The Importance of Internet Acceptable Use Policies for Large Businesses

By: Christopher B. Sykes

November 28, 2005
Abstract

Today, large businesses are facing the ever increasing threat of inappropriate Internet usage among company employees. This poses a great risk to organizations in many ways. Most notably, productivity loss, workplace law suits, bandwidth consumption, and breaches of confidential company data are some of the major issues large businesses deal with on an ongoing basis. In order to tackle this problem, Internet acceptable use policies are put in place to protect the employer and the employee. By establishing, educating, and enforcing these policies, employees will become more aware of the dangers involved with inappropriate Internet usage. Internet acceptable use policies will differ for each business, but they must cover all aspects of security for that particular organization in order to be effective. This paper will outline the problems within organizations that need to be addressed as well as how to write a policy that will deter Internet misuse.
The Importance of Internet Acceptable Use Policies for Large Businesses

An Internet acceptable use policy (IAUP) addresses employee behavior in terms of Internet usage and security. The purpose of an Internet acceptable use policy is to direct staff in the use of Internet services so that appropriate behavior is maintained throughout the organization. IAUPs are crucial for all organizations in order to maximize the benefits the Internet has to offer. Basically, an IAUP is a written document between the employer and employee that identifies the dos and don’ts of Internet usage within the workplace. The Internet can serve many useful purposes to an organization, so preserving the bandwidth and maintaining security is essential for productivity (Lichtenstein & Swatman, 1997).

Within large businesses, an Internet acceptable use policy involves everyone. It is the executive committee’s responsibility that a thorough policy is formed and communicated within the company. Next, network administrators or similar positions should ensure that the policy is actively monitored and is up-to-date. Lastly, end users should follow the policy and offer suggestions for improvement (www.About.com). It is important that Internet policies be written in the interest of the organization’s culture. The Internet policy will discourage inappropriate behavior amongst employees. However the organization culture will ultimately have the strongest affect on behavior (Kleiner & Welebir, 2005).

The Internet has given way to many uses within the workplace. Benefits such as increased revenues, lowered costs, improved customer service, and high tech communications have given employees an advantage in the business world. Conversely, some managers believe the Internet has resulted in a significant reduction in productivity.
This productivity loss is a direct result in the misuse of the Internet. Misuse simply means employees are using the Internet for personal use on company time. This is why IAUPs are needed in order to help maintain the control of employee productivity and the business itself (Kleiner & Welebir, 2005). There have been several surveys conducted that support this.

A company called Websense, Inc., the world’s leading provider of employee Internet management solutions, announced the survey results from the 6th annual Web@Work study in May 2005. This survey interviewed 354 IT managers from companies that have at least 100 employees. Also interviewed, were 500 employees from varies U.S. companies who work with at least 100 employees. These people were interviewed on Internet and software application usage in their workplace. Several of the results are as follows:

- 52% of employees stated they would rather give up their morning coffee than their personal use of the Internet at work while 44% would rather give up the Internet for coffee.
- Internet usage at work has increased to 93% of all respondents claiming they spend at least a little amount of time on the Internet; this is up from 86% the previous year in 2004.
- 50% of employees surveyed use the Internet at work for personal use and actual work use. Of the 50% that use the Internet for personal use, the most popular sites visited are news websites at 81%, personal e-mail such as Hotmail at 61%, online banking sites at 58%, travel sites at 56%, and shopping sites at 52%.
• The average time employees spent on non work related websites is 5.9 hours per week which is similar to 2004 results.

• According to this survey, men access more pornography related websites than do women. 23% of men who access the Internet at work admitted that they visited a pornography site while on company time compared to 12% for women. 17% of men who visited these pornography sites said that it was intentional with the women at 11% (Culter, 2005).

These are just a few of the results these surveys produced. However, one can see how the personal use of the Internet has increased since 2004 thus resulting in greater losses of productivity for U.S. businesses. The Wall Street Journal stated that, “The Internet is remaking business, but it’s also the greatest way to waste time that the human race has ever invented” (SurfControl). This statement supports the survey results listed above without question.

Another reason it is pertinent for large companies to implement IAUPs is to protect themselves from lawsuits. Without an IAUP, employees that surf the Internet on a daily basis and view websites such as sexually explicit, violent, hate and crime websites are subject to lawsuits, as well as the business. For example, if an employee is sending inappropriate content via instant messenger, the company will be at fault if the case is taken to court. This could possibly mean disaster for a business. So, implementing IAUPs can protect employees as well as the company from any legal action (Flynn & Hackett, 2005).

In addition, if inappropriate content is viewed on company time without an IAUP in place, it will most likely result in legal action and court. In court, electronic records
such as e-mail and Internet history can be subpoenaed and used for prosecution. Hence, it is not surprising that 68% of businesses in the U.S. state that legal liability is their number one Internet concern (Flynn & Hackett, 2005).

Three key areas company employees should be aware of concerning Internet resources and the legal issues involved are sexual harassment, copyright infringement, and misrepresentation. Sexual harassment can result from bringing offending material into the workplace. An example of such inappropriate material is pornography. If pornography is downloaded onto a computer from the Internet and a coworker sees it, the company could be liable. There are many ways to block such material from employees such as implementing an Internet web content filtering device into your network as you will read later (SurfControl).

Next, copyright infringement is another problem that large businesses should be aware of. Copyright infringement should always be monitored because it can happen unintentionally and the company can still be held liable. Example materials that can lead to copyright infringement are: downloaded pictures, certain documents, and software (SurfControl).

Lastly, like copyright infringement, misrepresentation can also happen without employees knowing they did anything wrong. It is very important for employees to communicate to their contacts that what they are stating is their views and opinions, not the company for which they work for. The reason for this is because some employees have the authority to represent the company which can lead to disaster if misrepresentation takes place. This is especially true when using e-mail (SurfControl).
Bandwidth consumption is another reason IAUPs are essential for large businesses. Bandwidth consumption can adversely affect the way a company and its network operates on a day to day basis. If employees take part in downloading/uploading large non-business related files in the workplace, the effects will be felt throughout the organization. When employees take part in casual Internet surfing and bandwidth consuming activities such as streaming audio and video, MP3 downloads, and image downloads, network performance will be dramatically degraded (Surf Control). This waste of bandwidth can make it more difficult for employees to perform their normal duties thus interfering with business Internet traffic. A properly written and implemented IAUP can drastically improve an organization’s bandwidth and free network resources for essential work related activities (Flynn & Hackett, 2005).

The network security of an organization is one of the most crucial aspects for companies. Without an IAUP, Internet and network security can be severely compromised. There are many risks associated with an organization’s Internet security. First, some of the most notable risks are using the Internet for non-business related activities. Some examples of this are surfing the Internet on company time, Internet relay chatting, downloading games and images, personal use of e-mail, peer to peer (P2P) applications, newsgroups, FTP and instant messaging (IM) programs. Other areas of major concern are hacking from within the organization by gaining unauthorized access and Internet transferred threats (Lichtenstein, 1997). It is highly important for employees to read and understand IAUPs in order to become familiar with online activities that are considered risky. This is essential because most employees understand there are risks associated with the Internet, but they do not know which ones. IAUPs will define all
activities that are prohibited within the organization. The IAUP should also state the implications for breaching such prohibited activities. These implications include verbal warnings, suspension of Internet privileges, and employment termination. Enforcing these policies in such a manner will reveal to employees how serious and concerned the organization is about Internet security risks (Welebir & Kleiner, 2005).

In order to effectively battle accidental and intentional Internet risks as mentioned thus far, St. Bernard Software and the E-Policy Institute recommends putting best practices to work with the three Es of electronic risk management. St. Bernard Software is a global leader in providing security solutions to businesses. The E-Policy Institute is an organization that specializes in speaking, training, and consulting as it relates to workplace e-mail, Internet, IM, and policies (Flynn, 2005).

79% of U.S. employers use e-mail policies and only 20% of those employers have written rules to govern usage (St. Bernard Software and e-Policy Institute)
The three Es are establish, educate, and enforce. First, the organizations above recommend establishing comprehensive, clearly written Internet, P2P, email and IM rules, policies, and procedures for all employees. These policies should be written so that employees can fully understand all content that is presented. Employees should also have easy access to these policies whether it be printed, shared on a networked directory or posted on the company Intranet. IAUPs should also be written to avoid any misinterpretation. Clear, concise words and grammar should be used throughout the policy. Lastly, Internet policies are to be updated annually in order to stay current with emerging risks and new technology that will continue to threaten Internet activities in the workplace (Flynn, 2005).

Next, educating employees is crucial to the organization’s security. Written rules and policies should always be supported with employee training throughout the organization. Employees must fully understand that written Internet policy compliance is mandatory and that there will be consequences if ignored. With proper employee training, a company’s culture will be free of discrimination, harassment, hostility, and other unacceptable behavior. In addition, the courts will favor a company that proactively educates employees about Internet related risks within an organization. This is good for employers, especially if the company is taken to court over a dispute.

Lastly, rules and policies must be enforced in order to remain effective in an organization. Employees need to be aware of disciplinary action if the IAUP is not followed. These actions are necessary in order to prove to other employees that breaking Internet policies is serious business. Other ways of enforcing an IAUP is to install a security appliance on your network such as an iPrism from St. Bernard,
An iPrism filtering solution installed on an organization’s network can filter and block access to inappropriate Internet content such as gambling sites, pornography sites, and violent sites. An Internet filtering solution such as the iPrism can give an organization mitigation of liability, security from threats, and savings in terms of resources and money. iPrism is a perimeter defense system that guards against Internet attacks. These network devices are beginning to gain popularity especially for large businesses with many employees and an IAUP to enforce. The iPrism will also enable a company to report on their IAUP as well. This will show management weak and strong areas in a company in terms of Internet content viewed within the organization. Also, the iPrism is easy to install, maintain, and requires no additional software or hardware to operate. The iPrism has a very low cost of ownership. It will also back an organization’s IAUP to effectively keep employees safe from inappropriate Internet content. In addition, the iPrism will also block against some of the worst threats known such as P2P, IM, spyware, malware, and phishing scams. In conclusion, iPrisms will significantly reduce a company’s liability, minimize security breaches, increase productivity, preserve IT resources such as bandwidth, and grow with new threats as they surface (Flynn, 2005).

For large businesses to properly write an Internet acceptable use policy, the policy must always address all issues of security within the company. Some of the first items that should be covered within an IAUP are certain sources of risk that includes web browsing, JAVA, file transfers, FTP, e-mail, and newsgroups. The IAUP should briefly explain each of these and the risks associated. In addition, disciplinary consequences should be mentioned as well. Minor consequences will be given as warnings and major consequences will result in suspension of Internet use or possible employee termination.
Another important issue that should be mentioned in an IAUP is file encryption. If file transmission of confidential company information is required, the IAUP should state specifically which data must be encrypted before being sent over the Internet (Welebir & Kleiner, 2005).

Next, another section that should be included within an IAUP for large businesses is monitoring and filtering. Discussing this within the policy is absolutely necessary. Employees should always be aware of what and how often activities in the workplace are monitored. The section of the policy should disclose if Internet usage and even deleted data will be recorded (Welebir & Kleiner, 2005).

Internet content to be filtered within a company should also be disclosed within an IAUP. The IAUP should describe the type of filtering software being used and which material will be filtered out. The IAUP should specifically list the types of inappropriate web content to be filtered, such as adult and illegal material. Also, employees should be aware of inappropriate material that may slide through the filter and end up being viewed by the user. If this happens, employees should be trained on how to handle such content (Welebir & Kleiner, 2005).

Also included in the IAUP should be privacy rights and their explanations. Basically, employees should not expect their use of the Internet to be private at the workplace. The IAUP should make it known that employees do not have privacy rights of any kind while on the job. Along with this, the IAUP should also state that the company has full rights to the employee’s local hard drive or any other media that may contain personal or company information (Welebir & Kleiner, 2005).
The next section of the IAUP for large businesses is intellectual property. The policy should state that all data stored on company computers and servers is the property of the organization which also includes downloaded content. Next, this section of the policy should state that downloading inappropriate content such as pornography or pirated software is against company policy. In addition, employees should be fully aware of how important it is to handle intellectual property correctly. Intellectual property is very confidential and sensitive data that does not need to leak out of the organization. If so, major problems could result for the company (Welebir & Kleiner, 2005).

Another very important section of the IAUP is organizational representation. Only certain employees should have the authority to represent the company. The policy should list the employees of the company that can represent the company. The policy should also state that employees can communicate with clients and customers over the Internet via methods such as e-mail, chat rooms, and newsgroups. The authorized personnel listed in the policy should be aware of how important it is to maintain a professional image that will reflect upon the organization (Welebir & Kleiner, 2005).

The next key element of an IAUP is acceptable personal use. Some organizations will allow personal usage of the Internet during working hours such as during lunch breaks. If so, the policy should specifically state which Internet websites may or may not be visited. Some companies will allow Internet use during regular business activities. If this is the case, the policy should state how much use is appropriate. Employees also need to be reminded in this section of the policy that Internet filtering is in place through the use of an Internet monitoring and filtering appliance which does not keep any content viewed by the employee private (Welebir & Kleiner, 2005).
Next, the policy should include a section labeled investigation of violations and corrective action. This section generally states how the investigation will take place if an infraction has occurred as well as the consequences for that infraction. Most policies for large businesses include certain consequences whether the employee is a first, second, or third time violator. The company management team should leave this section somewhat open as a result of the wide range of violations that can take place within the organization. In this section, one of the most important things to state is that employees can be terminated depending upon how severe the violation is. This statement will protect the company from disgruntled employees (Welebir & Kleiner, 2005).

Last but not least is a section on notification and distribution of policy. This section will come last in the policy and require a signature from the employee which states that they agree to the company Internet policy. Once signed, the policy should also be made available to the employee. Most policies are posted on break room bulletin boards, on company intranets, or near time clocks. In summary, it is absolutely necessary for all employees that access the Internet in the workplace be fully aware of the appropriate and inappropriate content that can be viewed. The sections included in this paper are just some of the major areas a company can use in their Internet policy. Some organizations may like to use a more general policy that is easier for employees to understand. However, some may want to use a more detailed and specific policy so employees have no room for question. It is entirely up to the company as to how they would like to structure their Internet acceptable usage policy (Welebir & Kleiner, 2005).
Network and computer security is paramount in an organization in order to keep the company, employees, and data safe. Below, are ten tips that all company’s should implement and include in their IAUPs. According to Michael Overly, the top ten tips for better computer security within an organization are as follows:

1. Develop and implement a written security policy that applies to all aspects of employee computer use, including e-mail and Internet access.

2. Conduct regular employee training sessions to keep employees updated on company security practices,

4. Configure employee computers so that only one user ID is used per machine.

5. Always shred or burn confidential, sensitive business information.

6. Use encryption to protect sensitive files and messages.

7. Keep network records updated and promptly delete users who are no longer employed.

8. Configure the network to require users to change their passwords on a regular basis.

9. Regulate and control employee use of the Internet such as monitoring and blocking software to prevent employees from accessing inappropriate sites.

10. Install and frequently update virus protection software. (Overly, 1999, p. 80)

New technology is also beginning to pose a threat to large organizations. Devices such as iPod media players, hard drives and memory sticks, digital cameras and recorders, and CD and DVD recording are beginning to pose serious threats to large businesses. USB and firewire ports on company PCs are alternative routes in which viruses can filter through a company network. With just the click of a mouse, files can be copied to and from these devices which could severely compromise a business computer system. These devices are also mass storage capable, meaning some can hold upwards of 80 to 100 gigabytes of potential confidential data. New technology such as this presents
a risk to the company by making the network susceptible to data theft or the implanting of malicious code (Thelander, 2005).

Basically, these devices need to be banned from large business environments. There is a two tiered approach to containing this ever increasing problem. First, organizations will need an acceptable use policy that includes policies for business and personal devices. Secondly, to help combat the problem, a solution such as a network based management tool that can monitor and enforce the policies should be put in place for such harmful devices (Thelander, 2005). Below are some sample rules that can be placed into a company’s acceptable use policy for such devices:

- Prohibit the use of portable data storage media and devices except with specific permission
- Prohibit the use of a computer’s USB ports without specific permission
- Prohibit the connection of MP3 and video recorders and players to PCs
- Restrict connection of personal PDAs to company owned PCs
- Prohibit the connection of personal mobile phones and cameras to PCs
- Limit the capacity of data storage devices issued by the organization
- Limit data copying to key staff or departments (Thelander, 2005, p. 27)

It is highly important for large businesses to ensure that all employees are familiar with the content of their Internet acceptable use policies. This is not an easy task and will take time and patience to accomplish. One of the most notable ways of ensuring that employees are familiar with company policies is to introduce them at employee orientation programs. The orientation program should include discussion of correct and incorrect computer usage, consequences for misuse, moral appeals, and methods of
enforcement. Also, the orientation program will ensure that employees understand organizational Internet policies from the beginning (Foltz, Cronan, & Jones, 2005).

In conclusion, there are two key ways large businesses can practice and teach proper Internet security throughout their organization. First, is to educate all employees on a regular basis. Through continuing education, employees will always be constantly aware of changes to policies and new security threats. The more employees know, the safer the organization will be. Next, organizational culture plays an important role in the way employees use the Internet in workplace. A positive organizational culture will result in employees enjoying their work and being productive rather than wasting time using the Internet inappropriately. However, a negative culture will cause an employee to deliberately use the Internet in harmful ways in order to retaliate against their perceived mistreatment. If companies concentrate on these two areas, employees and employers will become more knowledgeable about the dangers the Internet can pose (Welebir & Kleiner, 2005).
References


