Comvigo, Inc.

White paper

Employee Internet Access: Hidden Costs and Potential Risks

Abstract

Do you have a strategy for coping with the risks and costs that are created by employee internet access?

Internet access is a necessity for professional workers in today's business environment. Research, communication, and networking are all key activities in most businesses, and the internet is a lynchpin for these functions.

However, ungoverned internet access is an enormous time waster and a prolific source of risks to your business. According to a number of studies, employees spend from one to three hours a day surfing the web, depending on which survey you read. Your network and your data are at risk with internet-borne viruses and malware that can cripple your network and your users. And the widespread popularity of social networking provides an enormous and unregulated opportunity for your business to be exposed to risks to its reputation and to provide leaks of confidential internal information.

You may have system administration policies in effect that provide some measure of protection from the worst of viruses, malware, and employee internet abuse. But the problem facing any progressive business is that there is often great business value inherent in providing controlled access to online facilities, such as social networking sites, that may constitute large risks when abused.

This paper will give you an understanding of the risk profiles of the most common internet facilities, such as IM, social networking sites, and P2P networks. We will then show you how Comvigo, Inc. provides a simple, unified, and flexible approach to dealing with these challenges.

Web Surfing Risks and Costs: The Big Picture

Here we explore some of the costs and risks of unfettered employee internet access.

Payroll Costs

The "2008 Wasting Time at Work Survey" conducted by by Salary.com indicated that 73% of survey participants admit to wasting time on the job, and personal internet use topped the list at 48% of those participants. This includes online shopping, virtual "red light districts" (porn), online dating, watching online videos, online games, and online gambling.

Time and consequent payroll waste is a huge direct expense that you pay in exchange for allowing employees to use the internet with no restrictions.

Legal Risks

Your employees can get themselves, and your business, into expensive and potentially disastrous legal difficulties with reckless web usage. Examples of such risks include:

- Surfing and downloading pornography - creating an impression of a hostile work environment or violating statutes against certain materials such as child pornography
- Downloading of "warez", or pirated software - creating a liability for your business
- Use of blogs or social networking sites to damage the reputations of individuals or businesses or to leak sensitive internal information

Business Operation and Continuity Costs and Risks

Your business itself is at risk with some types of web usage. Here are some examples:

- Crashed and security-compromised PCs and networks due to downloads of viruses, spyware and malware
- Financial exposure through "phishing", the use of clever social engineering that induces even experienced professionals (like your employees) to enter sensitive account and password data into rogue web sites that are constructed to look like a reputable financial institution's web presence.
- Saturation of your network capacity with downloads of music and other content

The implication of the foregoing points is clear: control of employee web access is fast becoming a primary responsibility of the modern business.

"Social Notworking" Problems

Web sites that allow individuals to communicate as groups and as individuals and to locate and socialize with other like-minded individuals are part of the "social networking" phenomenon.

Examples of the most popular social networking sites that generally do not provide positive value to an employer's business are:

- **Twitter** (real time tracking and chat)
- **Facebook** (social)
- **LinkedIn** (professional relationships)
- **MySpace** (social)
- **PlentyOfFish** (dating)

Security Issues

Twitter is a web site that encourages users to "follow" their friend's activities by posting continual updates of a user's location. A high-profile employee who uses Twitter to document their movements may create a personal security challenge, particularly if they travel overseas. Outsiders may infer confidential company business from Twitter postings.

Facebook presents a unique challenge because users tend to publish full "resume like" information about themselves filled with personal data. Security vendor Sophos has found that 41% of Facebook users will reveal personal information such as their birthday or email address to complete strangers on the Internet. A user that publishes a key piece of personal information such as a birthday or an alma mater's name, plus an email address, may provide a hacker with enough material to guess successfully at their account passwords.

LinkedIn has great value for recruiting professionals who search for and communicate with job candidates. It also has great value for sales people. But LinkedIn is also a primary channel for job searches. Do you want your employees looking for a new job on your clock?

MySpace and similar sites such as **Fubar**, as well as dating sites, generally revolve around the non-professional "play time" interests of their users. Unless your business's activities relate to the study of social networking users in some way, the majority of such sites are "social notworking" sites and are major time wasters.

Lastly, the very culture of most social networking sites is problematic. Blogging is strongly encouraged, so users may write about their employer's internal projects, competitors, and plans. This is true especially at the more professionally flavored sites such as LinkedIn and Facebook.

A comprehensive approach to web access, as mentioned above, will provide a workplace solution to these issues.

Instant Messaging Risks

Instant Messaging (IM) software provides an easy way for confidential information to leave a business undetected and for security threats to enter the business. The lack of a unified logging and archiving facility with most IM clients compounds these problems because you literally have no idea what your users have written or discussed.

Unauthorized Instant Messaging creates "under the radar" vulnerability to companies in which it is taking place. According to a study conducted by Nemertes Research, up to 74% of all corporate IM use was started by employees without the permission of corporate IT. In addition to exposure to the same types of risks such as malware and waste of employee time that are presented by web access, unsanctioned IM use also exposes the business to litigation and regulatory risks due to the lack of a consistent framework for logging messages and for administering user accounts.

IM use can also become, as is the case with social networking sites, a subtle source of wasted employee time. Some employees will leave Instant Messaging clients running at all times, and permit themselves to be "interrupted" by the program whenever a friend wishes to chat. Sometimes there is a business justification for allowing this for some job roles, but generally, IM clients can distract workers.

Instant Messaging is usually done using dedicated software clients such as AIM (AOL Instant Messenger), or comparable products that are provided by Google, Microsoft and Yahoo.

IM use may be necessary to some, or all, of your employees in the conduct of their business. Control of IM usage within the business is key, so that you know who is using instant messaging, and you have records of all significant IM interactions that may affect your business.

P2P and Content Downloading Risks

Peer - to - peer networking, or P2P, is the sharing and exchange of content such as videos, music files, and other materials, via informal networks such as **Bittorrent** and **LimeWire**. As with Instant Messaging, P2P requires a dedicated software program that is easy to find, download and install by a user with no IT department sanction.

The content that travels via P2P networks is usually illegal, or it infringes on some party's rights. It usually consists of "warez" or copied software that may contain viruses, and content such as music or movies that have been duplicated without authorization.

To illustrate the problem, consider this. Retired General Wesley Clark characterized P2P use as a "new national security risk." He stated in a Government Reform Committee hearing "We found more than 200 classified government documents in a few hours search over P2P networks."

In addition, what users do with copyrighted content such as videos can also be done to your business's assets. A P2P user usually creates a "share" on their computer, which is essentially a back door from your network to the entire world. Anything on your network then may become available to the entire world for downloading.

P2P content is invariably large, since users are sharing multimedia that is hundreds of megabytes in size. Therefore, P2P becomes a large drain on your internet connection and on your internal network.

In general, there is little to no business case for permitting P2P on company owned computers and networks. In fact, there are huge potential liabilities in doing so. Your goal, as a responsible business owner, should be to control P2P usage strictly in your business.

Recommendations and Conclusion

Comvigo recommends and provides **IM Lock Enterprise** to support every business that has to deal with the issues that are described in this white paper.

IM Lock Enterprise is a proven, simple, unified solution. It allows your system administrator to block or allow the use of common internet-based distractions such as P2P, streaming media, and Skype, and to control the use of web sites with extensive whitelisting and blacklisting capabilities.

IM Lock is a Windows application that you install to every user PC that requires control of resources. Attractive multiple seat discounts are available.

IM Lock is extremely cost-effective, especially when compared to the risks and dangers of "going bare" with no unified solution for your Internet related risk exposure.

Please visit **http://www.comvigo.com** for more information.