



Productivity, Internet Abuse, and How to Improve One by Eliminating the Other

ABSTRACT

The Web can be an incredible business tool—and a potential threat. The change that the Internet has and will continue to produce in the world marketplace—and in life in general—is certainly comparable to revolutionary innovations in the past, such as the introduction of automobiles or even the printing press.

This white paper, however, will not focus on Internet highlights, but on some of the considerable downsides—and how to eliminate them. Specifically, we will discuss the effect of Internet abuse on employee productivity, which is huge and not fully appreciated. We will then examine the best strategies and technologies to combat abuse so that organizations can enhance the Internet as a tool and remove its potential as a productivity curse.

INTRODUCTION

The Web can be an incredible business tool—and a potential threat. The change that the Internet has and will continue to produce in the world marketplace—and in life in general—is certainly comparable to revolutionary innovations in the past, such as the introduction of automobiles or even the printing press. According to Cisco Systems, traffic on the world’s networks will increase annually 46 percent from 2007 to 2012, nearly doubling every two years¹. One can hardly imagine a successful commercial or non-commercial enterprise operating without an effective website, which is often indispensable for marketing and communication and can be set up for virtually any transaction, from selling widgets to applying for college. The impact on research and education is equally impressive. This white paper, however, will not focus on Internet highlights, but on some of the considerable downsides—and how to eliminate them. Specifically, we will discuss the effect of Internet abuse on employee productivity, which is huge and not fully appreciated. We will then examine the best strategies and technologies to combat abuse so that organizations can enhance the Internet as a tool and remove its potential as a productivity curse .

WASTING TIME, WASTING MONEY

Most people (perhaps not the reader) waste time on the job, particularly if their work is difficult, stressful, boring, or unrewarding, or when their primary interests lie elsewhere. Even people who love their jobs sometimes find it necessary to focus on non-job-related activities, if only to attend to pressing family concerns and other commitments. In general, employers expect workers to fritter away some time on the job, and “enlightened” employers recognize that a reasonable amount of employee time devoted to personal interests can benefit morale. What is surprising, however, is how little employers know about how much time is wasted. According to the most recent research, HR professionals assume that employees will waste around 1 hour each day. However, employees admit to wasting around two hours a day. The current UK average salary is £28,000 or £14.55 per hour. Even if you don’t include the one hour that employers expect to be wasted, the difference between the and actual time wasted costs an organisation around £3,8000 per year. The UK economy employs an estimated 29.56 million so the total cost to the UK economy of unplanned wasted time is approximately £11.2 billion per year. That’s a lot of money.

HOW MUCH TIME IS WASTED ON THE INTERNET?

A lot.

There is no way to prove that employees waste more time now than before the Internet became ubiquitous, but it certainly stands to reason. Internet surfing is often irresistible, largely because it can be so fascinating and has traditionally been so easy to pull off. Managers notice when employees linger too long at the coffee machine. But originally people could sit in their offices or cubicles and surf the Internet in private; all they had to worry about were prying eyes, which they could usually outmaneuver by minimizing screens or clicking from web pages to open documents.

However, in a US survey conducted by AOL/Salary.com², the highest percentage – 47.7 percent – cited “surfing the Internet” as their chief source of distraction, in contrast with “socializing with co-workers,” which came in a distant second at 23.4 percent³. An International Data Corporation (IDC) survey indicates that 30 to 40 percent of on-the-job internet use is non-work-related⁴. Other studies report that 64 percent of employees use the Internet at work for personal interests; and 37 percent say they “surf the Web constantly” while on the job⁵. Sixty percent of online purchases occur during normal work hours, as does 70 percent of porn traffic⁶. Forty-five percent of employees make travel arrangements while online at work; 37 percent search for jobs; and 11 percent play internet games⁷. Social networking sites

¹ <http://gigaom.com/2008/06/16/big-growth-for-internet-to-continue-cisco-predicts>

² http://www.salary.com/careers/layouthtmls/crel_display_nocat_Ser374_Par555.html

³ Ibid

⁴ <http://www.snapshotspy.com/employee-computer-abuse-statistics.htm>

⁵ Ibid.

⁶ Ibid

are also becoming a particularly tenacious distraction.

A United Kingdom study reports that employee visits to social networking sites cost businesses as much as \$15.5 billion a year⁸. Ninety percent of employees regard the Internet as addictive⁹. The strength of the addiction is indicated by the trend among even honest and reliable employees to violate company Acceptable Use Policies (AUPs) by visiting anonymous proxy websites when internet access filters are inadequate. Anonymous proxies essentially allow users to evade company blocking and visit blacklisted URLs. This phenomenon emerged around 2002, when there were only a few sites offering anonymizing services. Now there are over 100,000 registered anonymous proxy sites, an estimated 300,000 home-based anonymous proxies¹⁰, and given the open source nature of the software, more and more are cropping up every day.

HOW MUCH DOES INTERNET ABUSE COST?

Once again, a lot—both in wages and in indirect, less obvious impacts on productivity.

Wage losses are fairly easy to calculate. Let's assume that the average personal income is £28,000 a year or £14.55 an hour for an 8-hour day¹¹. Let's also suppose that a company has 100 employees, and, conservatively, each wastes 1 hour a day on the Internet (not including lunch or breaks). That would cost the company £349,200 a year. If we double the time wasted to take account of overheaded costs, we get £698,400 a year. Readers can experiment with their own numbers by using the cost estimator on the Bloxx website at www.bloxx.com/costcalculator.php.

Some productivity costs are not as easily measured but are no less real:

- *Lost business opportunities*—Employees are not only hired to fill a job, but to return multiples of their salaries. These would include sales people, of course, but also marketing and public relations personnel and often managers, product developers, and even CEOs. Time wasted surfing the Internet is time not spent selling, marketing or developing a product.
- *Clogging the corporate arteries*—Even if support personnel are not required to produce revenue, they are expected to sustain day-to-day organizational functioning. These workers operate within interdependent systems, where the completion of some people's tasks is required for the completion of work performed by others. For example, if the person who delivers mail and files to corporate offices is delayed by Internet surfing, the people in those offices may be unable to proceed with their jobs. Hence, the company not only wastes wages to the non-productive delivery person, but also for the wasted time of those who depend on that person's work. To the extent that activities within an organization are integrated, the Internet abuse of one person can affect the productivity of all.
- *Productivity and network performance*—Many employees need a fast and reliable network to maximize their own job-related speed and reliability. If some employees are visiting YouTube or other social networking sites to stream or download bandwidth-consuming videos, share files, or swap bandwidth, network performance can be significantly diminished, and this will delay the work of others. According to a UK study, workplace visits to social networking sites consume up to 20 percent of corporate bandwidth¹². Of course, this activity also weakens network security, but that is a topic for another paper.
- *Malware and productivity*—Social networking, pornography, and even anonymous proxy sites can be surreptitious sources of malware and viruses. These can diminish network performance and spread throughout an organization to disrupt or crash computers. One customer, prior to installing the Bloxx web filtering appliance, opened a MySpace site for corporate marketing purposes, and on the day it was opened, a hacker installed hidden malware. When the employee

⁷ <http://www.bloxx.com/web-filtering-for-sme.php> (Vault.com)

⁸ "Are Proxy Anonymizers Putting Your Enterprise in Peril?" The Forsite Group, p.3, http://www.8e6.com/white_papers/enterprise

⁹ <http://www.snapshotspy.com/employee-computer-abuse-statistics.htm>

¹⁰ "The Quandary of Web Anonymizers," p.3, <http://www.aladdin.com/esafe/whitepapers.aspx>

¹¹ <http://www.statistics.gov.uk>

¹² "Are Proxy Anonymizers Putting Your Enterprise in Peril? The Forsite Group, p.4, http://www.8e6.com/white_papers/enterprise

visited the site, his computer caught the virus, and he was unable to use his computer all day. This not only wasted his time, but the time of IT staff that had to fix the problem. This type of problem is not uncommon: for instance, TechTarget reported that in 2007 the MySpace profiles of Alicia Keys and other recording artists were serving up malicious code¹³. The Web has replaced email as the primary entry point for malware and spyware¹⁴. Google researchers ran an analysis of 4.5 million URLs in 2007 and found that 450,000 (or 10 percent) engaged in downloads of malicious scripts; another 700,000 were suspect of harboring malware¹⁵.

- *Productivity and abuse-related turnover*— Twenty-percent of companies say that they have fired employees for misuse of the Internet, and 65 percent report taking disciplinary measures for those offences¹⁶. If a company wants to implement an effective anti-abuse program, it will need clearly articulated and well-publicized AUPs, as well as a determination and tools to enforce them. Enforcement can sometimes mean firing employees, especially if they have been previously warned, have broken the law on the Internet, or have spent time engaged in particularly offensive abuse such as visiting pornography or hate sites. The downside is that firing and hiring is extremely expensive and time-consuming. Human resources staff have to settle all of the bureaucratic details with the terminated employee; they have to attract and interview new applicants and arrange interviews with the relevant managers; they may have to test the applicants and arrange medical exams; and when they hire someone, they have to pay travel, moving and pre-employment administrative expenses. Moreover, it takes time to train new employees, and, depending on the complexity of the job, additional time for employees to meet the skill levels of their predecessors.
- *Productivity and legal liability*—If a company has to spend large sums on lawyers to defend against lawsuits caused by employees downloading copyrighted or proprietary material or otherwise breaking the law, it will waste considerable funds that could be devoted to product development, sales, marketing and other revenue-generating activities.
- *IT expenses*—Last, but certainly not least, an organization will have hire extra and/or raise the pay of IT personnel to monitor and prevent Internet abuse, clean-up malware, and maximize network performance. Once again, this requires money that could be better spent on productive endeavors.

WHAT CAN ORGANIZATIONS DO?

Plenty.

First, organizations should articulate unambiguous AUPs that include an explicit ban on anonymous proxies, ask employees to sign a policy form, and enforce the policies. If the policies are not enforced continuously and consistently, people will return to their old behaviors. Second, organizations should invest in technology that will allow them to implement the rules. AUPs are entirely the provenance of management, but managers can rely on Bloxx's patented Tru-View Technology (TVT) to satisfy the second requirement.

Originally, organizations that have tried to limit Internet abuse relied on list-based filters to block access to unacceptable sites. Human classifiers examined the content of web pages and added them to a database blacklist, a white list, or a list of sites such as shopping, travel, sports, etc, that were blacklisted sometimes or for some people but not at other times or for other people. This strategy, however, became increasingly inadequate as the Internet grew exponentially each year, now over 8 billion +pages¹⁷. Humans just couldn't keep up. Vendors later supplemented the database approach with keyword scoring. Pornography sites, for example, use a common jargon that usually doesn't appear elsewhere. The filter scans a requested page for the frequency of keywords, and if the site scores above a preset level, the filter blocks it. But this enhancement is very hit-and-miss and sometimes blocks purely informational pages,

¹³ Ibid. P.3

¹⁴ <http://www.sophos.com/pressoffice/news/articles/2008/secret08q1.html>

¹⁵ <http://www.scmagazineus.com/Google-450000-websites-launching-drive-by-attacks/article/34986/>

¹⁶ <http://www.snapshotspy.com/employee-computer-abuse-statistics.htm>

¹⁷ <http://googleblog.blogspot.com/2008/07/we-knew-web-was-big.html>

such as cancer sites that frequently use the word “breast.” Moreover, keyword scoring is imprecise and problematic when it comes to subtle access decisions about inoffensive sites such as shopping, traveling, or sports, where the language is less uniform and overlaps with many other categories.

Bloxx offers a third-generation solution that combines, within a single appliance, URL databases and keyword scoring with Tru-View Technology, a far more intelligent identification and live contextual analysis that rapidly categories web traffic in real time. Tru-View has been taught to identify over fifty default categories with precision. It doesn't matter which of the categories a website's content belongs to—shopping, violence, travel, anonymous proxy—Tru-View controls the page with minimal effort from the IT staff. With respect to anonymous proxies, for example, the technology not only looks for common words and phrases, but for code structures characteristic of such sites, and analyzes the relationships between these elements. Tru-View also drills below home pages that display deceptively innocent content (e.g. cookery) to layers of sites containing pornography, proxy functionality, or other forbidden content. Tru-View provides extremely accurate, zero-day protection so that IT professionals need not waste excessive time examining its decisions. For more on Tru-View Technology, visit <http://www.bloxx.com>.

In short, while the Internet can be a marvelous productivity tool, it can also be a tremendous drain. Tru-View Technology maximizes the positives and eliminates the negatives so that organizations can meet the challenges of an 8+ billion-page Internet that is growing by almost 50 percent every year. The Web's expansion requires the kind of real-time, comprehensive, and discriminating Internet filtering that is only provided by Bloxx.

ABOUT BLOXX

Bloxx is a privately held company with offices in the U.S., U.K., The Netherlands, and Australia and offers web filtering appliance-based solutions for medium and large organizations in both the business and public sectors. In 2007, it was recognized by Deloitte as one of the U.K.'s Top 50 Fastest Growing Technology Companies in its prestigious "Fast 50." For more information please visit: www.bloxx.com.

ABOUT BLOXX TRU-VIEW TECHNOLOGY

Bloxx Tru-View Technology uses internationally patent pending technology to analyze and block web sites quicker and more accurately than other web filters, which use manual classification and keyword scoring. Tru-View Technology uses intelligent identification and analysis providing instant classification of web content as soon as it is accessed even if the content has not been seen by anyone before.

Bloxx Tru-View Technology helps organizations proactively manage users' access to web content which might lower productivity, expose the organization to risk and liability or pose a network security threat.

An estimated 1 million + users already benefit from enhanced security and performance with low administration and no cost per user charges. Additional protection is provided via anti-virus, anti-spyware and anti-phishing functionality, alongside onboard cache.

To learn more about Bloxx web filtering technology, book in for an online demonstration at bloxx.com/demo, call +44 (0)8700 4 25699 or email info@bloxx.com.



Deloitte. **Deloitte.**
Technology Fast50 Technology Fast50
EMEA 2008