Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Dangerous Technology: Management Beware

The purpose of this paper is to inform management and upper level administration of the legal liabilities and loss of productivity due to the inappropriate use of the Internet, email, interconnected computer systems and pirated software. While it's not the intent to cover all liabilities and associated laws, this paper will focus on Legal Liability (Discrimination, Harrassment, Obscenity and pornography) Software Licensure and Copyright infringement. Where applicable, there are resources provided to better educate the ...

Copyright SANS Institute
Author Retains Full Rights

AD

Dangerous Technology: Management Beware

Brent McKinley

March 27, 2002

GSEC Practical Assignment Version 1.3

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room Author retains full rights.

Dangerous Technology:
Management Beware

Brent McKinley

3-27-02

ABSTRACT

The purpose of this paper is to inform management and upper level administration of the legal liabilities and loss of productivity due to the inappropriate use of the Internet, email, interconnected computer systems and pirated software. While it's not the intent to cover all liabilities and associated laws, this paper will focus on the following and where applicable, provide resources to better educate the reader as to the tools and resources available to protect the employer should legal litigation arise and the employer's investment in their employees.

- Legal Liability
  - Discrimination
  - Harassment
  - Obscenity and pornography
- Cyberslacking
- Software Licensure and Copyright infringement

Introduction

The technical revolution has forced government, business and institutions of higher education to rely heavily on the ever-changing world of technology. Today, we are surrounded by technology everywhere we go. What most employees, managers and students don't realize is that although the technological advances in today's world can accelerate our knowledge, our competitive edge, and make us more productive, it can also lead to our demise, public embarrassment and huge punitive damages. Most MIS departments are understaffed, under trained and ill funded to protect against hardware failure, network down time, system compromise and legal litigation. Often, most information technologists are expected to be a "jack of all trades". This being so, it is almost impossible to catch everything and in most cases the effective operation of the technology takes precedence over the liabilities associated with the misuse. This simply boils down to an awareness issue.

As the reader, you may know that your company, organization or institution needs security policies, but do you know why?

LEGAL LIABILITY

Over the past ten years, we have witnessed an exponential growth in the Internet and the use of interconnected computer systems. Today, practically everyone depends on the Internet, email, and interconnected computer systems to do their jobs. That being so,

© SANS Institute 2002, As part of the Information Security Reading Room Author retains full rights.

technology is everywhere we go. It's used in government, business and institutions of higher learning. While this technology can simplify our lives, establish communications worldwide, promote our businesses or institutions, it can also destroy companies, cause public shame and result in huge punitive damages. As an administrator at an institution of higher learning, I've seen just about everything. Remember the old saying, "Where there is a will, there is a way"? This definitely applies to the World Wide Web, email and the use of interconnected computer systems. As a security specialist, information technologist or administrator, you should be aware of the liabilities associated with the miss use of this technology. It is the intent of this paper to focus on the following liabilities:

- Discrimination
- Defamation
- Harassment
- Obscenity and Pornography

DISCRIMINATION

Today, email is used practically everywhere, in government, business and education. For those who use email, it can be a great asset for communicating, marketing and receiving product updates and newsletters. However, email can also be misused. Often, employees and students will engage in jokes, spread offensive email and even explicit obscene material. This misuse can and will lead to discrimination if viewed by someone that finds the email offensive. Discrimination is defined as the prejudiced or prejudicial outlook, action, or treatment of an individual [1]. Discrimination can be categorized by the following:

- Age
- Sex
- Race
- Gender
- Religious beliefs
- Sexual orientation

DISCRIMINATION IN THE NEWS

> A Federal court in New York has allowed a class action discrimination suite on racial e-mails. The defendant is a large Wall Street brokerage firm and the plaintiffs are seeking $60 million in damages. [2]
>
> Female warehouse employees alleged that a hostile work environment was created in part by inappropriate e-mail. Plaintiffs ask for $60 million in damages; case settled out of court. [3]

HOW TO PREVENT ELECTRONIC DISCRIMINATION

The Aberdeen Group, a leading computer industry market research, analysis and consulting organization says, *"If employees are left unrestricted by policy and unchecked by monitoring software, then the corporation has exposed itself to significant legal liabilities, probable bandwidth abuse, and employee productivity gaps."*

© SANS Institute 2002, As part of the Information Security Reading Room Author retains full rights.

The first step to take when protecting your company or institution is to enforce an institutional e-mail policy that will explicitly state the acceptable use and unacceptable use of e-mail.

E-mail filtering is a great way to catch email with explicit material or language. While e-mail filtering is not foolproof, it will catch a majority of the offensive email before a user has the opportunity to view it.

There are several companies that specialize in filtering software and hardware. For reference, two products and their descriptions have been listed. When implementing a filtering solution, be sure to look at all vendors to ensure their will benefit you business or institution. When applicable, ask the vendor to demo the solution before purchasing. The following references have only been listed to provide the reader with an idea of what is available.

> Filter Control Technologies [4] offers a hardware solution to e-mail filtering called the Email Management "Black Box" solution. This solution will screen for offensive language, will reject email before reaching the mail server if content is deemed offensive, e-mail source blocking, attachment filtering, monitoring of employee email, reporting of blocked e-mail, and customized group filtering.
>
> Surf Control [5], a company that specializes in filtering software offers an e-mail filtering solution called Super Scout e-mail filter. This solution offers anti virus scanning at the gateway, has the ability to prevent confidential data loss, ability to implement encryption policy, remote reporting and administration as well as other features that may benefit your company or institution.

E-mail filtering has numerous benefits. Not only will it protect and catch offensive email, it can also catch viruses before entering your network. While it's not the scope of this paper to cover virus prevention or all of the benefits of e-mail filtering, I can tell you that you can save a lot of downtime by just catching viruses before entering your network.

Training is another way of preventing or aiding in the prevention of discrimination via e-mail. Users should be aware of institutional policies and should be informed of the penalties associated with misuse.

IS EMAIL MONITORING LEGAL?

E-mail monitoring is perfectly legal. In fact, in a recent *Journal of Biolaw & Business* article entitled, "Employer Guidelines for Workplace Email and Internet Policies," employment law attorneys Mark E. Schreiber and Emily C. Ehl state the following:

> *"A basic issue in employee rights cases is whether employees have a right to privacy in their email messages. As with most invasion of privacy cases, the core issue is whether an employee had a reasonable expectation that his or her personal email messages or web traffic would be private from his employer (and in the case of a public employer, whether the workplace search is sufficiently tailored under the fourth amendment to the government's interest in the efficient and proper operation of the job site). As the few reported cases indicate, employees have had little success in suing their employers for invasion of privacy when their employers accessed their emails or Internet activity, especially where the company had a clear and well disseminated email and Internet policy in place."*[16]

© SANS Institute 2002, As part of the Information Security Reading Room Author retains full rights.

Also, the Electronic Communications Privacy Act (ECPA) of 1986 gives employers, in the private sector, the legal right to monitor employee phone calls, e-mail messages, voice mail, computer files, and other communications made on company owned equipment in the "ordinary course of business." [15]

DEFAMATION

The First Amendment of the U.S Constitution provides us with the freedom of speech and expression. Although this amendment protects our speech and expressions, it will not protect us in the event that our speech or expression violates the rights of others. Defamation is defined as oral or written false statements that wrongfully harm a person's reputation. [1]Oral defamation is referred to as slander and written as libel. It should be noted that defamation laws differ from state to state and country to country.

DEFAMATION IN THE NEWS

> In September, 1998, the "barter exchange" site, Itex filed an action against some 100 Yahoo BBS authors for allegedly posting false and defamatory statements about Itex's management, including referring to Itex's management as "blind, stupid, and incompetent." In response to a court order, Yahoo provided Itex with the authors' email addresses it had on file. At the time, Yahoo's policies did not include verification of accurate email addresses for its visitors, including its chat room users. Relying on that information to obtain court orders against various ISPs, Itex eventually identified 5 of the "John Does." In part as a result of this lawsuit, Yahoo changed its policy and it now attempts to authenticate the email addresses given by visitors. [9]

> In March, 1999, Wade Cook Financial Corporation, the controversial Seattle-based financial seminar company, sued 10 unknown Yahoo message board users for posts that allegedly defame the firm and its CEO, Wade Cook. The plaintiff has indicated that like Shoney's and Raytheon, it intends to obtain a court order compelling Yahoo to identify the individuals responsible for the posts. [10]

HOW TO PREVENT ELECTRONIC DEFAMATION

The first step should always be enforcing your institution or company's policy on the acceptable usage e-mail. Also, managers should make the users aware of company and institutional policies and see to it they are enforced. The users should also be aware that email and documents are not secure or that they should not assume that they are.

While e-mail monitoring might provide some protection, this should not be relied on as a foolproof solution. Defamation is something that will be hard to protect against, but not impossible. If a defamatory message has been published it should be removed and a retraction or apology should be published immediately.

© SANS Institute 2002, As part of the Information Security Reading Room Author retains full rights.

HARASSMENT

Harassment as defined by the Standard Encyclopedic dictionary [6], means to persistently annoy. Today, many of us receive Spam or material that is unwanted. This material is not considered harassing, although we may beg to differ. Harassment is the unwanted and repeated behavior targeted at one or more particular individuals.

HARASSMENT IN THE NEWS

> International Microcomputer software pays a former employee $105, 000 after she received sexually harassing messages on the firm's electronic bulletin board, even though the company reported the incident to authorities and launched an internal investigation. [18]
>
> Chevron settles sexual harassment lawsuit for $2.2 million over e-mal postings such as: "25 reasons why beer is better than women".[19]

HOW CAN I PREVENT HARASSMENT?

The first step in prevention is to ensure that your institutional policies cover and explicitly state what actions are deemed as harassment.

Employee training is another way of curtailing harassment. All employees should be aware of institutional policy, but it never hurts to train.

E-mail filtering can catch e-mail that can be considered obscene or sexual, but should not be viewed as the only solution to the problem.

OBSCENITY and PORNOGRAPHY

With the continued growth of adult-oriented, X-rated web sites, concern and controversy have arisen regarding censorship and the legal issues resulting from the viewing of such material in the work place. The First Amendment is challenged every day in all aspects of life and legal litigation. Internet censorship is often a matter that will start a heated debate among a group of people. That being so, statistics show that employee will tend to visit sites that are categorized as obscene or pornographic. Not only does this pose certain liability issues such as, discrimination and harassments, it also wastes valuable employee time and network resources. Should the employee access a site that is against state and federal laws, criminal action may result, therefore bringing shame and humility to the company or institution.

JUST HOW BIG IS THIS INDUSTRY?

- In 1998, 970 million dollars was spent on visits to adult Web sites, an amount that could raise to 3 billion dollars by 2003. [20]

© SANS Institute 2002, As part of the Information Security Reading Room Author retains full rights.

- There are currently over 72, 000 sexually explicit Web sites. [20]
- The FBI has documented over 4, 000 cases of online child pornography [20]

The figures are astonishing. The continued growth of this industry shows that there is a huge demand for this kind of product. That being so, its inevitable that it will appear in the work place.

HOW TO PREVENT OBCENITY

The first step is to ensure your institutional policy explicitly states what material and web sites is deemed unacceptable. It never hurts to conduct frequent training seminars covering such issues as sexual harassment, discrimination and defamation. Remember, in the long run, it will save money by educating the employees.

There are several vendors that specialize in filtering software. Some of which include, but are not limited to:

- Elron Software [22]
- Websense [21]
- Pearl Software [11]
- SurfControl [5]

There are many vendors that specialize in filtering software and while it's not the intentions of this paper to list all of them, you should be aware that there are many more than the aforementioned. When implementing a filtering solution, make sure you look at several different options. Also, ask the vendor to demo their product at your company or institution.

CYBERSLACKING

Cyberslacking as defined by www.webopedia.com, is the recreational web surfing during work hours, resulting in the following:

- Bandwidth consumption
- Compromised Security
- Decreased Employee Productivity.

BANDWIDTH CONSUMPTION

It's almost impossible for any Government agency, business or educational institution to not have access to the Internet. The Internet has become a valuable tool for research, communication, marketing and Internet hosted applications. That being so, statistics show that users will tend to download various types of media including but not limited to the following:

- MP3 music files
- Streaming media
- Video and audio files
- Large graphic files

© SANS Institute 2002, As part of the Information Security Reading Room Author retains full rights.

- Software

The downloading of the aforementioned will result in wasted bandwidth, network congestion, network instability, and slow response time. If the network is not designed properly, this wasted bandwidth can be quite devastating. For many companies, network quality of service may be their most important business asset. In today's world, competition is fierce, therefore, a company that does not have control over its employees and bandwidth, might have trouble keeping pace with the competition.

COMPROMISED SECURITY

When users are allowed unrestricted internet access, this can often lead to the users downloading software that may contain source code for back doors, or in other words, laced with a Trojan horse.

DECREASED EMPLOYEE PRODUCTIVITY

Employees that surf the Internet all day or even just an hour are wasting invested money and valuable network resources. According to an article published by Pearl Software [11], a company that specializes in internet filtering solutions, indicated that a salaried employee earning $44, 000 a year can cost his or her employer at least $5, 000 a year just by playing around in the internet for one hour a day. In a paper entitled "Guide to Internet Usage and Policy", published by ELRON software indicates the following:

> If 50 users spend 3 hours each week on recreational surfing during work hours, the cost to your company will loose $3,322.50 in lost salary expenses each week, or $172,770 per year.

HOW TO PREVENT CYBERSLACKING

There are several ways to prevent cyberslacking in the workplace. The first step as mentioned before should be a sound institutional or company policy that explicitly states the acceptable use of the Internet. Also, Internet monitoring and filtering can deter from spending personal time on the Internet while at work. Real time monitoring along with random spot check should be enforced.

Cyberslacking is not an IT issue but rather a management issue. Manager should ensure that their employees adhere to institutional or company policy regarding Internet usage.

SOFTWARE LICENSURE and COPYRIGHT INFRINGEMENT

In the IT industry, no network administrator wants to hear the words software audit. Like accountants fearing an audit from the IRS, network administrators fear software audits. If you think no one will ever know that you've installed un-licensed software to several computers, think again. In fact, more and more companies are being found in violation of

© SANS Institute 2002, As part of the Information Security Reading Room Author retains full rights.

copyright laws. In institutions of higher learning there is a misconception that colleges and universities are exempt, well, I can tell you that is absurd.

WHAT IS SOFTWARE LICENSING AND COPYRIGHT INFRINGEMENT?

Software licensing can be viewed as the legal purchase of software and complying with the restrictions set by the copyright owner. In other words, when we purchase software, we are purchasing permission to use the software from the copyright owner to comply with Federal law regarding software copyrights.

Copyright as defined by the Standard Encyclopedic dictionary [7] is the exclusive statutory right of authors, composers, playwrights, artists, publishers and distributors to publish and dispose of their work for a specified period of time. The word infringement simply means violation. Therefore, copyright infringement is the violation of the restrictions set by the owner of the copyright.

BIG DEAL, WHO WILL KNOW?

The Software Publisher Association [8], a non-profit organization and the Business Software Alliance, an international organization, represents leading software companies and are conducting random audits of businesses and institutions of higher learning to find unlicensed software.

WHAT ARE THE PENALTIES?

Depending on the infringement, if your company is found to be in violation, you may be held liable under both civil and criminal law. If the copyright owner wishes to file civil action against you, they can stop you from using their software immediately and you can be fined up to $150,000 for each work infringed. In addition, if that's not worse enough, the United States Government can criminally prosecute you and if convicted you can be fined up to $250,000, or sentenced to jail for up to five years, or both. [16]

COPYRIGHT INFRINGEMENT IN THE NEWS

> **Washington D.C., (Monday, August 6)** -- The Business Software Alliance (BSA), a watchdog group representing the nation's leading software manufacturers, today announced that RISCO, a software developer headquartered in Lenexa, KS, paid $263,423 to settle claims relating to unlicensed copies of Adobe, Macromedia, Microsoft and Symantec software programs installed on its computers. In addition to the payment, the company agreed to delete any unlicensed copies, purchase replacement software and strengthen its software management practices. [17]

HOW TO PREVENT COPYRIGHT INFRINGEMENT

The first step in prevention is to explicitly state the un-acceptable use of software in your institution's "acceptable use policy." Many companies and institutions will develop policies forbidding the installation of software by anyone or any department other than the MIS department. With this type of policy, all software and licenses is kept in one

© SANS Institute 2002, As part of the Information Security Reading Room Author retains full rights.

place and you have the assurance that a qualified individual is installing the software. Another important aspect to look at is the procurement of software in your company or institution. If there is no centralized procurement method, you are setting yourself up for a real headache. The Internet posses a potential problem with users downloading copyrighted software from warez sites and now with the gnutella network.

The Business Software Alliance offers a software-auditing tool called GASP. This tool is free of charge and designed to help track unlicensed software on desktops, laptops and network servers. You can download this tool at, http://www.bsa.org/usa/freetools/gasp/.

There are many ways to audit a network and check for pirated software, some of which include Microsoft SMS, Network Scripts and various other technologies.

CONCLUSION

As technology continues to increase, so does its misuse. As managers, security specialists, and information technologists, it is extremely important that you understand the dangers and liabilities associated with the misuse of the Internet, e-mail and interconnected computer systems.

The intent of this paper is to raise awareness to the common misuse and the liabilities resulting of the misuse of the aforementioned technology. If you're company does not have security policies in place, your first step should be to present this document to management. There are several great resources on security policies on the internet, but one of the best can be found at http://rr.sans.org/policy/policy_list.php .

RESOURCES

1. Merriam-Webster. http://www.m-w.com/cgi-bin/dictionary
2. Owens and Hutton v. Morgan Stanley & Con., Inc., Case No. 96 Civ 9747
3. Harley V. McCoach, 928 F. Supp. 533, E.d. Pa. 1996
4. Filer Control Technologies.http://www.filtercontrol.net/en/index.html
5. Surf Control. http://www.surfcontrol.com/
6. Funk & Wagnalls. Standard Encyclopedic Dictionary. Chicago. J.G. Ferguson publishing company, 1966, 292
7. Funk & Wagnalls. Standard Encyclopedic Dictionary. Chicago. J.G. Ferguson publishing company, 1966, 141
8. Software & Information Industry Association. http://www.spa.org
9. Rogers., Sugarman., Barshak., and Cohen. "Itex Corp. v. John Does 1-100". URL: http://www.netlitigation.com/netlitigation/defamation.htm

10. Rogers., Sugarman., Barshak., and Cohen. "*Wade Cook Financial Corp v. John Does 1-10*". URL:http://www.netlitigation.com/netlitigation/defamation.htm
11. Pearl Software.http://pearlsw.com/
12. Netlitigation. http://www.netlitigation.com/netlitigation/defamation.htm

© SANS Institute 2002, As part of the Information Security Reading Room Author retains full rights.

13. Business Software Alliance http://www.bsa.org/usa/freetools/consumers/swandlaw_c.phtml
14. Ferrera, G., Lichtenstein, S., Reder, M.August, R., and Schiano, W.Cyberlaw Your Rights in Cyberspace. Thompson Learning, 2001.176
15. Elron Software. "Guide to Internet Usage and Policy." Elron Software, Inc 2002: 10
16. Business Software Alliance http://www.bsa.org/usa/freetools/consumers/swandlaw_c.phtml
17. Business Software Alliance. "Kansas Software Developer Pays Software Watchdog More Than $260,000 For Unlicensed Software."6 August. URL: http://www.bsa.org/usa/press/newsreleases//2001-08-06.681.phtml
18. Staff Writer, CNET News.com, April 14, 1999
19. Jerry Adler, Newsweek, "When E-mail Bites Back", November 23, 1998
20. Ferrera, G., Lichtenstein, S., Reder, M.August, R., and Schiano, W.Cyberlaw Your Rights in Cyberspace. Thompson Learning, 2001.164
21. Websense. http://www.**websense**.com
22. Elron Software. http://www.**elron**sw.com

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room Author retains full rights.

Last Updated: February 10th, 2016

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Northern Virginia - McLean 2016	McLean, VAUS	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS Munich Winter 2016	Munich, DE	Feb 15, 2016 - Feb 20, 2016	Live Event
ICS Security Summit & Training - Orlando	Orlando, FLUS	Feb 16, 2016 - Feb 23, 2016	Live Event
SANS Southern California - Anaheim 2016	Anaheim, CAUS	Feb 22, 2016 - Feb 27, 2016	Live Event
SANS Secure India 2016	Bangalore, IN	Feb 22, 2016 - Mar 05, 2016	Live Event
RSA Conference 2016	San Francisco, CAUS	Feb 28, 2016 - Feb 29, 2016	Live Event
SANS London Spring 2016	London, GB	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS Philadelphia 2016	Philadelphia, PAUS	Feb 29, 2016 - Mar 05, 2016	Live Event
SANS Abu Dhabi 2016	Abu Dhabi, AE	Mar 05, 2016 - Mar 10, 2016	Live Event
SANS 2016	Orlando, FLUS	Mar 12, 2016 - Mar 21, 2016	Live Event
ICS410 Dubai 2016	Dubai, AE	Mar 13, 2016 - Mar 17, 2016	Live Event
SANS Secure Singapore 2016	Singapore, SG	Mar 28, 2016 - Apr 09, 2016	Live Event
SANS Secure Europe 2016	Amsterdam, NL	Apr 04, 2016 - Apr 16, 2016	Live Event
SANS Northern Virginia - Reston 2016	Reston, VAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
SANS Atlanta 2016	Atlanta, GAUS	Apr 04, 2016 - Apr 09, 2016	Live Event
Threat Hunting and Incident Response Summit	New Orleans, LAUS	Apr 12, 2016 - Apr 19, 2016	Live Event
ICS Amsterdam 2016	Amsterdam, NL	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Secure Canberra 2016	Canberra, AU	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Pen Test Austin	Austin, TXUS	Apr 18, 2016 - Apr 23, 2016	Live Event
SANS Copenhagen 2016	Copenhagen, DK	Apr 25, 2016 - Apr 30, 2016	Live Event
SANS Security West 2016	San Diego, CAUS	Apr 29, 2016 - May 06, 2016	Live Event
SANS Baltimore Spring 2016	Baltimore, MDUS	May 09, 2016 - May 14, 2016	Live Event
SANS Houston 2016	Houston, TXUS	May 09, 2016 - May 14, 2016	Live Event
SANS Stockholm 2016	Stockholm, SE	May 09, 2016 - May 14, 2016	Live Event
SANS Prague 2016	Prague, CZ	May 09, 2016 - May 14, 2016	Live Event
SANS Secure Japan 2016	OnlineJP	Feb 15, 2016 - Feb 20, 2016	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced