SOPHOS

Effective web policies:

Ensuring staff productivity and legal compliance

Employees increasingly expect to use the internet at work for their own personal use in return for longer hours, taking work home with them and interrupting vacations. This has a number of security, productivity, bandwidth and legal ramifications that require organizations to create and implement a web usage policy that is backed up by effective web filtering tools. This paper discusses how to create a policy that balances an organization's need for protection against an individual's expectations.

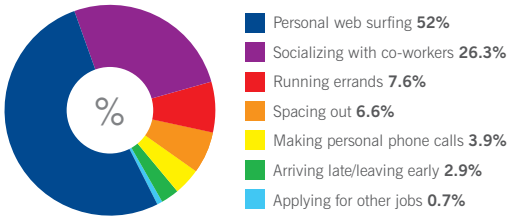
A Sophos white paper

April 2008

Effective web policies:
Ensuring staff productivity and legal compliance

Regulating internet access in the workplace is a delicate balancing act. The web provides employees with valuable information and tools that enhance productivity and competitive advantage, but it can also devastate business productivity with its endless supply of games, downloads, webmail, community sites and online retailers.

The evidence of web abuse is dramatic. Over half of respondents to an America Online and Salary.com survey cited web surfing as their biggest work distraction (Figure 1). While another survey revealed inside abuse of web access as the most prevalent security problem (Figure 2).



Source: America Online and Salary.com[1].

Figure 1: What is your biggest distraction at work?

The risks

Wasted time and productivity are two obvious risks of web abuse, but they are not the only hazards.

Lawsuits

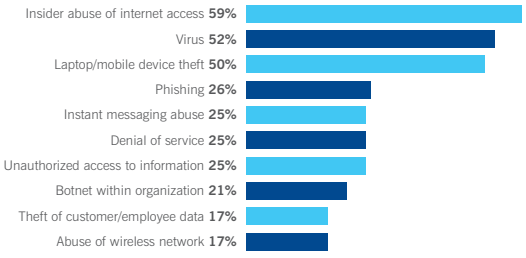
Employees surfing pornography sites at work can create the perception of sexual harassment and a hostile work environment. In some cases pornography has led to organizations being prosecuted, while the legal implications of viewing child pornography are even more serious. Other legal risks can come from:

- Downloading pirated content and using social networking sites
- Using web-based email or blogs to reveal sensitive personal or company information or to damage another employee's reputation.

Resource abuse

Overuse of video feeds, music downloads, gaming, and other high-bandwidth applications can affect organizations in two ways:

- Network performance is significantly slower
- Desktop and server hard disk space is filled, resulting in unnecessary technology expenditure.



Source: Computer Security Institute[2].

Figure 2: Top ten types of attack or misuse

Malware

As companies have become more effective at blocking email-borne viruses, hackers have increasingly turned to websites as a vehicle for infecting users with malware that steals confidential information or which builds botnets (networks of hijacked computers used to distribute spyware and viruses). In early 2008 it was estimated that webpages were becoming infected at the rate of 6000 per day, or one every 14 seconds[3].

Complex challenges

Internet access at work is both a blessing and a curse, and creating a web usage policy is not straightforward. Employees expect to use the web for personal use, while employers need to enforce some browsing constraints to prevent abuse and ensure productivity. Simply publishing a blanket policy for the entire organization based on generic definitions and lists of banned sites is likely to run into resistance from a disgruntled work staff. Why?

> *Employees expect some personal flexibility at the office in exchange for the expectation that they work longer hours.*

Defining abuse

Many organizations find the line between appropriate and inappropriate web use difficult to define. What is acceptable business use for one employee may be completely unacceptable for another. For example, marketing departments have had great success in harnessing social networking sites such as Facebook and MySpace to monitor markets and build relationships with current and potential customers. Several companies, including IBM and Circuit City, have even established a presence on virtual environments such as Second Life. A blanket ban of such sites could, therefore, be counterproductive to wider business interests, as could granting blanket access to them.

Work/personal life overlap

As work becomes increasingly mobile, the separation between work and personal life is less rigid. Employees expect some personal flexibility at the office in exchange for the expectation that they work longer hours, take work home and stay in touch during weekends and vacations. Indeed, many companies use such flexibility as a hiring incentive. Excessive regulation of personal internet use can become a recruitment barrier, breed low morale, both of which can lead to reduced competitiveness.

Building a workable policy

Technology awareness varies greatly in most organizations, as does understanding the business impact of internet abuse. Most employees know instinctively that watching YouTube during working hours wastes time, but many will not understand its true security, productivity, bandwidth and legal implications.

Communication

The first step in creating an effective web usage policy is educating employees about the effects web abuse can have on an organization. Communication should include HR and senior management in addition to IT. It should also be two way, with staff and business units encouraged to identify applications or websites that assist them achieve their goals.

Match policy to philosophy

A web usage policy should match an organization's overall goals and philosophy. Organizations that provide employees with leeway in how they do their jobs will be better served by a policy that sets expectations and outcomes, emphasizing their spirit and the reasons behind them. On the other hand, organizations that operate a top-down management structure that defines tasks granularly will benefit from clear rules and regulations.

Many organizations lie somewhere in between, while some vary according to management level or business unit, and a policy needs to mirror these differences.

Keep it simple

Regardless of the organizational philosophy, the policy should be written in a concise and easy to follow fashion. Language should be simple and the concepts relevant to each different department. It can also be useful to lay out a series of broad principles before concentrating on the finer details.

Enforcing the policy

Even organizations with an informal culture will need to enforce their web usage policy, which they can do through web filtering controls. Monitoring systems should employ screen alerts that inform employees if they are accessing a prohibited website or undertaking an unauthorized

An effective web usage policy should...

- Contain a general definition and listing of appropriate internet uses, such as work-related communication, educational and professional development.
- Contain a general definition of inappropriate internet uses that violate company, local, state, and Federal laws, any contracts the company has signed, and that interferes with the productivity and internet use of other users.
- Permit personal browsing of acceptable websites during personal hours and define a certain level of acceptable use outside these hours, on condition that it doesn't affect a user's productivity.
- List inappropriate websites where access is prohibited (unless used for legitimate business reasons), such as those that contain or promote pornography, violence and criminal activity.
- Prohibit access to websites and services offering illegal downloads. Even legal downloads from sites such as iTunes can infringe copyright if they are downloaded or copied to company networks.
- Offer guidelines on the use of blogs, social networking, webmail and other Web 2.0 applications. Access can be prohibited or restricted to personal hours, and harassment clearly outlawed.
- Prohibit participation in any peer-to-peer networks without prior approval by management.
- Specify how users can access bandwidth-hungry content, such as streaming audio and video and large file downloads. Employees could be encouraged to bring their own audio players to work.
- Allow a select group of individuals, such as IT staff, senior management and developers to download applications and large file types, when relevant to their job responsibilities.
- Restrict or prohibit access to websites known as proxies or translators. These sites are designed to bypass web filters by allowing access from within other websites.
- Allow transactions only with legitimate, authenticated websites and organizations that encrypt data. This reduces the risk of data leakage and prevents employees from accessing blocked sites through legitimate ones.

activity, while management software should allow temporary exceptions to be established. Auditing and reporting tools will be needed to deal with any incidents, with enforcement following a tiered approach: verbal warning, monitoring, retraining, written warning, dismissal, potential legal action. However, a well formulated policy will usually eliminate any temptation to violate it.

Regular reviews

Organizations will need to review and adapt their web usage policy at regular intervals to ensure that it is not impinging on legitimate internet use and is effectively supporting business goals. Some users may find that they need to access temporarily a prohibited site, and the policy needs to be flexible enough to allow that.

Policies should be able to be modified by category, website, time of day, user or group. Such exceptions should automatically dissolve after a pre-defined period of time, ensuring that temporary privileges remain temporary and avoid the need for manual cleanup, which can be time-consuming and error-prone.

These periodic reviews allow organizations to react to the evolving nature of the web. Uses that are unacceptable today may become acceptable tomorrow, and web usage policies need to reflect this to ensure that they do not stop employees working effectively.

Summary

Implementing a web usage policy is a balance between protecting the organization and avoiding measures that alienate employees or stop them performing legitimate business tasks. A policy should not just concentrate on monitoring and punishment, but should educate users and actively involve them in its evolution. This will minimize the need to take drastic measures and allow organizations to address the continuous change in internet technologies and services.

Sophos solution

The Sophos Web Appliance, part of Web Security and Control, enables fine-grained control of all web traffic to ensure that it is safe and appropriate to organizational policy. It protects against spyware, adware, viruses, malicious code, unwanted applications and undesirable content. It features an innovative, full-spectrum scanning engine that detects all threats through a unique combination of reputation-based filtering, real-time predictive threat filtering, and content-based filtering. Its easy to use management console and powerful reporting tools deliver rapid insight into web traffic, threats and user behavior, enabling secure browsing without the complexity of traditional web filters. As a managed appliance, the Sophos Web Appliance features remote “heartbeat” monitoring and on-demand remote assistance, ensuring it delivers the most dependable web security in the industry.

Sources

1 www.salary.com/careers/layouthtmls/crel_display_nocat_Ser374_Par555.html

2 www.gocsi.com

3 www.sophos.com/pressoffice/news/articles/2008/01/security-report.html

About Sophos

Sophos enables enterprises worldwide to secure and control their IT infrastructure. Our network access control, endpoint, web and email solutions simplify security to provide integrated defenses against malware, spyware, intrusions, unwanted applications, spam, policy abuse, data leakage and compliance drift. With over 20 years of experience, we protect over 100 million users in nearly 150 countries with our reliably engineered security solutions and services. Recognized for our high level of customer satisfaction, we have an enviable history of industry awards, reviews and certifications. Sophos is headquartered in Boston, MA and Oxford, UK.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

SOPHOS
WWW.SOPHOS.COM