

# Killer Surf Issues: Crafting an Organizational Model to Combat Employee Internet Abuse

Over the years, employees have been provided with uninhibited access to the Internet leading to a drain on time and budgets within organizations. With nearly 64% of employees claiming to use the Internet for personal interest during working hours, according to *Snapshotspy.com*, developing a policy is in your organization's best interest.

**Kimberly Young, Ph.D.**



**E**mployees who surf the Internet during work hours for personal reasons are forcing organizations to regulate its use. According to the computer monitoring software website *Snapshotspy.com*, more than 50% of employees use the Internet for personal use during an average work day, which decreases productivity, negatively affects customer service, drains network resources, and, in some cases, exposes an organization to legal liability.

## Productivity Issues

Internet abuse in the workplace can

hurt an organization's reputation for quality and service. As workers surf during work hours, they are slow to respond to customer needs, unable to meet deadlines, and fail to complete tasks. This translates into poor quality and customer service, which eventually hurt the organization's credibility. Over time, an organization that is unable to meet customer needs and deliver quality products will have a negative brand image.

## Technology Resource Drain

Employees who use the Internet for purposes other than job tasks place a

significant drain on network energy and decrease system responsiveness for job-related functions. This added load costs organizations additional fees to support servers, Internet service providers, and the hardware necessary to accommodate increased network traffic and data storage. An employee's inappropriate use may negatively affect other employees' speed of access or storage space available for work product. Or worse, system slowdowns can delay data retrieval and result in network malfunction or failure due to overload.

## Liability Risks

Employees who access inappropriate sites pose serious legal liabilities for the organization. But inappropriate sites include more than those with pornographic material. They also include Internet gambling sites, virtual casinos, gaming sites of any kind, and sites that facilitate illegal downloading of copyrighted books, music, or videos.

An even more alarming risk for organizations is the growing legitimacy of Internet addiction being diagnosed as a disorder, placing organizations under significant liability under the Americans with Disabilities Act (ADA). As reported in a 2004 *CyberPsychology & Behavior* article by Carl J. Case, Ph.D., and the author of this article, "Internet Abuse in the Workplace: New Trends in Risk Management," former workers have sued under the ADA for wrongful termination, claiming they suffer from a mental disorder and holding the company responsible for providing access to the "digital drug." While such claims seem frivolous, even ludicrous, to employers, more cases are being seen in court each year.

## Effective Risk Management

An organization should question how best to respond to incidents of abuse. Should it simply suspend the employee's Internet privileges – or take more drastic measures and fire

the employee to set an example? If it fires the employee, what will happen to the other employees' morale? How much will customer and investor goodwill be affected if the media report on the firings?

## A Framework for Managing Abuse

Organizations must carefully shape and structure decisions related to employee Internet management to cultivate a positive culture that will maximize productivity and reduce liability. Building upon a risk management theory they first conceptualized and published in a 2001 *Journal of Business and Information Technology* article, "Employee Internet Misuse: An Epidemic in Need of a Research Framework," Case and the author of this article outlined a comprehensive theoretical framework on employee Internet management explained as a range or continuum of approaches (see Figure 1).

Based upon this model, employee Internet management can be approached from the extremes of a proactive to a reactive perspective. Four management behaviors include practices relating to hiring, prevention, enforcement, and termination or rehabilitation.

*Hiring* practices incorporate screening prospective employees for Internet misuse tendencies in the form of a survey or interview that can be used

to assess the potential for online abuse.

*Prevention* includes developing policies that outline acceptable Internet use in the workplace, education initiatives to increase employee compliance, and management training in early detection of employee Internet abuse.

*Enforcement* examines the technological infrastructure within the organization. Aspects include electronic monitoring of networks, filtering that blocks inappropriate websites, and layered computer security to track employees' Internet use.

Finally, *termination or rehabilitation* examines the effects of firing or rehabilitation. Of interest are the legal implications of termination and the potential loss of an otherwise productive employee. The framework is important from a practitioner-orientation standpoint, as results may be used to improve the organization's employee Internet management to maximize productivity, limit risk, and minimize negative behavior.

## Evaluate and Screen During Hiring Practices

Organizations have begun to incorporate hiring practices that evaluate and screen applicants for their potential for online abuse. Recruiters incorporate questions that evaluate a candidate's prior Internet behavior or attitude toward using company band-



Figure 1: Framework for Internet Management from Proactive to Reactive Approaches

width and other electronic material as a means to identify applicants who might be at greater risk to abuse the Internet. Upon interview, candidates who demonstrate negative attitudes toward technology-related integrity or negligence about online security may be turned down for key job management positions or, if hired, monitored more carefully regarding their online usage.

Until recently, standardized assessment instruments were not available to measure or predict the potential of employee online abuse. However, a 2004 article by Laura Widyanto, Ph.D. and Mary McMurran, Ph.D. in *CyberPsychology & Behavior*, "The Psychometric Properties of the Internet Addiction Test," introduced the first theory-driven, validated scale to measure Internet use problems.

Coupled with specific interview questions during the hiring process, the Internet Addiction Test (IAT) was constructed to measure symptoms of Internet addiction, which are shared with other established compulsions (e.g., gambling, eating) and to evaluate specific symptoms unique to this population. The IAT provides an assessment tool for organizations to measure potential Internet addiction among prospective employees allowing them to make better hires, which will improve productivity and reduce corporate liability.

### Outline Internet Usage Policies

Attorneys should advise companies to write policies on e-mail and Internet usage (see "Sample Internet Usage Policy"), according to *AuditNet.org*. A formal Internet usage policy should:

- Specifically set out prohibited uses, rules of online behavior, and access privileges
- Spell out the penalties for violations of the policy, including security violations and vandalism of the system
- Require anyone using the organization's Internet connection to sign the

## Sample Internet Usage Policy

Employers should provide employees with guidelines about which uses of the Internet are proper, and which uses are improper. A clear policy that is enforced will help the employer reduce its risk of liability from improper Internet use. This sample is for information only, and does not constitute legal advice.

### ABC Co. Internet Usage Policy

This policy applies to all employees when they are using computers or Internet connections supplied by ABC, whether or not during work hours, and whether or not from ABC's premises.

1. **No privacy.** ABC provides computers and Internet connections ("facilities") to further its business interests. You should use those facilities only for ABC business. ABC has the right, but not the duty, to monitor all communications and downloads that pass through its facilities, at its sole discretion. Any information retained on ABC's facilities may be disclosed to outside parties or to law enforcement authorities.
2. **Improper activities.** You may not disseminate or knowingly receive harassing, sexually explicit, threatening or illegal information by use of ABC's facilities, including offensive jokes or cartoons. You may not use ABC's facilities for personal or commercial advertisements, solicitations or promotions.
3. **Nature of e-mail.** E-mail resembles speech in its speed and lack of formality. Unlike speech, e-mail leaves a record that is often retrievable even after the sender and recipient delete it. If you would not want your mother to read your message on the front page of the Los Angeles Times, do not send it by e-mail.
4. **Regular deletion of e-mail.** ABC strongly discourages storage of large numbers of e-mail messages. As a general rule, you should promptly delete each e-mail message that you receive after you have read it. If you need to keep a message for longer than a week, save it to your hard disk, or print it out and save the paper copy. The Systems Administrator will regularly purge all messages in employee inboxes and all copies of sent messages that are older than 30 days.
5. **Intellectual property of others.** You may not download or use material from the Internet or elsewhere in violation of software licenses, or the copyright trademark and patent laws. You may not install or use any software obtained over the Internet without written permission from the Systems Administrator.
6. **Report violations.** If you observe or learn about a violation of this policy, you must report it immediately to your supervisor, or to the Systems Administrator.
7. **Acknowledgment.** By signing on the line below, I acknowledge that I have read, understand and agree to comply with the foregoing Internet Use Policy. I understand that, if I do not comply with the Internet Use Policy, I may be subject to discipline, including loss of access to ABC's facilities and discharge from employment. I may also be subject to legal action against me for damages or indemnification.

Source: *AuditNet.org*

policy and understand it will be kept on file as a legal, binding document

Employees should be alerted regularly that their online activities may be monitored and that inappropriate use may result in disciplinary action, according to *AuditNet.org*. Organizations are also advised to update policies when upgrading technologies in the workplace to protect them if an employee abuses the new technologies and no policy specifically addresses its abuse.

Holding a series of Internet workshops with employees is one way to introduce your organization's policy. The sessions can address the sensitive issues surrounding Internet abuse in an open forum where employees can ask questions and provide input in a non-confrontational setting, according to *staffmonitoring.com*. This forum will allow organizations to discuss the types of sites it has decided to block and answer any questions from the employees. Organizations can also provide samples of the Internet reports, according to *staffmonitoring.com*, and discuss how they might be used in the future.

Corporate training regarding employee Internet use and its potential for abuse is emerging as an effective means to communicate policies and aid in the prevention of Internet abuse.

### **Enforce Internet Usage Policies**

What is the effectiveness of an organization's policy if it is unenforceable? Organizations are using filtering software, firewalls, and monitoring software to block access to inappropriate areas of the Internet and to detect incidents of Internet abuse.

*Filters* disable an employee's ability to access sites the organization finds unproductive or objectionable. In the past, the main target blocked was online pornography sites; however, any problematic website or area of the Internet can be filtered. While filters are effective, they are not fool proof, as computer-savvy employees can disable the filter or pass through the firewall.

## **Do You Need an Internet Usage Policy?**

- **64%** of employees say they use the Internet for personal interest during working hours.
- **70%** of all Internet porn traffic occurs during the 9:00 a.m. to 5:00 p.m. work day.
- **37%** of workers say they surf the Web constantly at work.
- **77.7%** of major U.S. companies keep tabs on employees by checking their e-mail, Internet, phone calls, computer files, or by videotaping them at work.
- **63%** of companies monitor workers' Internet connections, and **47%** store and review employee e-mail.
- **27%** of companies say they have fired employees for misuse of office e-mail or Internet connections, and **65%** report some disciplinary measure for those offenses.

Source: *Snapshotspy.com*

*Monitoring software* allows employers to monitor employee Internet accounts and generate usage reports that track an employee's online activities, such as websites visited, to detect if they are inappropriately accessing gambling sites, sports sites, news sites, or adult sites. However, a computer-savvy employee may be able to install software that erases any traces of inappropriate or objectionable online use.

### **Securing the Organization's Integrity**

According to a survey by technology analyst firm IDC, 30% to 40% of Internet access is spent on non-work-related browsing, and a staggering 60% of all online purchases are made during working hours. In addition, 90% of employees feel the Internet can be addictive, and 41% admit to personal surfing at work for more than three hours per week.

When confronted with cases of overt Internet abuse, many organizations quickly react with job suspensions or dismissals. While these actions put an end to an employee's abuse of the Inter-

net, they generate hidden costs for the employer; increased turnover rates mean additional recruitment and retraining expenses. Termination can also create a climate of fear, distrust, and resentment that will undermine productivity and cooperation among employees who use the Internet properly. With this type of negative publicity, an organization's clients can become less trustful of the integrity of the company.

Similar to how they may handle alcoholism or drug dependence, organizations may choose to rehabilitate, rather than terminate, the employee; costs involved in such rehabilitation efforts and possible litigation should be considered. Before taking any direct action, organizations should consider referring employees to their Employee Assistance Program.

A 1999 study published in *CyberPsychology & Behavior*, "Psychological Characteristics of Internet Addiction: A Preliminary Analysis," estimated 6% of online users suffer from Internet addiction, and more recent research suggests one in eight Americans suffers from at

**Organizations need to have an effective plan to respond to employee Internet use, which begins with implementing rehabilitation strategies that keeps the individual employed, while treating an underlying psychological addiction to the Internet.**

least one aspect of problematic online behavior. To individuals who use the Internet for work purposes only – and even those who sometimes use the Internet to unwind – Internet addiction may seem a little far-fetched. However, for those who have lost jobs, ruined marriages, or alienated themselves from their friends to spend “just five more minutes” on the Internet, Internet addiction is a very real and frightening condition.

**Implementing Internet Usage Policies**

An organization may be willing to acknowledge the legitimacy of Internet addiction – and may even be prepared to implement fair and appropriate strategies to offset productivity losses caused by inappropriate use of the Internet – rather than impose “zero tolerance” policies that alienate employees and leave the organization susceptible to litigation. The problem then becomes a lack of information about how to successfully create and implement an Internet usage policy that incorporates rehabilitation. Organizations must develop a concrete strategy to handle critical incidences of abuse to ensure fair and appropriate treatment.

In one instance, a *Fortune* 500 company employed the use of detailed record forms and reporting methods to monitor critical incidences of employee online abuse. Factors, such as work history, length of employment, and job status, were used to evaluate the action taken against an employee for a violation. Employees who had greater longevity with the organization and pos-

itive performance appraisals were offered job redesign options and clinical rehabilitation through the corporate EAP. Job redesign was offered in the form of new duties that did not entail use of the Internet and allowed only selective monitoring of online use after receiving treatment. Over time, by offering rehabilitation as an alternative to termination, the company was able to reduce job turnover and recruitment costs, as well as better protect itself from legal risk.

**Implications for the Future**

Having a clear system in place that incorporates policies and procedures allows organizations to handle incidents of employee Internet abuse swiftly and efficiently. Early detection is important in limiting incidents of abuse. Screening applicants to avoid hiring potential problem users, developing Internet use policies, and reinforcing and enforcing those policies are ways organizations can protect themselves.

Organizations need to have an effective plan to respond to employee Internet use, which begins with implementing rehabilitation strategies that keeps the individual employed, while treating an underlying psychological addiction to the Internet.

A December 14, 2006, article in *Business Week*, “Virtually Addicted,” reported a precedent-setting case of James Pacenza, a former IBM employee, who filed a \$5 million lawsuit for wrongful termination. By his own admission, he was spending too much time in Internet chat rooms and in some of them was discussing sex. He went so far as to call his interest in inappropriate websites a form of addiction that stemmed from the post-traumatic stress disorder he suffered after returning from Vietnam.

On the surface, it may appear to be

an open-and-shut case. The organization’s policy called for the termination of employees who access inappropriate websites. At the time of this writing, the case was still under review, but it illustrates the impact Internet misuse may have on companies and adds to the growing debate over whether Internet abuse is a legitimate addiction, such as alcoholism. Attorneys say recognition by a court – whether in this or some future litigation – that Internet abuse is an uncontrollable addiction and not just a bad habit could redefine the condition as a psychological impairment worthy of protection under the ADA. This would open the door for further lawsuits and increase the need for rehabilitation.

IT departments must be familiar with the development and the parameters of the organization’s Internet usage policy so they will be better equipped to:

- Recognize patterns of misuse and more proactively respond to incidents of abuse
- Understand enforcement expectations and procedural protocol to appropriately respond to suspected problems detected through firewall records and Internet usage reports
- Work closely with human resource managers to develop an effective procedure that responds to employee Internet abuse within a framework of treatment over termination
- Implementation of technology, including the purchasing of hardware, software, and telecommunication systems to maintain and upgrade networks, is expensive. Those investments should lead to an increase in productivity and enhance an organization’s ability to remain competitive in the global marketplace, rather than result in employee distraction and poor job performance. **END**

See this article online for references at <http://content.arma.org/IMM>.

*Kimberly Young can be contacted at [kyoung@sbu.edu](mailto:kyoung@sbu.edu). See her bio on page 47.*