



The Modern Approach to Employees' Internet Usage

Introduction

In the past 20 years, the world has seen amazing technological achievements, which have changed the way companies conduct their business forever. Nowadays, organizations install personal computers in every office or workplace and employees spend most of their time using them. Naturally, the management of these companies has become increasingly concerned with the productive use of computers and Internet.

According to an IDC study, **30 to 40% of Internet usage in the workplace is not work-related**. 37% of employees say they constantly surf the Web when they are at work, while **75% of all Internet porn traffic is done during the nine-to-five workday**. (Vault.com, SexTracker).

Contents

| | |
|--|---|
| Introduction..... | 1 |
| Internet influence on the workplace..... | 2 |
| Employee email use..... | 2 |
| Employee internet use..... | 4 |
| Prevention on growing threats on company productivity..... | 5 |
| The leading edge..... | 6 |
| Conclusions..... | 7 |



Internet influence on the workplace

After conducting a survey on 10,000 employees, the conclusion was that **the average worker wastes about 2.09 hours of the workday**, not counting lunch. The primary time-wasting activity of over 44% of respondents was personal Internet use (activities like instant messaging, e-mails, Internet polls, chat rooms, etc., were cited). (Salary.com)

The positive thing is that some of these activities might prove beneficial to the company. On occasion, discussions can bring inspiration and new ideas that can improve employees' work results. These breaks can also have a significant impact on employees' creativity, helping them to perform better on their tasks or projects. "Today, there are so many useful tools and Web sites on the Internet that have enabled people to become more efficient with accomplishing multiple tasks in a shorter amount of time", said Samara Jaffe, director of careers at AOL Find a Job.




In fact, the real surprise came when a follow-up survey, conducted on HR managers, showed that **employers expect workers to waste about one hour per day**. Employers have already built this expectation into the salary structure. Unfortunately, the **real amount of wasted time is about double what managers expect**.

According to the same survey, another interesting statistic is that, the younger the employee is, the more time he or she is wasting. Apparently, those who are 56 years or older, spend as much as 30 minutes per day on personal activities, while those 25 and younger waste about 2 hours daily.

Employee email use

Internet brings along a tremendous communication potential. In the recent years, telephones and faxes have almost become obsolete, as they have mostly been replaced by e-mail. According to a Pew Internet study, **52% of employees rate email as essential to their work** and an additional 34% rate it as moderately important.

E-mail usage at the workplace encourages communication:

-  72% of work emailers say email helps them communicate with more people.
-  62% of these users say email makes them more available to co-workers; however, about a third of all work emailers say email has made them too accessible to others.
-  59% of email users at the workplace say email improves teamwork.

However, **only about 50% of the employees consider the use of work email for personal purposes to be an ethical violation**. Even though, for most employees, inappropriate email habits carry few consequences, for others, misuse of email brings on disaster. In the summer of 2002, emails stood as solid evidence in the trial of Arthur Andersen for his accounting practices at Enron, and the SEC - US Securities and Exchange Commission - started prosecuting six major Wall Street firms for deleting emails before the 3-year statute of limitations. Hewlett Packard suspended 150 employees for sharing inappropriate content via email.

In several cases, authorities used email messages as evidence in court against big companies like Microsoft or Merrill Lynch, and against individuals, such as in Martha Stewart's case – and the list goes on.



Employees start being careful with the content of their emails, as about 10% of work emailers say they have accidentally sent an embarrassing email to the wrong person at work.

An interesting fact is that age influences the way employees use Internet. For example, those under 30 admit to handling more personal email at work:

- 59% percent of those under 30 said that part of the emails they received was personal, while
- only 50% of workers over 30, admitted the same behavior.

Regarding the emails sent:

- 37% of those under 30 admit to sending personal messages from work, while
- only 20% of those over 30 admit the same thing.

Younger work emailers are more easy-going about email standards than the older ones. They seem to be more liberal in the messages they send around at the office.

- Nearly double the number of younger workers use their work email to send gossip (24% vs. 13%), or discuss personal issues (40% vs. 22%).
- More employees under 30 send jokes or chain letters (43% vs. 38%).
- Probably because of this, many more of them (53% vs 42%) say email provides moments of relief during the working day. (www.pewinternet.org)

Another issue companies should be concerned about is their employees **breaking copyright laws**. There are many situations when employees take such actions, not even knowing they are illegal, such as: downloading the latest Coldplay album, sending it to a friend, or copying a newspaper article and sending it to another colleague or roommate. If any of this type of content is found on company's computers, the company is likely to be severely penalized, or worse. Furthermore, authorities can seize the entire computer system if office computers were tools in the commission of a crime.

Firms must keep their email system productive and protect its integrity. Companies' management must implement and enforce an email usage policy and effectively communicate this policy to employees. They, on the other hand, need to understand that **their employer owns everything they send through email**, from jokes to official papers.



Employee internet use

Productivity loss is one of the biggest concerns that come with Internet access at the workplace. Employees seem to be a prime target for spyware, since, according to recent polls, **two-thirds of the IT managers name spyware as the top threat to their network security.**

Also, employees can download and install a growing variety of applications, such as those for instant messaging, peer-to-peer file sharing or IP telephony, without approval. All these applications pose risks to companies' computer systems and some of them are actively malicious. Such programs often evade network defense systems using techniques like port agility (jumping around among open ports) or encryption. Most users do not realize some applications hijacked their computers, as malware can be downloaded via a seemingly harmless website, without their explicit consent. All of the threats described above are active distractions from the tasks the employee is supposed to do. In addition, all of them lead to major losses in productivity.

According to an IDC study, **one third of all the time spent online is not work related.** Apparently, 80% of companies reported that employees had abused Internet privileges, such as downloading pornography or pirated software. **75% of companies named employees as a likely source of hacking attacks.**

According to another study, conducted by Websense, nearly 80% of employees send instant messages over public IM services such as AOL, MSN and Yahoo, exposing companies to security risks. There are **more than 43 million IM users at work**, but only one quarter of the companies has a clearly defined policy on employee use of IM at the workplace.

Other relevant data of the same study state that:



45% of the executable files downloaded through peer-to-peer applications contain malicious code.



73% of all movie searches on file-sharing networks were for pornography.

As a result, a company can be liable for up to \$150,000 for pirated work if it allows employees to use the corporate network to download copyrighted material. Although 99% of companies use antivirus software, viruses and worms affect 82% of them. These activities slow down, or completely crash companies' computers, producing a major productivity and profit gap.

If employees log on to Internet chat rooms, social networks or leave e-mail messages with their company ID, authorities can attribute statements made by these employees to the company. This can lead to claims of defamation, discrimination and unfair competition if someone happens to see and print out a hard copy of the improper statements. Similarly, employees who shop via Internet or subscribe to services online may create liability for the employer when they do not pay their bills.



Prevention of growing threats on company productivity






The first step organizations have to take in fighting against the growing threats of Internet misuse is to establish an **Acceptable Use Policy (AUP)** - a set of rules that restrict the way the network or a website may be used. Corporations write AUP documents in order to reduce the potential legal action that a user may take.

Acceptable use policies are an integrated part of the information security policies framework. Usually, new members of an organization have to sign an AUP before they gain access to the information systems. This is why the **AUP must be concise and clear** in covering the most important points about what the users are, or aren't allowed to do with the company's IT systems. In addition, it should define what sanctions will be applied if a user breaks the AUP.

A **very efficient method** to enforce the AUP and manage employee Internet use is a **web filtering solution**. This type of software determines what content will be available on a particular machine or network, in order to prevent employees from viewing content which the company or the authorities may consider inappropriate. A very important fact to take into account is that, when imposed without informing the user, content control means censorship.

The most common approach to this issue is to completely block certain websites that contain pornography or gambling, and gaming websites. 96% of employers who block web access are concerned about employees visiting adult sites with sexual content.

According to the 2007 Electronic Monitoring & Surveillance Survey from American Management Association and The ePolicy Institute, Companies also use URL blocks to stop users from visiting:

-  game websites (61%),
-  social networking websites (50%),
-  entertainment websites (27%),
-  sports websites (21%) and
-  external blogs (18%), according to the 2007 Electronic Monitoring & Surveillance Survey from American Management Association and The ePolicy Institute

However, the **keyword for the modern approach of Internet filtering solutions has to be flexibility**. A growing number of managers realize that some employees might need more latitude than others. A good example is the HR department, which might use Facebook or LinkedIn for recruiting purposes. On the other hand, the Finance department might not have a work-related use for this kind of websites.

In addition, when blocking entire sites, or URLs, organizations have to be aware, that some over-zealous Internet filtering solutions will block various categories of websites, despite the fact that they have no prohibited content. An example is filtering all websites containing the word "breast", on the assumption that this word can only be used in a sexual context. As a result, a large number of websites, like the ones that discuss breast cancer, women's clothing, and even chicken recipes, are blocked. There have also been a number of attempts to block the word "sex". This led to blocking words such as "Essex" and



"Sussex". Another filter blocked the search of the word "swallow".

A fact that URL filtering does not take into consideration is that the Internet is constantly growing, URLs change, owners sell domains, and the content associated with that URL can be radically changed. The fact that major search engines use caches poses serious issues to URL-based filtering solutions. Search engines provide the same content but users' access the cached websites through URLs that are different from the ones of actual websites.

There is an increasing number of websites that provide constantly updated content that does not fit into a certain category all the time. Blocking the whole website might be an excessive act, while keeping track of each submitted news item would be counterproductive, since that content would need constant reviewing and classification – costly both in terms of time and in human resources.

The leading edge

The new trend of content filtering solutions is **blocking access** to most work unrelated websites, **but keeping flexibility** by combining this technology with image altering solutions. The latest filtering solutions include different filtering methods like text, image, URL, MIME, and protocol-based filtering. These technologies allow the system to practically block bad content and allow organizations to monitor the activity on their network.

The new trend is to use Artificial Intelligence in Internet filtering solutions. This way, the filtering solution reviews pages that are not located in the local database within seconds and, for example, it instantly replaces or modifies pictures that contain skin color. Another innovative technology that is being used more and more extensively in this type of solutions is pattern recognition. This is the imposition of identity on input data, such as speech, images, or a stream of text, by the recognition and delineation of patterns it contains and their relationships. Stages in pattern recognition may involve measurement of the object to identify distinguishing attributes, extraction of features for the defining attributes, and comparison with previously known patterns to determine a match or a mismatch. Pattern recognition has extensive applications in astronomy, medicine, robotics, and remote sensing by satellites.

(www.britannica.com)

Bandwidth is another issue businesses confront with. Some web filtering solutions permit organizations to establish exactly how much bandwidth each computer should receive, according to every employee's needs, making Internet use more efficient.

In a landmark case in 2006, on the subject of inappropriate behavior in the workplace, UK's House of Lords has changed the law, making employers liable for workplace harassment, even if they were not negligent in any way. They decided that the Prevention from Harassment Act of 1997 should cover the behavior of employees at work, even if the employer has not caused or failed to prevent the offending behavior. Therefore, **employers are now vicariously liable for the acts of their employees.**

For example, if an employer were facing a claim that he/she is liable for an employee's harassment, the Prevention from Harassment Act of 1997 would not protect him/her. This kind of harassment uses pornographic images, leaving **image-altering software as the best solution available**, in order to technologically interdict the access and use of pornographic images.

This new law makes implementing an effective image filtering solution the only way to avoid legal liability. In a modern, digital workplace, these technologies have become necessary to ensure a healthy work environment, as well as to maintain productivity and avoid harassment or discrimination charges.



Conclusions

As shown above, there are many concerns and issues regarding employee Internet use. It is a proven fact that it speeds up the communication process and makes research activities more efficient, but Internet use also has its downfalls. It has become a well-known fact that employees also use it for personal purposes - online shopping, chatting with friends or downloading copyrighted material - during work hours, **diminishing productivity and creating liability** for the company they work for.

Fortunately, modern solutions allow efficient prevention to these problems. Usage of a **modern, flexible, web filtering solution**, allows employees just enough access in order to do their jobs, but not enough to make companies "vicariously liable" for their online actions. Text or image altering solutions, URL, MIME, and protocol-based filtering are leading edge technologies that can help businesses radically **decrease productivity loss**.