

# Internet Grazing

Employees are roaming free on the Internet for their own personal use while at work, according to a recent survey of more than 10,000 employees by Burstek, a USA based Internet management consultancy.

Some of the findings of the study are fairly startling. For example, employees across all industries spend 20.42 percent of their Internet viewing time at work on personal business or personal entertainment activities.

Not surprisingly, 20.01 percent of all Internet access at work is for personal use, 22.39 percent of all Web pages accessed at work are for personal use, and 21.28 percent of all work bandwidth costs are attributed to personal use.

**Plainly, employers have good reason to be worried about personal Internet use in the workplace.**

Such personal use would appear to detract from time devoted to work-related tasks and can increase employer costs.

According to the study, 72.34 percent of all employee personal use of the Internet in the workplace has to do with "employee productivity draining Web sites," including the following types of sites in order of highest use: shopping, entertainment, personal e-mail, sports, chat rooms, job searches and game playing. This "employee productivity loss" group accounts for 93.99 percent of personal use bandwidth costs for employers.

As if this alone were not worthy enough for concern, the study goes on to document that 8.23 percent of the personal use of the Internet in the workplace involves visits to Web sites that pose potential legal liability for employers, such as pornographic and gambling sites and sites that contain hate speech and the like.

The study shows that the manufacturing sector has the highest abuse of Web sites that pose potential legal liability for employers, with almost 13 percent of users accessing pornographic, gambling, dating and other sites that can give rise to liability. Of further worry, 19.42 percent of personal use of the Internet by employees involves activities that pose potential threats to employer network security, such as file sharing, the use of malicious code, spyware and more.

As it turns out, governmental agencies have the highest incidence of employees accessing sites containing spyware and malicious code. In fact, almost 23 percent of governmental personal use is attributed to these high-risk activities.

Statistics from a number of experienced (Global) Security agencies provide a reverse view of this study. They state that 70% of Misuse and Theft of Data comes from inside organisations, creating serious threats of litigation; therefore internet activity is only 30% of the misuse and cyber slacking in today's modern environment.

Senior executives and managers commissioned to take responsibility for the "acceptable use" of company computer resources today have considerably heightened accountability to the business and employees; this to ensure that protection from outside and indeed inside their organisation is fully maintained. With the latest legislation, it is now frankly unacceptable to use the excuse "I didn't know".

Plainly, employers do have good reason to be worried about productivity levels and exposure. It is therefore important for employers to develop acceptable usage policies that are appropriate to their business.

So then why do we continue to watch the horizon and sit behind our outside barrier of firewalls? Instead, we should be proactively acting from the inside – using a combined approach of corporate and technology protection:

#### Corporate:

Developing and enforcing an Acceptable User Policy (AUP), which provides all employees with a solid set of rules that clearly states what, when and how they are expected to use business communications.

#### Technology:

Implementing the correct automated solution that monitors intelligently without infringing employee rights, all incoming, outgoing and importantly, internally circulated communications including Instant Messaging (Hotmail) and Internet sites.

#### Know what you are dealing with:

Knowing what risk is and what's at risk are the first steps in establishing a successful Acceptable User Policy (AUP). Understanding the myriad threats and vulnerabilities and keeping up with a shifting landscape are critical in maintaining a secure and safe operating organisation.

The rewards of a good AUP are difficult to discern at first. After all, it's difficult to point to things that didn't happen and call it a success. However, if the objective is to keep malicious events from happening, the lack of those events occurring is the barometer of an effective program's effectiveness.



## **Policy Central Enterprise™**

Policy Central Enterprise is a unique "behaviour management" software solution for all businesses and organizations. It captures logs and reports all violations either in invisible operation mode or as part of an organisations agreed (AUP) practice.

PCE is based upon a very simple but powerful idea. It enforces your (AUP) automatically, by monitoring all screen content and keyboard activity. The automated (real-time updated) data engine, contains 8 violation libraries such as: pornography, paedophilia, profanity, racism, drugs etc. Recording in real-time, any triggered violation is screen captured and maintained within a secure SQL database enabling a comprehensive audit log and flexible reports to provide detailed forensic evidence.

It can be configured to monitor all Instant Messaging, Chat, Windows applications, documents and E-mail including all attachments, in fact any content that is displayed on the screen. Once identified, Policy Central Enterprise can be utilised to secure system usage, implement Site Blocking and undertake time management for all applications and Internet access.

To obtain an outline copy of AUP Guidelines and further details on Policy Central Enterprise, go to [www.forensicsoftware.co.uk](http://www.forensicsoftware.co.uk)

Colin Dean  
Forensic Software  
April 2006