Internet Acceptable Use Policies: Drawing the line between freedom and protection.

Raymond E. Pitzen

April 15, 2012

Abstract

I am sure it was not long after the Internet infiltrated the workplace that Internet acceptable use policies (IAUP) followed. The IAUP serves two purposes. It protects the organization and it protects the employees. By following the IAUP employees know the boundaries in which to freely use the information systems and equipment at their disposal. By establishing and enforcing said IAUP, the organization protects it assets from malicious attacks, ensures availability of resources, provides a productive work environment, gives itself legal recourse to discipline employees who violate the policy, and saves money.

A well-defined Internet acceptable use policy (IAUP) can mitigate many of the risks associated with exposure to the Internet. This paper will discuss the background and importance of an IAUP and its role. It will also take a look at some of the consequences and advantages in either being too strict or too liberal as well as examine some of the components that define an IAUP.

Internet Acceptable Use Policies: Drawing the line between freedom and protection.

At the rate at which technology evolves faster and faster, the challenges for network administrators and information systems security personnel also change. Companies, corporations, and even schools are trying to leverage the information super-highway in order to give themselves a competitive advantage, or at the very least keep themselves from being at some disadvantage. Connecting corporate intranets to the Internet can lead to a more productive workforce, yet at the same time it has its own set of obstacles and challenges. In the same way, schools are scrambling to find ways to embrace access to the Internet to enhance their curriculum and discover new ways of delivering information to their students. When used responsibly, the Internet can provide a wealth of information and services previously unattainable to increase productivity and the sharing of information. Conversely, unmanaged and unrestricted Internet access by employees, students, or faculty can lead to dire consequences (Stewart, 2000).

A well-defined Internet acceptable use policy (IAUP) can mitigate many of the risks associated with exposure to the Internet. This paper will discuss the background and importance of an IAUP and its role. It will also take a look at some of the consequences and advantages of either being too strict or too liberal in the application of an IAUP as well as examine some of the components that define an IAUP.

Background

In 2005 Websense, Inc. released the results of their sixth annual Web@Work study. Some of those results are listed below:

- 52% of employees surveyed who use the Internet at work for personal reasons said they would rather give up their morning coffee, while 44% said they would give up their Internet access.
- 93% percent of all employees surveyed said they spend at least some time accessing the Internet at work.
- Among the employees surveyed who access the Internet at work, the average time spent accessing the Internet at work is 12.6 hours per week.
- 48% of the employees surveyed said they use the Internet at work purely for work-related tasks. 40% utilize the Internet for work-related duties and some personal tasks such as online banking. 10% of employees surveyed use the Internet at work for both business and pleasure in equal amounts.
- Whether it was by accident or on purpose, 23% of men who access the internet at work said they had visited a porn site while at work, while only 12% of women had done so.
- Listening to or watching streaming media (18%) and using instant messaging (16%) are still the most popular computer-based applications used at work at least once a week by those employees surveyed with internet access at work. (Websense, Inc., 2005)

These are just a few of the statistics of how the Internet is changing the face of business. The U.S. Treasury Department has also found that non-work-related computing, such as online shopping, checking personal finances, answering personal emails, and using chat rooms accounted for 51% of an employee's time online (Ugrin & Pearson, 2008). These non-work-related activities just don't decrease productivity; they also open the door to other problems such

as security concerns, legal issues and litigation, corporate or brand image being tarnished, illegal activity, violations of regulations, and liability for offensive content.

Social network sites like LinkedIn, Facebook, and MySpace have brought a new spin on IAUPs. These site are personal and private, however when they are not designated as private and all the information contained in them is exposed to the public, problems can arise. When you claim to be an employee of some company, your Internet presence acts like an ambassador for that organization. If you post flaming comments about your job, boss, or coworkers, you not only open yourself up to possible litigation, but your employer as well. IAUPs should include language addressing social networking sites and blogs (Adams, 2008).

Table 1 (Siau, Nah, & Teng, 2002) describes some of the different types of Internet abuses.

Table 1. Definitions of Different Types of Internet Abuses

Internet Abuses	Definitions
General Email Abuses	Include spamming, harassments, chain letters, solicitations, spoofing, propagations of viruses/worms, and defamatory statements.
Unauthorized Usage and Access	Sharing of passwords and access into networks without permission.
Copyright Infringement/ Plagiarism	Using illegal or pirated software that cost organizations millions of dollars because of copyright infringements. Copying of Web sites and copyrighted logos.
Newsgroup Postings	Posting of messages on various non work-related topics from sex to lawn care advice.
Transmission of Confidential Data	Using the Internet to display or transmit trade secrets
Pornography	Accessing sexually explicit sites from work place as well as the display, distribution, and surfing of these offensive sites.
Hacking	Hacking of Web sites, ranging from denial-of-service attacks to accessing organizational databases.
Nonwork-Related Download/Up load	Propagation of software that ties up office bandwidth. Programs such as Gnutella and Napster allow the transmission of movies, music, and graphical materials.
Leisure Use of the Internet	Loafing around the Internet, which includes shopping, sending e-cards and personal email, gambling online, chatting, game playing, auctioning, stock trading, and doing other personal activities.
Usage of External ISPs	Using an external ISP to connect to the Internet to avoid detection.

Moonlighting	Using office resources such as networks and computers to organize and conduct personal business {side jobs).

Role of IAUPs

The purpose of an IAUP is to outline specific requirements for rules that must be met. It defines rights, responsibilities, and privileges of users and administrators accessing information systems (Perks, Gavitt, & Olivo, 1997). In general, it should be legitimate, legal, and enforceable. Employers and employees can create a more productive work environment if they work together to jointly develop the IAUP to balance the interest of both parties (O'Daniel, 1999).

Where To Draw The Line

When crafting an Internet acceptable use policy, it may be difficult to pin down how strict or liberal the policy is. It is a fine line and there are consequences to moving too far one way or the other. For example, email is the communication medium of choice when it comes to networks. Privacy concerning that email is not clear-cut though. The messages are sent and received using corporate equipment. They are stored on company assets or servers for an indefinite amount of time. Does the employer have the right to access these communications? Unlike letters, faxes, and other communication means, system administrators are allowed to read emails. Most policies state that all communication will be monitored. In essence, this means that employees will have no right to privacy in their email.

When a policy is written in such a draconian way it may inhibit casual communications between employees and customers. This could then have an adverse effect of sales and support. Companies may want to allow personal email during company time. To facilitate this, though, they may want to encourage employees to have a separate personal account (O'Daniel, 1999).

The system administrator may then be able to scan any attachments before they are opened thereby protecting the network without having access to the text portion of the email.

Blocking specific websites through software and firewalls is another solution that could have the same effect. When you shut down all communication except that which is internal to the company, you could bring your company to its knees. There are a host of things that a company must do on outside sites that still relate to the business needs of the company. When deciding what sites to block, care must be taken to not infringe on the business needs of the company.

Kinds of Policies

Most policies today are a collection of rules with consequences attached for violations of those rules. Although in and of themselves they are not bad policies, they do not convey to the end-user the risks that the organization is exposed to should such a rule be transgressed. Ruighaver, Maynard, and Warren suggest that the traditional approach to acceptable use policies where they are prescriptive in nature, detailing which behaviors are allowed and which are not, may not be enough (2010). They suggest a policy based on ethical decision making instead.

Traditional acceptable use policies rely mainly on deterrence to be effective. Violate this policy and pay this consequence. While simply listing punishments for violators may have worked a decade ago, nowadays only works if the employees feel that the organization is serious about enforcing the policy and that they will actually follow through with the punishment (Ruighaver, Maynard, & Warren, 2010). Deterrence is undermined when there is a lack of accountability after an unacceptable behavior is identified.

(Ruighaver, Maynard, & Warren, 2010) suggest that clearly defining or identifying the risk posed to the organization resulting from employee behavior, the seriousness of the risk, as

well as the how the organization would like to control that risk, is a better approach. They state that by allowing the employees to make ethical decisions instead of conforming to a defined set of rules, it will foster a shared sense of responsibility and accountability. Although they are currently seeking an organization with which to research and implement such an approach to prove their theory, it seems to make logical sense.

Components of an IAUP

Establish

When drafting your policy, weigh the factors that apply to your corporate culture and balance them accordingly. The following objectives should be woven into your policy:

- The underlying purpose of Internet use and the policy itself is to foster a more productive work environment.
- The policy should sufficiently mitigate liabilities to the company and its employees while at the same time being practical.
- Employees must remain cognizant of security requirements and the protection of data, both the company's and the customer's.
- Training to prevent unlawful or inappropriate employee conduct is the company's responsibility.
- Employees must adhere to copyright protections and other laws.
- The policy should protect the company from litigation while respecting employee privacy.
- Supervision of employee usage must occur regularly.
- Internal and external auditing requirements must be addressed.

- Enforcement actions must be taken seriously, quickly, and consistently. (Zavoina, 1998).

The policy should also address limits on personal use of corporate accounts, disclosure or transmission of confidential materials, discussions of the employer and its business, prohibit access to or the display of illegal or objectionable material, prohibit the downloading of copyrighted materials, and prohibit communications online that would be illegal if communicated orally or in written form. It should affirm the employer's right to monitor email and online traffic and finally encourage the reporting of improper conduct (Zavoina, 1998).

Educate

Having a well written IAUP posted if a folder or hanging on a wall somewhere does not absolve the company of any liability. An IAUP cannot actually become useful until it has been communicated to its employees. Training must be conducted on the policy to ensure that it is understood and to explain to employees the risks as well as the rewards of using online services. Employees must fully understand that written Internet policy compliance is mandatory and that there will be consequences if ignored. Most company's already conduct training on various subjects like discrimination, sexual harassment, hostility, and other unacceptable behaviors. Not only should this be a stand-alone class, but the topic could be interwoven into the other classes as well. For example, sending a coworker sexual messages in an email is in violation of both the acceptable use policy and sexual harassment policy. The courts will have favor for a company that proactively educates its employees about Internet related risks in an organization (Sykes, 2005).

Monitor

Often the mere existence and promulgation of a clear policy is enough to stem most forms of Internet and network abuse (Stewart, 2000). At he very least it forms a foundation for communicating with employees whenever policy violations lead to the need for corrective action. However, like any other rule that is not enforced, IAUPs that are not backed up by proactive monitoring and access control measures will quickly turn into a paper tiger – all bark and no bite. It will lose its effectiveness in guiding users' behavior and protecting the organization from liability (Stewart, 2000).

Monitoring software is increasingly used to combat abuses. Siau, Nah, & Teng, (2002) cited a study stating that statistics have shown 58% of employers who monitor Internet usage do so to control recreational use; 47% do so to reduce bandwidth abuse; 47% do so to eliminate downloads of pirated software; and 33% monitor to reduce sluggish Internet connections due to nonwork-related use. The primary target for monitoring is email traffic. Companies go to great lengths to safeguard their intellectual property.

Next would be use of the Internet. Employers monitor where employees surf. Privacy groups have a problem with this. They feel it is alright to monitor excessive usage but feel that monitoring where the employee surf is a violation of their privacy. For example, employees would not like it if their employers knew that they were online looking for advice on drug and alcohol addiction (Siau, Nah, & Teng, 2002). Employees may also be worrying that their employers are collecting information about them that would later show up in their personnel record (Siau, Nah, & Teng, 2002). In response to this I would say that if you want something to remain private, do it in the privacy of your own home.

Again, finding that fine line between protection and big brother can be difficult. In order to create a harmonious relationship between employee and employer, there must be a certain

degree of control bonded together with adequate sensitivity training for both employees and employers (Siau, Nah, & Teng, 2002). For example, because employees are consistently working longer hours, would it be too much trouble if one logs on to their bank account to make sure their mortgage got paid in time or ordered their wife a dozen roses for their anniversary? The bottom line – employers should inform their employees in ways in which they are being monitored. Also, if there are any changes in policy, employees should also be notified of such changes.

Enforce

Companies should always back up their policies with decisive actions. However, it is imperative that the enforcement it applied equally and justly to all offenders. Employers should follow whatever disciplinary actions are spelled out in the policy. This means that employees who have violated the policy should be disciplined and the employer has to be consistent in carrying out such discipline (Siau, Nah, & Teng, 2002).

Proactive enforcement is enforcement that keeps employees from breaking the policy even when they deliberately try to. For example, network-filtering solutions can monitor network traffic and block access to inappropriate site such as gambling sites, pornography sites, and violent sites. They provide the organization mitigation of liability, security from threats, and saving in terms of resources and money (Sykes, 2005). They can also serve as a perimeter defense system that guards the network from outside malicious attacks. They can block bandwidth-robbing programs like P2P (peer to peer) file sharing, instant messaging, streaming audio and video, spyware, malware, and phishing scams.

Conclusion

Internet acceptable use policies are written documents that coalesce two aspects of a business that provide the avenue for safe and productive Internet access; education and training, and a positive organizational culture. By educating employees about the proper use of network assets and Internet security on a regular basis, employees will be aware of changes to policy and the emergence of new security threats. The better informed they are, the safer the organization will be. A positive organizational culture will result in employees enjoying their work more and being more productive. However, a negative culture will result in just the opposite. Employees will use the Internet in harmful ways in order to retaliate against their perceived mistreatment. If employers can balance the line between protection and an Internet free-for-all in an acceptable use policy, they will have a more productive workforce and a better-protected network.

The Internet has many resources to get you started. The SANS Institute, www.sans.org, is a great place to start. They specialize in computer security training, network research, and resources (SANS: Information security policy templates). They have example policies and templates to fit your organization.

Bibliography

Acceptable use policies for Internet use. (n.d.). Retrieved 07 01, 2011, from Media Awareness Network: http://www.media-awareness.ca/english/resources/special_initiatives/wa_resources/wa_teachers/backgrounders/acceptable_use.cfm

Adams, H. R. (2008). Dusting off the acceptable use policy. *School Library Media Activities Monthly , 25* (4), 56.

Fabiano, K. (2011). Social media @ the workplace: What's your policy? *CustomRetailer , 10* (4), 8.

Merritt, T. (2003, April 1). *Creating and inforcing an Internet acceptable use policy*. Retrieved 05 13, 2011, from Novell.com: http://support.novell.com/techcenter/articles/ana20030402.html

O'Daniel, M. (1999, October 16). Internet acceptable use policies. *Malaysian Business* , 25.

Perks, D. J., Gavitt, D. R., & Olivo, J. J. (1997). Do you have an Internet acceptable use policy? *Computer & Education , 29* (4), 147-151.

Ruighaver, A. B., Maynard, S. B., & Warren, M. (2010). Ethical decision making: Improving the quality of acceptable use policies. *Computers and Security , 29*, 731-736.

SANS: Information security policy templates. (n.d.). Retrieved May 20, 2011, from SANS: http://www.sans.org/security-resources/policies/

Scott, M. D. (1997). Liability in cyberspace - III: Creating a corporate internet acceptable use policy. *Computer Law & Security Report , 13* (6), 451-453.

Siau, K., Nah, F., & Teng, L. (2002). *Acceptable Internet use policy , 45* (1), 75-79.

Stewart, F. (2000). Internet acceptable use policies: Navigating the management, legal, and technical issues. *Information Systems Security , 9* (3), 1-7.

Sykes, C. (2005, November 28). *The importance of Internet acceptable use policies for large businesses.* Retrieved 06 04, 2011, from www.infosecwriter.com: http://www.infosecwriters.com/text_resources/pdf/IAUP_Sykes.pdf

Ugrin, J., & Pearson, J. (2008). Exploring Internet abuse in the workplace: How can we maximize deterrence efforts? *Review of Business , 28* (2), 29.

Websense, Inc. (2005, May 5). *Surfing the web at work may be as addictive as a cup of joe.* Retrieved July 10, 2011, from Websense: Essential information protection: http://investor.websense.com/releasedetail.cfm?ReleaseID=285219

Zavoina, A. (1998, July/August). Crafting an Internet acceptable use policy. *ABA Bank Compliance* , 29-31.