Global Information Assurance Certification Paper

Acceptable Use:
Whose Responsibility Is It?

By Patti Lawrence

GSEC Assignment Version 1.3

March, 2002

Acceptable Use: Whose Responsibility Is It?

By Patti Lawrence

Abstract

Responsibility for investigating acceptable computer use violations often falls within the scope of the Information Technology department of an organization, because that is where the technical expertise resides. Either the system administrator or a focused information security response team member becomes the coordinating point of the effort. But is acceptable use really an Information Security policy, or is it a Human Resources policy? Where does the Legal department fit into the equation?

This paper focuses on the Information Technology and Information Security ramifications of acceptable computer use policy and attempts to show how responsibility can be shared with the less technical Human Resources and Legal departments. The goals of the policy are to (1) meet productivity goals of the Human Resources department; (2) meet liability concerns of the Legal department; (3) protect the organization's information and technical resources; and (4) meet the security goals of the Information Technology and Information Security departments.

Background

As long ago as 1997, Information Technology leaders already realized the widespread use of computers and the Internet within their organizations and the potential costs of misuse. An article in *CIO Web Business Magazine*[1] reviewed this potential and presented the opinion that the misuse and policies covering it had always been around in other, less technical forms. Some examples of pre-Internet policy violations include:

- Unauthorized release of sensitive data via newspaper, radio, book, telephone, etc.;
- Wasting time by the water cooler discussing non-business topics;
- Telling racist or sexist jokes (promoting a hostile workplace);
- Speaking on behalf of the company without authorization.

The article suggests that policies need to be updated and/or new ones created to apply the existing policy to the new technological tools, keeping in mind that:

- Use of the Internet exploded much faster than laws and policies related to its use were able to keep up;
- Internet legal problems include privacy, security, productivity, and responsibility;
- Written policy limits liability and misuse;

[1] Bennett and Fena.

- A cross-functional team is needed to ensure all issues are covered:
    - Human Resource and Legal cover liability issues
    - Marketing and Strategic Planning ensure positive uses of the tools
    - Information Technology and Information Security ensure security and efficiency of the technological tools.

Issues

Consider how an organization's management, stockholders, employees, customers, etc., would react to the following news:

- An employee posts sensitive product information or internal CEO memo on the state of the company to a financial web site's message board. Changes in the stock price may be attributed to the effect of this news.
- A well-known pornographic web site posts a list of their site's biggest hitters by IP (Internet Protocol) address, and one of these turns out to be your organization's firewall. Anyone can translate that address into your organization's name just by going to http://www.samspade.org, typing the IP address, and clicking on the "Do Stuff" button.
- A system administrator accidentally stumbles upon child pornography while backing up an end user's workstation. He is not sure whether to continue the backup or stop and call someone.
- The cell phone used by an accused stalker to make harassing phone calls is traced back to the company he/she works for.
- Your organization's Internet proxy logs reveal someone inside the company is posing as a teenager looking for dates in a teen chat room. Even worse, law enforcement has already traced the person back to your network and is knocking at the door asking you to find out who is responsible for the activity.
- The company is held to promises made by one employee's electronic mail to customers.
- An employee is accused of hacking into the Human Resource database to compare salaries of co-workers.
- Pirated software found on company computers opens the company to legal action and possible confiscation of critical computing resources.
- An unauthorized employee downloads hacking tools and runs vulnerability scans on the corporate network to see how secure it is.

Most of these incidents are violations of existing policy, with the addition of organization-provided technology to enable the violations. How do you respond? Do you turn the other way and pretend you did not see anything, or do you make sure you have policies and procedures in place to prevent, detect, and react to this potential misuse? Have you made the policy known by publishing online, by electronic mail, and in print? If misuse

still occurs despite your policies, do you have documented processes to respond quickly to minimize the effect on the bottom line? And whose policy should it be, anyway?

Granted, the Human Resource and Legal departments need to be visibly involved in the policy-setting process. In fact, it actually makes sense in many organizations for the Human Resource department to own the policy, since violations will typically result in some type of disciplinary action for which they have the expertise and final responsibility. On the other hand, the Information Technology and Information Security departments have a large stake and expertise in what the policy needs to cover. For one thing, the policy relates to hardware and software that is put in place and supported by the Information Technology department. Information Security in particular is responsible for the secure and responsible use of those technological tools.

Information Security Perspective

The Information Security department is concerned with acceptable use of the technological tools they provide because of their focus on Confidentiality, Integrity, and Availability of computer-based information resources.

Confidentiality

To the Information Security professional, confidentiality refers to ensuring that all information stored on computers and networks they are responsible for is protected from unauthorized disclosure. It involves working with data owners to determine the sensitivity of the information and determine what level of protection is required to balance the risks of such disclosure and value of the information against the cost of such protection. Networked computers are vulnerable to attack from both inside and outside, so it also requires being able to focus on both at the same time, not unlike those eyes that our parents must have had in the back of their heads when we were younger.

For example, Sperry[2] highlights the risks of an Internet porn-surfing scandal at the White House. Although nothing has been reported to suggest that any high-level public officials were blackmailed over the incident, it is easy to imagine how demands could have been made for network access that might provide trade, economic, and/or geopolitical secrets to unauthorized individuals, special-interest activist groups, corporations, or hostile governments.

In a more recent incident, an improperly secured FormMail program was exploited at BowieNet in order to send out fraudulent order confirmations for Microsoft Xbox video game systems on Ebay.[3] A link within the fraudulent message directed careless or naïve users to a fake Ebay web site, where they were prompted to enter personal confidential information to request order cancellation. Although this attack was intended to collect

[2] Sperry.
[3] McWilliams.

personal information such as valid credit card accounts and addresses, it could as easily have requested proprietary information related to a business, government, or other organization.

Viruses are more often thought of as threats to availability and integrity than confidentiality, but consider some of the actions of electronic mail based virus attacks from the past two years – those that generate new messages to everyone in the address book, and attach a random file selected from the computer's hard drive. Since the bulk of these attacks are against Microsoft applications, it is not difficult for the attacker to create a virus that picks up files that have Microsoft Office extensions, such as .xls (Excel spreadsheets), .doc (Word documents), or .ppt (PowerPoint presentations), which are most likely to contain sensitive information.

Finally, an organization must also be aware of and prepared for intentional or unintentional leaks of proprietary information by the authorized users of the network. Electronic mail and web-based bulletin boards have long been likely electronic avenues for sensitive information to be made public, but peer-to-peer applications introduce a whole new set of confidentiality issues. Although this technology can bring about productivity gains through collaboration, the Information Technology and Information Security departments need to research thoroughly before allowing this type of application to run (or continue to run, since it is probably already there!) on the network. Among the risks, according to *Information Security Magazine,* are:

- Application security flaws might allow an attacker to access confidential information.
- By social engineering, an attacker could convince a user to download an executable file that provides access to sensitive information stored on the computer or network.
- A user could misconfigure the software's sharing capabilities in such a way that sensitive information is accidentally exposed.
- Peer-to-peer provides cover for a disgruntled employee to move sensitive information outside the organization, bypassing protective filters that may be in place. For example an application called Wrapster can transform any file into an MP3 look-alike.[4]

Integrity

Integrity is achieved when there is assurance that the information and programs used to access and report that information have not been changed from their original values without going through an authorized, documented change process. Several issues related to acceptable use of the organization's computer resources could affect the integrity of our systems and information. Harold Kester recently predicted "Employee surfing may be

[4] Berg.

your biggest security threat in 2002"[5] and much of this threat involves attacks on integrity.

Viruses and other malicious code are among the first things that everyone thinks about when asked about the health of their security program. These attackers can enter our systems in a number of ways, including online greeting cards, jokes, and executable programs of all kinds. They make changes to or even delete critical operating system files, program executables, and data. Most of today's viruses enter our networks through electronic mail or other tools that allow active content or macros. (For a good write-up on security risks of active content, see the bulletin from the National Institute of Standards and Technology.[6]) Thurman reminds us to look beyond the organization-provided tools and consider that any protection installed on the enterprise's standard gateway can be bypassed by the use of web-based electronic mail services such as Yahoo! and Hotmail, as well as direct downloads from the Internet.[7]

Another means of attacking the integrity of an organization's electronic system is through pirated software. "Pirated" refers to illegal copies of well-known software that often come from hackers. Kester reminds us that we cannot trust the originators of illegal software to provide non-malicious products. This software could contain code that damages programs and/or data.[8]

Peer-to-peer applications also enable integrity attacks. According to Valiente, if care is not taken to limit what resources are shared, an organization may be offering network drives containing critical information without even knowing it, and thus making the entire peer-to-peer community part of its Local Area Network. Once a malicious attacker has access to such a shared area, it is only a matter of time before file integrity can be compromised. Until security measures surrounding peer-to-peer applications mature, "they should be treated with the same level of scrutiny as back-door hacking programs like Back Orifice and similar collections of tools used by hackers to mask intrusion and obtain administrator-level access to computers or computer network programs."[9]

Possibly one of the most frustrating of all integrity attacks is what Spector calls "Invasion of the Browser Snatchers."[10] He relates the story of an individual who misspelled the address of *PC World's* web site and was redirected to a pornographic web site. But it did not end there. He later found that the site made changes to his web browser's settings to point back to that page every time the browser was opened and every time he attempted to run an Internet search. Even if he changed the settings back, they reappeared the next time he booted the machine. To add insult to injury, some unscrupulous web sites will

[5] Kester.
[6] Jansen and Karygiannis.
[7] Thurman.
[8] Kester.
[9] Valiente, Jr.
[10] Spector.

install a program that dials a 1-900-xxx-xxxx phone number to access even more pornography. Of course, the calls are not free, and the victim will typically spend an enormous amount of time and energy fighting any charges that appear on their phone bill.

Availability

The Information Security department is ultimately responsible to ensure that the computer and network resources of the organization, including programs and information stored electronically, are available for use when the organization's employees and authorized business partners want to use them. In today's fast-paced, global society, this could mean around-the-clock, year-round availability. Inappropriate use of internal computing resources can have a negative effect in many areas of the business.

We have already looked at viruses and malicious code as an integrity issue; however, they can also become an availability issue in cases such as a denial of service attack. For example, recent viruses introduced through electronic mail have clogged messaging servers of both large and small enterprises to the point that their entire networks were unavailable for hours or even days at a time before they could stop the activity long enough to clean up the mess.

Possibly the most debated availability issue is bandwidth. Valiente points out the hidden costs of bandwidth use caused by peer-to-peer applications: "remote and Internet network connections are over-utilized, and then [organizations] pay for additional bandwidth to keep pace with the demand, only to find that the traffic is generated by non-business applications." He goes on to point out that these applications also increase backup storage and processing resource requirements.[11] In addition, we need to remember that the first thing a person does with peer-to-peer is download, install, and run a program in order to participate. A denial-of-service situation could result if the application is not compatible with the network standard environment.[12]

Even legitimate business uses of Internet technology can become bandwidth availability issues, such as when BMW listed their web site on a television commercial with an invitation to view a video stored there. The level of traffic experienced on that connection within the first week was estimated to be the "equivalent of dedicating an entire T1 line for a little over 57 days just to view a car commercial."[13] For BMW this was a legitimate business use of their systems, but for the individuals who accessed the commercial from within their employer's network it was non-business use.

Availability of storage resources also becomes an issue when employees store music, video, and other large graphic files on network file servers that are intended for storage of

[11] Valiente, Jr.
[12] Berg.
[13] Wynn and Trudeau.

business information. These unnecessary files contribute to the time and media requirements for system backups and increase the amount of time to restore critical information in times when a disaster recovery plan must be activated to recover business operations. Lawson recommends that removal of files from the network that violate acceptable use policy should be included in procedures supporting the policy.[14]

Forwarding hoax electronic mail messages can also become an availability issue. These messages often sound like reasonable requests to help someone in need when actually they have been making the rounds for years and are well-known urban legends[15] that can be found by searching web sites dedicated to stopping the rumors. (For more information, see http://hoaxbusters.ciac.org).

Although we do not always consider software license compliance to be an availability issue, it can become one. Consider a situation in which systems are confiscated as evidence of illegal use of licensed software. Law enforcement will, under most circumstances, do whatever they can to avoid confiscating all of an organization's resources if it will put the organization out of business. The possibility still exists, however, that some critical electronic resources will not be available for an extended period of time.

Other Information Technology/Information Security Issues

The Information Technology and Information Security departments typically are responsible for implementing and operating the technologies that are useful to prevent, detect, investigate, and report violations of acceptable computer use policy. In addition, Information Technology managers are responsible for keeping up with new technologies and understanding how use and misuse of those technologies will affect security of the electronic information systems of the organization.[16]

Management, Human Resources, and Legal Perspectives

The main acceptable use issue that we think of in terms of Human Resources is that of productivity. When employees are surfing non-business Internet sites when they should be working, Human Resources and Management must become involved. Many times the issue is that the manager does not really know what the employees are doing and needs to pay more attention by looking into the reasons why their work is not getting done. Human Resources can provide training to managers in how to spot and deal with productivity issues, along with how to motivate workers to take pride in being productive contributors to the organization's success.

A concern shared by both Human Resources and the Legal department is when non-

[14] Lawson.
[15] Paul.
[16] Cohen.

business computer use results in creation of a hostile workplace by individuals who are downloading, transferring, and storing sexually explicit, illegal, or harassing material on office computers. "The U.S. Supreme Court has decided that companies can be held accountable when their employees use the Internet inappropriately, such as forwarding offensive messages."[17]

Top-level management may also be concerned when availability issues created by unacceptable use of the internal network resources affect external network resources such as electronic commerce. Berg points out that this translates into lost money for the organization –it hits the bottom line directly.[18]

The Legal department must be aware that software license compliance violations can result in fines, criminal records, and personal liability issues for company directors, which may include arrest and imprisonment.[19]

Peer-to-peer applications also have legal consequences. They often enable distribution of copyrighted materials. They also create long sessions that make it easier to trace illegal activity back to the source.[20] If this source is an enterprise network, the enterprise could become liable even if unaware that the material had been stored within their network.

Lawson reminds us that the company could be breaking the law by providing the tools and access to illegal files such as pornography in general in some jurisdictions[21] and, as a recent FBI press release notes, child pornography is illegal in most jurisdictions.[22] In a more interesting twist, many organizations have discovered employees using company-owned Internet tools to access web sites that pay end-users to surf. In addition to adding to productivity problems, legal questions arise as regarding use of these tools for personal financial gain. Some legal experts have even suggested that organizations may be able to claim any profits or prizes acquired using the resources they provide for their employees. It will be interesting to follow as these cases develop over the next few years.[23]

Although one of the most critical productivity tools in place today, electronic mail presents all sorts of legal problems. Chevron, for example, settled a suit with a female employee who felt harassed by an electronic mail joke comparing beer to women. Storage of electronic mail messages also presents legal issues, because such archives become subject to discovery in a legal case. As Paul reports, "E-mail more often yields incriminating rather than exculpatory evidence." Failing to deal with issues arising from

[17] Wynn and Trudeau.
[18] Berg.
[19] Willmott.
[20] Valiente, Jr.
[21] Lawson.
[22] U.S. Department of Justice, Federal Bureau of Investigation.
[23] Marsan.

unacceptable computer use can be interpreted as tolerance of the behavior and make a difference in the outcome of legal action.[24] SurfControl, a company that makes Internet monitoring tools, has published several White Papers related to acceptable use of organization-provided computer resources. One such paper points out that electronic mail also is seen as official correspondence when it comes from within an organization's network. This has the potential to make any communication legally binding.[25]

The Legal department may also need to be involved if a virus is carried by electronic mail from an organization's network to other organizations.[26] While it is common courtesy to report to the external organization, more research needs to be done into who has legal responsibility for any damage that may have been avoided if the proper controls had been in place.

Online message boards also pose a dilemma for businesses. On one hand, they provide a forum for sharing information about a topic of common interest. On the other hand, they are often used to post information about an organization that is untrue or causes unnatural fluctuations in stock prices. Agulnick reports that use of such boards to manipulate stock prices has already resulted in prosecution. He also points out the risk of employees or executives being tempted to respond to false information that has been posted or argue about criticism of the argument,[27] not realizing that they could be violating policy or even finance laws by representing the views of the organization without authorization.

Last, but certainly not least, any effort to monitor the use of an organization's network absolutely must be limited by policies and local laws governing each business site.

Response: Working Together

Exhibit 1, Matrix of Issues and Responsibilities, was generated from the research for this paper and my own personal experience. It suggests how the issues fit into each functional department's domain with respect to Information Technology and Information Security (confidentiality, integrity, and availability), Human Resources and Management (productivity), and Legal (liability). The list is by no means exhaustive. However, we can see that it is beneficial for Information Technology, Information Security, Human Resources, and Legal departments to share responsibility for developing and enforcing the acceptable use policies of an organization. If joint ownership of the policy is not feasible in an organization, I recommend that each of these departments be included in the review process at a minimum and be allowed to participate in content development from the beginning if at all possible. This will ensure that the concerns of all are covered without duplicating policy in diverse areas of the organization.

---

[24] Paul.
[25] SurfControl.
[26] Ibid.
[27] Agulnick.

Exhibit 1: Matrix of Issues and Responsibilities
Confidentiality, **I**ntegrity, **A**vailability, **P**roductivity, and **L**iability

	IT/IS			Management, HR, Legal	
Issue:	**C**	**I**	**A**	**P**	**L**
Employee posts sensitive product information or CEO memo	X				X
Organization's IP address published as a heavy hitter at porn sites	X			X	
Child pornography discovered on employee's hard disk			X	X	X
Company-issued cell phone used for stalking					X
Employee looks for date in a teen chat room	X			X	X
Employee sent electronic mail to customers making unauthorized promises					X
Employee collects salary information from HR database	X			X	X
Pirated software is downloaded from the internet and installed on company computers		X	X	X	X
Shareware is downloaded for business use, still in use but no payment ever made			X		X
Employee runs unauthorized vulnerability scans			X	X	
Employee downloads hacking tools		X		X	X
Employee surfs non-business web sites during working hours				X	
Employee surfs pornographic web sites at any time		X	X	X	X
Employee receives electronic mail at work asking for personal information at a fake web site	X				X
Employee shares non-business files through peer-to-peer application	X	X	X	X	
Employee shares copyrighted files through peer-to-peer application	X	X	X	X	X
Virus or other malicious code enters network through electronic mail or web surfing	X	X	X	X	
Virus was not contained and hit customer's network as a result		X	X		X
Employee's MP3 (music) collection, organized by style of music, artist, and CD title, takes up 6 gigabytes of network storage space			X	X	X

Resources and Additional Reading

Agulnick, Seth. "Online Message Boards Bedevil Companies." Gannett News Service, published in *USA Today* online, June 14, 2001. http://www.usatoday.com/life/cyber/2001-06-14-message-boards.htm.

Armstrong, Illena. "Searching for Internet Privacy." Special Feature, *SC Magazine Online.* March 2002. (NOTE: online edition contains more material than the hard-copy edition of the magazine). http://www.scmagazine.com/scmagazine/2002_03/special.html.

Bennett, Wayne D., and Lori Fena. "Looking Both Ways: Two Views on Policies that Govern Internet Use at Work." ("The Employer Perspective" by Bennett, and "The Employee Perspective" by Fena.). *CIO Web Business Magazine.* October 1997. http://www.cio.com/archive/webbusiness/100197_gray.html.

Berg, Al. "P2P, or Not P2P?" *Information Security Magazine.* February 2001. http://www.infosecuritymag.com/articles/february01/cover.shtml.

Cohen, Sacha. "Monitoring E-mail: Management or Thought Police?" *IDG on CNN.com.* February 27, 2001. http://www.cnn.com/2001/TECH/internet/02/27/management.thought.police.idg/index.html

Elron Software. Series of White Papers on Internet usage and policy, Cyberliability, and other related topics. Available by completing forms at web site (1 form per white paper requested – Expect to receive a follow-up sales call if you download.) http://www.internetmanager.com/productfamily/whitepapers.shtml.

Griffin, Brad. "An Introduction to Viruses and Malicious Code Part Two: Protecting Your Computers and Data." Infocus. *SecurityFocus.* December 27, 2000. http://www.securityfocus.com/infocus/1189.

Jansen, Wayne, and Tom Karygiannis. "Security Implications of Active Content." National Institute of Standards and Technology. Undated article. http://csrc.nist.gov/publications/nistbul/itl00-03.txt.

Kester, Harold. "Looking Out vs. Looking In." *SC Magazine*, March 2002: 74.

Lawson, Todd. "The Most Commonly Overlooked Security Holes." *SC Magazine Online.* January 2002. http://www.scmagazine.com/scmagazine/sc-online/2002/article/03/article.html.

Marsan, Carolyn Duffy. "The Latest Headache for Network Professionals: Sites That Pay You to Surf." *Network World Fusion,* March 6, 2000. http://www.nwfusion.com/news/2000/0306surf.html.

McWilliams, Brian. "Holy Cow! Bowie Among Innocents Used in Ebay Scam." *Newsbytes*. January 25, 2002. http://www.newsbytes.com/news/02/173962.html.

Paul, Lauren Gibbons. "How to Tame the E-mail Beast." *IDG on CNN.com.* October 18, 2001. http://www.cnn.com/2001/TECH/internet/10/18/email.beast.idg/index.html.

Riptech, Inc., "Riptech Internet Security Threat Report." This report is available at no charge by filling out a form at http://www.riptech.com.

Spector, Lincoln. "Invasion of the Browser Snatchers." *IDG on CNN.com*. February 18, 2002. http://www.cnn.com/2002/TECH/internet/02/18/browser.snatchers.idg/index.html.

Sperry, Paul. "Web Porn Scandal Rocks White House." *WorldNet Daily*. August 9, 2000. http://www.warroom.com/Whitehouse/pornscandal.htm.

SurfControl "The Email Guide: How To Use Email in the Workplace." Undated Whitepaper. http://www.surfcontrol.com/general/assets/whitepapers/using_email_in_the_workplace.pdf.

Thurman, Matthias. "Virus Attacks Can Enter Through Many Doors." *Computerworld*. January 28, 2002. http://www.computerworld.com/itresources/rcstory/0,4167,STO67720_KEY73,00.html

Trudeau, Chris. "Email Policy – A Necessary Evil." Guest Feature. *SecurityFocus*. November 13, 2000. http://www.securityfocus.com/guest/3818.

U.S. Department of Justice, Federal Bureau of Investigation. "Operation Candyman." Press Release March 18, 2002. http://www.fbi.gov/pressrel/pressrel02/cm031802.htm.

Valiente, Jr., Carlos. "P2P: Who Pays the Piper? Don't Let it Be You." *SC Magazine Online*. September 2001. http://www.scmagazine.com/scmagazine/sc-online/2001/article/039/article.html.

Willmott, Richard. "Software Compliance: A Helping Hand in an Economic Downturn." *SC Magazine Online.* January 2002. http://www.scmagazine.com/scmagazine/sc-online/2002/article/05/article.html.

Wynn, Annie, and Paris Trudeau. "Internet Abuse at Work: Corporate Networks Are Paying the Price." Surf Control White Paper, September 2001. http://www.surfcontrol.com/general/assets/whitepapers/InternetAbuseAtWork_9_2001.pdf.