A White Paper From Burstek Serious Internet Security Software

Creating an Enterprise Level Acceptable Use Policy for the Internet

BURSTEK
The World's Choice for Internet Security.

9220 Bonita Beach Road, Bonita Springs, Florida 34135 www.burstek.com 239.495.5900

Creating an Acceptable Use Policy for the Internet

Table of Contents

Creating an Acceptable Use Policy for the Internet

Overview

There has been a rapid increase, in the past few years, of organizations providing employees with access to the Internet. Most companies have embraced Email, Internet connectivity and FTP as boons to overall productivity and as specific tools of efficient communication within and outside the organization. Internet access has become a critical factor in the success of most companies and organizations around the world. Everyday, more and more employers are granting Internet access to employees, enabling them to take advantage of the wealth of readily available information and improving internal and external operational efficiency.

Consequently, many organizations have discovered that unrestricted and unmanaged employee Internet access can result in consequences to the enterprise. Increases in wasted time, lost productivity, misappropriation of resources, loss of sensitive company information and network failures are common problems reported. Most of these problems occur from malicious code and increased bandwidth consumption. More importantly, an organization's failure to take the appropriate steps of defining, managing and controlling Internet usage by employees can pose additional and very serious risks in the form of legal and financial liabilities.

As organizations rush to address these Internet access risks, management typically has involved everyone from top executives to IT to HR and the legal department, resulting in disparate and fractured policies as an attempt to manage Internet usage. There is no doubt that every enterprise needs a comprehensive and implemental Acceptable Use Policy (AUP). The critical issue has become how to effectively formulate an enterprise wide policy that can address all of the risks inherent in Internet access without limiting an organization's ability to leverage the Web as a business asset.

In many cases, AUP shortcomings occur because management fails to understand the full extent of the risk, while in other instances there is reluctance to come across as "big-brother" for fear of harming company morale. Sometimes AUP efforts fail to adequately address the legal issues involved and other times the policies are simply ignored because they are too full of "legalese" to be understood by rank and-file managers and employees. Or, even with extremely well intentioned and well-crafted AUPs, the failure to deploy appropriate technologies for comprehensive monitoring and restricting can dilute the policy's enforceability or, on the other end of the scale, can severely restrict Internet usability to the point of compromising its overall benefits.

The bottom line is that an effective AUP must take into account the whole spectrum of policy and technology issues, within the framework of the specific organization's unique set of goals and culture. When it comes to potential employee abuse of their Internet access, the most prominent concerns are loss of productivity, degradation of available computing resources and the high risks of legal liabilities — for example, those associated with sexual or other types of harassment based upon access and display of inappropriate web content. In this article, we will take a closer look at the benefits and risks of employee Internet access and explore the specific issues involved in the developing, deploying and enforcing of Internet AUP.

Productivity Drain

The dollar amount associated with loss of productivity from non-work related Internet use is staggering. According to a 2001corporate Internet surfing report, unauthorized Internet surfing accounted for a $5.3 billion dollar loss in productivity. Michael Erbschloe, vice president of research at Computer Economics explains, "Online shopping, stock trading, car buying, looking for a new house, and even visiting porn sites have become daily practices for about 25 percent of the workers in U.S. companies that have access to the Internet in their offices. The illegitimate and personal use of the Web by employees has become commonplace. And when the boss is not around, improper use of the Web is normal. Inappropriate activities can even include employees starting their own e-business operations and building and promoting their own Web sites while in the office of their full-time employer."

Most organizations that provide Internet access for their employees expect and accept that there will be a small amount of personal use by the employee, just as a reasonable amount of using the company phone system to make personal calls is expected. Unfortunately, the Internet poses a much greater potential for abuse than does the telephone. An employee may start with a quick check of the daily news and sports, activities that seem acceptable and innocuous enough. What happens when that same employee begins to bet on sporting events and expands to continual tracking of current betting lines, account balances and other activities associated with gambling? That valuable Web access has now turned into a serious liability as this particular employee not only wastes more company time on his gambling, but exposes the network to undue risk from malicious content.

There aren't many among us who haven't occasionally experienced how easy it is to get sidetracked on the Internet, even when going to a specific Web page with a specific objective. The combination of hyperlinks, enticing graphics and good old human curiosity can lead even the most inexperienced users to explore areas they had not even considered before. There has been significant research recently about the phenomenon of Web surfing and the conclusion is that the overwhelming amount of content available on the Internet is exactly the reason that surfing can become a compulsive behavior for a percentage of Internet users. For anyone who has spent a few hours following the maze of links from a particular Web site, it's easy to see how even a valuable and trusted employee can get caught up in compulsive surfing. However, it is imperative that companies establish specific policies addressing such behavior and have tools in place for monitoring and enforcing said policies. The dangers of unrestricted surfing have grown exponentially in the past few years as more Web criminals begin to capitalize on typical human behavioral responses.

Without a policy in place, what begins as a small amount of Internet abuse by a handful of users can quickly turn into a "climate" of misuse. The attitude of "everyone's doing it" becomes the norm and even those who normally act fastidiously and in the best interest of the organization may come to think there is no harm in unchecked Web surfing. Climbing on the net constantly during the work day to check and send email, pay bills and purchase airline tickets becomes part of the normal workday with no correlation made by the user between excessive Internet use and low productivity. If this sort of attitude becomes pervasive throughout the organization, there is certain to be a measurable drop in overall productivity as a result of too much time being spent online for non-business purposes.

Loss of Resources and Bandwidth

Another major concern that can surface as a result of certain employees abusing their Internet connection and privileges is clogged bandwidth and network slowdowns. These consequences cause a ripple effect throughout the enterprise, affecting the computing abilities of all employees and taxing the functionality of an organization's finite Internet resources. Bandwidth consuming content such as streaming audio and video create a constant drain on the network, potentially blocking access to mission- critical data. This content seems harmless enough on the surface, but when multiplied times a few employees, a serious bandwidth consumption problem arises. Unfortunately, without proper tools to monitor where and how much bandwidth is being used, the impact on company performance can be insidious and difficult to detect.

For today's businesses, the Internet has become a valuable and indispensable part of their operation. The informational access and communication abilities it delivers to employees are used by all departments from financial to HR. The Web has also become a major source for business opportunity, as more buyers look to the Internet as at least the starting point for researching purchasing options. More and more companies now turn to search engine optimization, pay-per-click, banner ads and other means of Internet advertising to promote their Web presence in order to take advantage of this buying phenomenon. In addition, many companies now depend on the Internet for response driven communication and e-commerce transactions with their customer base. When network performance is degraded, companies are often forced to respond with major new investments in system improvements and expanded bandwidth, even though they may be unaware that a significant part of the demand is coming from inappropriate Internet usage by employees.

The amount of inappropriate use of company bandwidth by employees is greatly determined by the ability of Internet users to install .exe files on their workstation and the ability to set up "push" applications that allow remote web sites to update or "push" data to their computers automatically. Most streaming media requires a separate player to run the files and the media players typically require regular updates to be installed on the individual computers. Media files are typically very large and therefore tie up large amounts of bandwidth in streaming mode. The users may not even be aware of the amount of bandwidth being siphoned off for these types of applications and are therefore unaware of how great the impact to expensive company Internet resources.

Legal Liabilities

Beyond the aforementioned concerns about bandwidth and productivity losses, most organizations have now come to realize the enormous potential costs posed by the legal risks inherent in unauthorized Internet usage. The first risk that comes to mind for most is the legal liability of exposure to inappropriate or sexually-explicit Internet content at the workplace. The courts have repeatedly stated that it is the employer's responsibility to protect workers from this kind of work environment and that companies must take prudent steps to insure a safe workplace.
As described by Frank C. Morris, Jr., director of the Employment Law Department at Epstein, Becker & Green in Washington D.C., "since the number of discrimination lawsuits have been on the rise, the workplace has become more politically correct. Rarely will employees engage in the same offensive conduct that was commonplace just a few years ago. As a result, potential plaintiffs have had to look elsewhere for 'smoking guns' to prove their cases, and many are now finding them with the increased presence of the Internet in the workplace."

Morris further explains, "Few employees would believe that their seemingly innocent Web-surfing could expose their employers to insurmountable liability. But it is this improper use of the Internet that is now the smoking "e-gun" of current plaintiffs. For a plaintiff, there is nothing better than walking into court with a piece of paper illustrating a discriminatory statement, joke or picture downloaded off the Internet and sent through e-mail."

Fortunately, today's management style eliminates the posting of sexually suggestive pictures and jokes in conspicuous places around the workplace as was common only a few years ago. Unfortunately, many employees today fail to see the similarity between the posting of offensive materials on walls and bulletin boards and posting it on a computer screen. The courts, however, have consistently ruled that the presence of sexual or offensive material from the Internet at the workplace is sexual harassment and can be dealt with as prescribed by law. Employee rights dictate that an employer take preventative measures to provide a workplace safe from exposure to offensive materials.

There are other legal liability concerns besides just keeping the workplace free from offensive material. Legal liability can be accrued by an employer when an employee uses company Internet resources to violate copyright laws or disseminate misinformation that slanders other companies or people. Although Internet case law is still being formulated and tested in the courts, there seems to be a movement by the courts towards holding an organization liable for certain illegal activities committed by the employee using company Internet resources. Criminal activities such as Internet scams, Phishing and spamming are in the realm of actions the court deems potentially libelous to an employer if company Internet resources were used.

In addition to the legal liabilities, a company can also sustain real and lasting damage to its reputation and as a result of the negative publicity that surrounds employee misuse of the Internet. The company may appear to be badly managed for allowing such practices or, it can actually lose business from customers that are worried about lack of adequate controls and security.

Developing an Effective Internet Acceptable Use Policy

Developing a policy that effectively controls Internet usage within an organization requires an in-depth look into corporate structure, organizational goals, particular Web usage objectives and the overall culture within that organization. In all but the smallest of businesses, there needs to be significant input from all departments involved, such as HR, IT, executive, financial and department managers.

According to Ira G. Rosenstein, a New York-based partner in the Employment Department of Orrick, Herrington & Sutcliffe, "The Internet is a valuable tool and therefore it is very important to craft the usage policy in such a way that it reinforces productivity and employee morale, without becoming unmanageable. For example, if a policy inflexibly mandates very draconian measures for the slightest infraction, it greatly reduces management's ability to apply a measured or proportionate response to different types or levels of Internet abuses. With any policy covering areas that could be deemed the 'personal' activities of employees, it makes sense to build in some degree of discretion. However, in order to ensure that the policy is sufficiently enforceable, employers need to clearly define what does and does not constitute acceptable behaviors with regard to Internet usage."

Rosenstein adds, "in some instances, a 'zero-tolerance' stance may be necessary, such as if an employee knowingly and repeatedly accesses pornographic or hate-inciting Web sites. Obviously, these offenses are very different than going to an e-commerce site and buying the latest NY Times bestselling novel, especially as it relates to the liability risks of litigation from other impacted employees. The ability to distinguish between 'casual' and 'chronic' behavior is also a useful concept to build into the policy. For instance, even relatively innocuous behavior can rise to the level of a serious offense if it becomes chronic, such as the difference between an employee quickly checking out an item on eBay or spending half a day bidding and tracking various auction items."

Without a doubt, the most important factor in the formulation of an effective Acceptable Use Policy for the Internet is to avoid a "one size fits all" mentality, both across an industry and within a specific organization. To maximize effectiveness, the policy needs to incorporate the particular organization's goals and culture and be very clear in conveying the underlying reason that is driving the policy formulation. The policy needs to take into account the differences within each organization of how, why and when each business unit accesses and uses the Internet, and maintain the flexibility so necessary in today's dynamic business environment.

Communication and Implementation

Once a policy has been designed and developed it will need to be effectively communicated to both existing and future employees. This communication needs to be in a standardized, documental format. Most companies have a written policy document that new employees are required to read and sign. This document also serves as official notification for existing employees. For many companies, especially those with a more open form of management, including a short orientation to the new policy will prove helpful in conveying those important issues that drove the policy formulation.

Ira Rosenstein agrees; "Essentially the company needs to inform every employee of the policy's provisions as soon as they are given access to the Internet and then also to reinforce the employee's obligations on a regular basis. For example, some companies set up a short summary of the policy as a 'splash screen' that appears for a brief period during boot-up and whenever an employee signs on to the Internet."

All organizations that implement an Acceptable Use Policy need to design and deliver a policy that can integrate smoothly with their existing management culture and philosophy. If the flow of the policy accurately mirrors the flow of the management style, understanding of and compliance with the policy within the organization is greatly enhanced. However, a policy that contains an excessive amount of legal jargon can be misunderstood and ultimately will be unenforceable, leaving the organization with an impotent policy. The actual terms and phrasing of the document need to be understandable by the diverse groups that exist within the framework of most organizations and need to mesh with the company's current management style. Although their goals may be very similar, a traditional law firm will use language that may differ greatly from that used by a leading edge software developer. Here again, it is important to keep in mind that the ultimate objective of the AUP is not so much to catch people doing something wrong as it is to proactively prevent abuse through a well-crafted and well-communicated policy.

Utilizing Technology for Monitoring and Enforcement

In some instances, the formulation and dissemination of a clear cut Acceptable Use Policy is enough to stop most forms of Internet abuse within an organization. At the very least, it provides a firm basis for communicating with employees whenever policy violations lead to the need for corrective action. But, like any rule that is not enforced, an AUP for the Internet that is not backed up by proactive monitoring and control measures will quickly lose its effectiveness and become "toothless." Without the ability to see precisely when and where Internet users are going and prevent access to potentially libelous and inappropriate content, an organization has no power to guide user behavior and to minimize risk to the organization itself. Consequently, the most effective strategy, and the one used by most organizations, is a dual strategy of formulating clear AUPs combined with instituting comprehensive, precise Internet access control over Internet activities.

Recently, the need to proactively manage and control web access has driven the development of a variety of web filtering technologies. The exponential growth of Internet content along with the growing need for more transparent network installation, easy to use administration for large numbers of users and smaller footprint applications has given rise to a new breed of sophisticated, server based applications that use continually updated databases to categorize Web content. These robust applications give administrators the ability to control access with different levels of access granted to different departments or business units.

Combining these type of robust Web filtering tools with an Internet use reporting application gives an organization the control they need in order to enforce their AUP and keep their networks secure. Being aware of the potential risks inherent with Internet connectivity is only part of the solution. There must be an accurate ability to track specific Internet use with easy-to-read reports. The technology used to monitor where users go on the Internet needs the functionality to report on activity at different levels of the organization. Management needs reporting that will show, not only use and risk level by departments and business units, but can also drill down to identify individual users who pose the most risk with their surfing habits.

Regardless of the blocking approach, a filtering solution must be flexible. Not only does an AUP need to adapt to a company's culture and specific needs, but so do the tools used to enforce that policy. IT administrators need the ability to custom tailor and control their filtering rules and databases. Local control of how site categories and specific sites are rated and handled is very important. The ability to tailor blocking on a group-by-group or individual user basis is needed. And being able to control access based upon time of day or day of week is becoming increasingly important. Flexibility is also needed in the range of Internet services controlled. As the variety and type of Internet content have proliferated, the issue of access control has now expanded way beyond just HTML-based web pages. Unauthorized access to other Internet services, such as IRC chat, FTP downloads and streaming media, can easily consume significant bandwidth and resources while degrading employee productivity, all without triggering mechanisms in less functional filtering applications.

In order to be truly effective, Internet access management technology must be accurate, dynamic, automatic, tailorable and comprehensive. But it also must be transparent to the installed network hardware and software, easy to set up and maintain, non-performance degrading and scalable enough to grow with the corporate IT environment. By combining subscription-based filtering with the easy installation and administration of "plug-and-protect" server based reporting, these new alternatives provide highly customizable filtering mechanisms and user profiles, sophisticated monitoring and filtering of all Internet content types, plus a high degree of scalability and maintainability.

Bottom Line

With the ever-increasing risks of legal liability, loss of productivity and bandwidth drains, it is evident why organizations today need a comprehensive Acceptable Use Policy for the Internet. It is important, however, that the AUP be specifically tailored to meet the needs of each organization. Policies that don't reflect the management style and culture of the organization they are designed for, run the risk of providing inadequate protection or possibly an employee backlash against a harsh, overly restrictive policy. Once formulation of an AUP is completed, effective communication of the policy to employees is critical. Employees must be clearly notified of policy requirements, in a language understood by all, in order to comply with the policy. Tools are then needed to help ensure compliance by all employees. Without the tools or means to monitor and enforce the policy, an AUP will lack the potency needed to provide the protection desired. Like the usage policies themselves, a company's monitoring and control mechanisms must also be tailorable to meet the specific requirements of the organization and include the capability for evolving and adapting with changing requirements.

Ultimately, the organization's Internet Acceptable Use Policies, management/supervision practices, employee training/education programs, and the Internet access management technologies all have to mesh together to form a unified and proactive system for effectively managing all employees' online behavior.

In the end, the organization's Acceptable Use Policy, employee notification and education, management practices and Internet management tools all need to work together cohesively to optimize Internet security.

For more information on Acceptable Use Policy in schools, visit http://www.education-world.com/ or http://205.146.39.13/linktuts/inteaup.htm

For more information on Acceptable Use Policy in corporations, visit: http://compnetworking.about.com/library/glossary/bldef-aup.htm

For information on AUP and technology, call us at 239-495-5900 or 800-709-2551 or visit our Web site: www.burstek.com

About Burstek

As an industry leader in the development and deployment of Enterprise Internet Management solutions, Burstek has been on the forefront of Internet security since 1997. Burstek's core products, bt-WebFilter and bt-LogAnalyzer have won numerous awards and accolades and are the first Internet content filtering and reporting applications developed specifically for Microsoft server technology. By combining leading edge software solutions with the most competent technical support in the industry, Burstek has built a loyal customer base of education, industrial, financial, legal, government, and military organizations across the globe, including many Fortune 100 companies.