MANAGING EMPLOYEE INTERNET ABUSE:

A COMPREHENSIVE PLAN TO INCREASE YOUR PRODUCTIVITY AND REDUCE LIABILITY

By Dr. Kimberly S. Young

In March of 2000, the number of online users had grown to over 304 million (80% from 1999) and the amount of data available also continues to grow with estimates of 2.1 billion unique web pages and growing by 7 million pages per day. Telecommuting is also on the rise as a mere 24% work exclusively from regular office location. The number of PCs sold in past 20 years approaching 1 billion - triple the number of automobiles sold during that time. Estimates on volume of email vary, with high-end projections of about 4 trillion annually, 40 times greater than the snail mail delivered by U. S. Postal Service. It has become ubiquitous with our personal and professional lives.

While the Internet is a practical tool, it can easily be misused in the workplace. Online industry analysts estimate that over four billion dollars a year are lost due to lost employee productivity and organizational efficiency when wired workers utilize Internet access at work to view news sites, send and receive personal email, view online pornography, play interactive games, or chat with friends.

When it comes to Internet access, many companies who had opened the barn door wide are now finding that they need to selectively bar it shut and establish usage policies for Internet access. Here are just a few statistics that measure employee Internet abuse:

- Nearly 55% of workers are exchanging potentially offensive messages at least once a month (PC Week).
- In a recent survey of 224 firms that utilized monitoring software, 60 percent of the managers said they had disciplined employees for online misuse, and 30 percent had fired people for such behavior, which included downloading pornography and shopping and gambling online (Websense Security Software).
- 47% of employees send up to 5 personal emails per day, and 32% send up to 10 personal emails daily, and 28% receive up to 20 personal emails per day (Vault.com).
- Almost one in five people go to cybersex sites while at work (MSNBC poll, June '98).
- Recently a major US computer manufacturer installed monitoring software and discovered that a number of employees had visited more then 1,000 sexually oriented sites in less than a month. Twenty people were fired for misusing company resources (USA Today).
- 68% of companies characterized messaging misdemeanors as widespread, with losses estimated at $3.7 Million per company a year (Datamation).

- Employees from the top technology firms including IBM, Apple Computer Inc., and AT&T have accessed Penthouse thousands of times each month (Nielson Media Group, '97).
- 52 of the Fortune 100 companies have an Acceptable Internet Use Policy (The Aberdeen Group).
- 58% of employers who monitor do so to control recreational use; 47% do so to reduce bandwidth abuse, 47% hope to eliminate downloads of pirated software, and 33% hope to reduce sluggish Internet connections due to recreational use. (PC World).

Sexual harassment and discrimination liability suits caused by misuse of personal email by employees is major employee Internet abuse concern. In Strauss vs. Microsoft Corporation, a supervisor sent inappropriate e-mail to female employees, and the e-mail was used as evidence from which a reasonable jury could find that failure to promote a woman was based on gender. Recent legislation amending harassment/stalking laws to include e-mail has been passed in Washington, Arizona, California, Indiana, Michigan, New Hampshire and Wyoming, placing companies at further risk. California also legislated against spoofing with fines of $1,000 and jail terms of up to six months.

Employee Internet misuse and abuse has gotten to be such a problem that is has become one of the leading causes of job termination with hi-profile cases such as The New York Times, Xerox, Dow Chemical, and Merck & Company who have disciplined and dismissed employees for Internet abuse. A recent study surveyed 224 of 1500 companies. The study was commission by Websense, Inc., a monitoring software

company, and results showed that despite implementing Internet use policies, companies continue to identify incidents of employee Internet abuse and subsequent job dismissals are on the rise:

- 83% have Internet access policies
- 64% have disciplined, 30% have terminated for:
- Accessing pornography (42%)
- Online chatting (13%)
- Gaming (12%)
- Sports (8%)
- Investing at work (7%)
- Shopping at work (7%)

Despite these concerns, full-scale computer audits are completed by less than 25% of US companies. When audits are conducted, zero-tolerance is enforced and those employees who are found to abuse the Internet are fired. However, zero-tolerance policies for employee Internet abuse cost companies extraneous expense in the recruitment for new hires, especially in a tight labor market, where qualified candidates are limited. Furthermore, dismissals based upon Internet abuse result in significant production delays and repeated turnover costs that cut into the corporate bottom line. While the focus has revenue losses generated by poor worker productivity and job turnover increases, dollar estimates haven't even been placed on the cost to the growing

climate of corporate distrust and low employee morale generated by such monitoring practices and related job firings.

In general, the costs of employee Internet abuse can be divided into two general categories: direct costs and indirect costs. Direct costs include tangible and measurable items such as monetary theft and stolen trade secrets and information breeches. Indirect costs include less tangible and harder to measure items such as the loss of customer goodwill or potential sales revenue or the increase in corporate liability associated with employee Internet abuse. Each of these will briefly be discussed.

DIRECT COSTS

A direct cost that I mentioned at the beginning of this guide is the lost productivity that can take on several forms:

Corruption of Data and Jeopardized Information Security – The integrity of sensitive data on a computer system such as company plans, customer demographic data, product designs, or proprietary information may be risked due to information security breeches caused by Internet misuse. For instance, Elron Software conducted a study in 2000 and found a 170% increase in the number of employees who received confidential information via email. Furthermore, the survey revealed that confidential email leaks rose from 9.2% in 1999 to 24.1% in 2000 and email with attachments rose from 63.6% in 1999 to 73.5% in 2000. This can easily result in the spread of computer viruses that lead to complete network shutdowns or corrupt valuable databases that stop daily operations and lead to costly repairs, especially if efficient disaster emergency plans are not in place.

Ultimately, such abuses may leave companies vulnerable to hackers and compromise the security of trade secrets and vital system information.

Diversion of Funds – Companies must allocate funds for additional hardware, software, and labor costs necessary to monitor employees for cases of potential abuse. Hardware costs are incurred to install monitoring and filtering software, computers, and firewalls to build a responsive technological infrastructure to deter and detect incidents of employee Internet abuse. Labor costs are incurred for additional personnel to maintain firewalls, monitor employees, interpret Internet usage reports, and respond to incidents of abuse. As corporate funding is often limited, these additional expenditures allocated to employee monitoring deplete and detract funding from other needed resources thereby decreasing organizational performance and efficiency.

Network Slowdowns and System Failure – Recently, a large technology firm conducted an internal network audit to review online transmissions for one week. Their review found that only 23% of online transmissions were work-related, while the remainder was used for employee personal use such as to view sports sites, news sites, and gaming sites, which explained the continued drain on network performance. Stories such as this are frequently heard. Employees who utilize the Internet for other than job tasks place a significant drain on network energy only to decrease responsiveness of the system for job related functions. Access to the Internet costs a business money, either in fees to Internet Service Providers, or in hardware costs 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 for work product. Or worse, system slowdowns can delay data retrieval and possibly result in network malfunction or failure due to overload.

Poor Job Performance – For every minute, hour, or day that an employee utilizes work access to the Internet for recreation use that is a minute, hour, or day the employee is not working, which results in billions of dollars of lost productivity for the company. For example, in the summer of 2000, Victoria Secret launched a 44-minute web cast to show off their new work line. The broadcast was in the middle of the workday. Over 2 million viewers were reported and productivity losses were estimated at $120 million, just for that one afternoon. Computer Economics, an industry research firm, estimated that $5.3 billion was lost in 1999 due to recreational surfing and ZDNet estimated that $470 million was lost because of employees reading Clinton-Lewinsky documents online. In 1999, Vault.com surveyed 1439 workers and found that:

37% admit surfing constantly

32% surf a few times per day

21% surf a few times per week

Based upon these survey findings, Vault.com projected that $54 billion was annually lost in worker productivity. These estimates from a cross section of industry analysts show that employee Internet abuse is a serious financial concern for any company that provides online access to workers.

INDIRECT COSTS

A company can also experience indirect or secondary costs related to employee Internet abuse, which are less tangible and harder to measure, although more costly to the company over time.

Negative Brand Impact – The one thing a company strives to build is its reputation. Its reputation for being a strong and reliable company. Its reputation for being able to succeed. Its reputation for quality and customer service. As wired workers surf during hours, they are slower to respond to customer needs, unable to meet deadlines, and fail to complete tasks. Employees who abuse the Internet under-perform. This translates into poor quality and customer service, which eventually hurts corporate credibility. Organizational efficiency is compromised because the firm is unable to meet consumer needs and/or delivery quality products. Over time, these factors will create a negative brand image as the reputation of the company becomes tarnished and the firm is labeled unreliable and unresponsive.

Loss of Goodwill – Corporate goodwill rests on three interdependent levels within a firm that equally impact organizational productivity, efficiency, and cohesion. First, employee Internet misuse and abuse compromise customer goodwill. As customers learn about firings due to Internet abuse at the firm, consumers are less trustful of the integrity of the company. Customers may turn to competitors who they view as more dependable and reliable, which results in lost revenue for the firm. Secondly, employee goodwill is

compromised when employers decide to monitor all Internet use and take a zero-tolerance stance on any incidents of Internet misuse. Often, employees fear employers and this creates poor morale among wired workers that can lead to poor job motivation and output. For example, a recent study conducted by PC World Online found that 26.8% of employees surveyed believed companies did not have the right to monitor Internet activities. Ultimately, a dissatisfied employee becomes resentful of these workplace restrictions and will look for alternative employment. While this individual may not have been the best employee for your firm, repeated turnover due to poor morale is an unhealthy trend for any firm. In order to combat these morale issues, firms must learn how to effectively implement appropriate policies and monitoring strategies that cultivate an open and positive work environment for wired workers. Finally, investor goodwill is hurt due to underlying production delays and sale losses created by employee Internet abuse. Specifically, the stock value of the company may decline or it may be more difficult for the firm to obtain new financing.

Potential Sales – Employee Internet abuse not only jeopardizes existing accounts, but such abuse will make it more difficult to generate new sales due because of a damaged corporate image and loss of customer goodwill. Consumers grow weary of the firm and this fear makes them avoid an initial investment in a company that seems unpredictable. Basically, a downward spiral is created. Employee Internet abuse leads to poor job performance which leads to an inability to meet consumer demand which leads to poor brand image and goodwill which leads to a loss in potential sales. Business longevity is

significantly hindered and potential revenue is lost to competitors and that spells danger for any company.

Discrimination or Harassment Suits - At a recent lecture given to a group of human resource professionals, I asked the audience how many of had received a joke via email at sometime in their lives. The entire audience raised their hands. Jokes emailed to coworkers may seem like just an innocent way to brighten up another's day; however, these jokes can also lead to costly harassment suits as email that is perceived to be sexually or racially discriminating can be grounds for a harassment lawsuit. And it is not just the person who sent the email, but the entire company may be liable if the email was sent over a firm's Intranet or network mailing system. For example, Chevron was liable for two million dollars in damages related to a racial discrimination case launched by several offended employees. A manager sent the discriminatory email, but the entire firm was held liable because it was sent during work hours and on the work email system. Increased corporate liability means that firms must be extra vigilant about the type of information distributed online. To combat the problem, managers institute a specialized email use policy in additional to a more generic Internet use policy, however, this rarely resolves the entire problem. Despite these efforts, the problem seems quite pervasive as a recent study commissioned by Elron Software found that 1 out of every 5 employees was sent offensive email. Beyond email abuse, other types of discrimination and harassment issues can emerge because of the Internet. For instance, sexually explicit material in the form of pictures, video, sound, and text abound in cyberspace. If such material is brought into the workplace, it carries with it the potential to create a hostile work environment, thereby presenting a potential risk of exposure to the employer under federal or state

prohibitions against sex discrimination. These costs can be enormous and perhaps even put a company out of business.

Wrongful Termination under ADA - Accessing pornography, online chatting, gaming, investing or shopping at work are the leading causes for disciplinary action or termination. The latest business trends show a rise in the number of wrongful termination suits based upon disability claims under the ADA due to Internet addiction as a new mental disorder. The movement toward classification of Internet addiction as a legitimate mental disorder has already been discussed by such organizations as the American Psychiatric Association and the National Council on Alcoholism and Drug Dependence. Furthermore, Daubert Hearings in the court system which are designed to be the legal gatekeeper for new medical and psychiatric areas of research has found Internet addiction to be a scientifically valid disorder. Therefore, disability claims based upon Internet addiction are a serious concern for companies who have given employees direct access to something with an addictive potential. Especially as online pornography and sex chatting transform a work computer into a sex toy, and employees learn to associate Internet use with sexual fulfillment. While many factors must be proven in order to diagnose an individual as an Internet compulsive, the merits of the disability claims place firms at significant corporate risk and liability.

Turnover and Recruitment Costs – As companies like Xerox or Dow Chemical fire employees for abuse, new issues emerge. Employee termination for Internet abuse may solve one problem – the abuse. However, it can lead to new problems such as expanded job turnover and recruitment costs. Frequent job turnover can result in productivity

slowdowns due to increased job vacancies and production delays while recruiting for open positions. Zero-tolerance policies for employee Internet abuse cost companies extraneous expense in the recruitment for replacements. And once hired, these new recruits must be trained, and during that training period are not as efficient in the capacity that is expected to increase organizational efficiency.

THE SEVEN STRATEGIES

Managers are growing increasingly concerned about employee Internet abuse. Telemate.com surveyed more than 700 companies and asked senior executives, information technology managers, and human resource managers about employee Internet abuse and 70% indicated surf abuse results in real costs to their companies and 83% were concerned about what to do to solve the problem.

These concerns range on a variety of issues. Managers struggle with how to effectively monitor employee Internet use while maintaining employee productivity and morale. Managers also question the utility of monitoring techniques because monitoring only seems to be a tool to detect cases of employee Internet abuse rather than being an effective agent to actually **stop** the abuse. Human resource managers try to develop comprehensive Internet abuse policies that will not only curb employee Internet abuse but also will effectively reduce corporate risk and liability, which is sometimes a very tricky legal issue. Managers question the best way to respond effectively respond to incidents of abuse. Should they simply suspend the employee's Internet privileges or take more drastic measures and fire the employee to set an example? If they fire the employee, how will this employee morale? How much will customer and investor goodwill be impacted

if the media reports on the firings? As you can see, managers today must carefully shape and structure decisions related to effective employee Internet management in order to cultivate a positive corporate culture that will maximize productivity and reduce liability. To assist in this effort, I outline the following outlines seven strategies to guide managers on how to build an optimal employee Internet management plan of action:

1. Assess your firm's current risk of employee Internet abuse.
2. Develop a comprehensive employee acceptable Internet use and abuse policy to protect your firm from corporate liability.
3. Educate and re-educate employees on company policies to increase compliance.
4. Employ comprehensive and effective monitoring strategies to enforce policies.
5. Improve cohesion between human resources and information technology departments to maximize their efforts.
6. Train managers in early detection of employee Internet abuse problems to aid in prevention.
7. Analyze cost-benefit of employee termination for critical incidents versus rehabilitation to reduce job turnover and recruitment costs.

While these seven strategies are interdependent, each will be discussed in more detail.

1. Assess your firm's current risk of employee Internet.

The first step is to conduct a self-evaluation. This will allow you to assess the level of employee Internet management techniques that your firm currently

employs. Below is a simple ten-item questionnaire that outlines various employee Internet management practices. For each question, answer "yes" or "no" if your company currently has this practice in place.

___ Yes ___ No 1. Do you have an Internet use policy or code of conduct?

___ Yes ___ No 2. Do you have an email use policy or code of conduct (separate from Internet use policy)?

___ Yes ___ No 3. Do managers receive training on how to identify early warning signs of employee Internet abuse?

___ Yes ___ No 4. Do you randomly search employee Internet accounts?

___ Yes ___ No 5. Do you use monitoring software to regulate employee Internet use?

___ Yes ___ No 6. Do you use firewalls to block inappropriate Internet access?

___ Yes ___ No 7. Do you routinely communicate acceptable Internet use practices and policies to employees?

___ Yes ___ No 8. Do you provide employee training on appropriate Internet use and its potential for misuse and abuse?

___ Yes ___ No 9. Do you offer counseling for employees who abuse the Internet?

___ Yes ___ No 10. Does your firm post symptoms of Internet addiction for employees?

Review your responses, the higher the number of "yes" responses, the greater awareness and proactive response to employee Internet management your firm has employed. Less than four "yes" responses suggests that your firm may not

employ Internet use policies, employee monitoring, or training to provide maximum protection of your network resources and minimize the potential risk of abuse. If you are in this category, your firm is at substantial corporate risk, as incidents of employee Internet abuse most likely go undetected. Undetected abuse impacts your bottom line through lost worker productivity and impaired organizational inefficiency. Furthermore, employee Internet abuse that is not monitored or patrolled may cause breeches in information security that gives competitors access to your firm's trade secrets and databases. You are in particular need of the material contained in this booklet as a guide that will help your firm implement a comprehensive plan to manage employee Internet abuse.

Four to seven responses suggests that your firm has employed a medium to high level of access control through the institution of an acceptable Internet policy or employee monitoring or firewall blocking. Having policies and monitoring software build an excellent foundation, but while your firm has put forth these measures, it must routinely communicate these policies to employees and utilize seminars to educate employees about Internet use and its potential for abuse. Therefore, the material contained in this booklet will teach you additional techniques and strategies to increase your employees' compliance with the firm's acceptable Internet use policy and enhance their cohesion with workplace technologies in order to maximize profits and minimize abuse.

If answered "yes" to all more than eight of the items, then your firm already does an outstanding job in managing employee Internet use and possible abuse. Therefore, the following information will be helpful to refine your current processes to enhance the techniques and strategies that you already employ.

2. Develop a comprehensive Internet use and abuse policy to protect your firm from corporate liability.

Business use of the Internet has experienced extraordinary growth in this decade. It is now common-place for employees to have access to the Internet, and as the United States moves ever closer to an information worker/service type of economy, even more workers will need access to the Internet to do their job effectively. Given the rise of employee Internet abuse, many employers have recognized that unrestricted use of the Internet by employees has the potential to drain, rather than enhance productivity. The solution may be to implement a policy outlining the permissible parameters of employee Internet use, or an acceptable Internet use policy.

This policy is a written agreement that establishes the permissible workplace uses of the Internet. In addition to describing permissible uses, an effective Internet use policy should specifically set out prohibited uses, rules of online behavior, and access privileges. Penalties for violations of the policy, including security violations and vandalism of the system, should also be covered. Anyone using a

company's Internet connection should be required to sign the policy, and know that it will be kept on file as a legal, binding document.

A comprehensive policy will help minimize employee Internet abuse, shield the employer from possible sexual harassment suits, prevent drains on network resources for frivolous use, and reduce corporate risk and liability, especially in the event of legal action taken by an employee terminated for abuse. A comprehensive policy should outline acceptable and unacceptable Internet use, communication practices, restrictions on software downloads, copyright issues, security, online harassment, and how violations will be handled. The following is a general Internet use policy adapted from our eBehavior, LLC corporate seminars will help guide in your firm's development of an effective and comprehensive policy:

Acceptable Uses of the Internet

Employees accessing the Internet are representing the company. All communications should be for professional reasons. Employees are responsible for seeing that the Internet is used in an effective, ethical and lawful manner. Internet Relay Chat channels may be used to conduct official company business, or to gain technical or analytical advice. Databases may be accessed for information as needed. E-mail may be used for business contacts. (An employer may wish to include a separate policy exclusive to email dependent upon how much personal email abuse is a problem).

Unacceptable Use of the Internet

The Internet should not be used for personal gain or advancement of individual views. Solicitation of non-company business, or any use of the Internet for personal gain is strictly prohibited. Use of the Internet must not disrupt the operation of the company network or the networks of other users. It must not interfere with your productivity.

Communications

Each employee is responsible for the content of all text, audio or images that they place or send over the Internet. Fraudulent, harassing or obscene messages are prohibited. All messages communicated on the Internet should have your name attached. No messages will be transmitted under an assumed name. Users may not attempt to obscure the origin of any message. Information published on the Internet should not violate or infringe upon the rights of others. No abusive, profane or offensive language is transmitted through the system. Employees who wish to express personal opinions on the Internet are encouraged to obtain their own usernames on other Internet systems.

Software

To prevent computer viruses from being transmitted through the system there will be no unauthorized downloading of any software. All software downloads will be done through the MIS Department. Furthermore, downloading games or other

non-work related files, or restrictions on downloading large files that can be obtained off-line are forbidden.

Copyright Issues

Copyrighted materials belonging to entities other than this company may not be transmitted by staff members on the Internet. One copy of copyrighted material may be downloaded for your own personal use in research. Users are not permitted to copy, transfer, rename, add or delete information or programs belonging to other users unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action from the company or legal action by the copyright owner.

Security

All messages created, sent or retrieved over the Internet are the property of the company, and should be considered public information. The company reserves the right to access and monitor all messages and files on the computer system as deemed necessary and appropriate. Internet messages are public communication and are not private. All communications including text and images can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

Harassment

Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual or group's race, religion, national origin, physical attributes, or sexual preference will be transmitted.

Violations

Violations of any guidelines listed above may result in disciplinary action up to and including termination. If necessary the company will advise appropriate legal officials of any illegal violations.

3. Educate and re-educate employees of company policies to increase compliance.

Over the past few years, corporations have recognized the need to establish acceptable Internet use policies for employees. In 2001, the American Management Association found that nearly 80% of firms surveyed instituted some form of an Internet acceptable use policy. Once your firm has developed an appropriate policy, the next step is to clearly communicate these policies to employees.

What is the best method to communicate an acceptable Internet use policy that will achieve employee compliance? The answer varies. Some companies include the Internet use policy within an employee manual given to new hires, while other companies have a separate Internet use policy that new hires must read and sign, while still other corporations utilize policy management software to distribute and update policy information via emails. Each method has its own set of unique

problems to overcome. Perhaps new hires don't actually read the employee handbook, or they don't fully absorb what they sign, or the policy management software is expensive and difficult to implement.

In the past, companies relied upon written communication alone to convey the importance of appropriate Internet use within the workplace. However, as I have outlined, statistics reveal that employee Internet abuse is on the rise despite the implementation of an acceptable Internet use policy.

Another difficulty that companies face is how to communicate policy updates that stay current with new technologies in the workplace. For instance, lets say Company XYZ moves from Intranet-based email access to a wireless system, supplying employees with Blackberry Palm devices to access web accounts. The corporation must then modify the firm's Internet acceptable use policies to incorporate these new applications. However, corporations often upgrade workplace technologies without updating policies, leaving themselves at great corporate risk if an employee abuses the new technologies and no policy specifically mandates its abuse.

So, how do corporations effectively communicate and update policies to employees? New trends are emerging in the field that find that corporate training regarding employee Internet use and its potential for abuse is one of the best methods to communicate polices and aid in the prevention of Internet abuse.

These corporate training programs are akin to sensitivity training for sexual harassment or diversity training that increases employee awareness of the issues, reduces the occurrence of future incidents, and decreases corporate liability.

Ultimately, these type of corporate seminars are a proactive response on the part of management to implement education that increase employee awareness about such topics as: (1) battling techno-stress, (2) clearly defining what is acceptable and unacceptable Internet use, (3) identifying the warning signs and risk factors for abuse, and (4) how to address underlying problems in an employee's life that contribute to Internet abuse. Such seminars utilize didactics, small group discussions, and concrete exercises to convey material in an organized and meaningful fashion. Over the past few year, I have conducted numerous corporate seminars on employee Internet misuse and abuse, and manager evaluations report the following benefits:

1. Complements the written policy with didactic instruction that reinforces the message.
2. Enhances employees' understanding about what is acceptable and unacceptable use of employee Internet accounts.
3. Increases compliance to acceptable Internet use policy.
4. Provides training to long time employees as well as new hires.
5. Increases employee accountability and ethical integrity when online.
6. Improves employee morale and job productivity.

7. Enhances employee interdependency with workplace technologies that increase overall organizational efficiency.
8. Reduces corporate risk and liability when violations occur.

4. Employ comprehensive monitoring strategies to enforce policies.

Once appropriately communicated, the next level of employee Internet management is to develop a system to monitor employee Internet accounts in order to enforce policies. After all, what is the effectiveness of a policy that you as a firm are unable to enforce? Not vary. Therefore, corporations have begun to rely upon filtering software and firewalls to block access to inappropriate areas of the Internet and employ the use of monitoring software to detect incidents of employee Internet abuse.

Filters are an effective deterrent as they disable an employee's ability to access sites that the corporation finds unproductive or objectionable. In the past, the main target has been blocked access to adult entertainment web sites; however, any problematic web site or area of the Internet can be filtered. For example, at a recent seminar, a computer security manager for an airforce base shared with me that they had to block access to eBay because it had become a problem on the base. While filters are effective, they are not full proof, as computer-savvy employees can disable the filter or pass through the firewall with ease.

Employers must also monitor employee Internet accounts with software that generates Internet usage reports that tracks an employee's online activities such as web sites visited and duration of use. Excessive time spent at entertainment sites, sport sites, or e-tailers can be detected or visits to adult entertainment sites can be tracked. Here again, a computer-savvy employee may be able to apply software that erases their Internet tracks and wash away traces of inappropriate or objectionable online use.

Given the complexity of the issue, management should follow several steps in order to implement an optimal technological infrastructure that will effectively reduce and minimize employee Internet misuse and abuse.

Step 1: Companies must carefully consider what type of filtering and/or monitoring software is right for their firm. Given the size and scope of the firm, management must consider what type of network solutions to employ. Does the firm need to install special application-oriented terminals or can a general-purpose terminal be used for computer security and employee monitoring? What types of operators will use the terminals? Will additional training be necessary? Are proposed terminals compatible with existing equipment? What web hosting modifications are necessary to achieve this?

Management must then evaluate how best to maintain records and manage databases collected from employee monitoring. Managers must also consider

how monitoring will increase overall organizational efficiency and what projected impact this will have on production, sales, and revenue for the business. Ultimately, management must consider its funding limitations in order to select a network system and monitoring software package that will provide maximum utility for the least long-term cost.

Step 2: The additional funds in hardware, software, and labor to install and maintain these monitoring or filtering systems are considerable, therefore, a thorough cost analysis must be conducted. Many companies try to cut corners, especially in a down market, only to install a system that does not provide adequate employee monitoring or blocking capability. While this may save on initial costs, corporations' end up spending more in the long run on network upgrades because the current firewall and monitoring systems are ineffective.

Step 3: Once an appropriate system is in place, employers must then properly define employee Internet abuse. What criteria will be used to define misuse and abuse? Will the criteria be based upon the type of online activity, say downloading pornography? Or should it be based upon how much time an employee spends using the Internet for recreation during work hours?

For instance, which of the following employees would you consider in violation of an acceptable Internet use policy? Employee A spends one hour a week viewing adult web sites. Employee B spends ten hours a week surfing sports and

news sites. Employee A's Internet use will most likely be viewed as a policy violation because of the nature of the online activity even though Employee B is actually wasting more time at the computer.

As we can see, managers must consider a range of factors in order evaluate the data received by employee monitoring efforts before taking any disciplinary action. Questions to ask include: How long has the identified abuse occurred? Is the abuse just a one-time event or is the abuse chronic? How long has the employee been employed with the firm? Has the employee's Internet misuse significantly reduced his or her job performance? What is this employee's work history? If the employee's work history has always been below average, then most likely the employee has always been a slacker and abusing the Internet is just another way to waste time. But if the employee has shown exemplary performance in the past, then he may be dealing with an underlying issue contributing to the Internet abuse such as a recent divorce, a death of a loved one, or problems within his family. Certainly, it is important to place the violation in some sort of context so that management can make the best and most informed disciplinary decisions.

Step 4: The final step in the process is to decide who should be monitored. Should all employees be monitored or should job status influence that decision? If everyone is to be monitored, how will senior management and the policy makers themselves feel if they are among those being monitored? To deal with

this issue, many corporations only monitor middle to lower management, skilled labor, clerical staff and the like, offering unrestricted Internet access as a perk to senior management. The belief is that senior managers will not abuse the Internet because of their job responsibilities within the firm.

However, I have frequently noted in my consultation with corporations that senior level executives are equally likely, if not more vulnerable, to develop an unhealthy or addictive habit towards the Internet. For example, I worked with Donald, a 48-year-old CEO of a major manufacturing firm from Pennsylvania. Two years ago he was first introduced to the Internet. Initially, his use was limited to web searches and email to colleagues, coworkers, and family members. One evening, alone in his office, he accidentally stumbled upon a pornography site. Out of curiosity scanned through several of its pages. The next week, while stressed after a long workday, he returned to the site for a little relaxation. "Just a few minutes won't hurt," he rationalized to himself as he surfed. Over the next few months, Donald found himself going to work early, taking more breaks, and even coming in on the weekends to view online pornography as a way to escape his job pressures, until his behavior grew more out of control. Over a period of ten months, he was able to conceal a twenty-hour a week online habit from his colleagues and board.

Scenarios like this are more common than people imagine. Senior level executives are placed in situations that lead themselves easily to the development

of abusive use of the Internet. They have unlimited and unsupervised access, often in a private office. Having such job independence most likely means that this person is free from corporate big brother, making it that much easier for problems to develop as counterproductive and maladaptive online behavior can be easily concealed. It may not be until job productivity is significantly compromised before colleagues and coworkers detect that that there is a problem.

5. **Increase cohesion between human resources and information technology departments to maximize their efforts.**

Some corporations are structured so that IT is a separate department within the firm while others have technology professionals integrated within each of the other departments to respond more directly with the specific needs of its end users. In either case, it is important for the IT professionals in charge of computer security and Internet access management to understand the needs and requirements of the human resource department. And conversely, for the human resource department to understand the tools and technology involved in employee monitoring so that your firm can promptly respond to potential problems. Therefore, it is vital for corporations to increase the cohesion between human resources and information technology departments and/or specialists to improve the overall effectiveness of employment Internet management.

Cross training is an essential step in building this cohesion. That is, IT Access Managers should be familiar with the development and parameters of the

company's acceptable Internet use policy. As IT Access Managers are more knowledgeable about such policy development issues, they will be better equipped to recognize patterns of misuse and able to more proactively respond to incidents of abuse. IT managers should understand enforcement expectations and procedural protocol to appropriately respond to suspected problems detected through firewall records and Internet usage reports.

Alternatively, human resource managers must grasp a certain level of technological background in order to understand monitoring capabilities. Each monitoring software system provides its own reporting systems containing various information such as web sites visited, duration of the visit, and emails sent and received from each end user. Therefore, it is important to educate human resource personnel on how to accurately review and interpret Internet usage reports. Human resource personnel should also understand firewalls and what type of information is prevented from being accessed and the data collected from these networks.

While human resource managers focus on acceptable Internet use policies to help curb incidents of abuse, they should also consider the utilization of reliable and valid psychological tests to screen out individuals with the propensity to abuse the Internet. For new hires, pre-employment screening measures can be used to highlight individuals who might later have a problem with Internet use. For current employees, diagnostic instruments can be utilized to detect the presence

and severity of Internet addiction among workers who show chronic and persistent patterns of online misuse. Such tests are currently in development and being validated through acceptable psychometric testing to establish reasonable norms, and thus have predictive value (contact Stephen Silver at Walden Testing at www.waldentesting.com for more information).

Ultimately, a cohesive relationship between these human resource personnel and Internet access managers will enable norms to be developed that differentiate normal from abusive patterns of employee Internet use within your firm. This information enables managers to swiftly respond to problems and reduce the incidence of abuse.

6. **Train managers in early detection of employee Internet abuse problems to aid in prevention.**

Early detection of problems reduces your firm's risk that employee Internet abuse will occur. Therefore, as more companies in industries from engineering to journalism are venturing online every day, it is important for managers to learn the early warning signs that differentiate healthy from abusive patterns of Internet use among employees.

1. Decrease in productivity – A sudden drop in work productivity is a warning sign that a previously industrious employee is hooked on the Internet. While many factors can contribute to a worker's diminished capacity to get the job done,

companies that recently adopted the Internet should be especially sensitive to the possibility that output may be sagging because workers have discovered the Internet's interactive applications that can hook anyone quickly. Workers likewise should know that if they're not producing as much, those fun new games and chat rooms may be getting in the way.

2. Increase in mistakes - Most workers getting hooked on the Internet tend to shift back and forth rapidly between legitimate work and interactive Net play. This makes it more difficult to concentrate on work details, especially when they're spending a lot of time in playing interactive games or talking in chat rooms, where little care is given to correct grammar, spelling, punctuation, or even logical thought patterns. Anything goes on the Internet, but not so with work details. An unaware manager may assume wrongly that a sudden influx in employee error is being caused by stress at home, when it's really triggered by bad habits cultivated on the Net.

3. Less interaction with co-workers – Employees spending greater time online may ignore all other social activity because of the relationships they're developing over the Internet. Look for once sociable employees who suddenly shun all coffee break chatter or friendly morning greetings, or turn down invitations for shared lunches or after-hours socializing in favor of sticking with their chat-room regulars.

4. Startled looks when approached at their stations - If the employee enjoys relative privacy during his computer usage, notice how he responds when approached unaware. Many workers hop in their chairs, shift their bodies, or quickly type a command to change what's on their screens. If you notice employees who become secretive about online activities, it may indicate that they are using it for fun rather than business.

5. Less tolerant of workplace conditions - That once agreeable employee may suddenly balk at requests to work overtime and in staff meetings mounts vehement protests about longstanding company policies and procedures. There could be a natural explanation - chat room regulars in the workplace love to complain about their respective bosses and work conditions. The complaints may trigger action or at least a more sullen and withdrawn demeanor.

6. Excessive fatigue – Employees work extra hours to compensate for their Internet activities and often get exhausted by the effort. Employees find that they're tired all the time at work, not because their employer gave them more to do, but rather that they've given themselves more activities to keep up with in the form of personal Internet usage.

When confronted with cases of overt Internet abuse, many managers quickly react with job suspensions or dismissals. While these actions put an end to an employee's abuse of the Internet, they generate hidden costs for the employer such as increased

turnover rates and recruitment and retraining expenses. These actions also create a climate of fear, distrust, and resentment in the workplace that will undermine productivity and cooperation among those workers who are using their Internet accounts properly. Therefore, it is vital for your firm to develop a comprehensive plan to effectively handle critical incidents of employee Internet abuse.

7. **Analyze cost-benefit of employee termination for critical incidents versus rehabilitation to reduce job turnover and recruitment costs.**

   How exactly will management respond to the employee? What steps should be employed? Who should confront the employee – the IT manager who first notices the abuse or the HR manager? If it is a first offense, is it possible to simply reallocate Internet access for the employee as a means to remedy the situation? How will the firm ensure employee objectivity to prevent an IT supervisor from being more lenient with friends about their Internet use during work hours? While corporate Internet use policies guide the general nature of how violations and incidents of abuse may be handled, many questions still remain. Management must therefore develop a step-by-step strategy to handle critical incidences of employee Internet abuse to ensure fair and appropriate treatment of the situation. Some helpful guidelines in your strategic development are:

   1. Construct detailed record forms and reporting methods.
   2. Decide who will approach employee about abuse.

3. Decide how to approach employee (e.g., through email, a formal report, or a personal meeting).
4. Determine the information necessary to present to employee.
5. Determine how work history, length of employment, and job status will influence action taken against employee for a violation.
6. Understand the implications of Internet addiction in the workplace.

Internet Addiction in the Workplace - With the increase in Internet use within the corporate environment, there is a new threat to employers –the threat of litigation due to the mistreatment of an employee suffering from a condition appropriately labeled "Internet Addiction." To those who use the Internet for work purposes only (and even to those who sometimes escape on the 'net to unwind while at work), a condition called Internet addiction may seem a little far-fetched. However, for those people who have lost their jobs, ruined their marriages, or alienated themselves from their friends in order to spend "just 5 more minutes" on the Internet, Internet addiction is a very real, and very frightening, condition.

An employer 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 imposing "zero tolerance" policies that alienate employees and leave the employer susceptible to litigation. As I previously mentioned, the problem then becomes a lack of information about how to successfully create and implement an

Internet use policy that incorporates education and training as well as outlining a plan for fair and equitable enforcement.

There is good news and there is bad news as employers struggle to maintain productivity and keep employee morale high. The bad news is that there is still very little information available about Internet addiction and its toll on the personal and professional lives of its victims. For those who suffer from Internet addiction, it can be a very lonely and painful process to try to break free of the power the Internet has over them. Employers are also faced with a lack of information as they attempt to deal with a new, easily misunderstood condition. However, resources for those suffering from Internet addiction (and their employers) are becoming more readily available as more experts realize that this is a problem that can not be ignored.

The good news for employers is that implementing an Internet policy that incorporates appropriate measures for assessing Internet abuse and taking suitable action is not as difficult a task as it may seem. In fact, the solution is surprisingly straightforward. It is essential to understand that creating fair corporate policies does not replace the need for professional help if an employee suffers from a mental health condition.

In a similar manner as alcoholism or drug dependence are handled in the workplace, employers may wish to rehabilitate rather than terminate the employee. So before taking any direct action, employers should consider a referral to the firm's Employee Assistance Provider to assess the employee for the presence of an underlying addiction to the Internet. Employers must consider the costs involved in such rehabilitation efforts and they must also consider the legal liability of terminating an employee who suffers from Internet addiction. Under the Americans with Disability Act, former workers have sued an employer for wrongful termination claiming that they suffer from a mental disorder and often hold the company responsible for providing access to the "digital drug." While such a claim may seem frivolous and even ludicrous to employers, more and more cases are being seen in court each year. While such cases are frequently dismissed, the risks are clear for employers as the psychiatric field moves closer and closer to classifying Internet addiction as a medically valid disorder, forcing employers to exercise caution about how to address this condition in the workplace. In fact, in the not so distant future**,** Risk Management Programs on Internet addiction may be encouraged and even initiated by workmen's compensation carriers and self-insurers to keep costs down as the incidence rates of the disorder go up.

SUMMARY

Employee Internet costs billions of dollars in lost productivity, lost goodwill, and lost potential sales. Therefore, corporations must employ effective Internet use

management strategies that range from policy development, employee monitoring, to training seminars. Collectively, these efforts will enhance employees' interdependency with workplace technologies and enable you to successfully integrate the Internet within your organization.

For more information on our management training and seminars, please contact the Center for Online Addiction, on the web at

www.netaddiction.com