause mistake
 - ✓ Deceive

79

Copyright © 2004 M. E. Kabay. All rights reserved.

Lanham Act - cont'd



- > 15 USC §1125 = Lanham Act §43
- Word, term, name, symbol, device, or combination
 - □Likely to cause confusion, mistake or deception
 - □ Affiliation, connection, association with person
 - □Origin, sponsorship, approval
 - □Goods, services, commercial activities
- ➤ Commercial promotion or advertising
 □Nature, characteristics, qualities
 - □Geographical origin

8

Copyright © 2004 M. E. Kabay. All rights reserved.

Classes of Marks



- > Fanciful
 - □Invented words; e.g., Alera, Adario, Elantra
 - □Arbitrary; e.g., Cougar, Pavillion
- > Suggestive ordinary words or combinations
 - □Connotes quality, ingredient, characteristics but not substance; e.g., PestPatrol, SaferSite
- Descriptive ordinary words w/ secondary meaning – primary meaning is source
 - ☐ Yellow Pages, Blue Flame
- Generic class of product/service no protection under Lanham Act
 - □You have mail, Instant messaging □E-mail, Web site, e-commerce

Nature of Protection for Trademarks



- > Prevent confusion by users
- > Factors considered by the courts
 - □Similarity of marks
 - □Similarity of goods
 - □Relationship between parties offering goods
 - □Classes of purchasers
 - □Evidence of confusion
 - □Defendant's intent
 - □Strength of plaintiff's mark

8

Copyright © 2004 M. E. Kabay. All rights reserved.

Checkpoint Systems Inc. vs Check Point Software Technologies



- > The companies
 - □Checkpoint Systems provides antishoplifting equipment
 - □Check Point Software provides firewalls
- ➤ The claim
 - □Checkpoint accused Check Point of infringing on its trademark
- > The ruling
 - □Court refused to grant injunction
 - □Argued there was no likelihood of confusion

_

Relief for Violation of Trademarks



- > Injunction prohibiting continued violation
- > Seizure of goods and counterfeit marks
- > Recovery of plaintiff's profits
- > Destruction of infringing goods and advertising
- Recovery of actual damages incurred (loss of profits, goodwill)
- Recovery of legal costs including attorney's fees in some cases

84

Copyright © 2004 M. E. Kabay. All rights reserve

Domain Names



- > The Domain Name System (DNS)
- ➤ Dispute resolution
- > Hyperlinks
- > Cybersquatting Cases

85

opyright © 2004 M. E. Kabay. All rights reserve

The Domain Name System



- Converts words (e.g., <u>www.norwich.edu</u>) into IP addresses (e.g., 192.149.109.153)
- > Early years DARPA contract with USC
- ➤ 1992: NSFNET opened to .com users
 □Network Solutions Inc. became registrar for .com, .net, .org
- ➤ 1998: ICANN (Internet Corporation for Assigned Names and Numbers)
 - □Established by US government
 - □Highly controversial much political turmoil over actions, governance

86

Copyright © 2004 M. E. Kabay. All rights reserved.

Hyperlinks and Trademarks



Cannot legally use

- Others' trademarks or logos on a Web site without permission
- Framing to bring another's content directly into a page that appears to be created by another site
- Others' trademarks in invisible metatags visible to search engines

87

Copyright © 2004 M. E. Kabay. All rights reserved.

Federal Trademark Dilution Act of 1995



- Prior to 1995, courts had to rule against plaintiff if no confusion could be shown
 - □Thus radically different businesses could use existing trademarks without infringing the Lanham Act
- But large companies with famous trademarks argued that frequent use diluted value of their marks
- Congress passed TDA of 1995 to protect such plaintiffs even when no confusion likely

88

Copyright © 2004 M. E. Kabay. All rights reserved

Cybersquatting Cases Have Used Trademark Dilution Act



- Many examples of parasites who register famous trademarks or people's names as DNS entries
 - ☐ Hope to capitalize by extorting money to sell registration to legitimate users
 - Many firms have appealed under ICANN rules or gone to court for trademark dilution
- > Intermatic Inc. vs Toeppen an excellent example of case illuminating the issues
 - ☐ Defendant registered 240 domain names using famous company names and trademarks
 - □ Intermatic argued that Toeppen should not be able to block its use of its TM in domain name
 - □ Judge ruled in favor of plaintiff because of dilution

Anticybersquatting Consumer Protection Act of 1999



- > Increasing complaints about cybersquatting
- Bad faith use of TM, company name or person's name defined clearly for domain names
 - □Multiple criteria
 - Most significant: offer to sell or transfer domain name
 - √For financial gain
 - ✓ Without prior use for real business
 - □Registration of multiple similar infringing domain names
- > Statutory damages of \$1,000-\$100,000 per domain name

90

Copyright © 2004 M. E. Kabay. All rights reserved.

International Protection of Trademarks



- > Paris Convention for the Protection of Industrial Property (1883)
- ■National treatment same rules for all
- □Rights of priority for filing of registration
- □Similar rights of refusal of registration
- □Seizure of contraband / counterfeits
- > Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS, 1994)
 - □Includes TM protection
 - □7-year terms of protection with unlimited renewals

Video: get.net.smart



- > Commonwealth Films: excellent source http://www.commonwealthfilms.com/1060.htm
- > Topics:
 - □Monitoring Internet usage
 - □Personal use of corporate resources
 - □Sites that are off-limits
 - □Denial of service
 - □Confidentiality
 - □Illegal activities
- > Free preview copies available
- > Preview copy being used today by permission

Protecting Your Systems (Top-Level Overview Only)



- > Fiduciary Responsibility
- > Security Policies Not Shelfware
- > System & Network Management
- > Computer Emergency Response Team
- > Disaster Recovery Procedures Updated & Tested

Fiduciary Responsibility to Protect Systems



- > Failure to protect assets
 - □Can result in lawsuits for damages from stakeholders
 - □Includes shareholders, employees, clients
 - □Terrible publicity
- > Downstream liability
 - □Attacker invades your systems due to faulty
 - □Uses your systems to launch attack on third party
 - □Legitimate basis for tort
 - □Viewed by some tort experts as potential

Security Policies Not Shelfware



- > Up to date & realistic
- > Adequate education & training
- > Active monitoring and enforcement
- > Ongoing awareness programs changes

System & Network Management



- > Monitor vulnerabilities & patches
- > Intrusion detection systems & response
- > Firewalls, antivirus systems

Computer Emergency Response Team



- > Drawn from throughout organization
- > Analyze priorities for response
- > Collect evidence for analysis, correction, prosecution
- > Initiate rapid recovery

Disaster Recovery Procedures



- > Team drawn from entire organization
- > Documentation absolutely up to date
- > Safeguard people, corporate assets
- > TEST plans thoroughly
- > TEST plans often
- > TEST plans thoroughly and often
- > TEST plans often and thoroughly
- > Did I mention you have to test plans?



For Further Reading

- ➤ Doubilet, D. M., V. I. Polley & J. R. Sapp (2002), eds. Employee Use of the Internet and E-Mail: A Model Corporate Policy: With Commentary on Its Use in the U.S. and Other Countries. American Bar Association. ISBN 1-590-31046-2. 103 pp.
- > Kabay, M. E. (2002). E-mail and Internet Use Policies. Chapter 33 from Bosworth, S. & M. E. Kabay (2002) Computer Security Handbook, 4th Edition. Wiley (ISBN 0-471-41258-9).
- Flynn, N. L. (2000). The E-Policy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies. AMACOM (New York, NY). ISBN 0-814-47091-2. 256. Index.

Further Reading (cont'd)



- > Overly, M. R. (1998). E-Policy: How to Develop Computer, E-Policy, and Internet Guidelines to Protect Your Company and Its Assets. AMACOM(New York, NY). ISBN: 0-814-47996-0. 144. Index.
- > Whelan, J. (2000). E-Mail @ Work. Financial Times Prentice Hall. ISBN 0-273-64465-3. 222

Contact Information



> M. E. Kabay, PhD, CISSP

Associate Professor of Information Assurance

Program Director, Master's and Bachelor's Degrees in Information Assurance

Division of Business & Management, Norwich University, Northfield VT

- > mailto:mkabay@norwich.edu
- Web site: http://www2.norwich.edu/mkabay
- > MSIA information: http://www3.norwich.edu/msia
- > BSIA information:
 - http://www2.norwich.edu/mkabay/bsia
- > Norwich Graduate Portal: http://grad.norwich.edu

DISCUSSION