WHO'S WATCHING THE WATCHERS?

A CEO'S GUIDE TO EMPLOYEE INTERNET MANAGEMENT

DAVID A. FERTELL

WHO'S WATCHING THE WATCHERS?

WHO'S WATCHING THE WATCHERS?

A CEO's Guide to Employee Internet Management

DAVID A. FERTELL
CEO, Pearl Software, Inc.

Pearl Software Web site: http://www.pearlsoftware.com

ISBN: 0-9654232-9-8

For Judy,
always there for others.

Contents

Introduction

Undoubtedly, you are reading this because you're a responsible steward of your corporation and you take seriously your fiduciary and moral obligations to yourself, to other company stakeholders and to your employees. You're also probably concerned that the all-important, can't-do-business-without-it Internet that you provide your employees is becoming your worst nightmare. How do you know people aren't wasting time surfing the Web for vacation deals or haven't strengthened their gambling habit with real-time online gaming complete with simultaneous built-in chatting? How do you know that the corporate reputation you have toiled to build and strive every day to maintain isn't being carelessly sullied by someone on your team that just won't drink the corporate Kool-Aid? What are people doing with your laptops and smart phones when they're out of the office? What's going on in the office at night after you leave? What's the cleaning crew up to

on your computers? You hear about countless creepy pedophiles on TV news shows. Are your computers being used to solicit children? Finally, how do you know the people you've entrusted to manage these issues are not the culprits in these very same misdeeds that will land you in legal hot water, waste resources and create a hostile work environment?

This book will help you answer these questions and help guide you through the issues that plague every business, small and large, when it realizes its Internet connection has become a vital component of its communications and marketing strategies. Though we will delve into some technical aspects surrounding the issues of Internet governance, this book is written by a CEO for executives with P&L responsibility. My early start was in the area of computer science and robotic imaging for large enterprises. However, much of my professional life has been on the operations side of business, frequently playing interpreter between IT and those that they serve. I've written this book because I realize you're probably not strongly versed in geek-speak and may not have a complete grasp on the technical realities that define the Internet. It is my goal to arm you with enough relevant information so that you can be comfortable asking your managers pointed questions and have a degree of confidence that the answers you get are consistent with your expectations.

WHO'S WATCHING THE WATCHERS?

Part One

What is the Internet?

We've heard that a million monkeys at a million keyboards could produce the complete works of Shakespeare; now, thanks to the Internet, we know that is not true.

-Robert Wilensky

Though used synonymously by many, the Internet and the Web do not mean the same thing. The Internet is a constantly growing group of computers networked together by communications lines. These computers can be high powered servers or run-of-the-mill laptops. The Internet was created in the 1960s as a US Government endeavor to connect various computer systems in a fault-tolerant manner. The goal was to ensure that any single point of failure to a computer or communications link on the network would not disrupt the communications of all other computers on the network. Unlike telephones, computers communicate through ports that open to the Internet for data exchange. These ports are the gateways by which computers send and receive data. It is these same necessary communication ports that leave computers vulnerable to viruses, hijacking, and identity and file theft.

Functionally, the Internet is now used by over a billion peo-

ple, from commercial and educational institutions to individual consumers. The US comprises over 225 million Internet users[1]. Accessing the Internet is easy. All that is needed is a computer or portable device like a laptop or smart phone and a communications link like a telephone connection, cable "broadband" connection or wireless access connection freely available at your local Starbucks or pay-for-use at an Airport or now, the entire city of Philadelphia.

The Internet provides a host of ways of interacting in a global way – inexpensively and comprehensively. Interaction occurs through chat rooms, instant messaging sessions, social media Web sites, the World Wide Web, electronic mail and file transfers. The Internet is an umbrella term that comprises these various means of communicating. It makes sense to spend a few moments discussing each of these separate segments of the Internet as each has a place in the workplace and so each has unique management issues associated with it.

- Chat -

Chat, or more formally Internet Relay Chat, differs from Instant Messaging. Chat makes it possible for multiple users of the Internet to converse with each other in real time by typing messages for others to see. It is the modern day equivalent of the CB Radio but instead of truckers avoiding police traps, users find topical chat rooms in which to engage an audience of participants. Posted topics can be positive such as health discussions, education and age based areas. They can also be garish including cyber sex, illegal purchases and deviancies. Users

1. Nielsen Net Ratings, 2009

may say - and do - things they normally wouldn't say - and do - in public because of the anonymity chat rooms provide. This anonymity makes chat rooms a potent area for pedophiles to troll for young children. And, as the Assistant District Attorney for New York County stated in a Cyber Crimes forum I attended in October of 2000, "Guess where these pedophiles access the Internet? From work. Using your [corporate] computers."

In order to access chat rooms, users need to connect to the same Internet Relay Chat server. To connect to an Internet Relay Chat server, users need a software program like mIRC or any of the dozen freely available packages you can download from software shareware sites. Although many of these software programs have been usurped of late by the overwhelming popularity of chatting within social networking sites, the Internet Relay Chat network remains alive and continues to function as the chat backbone built into many interactive sites.

- Instant Messaging -

Instant Messaging, or IM, differs from Chat in that conversations occur between two users who know each other's "screen name". This implies that the users either know each other in the real world or have found each other online either through a directory of screen names or potentially in a public chat room or on a social networking site. Think of IM as the text version of a telephone system. The IM system will alert a user when someone on their list of screen names is present on the IM system. The two most popular IM programs are AOL's AIM and Microsoft's Windows Messenger. Yahoo! and

Google also provide the popular IM programs Yahoo! IM and Google Talk. All are free. Microsoft's product is built into Windows and is available immediately to users. There are also corporate versions of IM that contain the conversation to inter-company users only. Novell's GroupWise IM is one such example. IM can be an efficient way for employees to communicate. It is instantaneous, cuts through the clutter of e-mail and avoids telephone voicemail. The downside is that incoming IM messages can be disruptive to an employee's train of thought. IM'ing can easily become water-cooler conversation without the participants being seen at the water-cooler. Like the telephone, IM can easily be abused for personal use and can be an information security hazard as users may be aware that there is no record or store of their IM conversations.

- News Groups -

Newsgroups are the electronic version of a bulletin board. Users use programs like Microsoft Outlook to access News Servers and post questions to topical newsgroups, for instance gardeners may post to rec.gardens. Over time, other users will answer the question. The original poster can respond or ask for clarification to their original post. The entire conversation is stored as a "thread" for others with a similar interest to read. Newsgroups are typically self policing so if incorrect information is provided in response to a question, others in the group will pounce on the incorrect post with corrections. There is little tolerance in newsgroups for advertising, providing misleading information or posting information that has nothing to

do with the topic of the newsgroup. Purists feel that the News Groups are one of the last segments of the Internet that have not been debased by advertisers. In its day, newsgroups were an excellent means to freely and quickly access a circle of experts in nearly any subject matter. Topics ranged from asking how to fix a dishwasher in misc.consumers.house or how to print mailing labels in microsoft.public.word to advice on corporate tax issues in misc.taxes. Newsgroups also exist that provide access to illegal materials like downloading pirated software, movies, video games and child pornography. In addition to being illegal and making you susceptible to copyright infringement, these downloads may contain viruses or "trojans" that provide external access to the computers and then, by extension, the network on which the materials have been downloaded. It is generally agreed that newsgroups are a dying segment, replaced by the more searchable Google Groups, interactive Web sites and hosted forums. Newsgroup servers are typically maintained by ISPs, many of which have dropped support for them given the exodus of legal activity coupled with the unabated illegal and anonymous distribution of massive quantities of pornography and pirated media. It's hard to dismantle something as decentralized as newsgroups and as long as two servers agree to share the newsgroup protocol, newsgroups will continue on for the foreseeable future.

- The Web -

WWW, the World Wide Web, Web site, home page, URL, Web Log (Blog) – you probably know that the Web is a great

way to do research, find deals on travel, check stock quotes and avoid going to the mall. Like the other segments of the Internet, users use a specialized program - a Web Browser - to connect to specialized servers - Web Servers - that contain Web pages. In 1996 when the Internet was becoming a commercially viable entity, Netscape was the Web Browser of choice. Though late to the game, Microsoft soon dominated the market with their freely available and built-in Internet Explorer. Netscape has become a fond remembrance. Firefox, Google Chrome and Apple's Safari are additional Web Browsers that are freely available. All are variations on a theme; popular due to some unique features but also because they give Microsoft-bashers something new to tout. Microsoft then releases a new version of Internet Explorer containing many of the niceties offered by the other browsers and the cycle continues. In the end, they all display web content. Many misconceptions exist regarding the Web. As mentioned in the introduction, many use the term Web and Internet interchangeably but, as I described, the Web is really one aspect of the Internet. The other misconception is pornography. Yes it's out there in droves. Yes it has no place in the workplace. Yes it's easily and freely accessible. When we started Pearl Software in 1996, our Internet Monitoring and Control software, Cyber Snoop, received an inordinate amount of free press from all the major TV networks and popular press because easy access to pornography on the Web was a new, sexy and titillating - pardon the pun - topic which got viewers' attention. The truth of the matter is that people waste much more time shopping and socializing on-line

while at work than those brave or stupid enough to access pornography from their cubicle; more on this later.

The Web has become ubiquitous as the Web protocol has broadened in scope (Web 2.0) and Web Browsers have evolved to handle new requirements. This has caused lines to blur. For example, applications can be written to provide a chat or IM session within a Web Browser. Newsgroup questions can be posted through a Web site. Files can be uploaded to photography sites and e-mail can be sent through a mail portal, all accessed through a Web Browser and all driven by Web Servers. The versatility of the Web brings us to our next topic, social networking.

- Web 2.0 and Social Networking -

Social networking Web sites focus on bringing people together to interact with each other through chat rooms and postings and encourage users to share personal information and ideas via personal Web pages. Unlike chat and IM which are temporary in nature, social networking sites are temporal, maintaining a history of communications, postings, and comments made at different times by different users. Chatting is also available within the social networking sites. Social networking Web sites have dramatically changed the way users interact with the Web. In the past, the Web was somewhat passive in nature, providing content to users that visit a Web page. Web 2.0 and social networking sites like MySpace, YouTube, Facebook and Twitter enable and facilitate interaction and collaboration. One's utilization of these resources determines how the sites

are perceived. From a marketer's perspective, advertisements reach millions of people closely aligned to a product's positioning at a nominal cost. On the other hand, from an employee management perspective, social networking can pull your employees into a time consuming vortex of the inane where work hours are spent commenting on such things as kitten videos and posting announcements of seemingly insignificant substance.

- File Transfers -

File transfers occur when users copy electronic files from one location to another. Files can be digital music, videos, spread sheets, drawings or just about anything else that can be digitized and stored on a computer. Users copy files to and from specialized servers or other workstations. Apple's iTunes is a popular file transfer server. Users access the iTunes music store with a specialized program, purchase songs or entire CD's that they then transfer or download to their computers or iPhones. The infamous Kazaa is an example of a "peer-to-peer" file transfer system. With peer-to-peer programs, users turn their computers into file servers in order for others to access their stored digital music, movies, porn, etc. In return, users access other participant's stored digital music, movies, porn, etc. You can quickly see why the music industry ferociously went after Kazaa to kill this free exchange of copyrighted content.

In the days before the Internet, people feared floppy disks as the means in which secure files left the office and viruses entered the corporate network. The same concerns exist with file

transfers with the added fear that file transfers are instantaneous and difficult to trace.

- Electronic Mail -

E-mail enables users to efficiently, inexpensively and effectively communicate globally by transmitting notes and electronic files stored on disk. Messages are sent and received by users using a specialized e-mail program like Microsoft's built-in Outlook Express. Messages are sent to a recipient by specifying the recipient's e-mail address. You can send the same message to several users at once. This is called "broadcasting". Broadcasting messages to a large number of users that have no direct relationship to the sender is called "spamming". Sent messages are stored in electronic mailboxes on specialized Mail Servers until the recipient retrieves them. The Mail Server may be resident in your company, (e.g. Microsoft Exchange Server) or may be provided by your Internet Service Provider. Once the message is received, it can be stored locally on the user's machine, remotely on the Mail Server or in both locations.

In the mid to late '90s, unsolicited e-mail was responded to with everything from a polite "please remove me from your e-mail list" to a threatening or hostile "flaming" reply. Spammers have gained so much inertia that the battle for pure e-mail has long been lost. Similar to the way Web search engines "spider" or "crawl" Web sites in order to index and categorize content, spammers harvest e-mail addresses from Web sites, news groups and purchase lists from list providers such as trade show organizers and free trade publications. Spammers

will typically entice users to purchase products, visit porn sites or try to fool users into financial scams.

- Trojans, Viruses and Spyware -

Programs that compromise electronic data or disable the security of computers are not new however their prevalence has been exacerbated by the connectivity that the Internet provides. Trojans are malicious software programs that pretend to be something useful like an image file or desktop screen saver. When a user executes the program, it overtly does what one expects while covertly carrying out the program's real objectives such as modifying or deleting files, changing the configuration of the computer or using the computer to attack other machines on your network.

Computer viruses, unlike trojans, replicate themselves across systems and start themselves typically by replacing existing programs with a virus-infected copy. Like trojans, viruses can be destructive or merely annoying.

Spyware programs surreptitiously monitor user activity for the benefit of a third party. For example, a spyware program may collect a user's online shopping habits and send the information over the Internet to an advertising agency. Malicious spyware may capture user login information or credit card information typed at the keyboard. Spyware programs are installed by deception, typically by attaching to a piece of desirable shareware software or by tricking a user to do something that installs the software without realizing it.

Why do programmers take the time to create trojans,

viruses, and spyware? Many do it for the same reason people put toilet paper in trees on mischief night - it's mischievous and disruptive. Others do it for bragging rights, to distribute political messages or for financial gain from identity theft. Their effects are at the least annoying and in the worst case extremely costly when data is lost or security compromised.

Part Two

What's the Downside?

I myself am made entirely of flaws, stitched together with good intentions.

-Augusten Burroughs

Competitive enterprises exist to prosper and therefore must operate with efficiency. Corporate stakeholders are tasked to keep labor and material costs low, justify investment in capital and variable expenses and protect the enterprise from contingent and potentially crippling liabilities derived, for the most part, out of negligence (lawsuits, product recalls, negative publicity, physical and IT infrastructure damage and disrepair). We continue to hear that productivity gains are paramount to controlling inflation and keeping manufactured goods competitive in world markets. In order to control costs and maintain your company's competitive advantage, it is incumbent upon Management to identify and rid the corporation of malingerers and identify those that are less productive. Functional units need to keep their house in order to reduce the probability of extraneous costs. Operational efficiency takes on new meaning in times of economic contraction. Add the con-

stant spate of corporate governance and consumer privacy legislation and you have a recipe that only disturbs the delicate balance managers must deal with as they attempt to meet requirements without destroying employee morale. In considering the various segments of the Internet, clear thought needs to be given to productivity, liability and security.

- Productivity -

American employees of all ages and income brackets are growing increasingly unhappy with their jobs. Less than half of all Americans today say they are satisfied with their jobs, an all time low and down from an already dismal 60 percent in 1995. But among those who say they are content, only 14 percent say they are "very satisfied."[2] A major source of employee dissatisfaction stems from American employees feeling overworked. The United States now surpasses workaholic Japan in average hours worked. According to a widely referenced report from the International Labor Organization, Americans who are employed worked an average of 1,979 hours (49 1/2 weeks) in 2000, up over 36 hours from 1990. This was 137 hours (3 1/2 weeks) more than Japanese workers, 260 hours (6 1/2 weeks) more than British workers and 499 hours (12 1/2 weeks) more than German workers.

Why has overwork been so persistent? One reason is that it is generally more profitable for firms to employ a small work force for long hours. The labor costs are lower, the benefits costs are lower and employers can be more selective about whom they hire. Technologies and modern "conveniences"

2. Conference Board Report, 2010

like wireless access points, laptops, smart phones, voice and electronic mail and cheap bandwidth worsen the issue. Each of these innovations has contributed to creating what I like to call "the always-on employee", further blurring the traditional and perhaps once-sacred boundary of work and personal time. As a result, your employees feel warranted with the self-proclaimed right to managing their own time while at work. Since the enterprise unabashedly reaches into the employee's personal time, the employee feels justified in extending his or her personal life into the enterprise. Activities like online shopping, vacation planning, social networking, personal e-mail and IM'ing are considered quid pro quo by the employee. This is supported by a national survey that our company conducted which reveled that nearly one quarter of employees with online access at work said their company has a formal policy that does not allow personal Internet use. Yet, one third of these employees volunteered that they knowingly violate their company's Internet use policy prohibiting shopping at work.

So how are employees managing their on-line time when they aren't working? Social networking sites, such as Facebook and Twitter, are the most-used sites for wasting time at work. Seventy-seven percent of employees with access to Facebook at work logged into their accounts at least once per day during work hours. In a close second place, employees play games online when they should be working. Personal e-mail is the third most prevalent employee time waster. Employees visit web portals that aggregate information, such as news, sports, entertainment, humor, and more, as the fourth biggest waste of

time. The fifth way employees most commonly waste time is by instant messaging. Playing online fantasy football, viewing pornography, watching videos, using search engines, and shopping online round out the top 10 ways employees waste time on the internet at work.[3]

Who in your organization is managing this 12.5% hit to productivity and, consequently, your higher labor costs? Anyone with P&L responsibility that is used to working near the margins knows this is a huge number. When this book was originally released in 2006, the mix of activities on which employees wasted time was a bit different but the bottom line number was nearly the same; about five hours wasted per employee per week. From then until this writing we have seen a tremendous decrease in the availability of US jobs. Yet consistent with our study many years ago, many employees don't sweat the fact that they waste time on the Internet during business hours.

- Liability-

Managing liabilities is part of the cost of doing business; Extraordinary liabilities such as hostile workplace suits, negative public relations and the negligent disclosure of personally identifiable information can go a long way towards sinking your business. So what new liabilities have you brought upon yourself since your company decided to connect to the 'Net?

The term "hostile workplace" conjures up images of screaming supervisors publically berating their employees. All that has changed: Sally walks past Fred's cubicle and Fred has a

3. Nucleus Research, 2009

clip from the latest Girls Gone Wild video running on his screen. Then Fred, who has always had a weird sense of humor, e-mail broadcasts an off-color joke that he thinks is a riot. Most of the recipients think Fred's joke is marginally funny, if that, but Sally, who is miserable to begin with, is now sent over the edge and decides to retire by slapping a hostile workplace lawsuit on you. Sound like an exaggeration? The Internet has broadened the definition of sexual harassment. Edward Jones, one of the world's biggest brokerage firms, issued a memo demanding its workers disclose if they sent pornography or off-color jokes over the brokerage's e-mail system. Forty-one employees who confessed were disciplined, but 19 who failed to come forward were fired. Dow Chemical fired 24 employees and disciplined hundreds of others for storing and sending sexual or violent images on the company's computers. Twelve librarians in Minneapolis filed a complaint saying that library visitors were downloading porn, including bestiality and child molestation, and leaving it for librarians and patrons to see. The Equal Employment Opportunity Commission ruled against the library in favor of the librarians saying that the library "did subject the charging party to [a] sexually hostile work environment." Losing these lawsuits can be very costly. Recommended restitution for the librarians was $900,000. Chevron agreed to a $2.2 million settlement for a lawsuit brought against it for e-mails offending women. According to EEOC statistics, American businesses pay in excess of $50 million a year in judgments relating to sexual harassment charges. This bill doesn't include monetary benefits obtained through litigation nor does

it include legal fees and the totally unproductive time of defending these lawsuits. And this doesn't just apply to blue chip companies. According to AIG insurance, the EEOC is fervently pursuing small to medium sized businesses with average awards on the order of $1 million. One customer of our Employee Internet Management software implemented our solution in her business because she suspected employees were wasting too much time on the Web and sending an inordinate amount of personal e-mail. Not only did her instincts prove correct, she also found one employee who was starting her own Internet adult Web site – while at work! While on the company dime, this employee was developing her Web site including downloading porn to post on her Web site and creating lurid sex stories for her potential customers. Talk about a productivity hit combined with a potential hostile workplace claim – yes, men filed 16% of the charges of sexual harassment in 2011[4]. The offending woman was summarily dismissed from the customer's business before the situation worsened.

Public image and how customers perceive your company is crucial to any business' success. Goodwill is an intangible asset that adds significant value to the equity in your company. One need only think of Enron to realize the host of issues beyond the Internet that can negatively affect a company's image forcing the company to fold or spend an inordinate amount of money to rebuild the way people perceive it. But the Internet brings a new dimension to potential PR nightmares. In one case, an associate editor for Ladies Home Journal decided to publish work details in her then anonymous and very popular

4. EEOC Web site, http://www.eeoc.gov

Web Log (Blog), Jolie in NYC. She wrote about lavish perks given only to executives, detailed a "beauty hierarchy" within the organization and named names of favored employees. When the editor was outed as the author of the blog, her criticism of her employer was an embarrassment to Ladies Home Journal with its customers, agents and competitors.

One of our company's service industry customers is wisely concerned that his customer billable hours are correct and verifiable. Our customer feels that his credibility would be destroyed if a disgruntled employee were to lead customers to believe they were being charged for time his employees are spending on personal Internet use. Whether you're a small or large organization, if you're a company that spends time or money building an image, nothing can tarnish that image and erase the value of those advertising dollars quicker than being associated with child porn. One of our multinational manufacturing customers quickly dismissed an employee for intentionally downloading child porn and reported the individual to authorities. Our customer not only realized that they had to circle the wagons to protect their image but had a legal and moral responsibility to the community in which the offender resides.

Issues abound protecting privacy on the 'Net. In 2005, Bank of America and Wachovia notified over 100,000 customers that their accounts and personal identity information were at risk because of a scheme by bank employees who allegedly sold the data to a middleman who then brokered it to collection agencies. In February of the same year, a Florida statistician working for the Palm Beach Health Department inadvertently sent a

broadcast e-mail containing a highly confidential list of the names and addresses of 4,500 Palm Beach County residents with AIDS and 2,000 others who were HIV positive. The e-mail was sent to more than 800 county health department employees. Hospitals, financial institutions, and retailers are all highly
regulated due to the high volumes of confidential data each organization manages. For example, a regional-healthcare provider must ensure the protection of patients' Personal Health Information (PHI), as required by the federal Health Insurance Portability and Accountability Act (HIPAA). Banks and financial institutions must protect customers' confidential Personally Identifiable Information (PII). Internally, enterprises need to monitor adherence to corporate governance issues (i.e., employee handbook issues like harassment) that might also put the company at legal risk.

- Security -

One of our quickest success stories was a customer who kept losing competitive bids for contracts based on price. Fearing an inside leak, the customer installed our Employee Internet Management software and quickly discovered that one of his employees was being compensated for e-mailing confidential bid details to a major competitor. Another of our customers, a large hospital, was inundated with viruses – the digital sort. Computer viruses were frequently plaguing its systems, rendering them useless at times. Antivirus and antispyware software tools would successfully clean up defiled systems, but only af-

ter they wreaked havoc for users and the IT staff. The hospital installed our solution in order to identify usage patterns and determine and block likely Web sites and users that were the root cause of their issues. The hospital's primary concern was that an employee could inadvertently download a trojan, making an infected computer a gateway to external hackers and providing unauthorized access to patient information.

Industrial espionage has always been a security concern. Cyber crime also involves the buying and selling of intellectual property—a company's new product designs, proprietary financial information and confidential memos. An increasing percentage of valuable corporate data is being electronically siphoned and sold to the competition. As the Wall Street Journal reported, the biggest threats to information security often don't come from hackers. They come from a company's own employees. The insider threat and internal surrogates are the focus of the Department of Homeland Security's National Cyber Security Division. Malicious acts by disgruntled employees, viruses picked up in e-mail spam or from seemingly innocuous Web sites and corporate espionage are all areas that require conscientious governance. Security risks may also be inadvertent. Take Phishing for example. Here, a phony Web site dupes unsuspecting users by publishing Web pages with the look and feel of the authentic Web site it intends to mimic. Suppose your accounts payable clerk receives an e-mail from what appears to be your company's bank. She responds to the e-mail which asks her to click on a Web link to update her e-mail address. As expected, her Web browser opens and she is taken to

a site that has been built with the exact look and feel of your bank's Web site. As usual, the clerk is prompted to enter her secure user name and password. After entering her credentials, nothing visually happens. However, something very damaging does happen; The Phishing site has captured her credentials and the authors of the phony site can now access your account at the authentic bank Web site. The Internet security team at CERT believes that most insider crimes go unreported not because they are handled internally, but because they are never discovered in the first place. The bottom line is if you are in business and your employees use computers, you need to protect your data against unauthorized access – both internally and external – and the best methods for doing so are always a balance between technology and personnel management.

Part Three

How do I Deal with This?

You can observe a lot just by watching.
-Yogi Berra

As we've seen, gone unchecked, the Internet can work against your executive obligations by sapping productivity, increasing your exposure to negligence and creating a corporate security hole. The most expedient solution to this problem is to pull the plug – get rid of the Internet. This is also the most impractical solution as taking yourself off the grid makes it more difficult for customers to find and communicate with you. This will help your competition more than it will help you.

In 1996 I was taking a course on methods for developing a corporate Web site. My programming background came into play as this was a time before any tools existed that magically transformed a simple word processing document into nicely formatted and automatically published Web pages. During a break in the session, the professor explained to us that he volunteered his time on weekends teaching people how to use the

Internet. Again, this was 1996 and most people didn't know what e-mail was and had no concept of Web sites. During this discussion, the professor recounted a story about a time when he had a pack of Boy Scouts in the lab and was teaching them the concept of Web searches. AltaVista was the Google of the day. The professor amusingly described that in ten minutes, all the screens were filled with pictures of naked women – each Boy Scout educating his lab neighbor where to go to similarly fill the screen. From that story came the birth of Pearl Software. Our goal was to provide parents, teachers and business owners with a tool to monitor online behavior in order to manage that behavior. As parents of young children, our thought process was based on the notion that we watch our kids play outside with others. When they pick up a rock, push, talk to strangers or generally misbehave, we reprimand them in a manner that hopefully corrects their behavior. Our goal, as parents, is to protect them and to make sure they behave within the expectations and norms of their community. When children are very young, we are increasingly vigilant and less so as they develop into responsible adults. To me and my company's cofounder, the Internet was a virtual extension of the real world. In our eyes, the Internet was filled with promise but there were real dangers and real strangers with real bad intentions on the Internet and parents and educators had a need for computer tools that would enable them to remain ever vigilant.

The same pattern of thought is easily extended to the corporate enterprise (how many times have you said to yourself, "My employees are like children") but instead of parenting, you need

to manage and, in many ways, protect your employees. Since those early days of keeping the Boy Scouts out of trouble, a whole industry has been created around solving this problem. The vernacular is commonly referred to as Employee Internet Management (EIM) or Data Loss Prevention. Both fall under the general umbrella of Internet Security.

Soon after we began offering a monitoring solution, other company's came on the scene with products that focused on blocking access to pornography so readily available on the Web. These were Web Filtering programs as opposed to Internet Monitoring programs. To us, this seemed to be a myopic view of the problem. Filtering, by itself, is a great idea in theory but is an incomplete solution given the dynamic and rapidly changing nature of the Internet, not to mention the unaddressed issues relating to the interactive mediums like chat rooms and e-mail scams. Today, leading EIM solutions provide both monitoring and filtering capabilities in order to allow you to simultaneously manage your employees while thwarting deliberate or accidental access to inappropriate Internet content.

- Where do I Start? -

The first thing to understand is that there are three primary approaches to EIM; each has its upside and each has its downside. The first and most basic approach is a proxy or pass *through* solution. Here, a computer is placed at a choke point between your network and the Internet in order to view all traffic and apply go/no go rules based on Internet access policies you create. This approach is expedient because it requires a

single piece of hardware on your network. But with expediency comes consequence; the same single piece of hardware is also a single point of failure for your network communications. In addition, all traffic must flow through the proxy so bottlenecks are created. It's like deplaning after a long, full flight. Everyone must file through the same small door as the flight crew bids them farewell. You know there's got to be a better way. Comprehensiveness is also an issue. Bypassing the choke point is easy for computers with modems and mobile users typically connect directly to the Internet at home or from a wireless hotspot or through their mobile phone provider, completely circumventing the proxy server.

The second approach is a "sniffer" or pass *by* solution. This solution is based on the idea that all machines connected to a local network can see all the network traffic to and from all other machines on the same local network. Like the office mail room, employees can see everyone's mailbox but protocol dictates that employees only read the mail in their own mailbox. The same is true of your local area network. If the network traffic is not addressed to a machine, network protocol dictates that the machine's network connection ignore it. Sniffer computers, on the other hand, don't ignore traffic that is not addressed to it. The sniffer computer will read the traffic and determine if it violates Internet access policies that have been defined. If so, the activity is blocked by the sniffer posing as the intended recipient and telling the originator that the requested content is not available. This works well until the sniffer can't keep up with all the traffic. In essence, the rightful recipient of

the traffic may receive and respond to the requesting computer with the content before the sniffer can process and deny the transaction from proceeding. In addition, the sniffer computer has no idea what's going on with machines off the local area network. This doesn't only apply to mobile laptops, smart phones and telecommuters. In order to improve efficiency, most networks are comprised of multiple local area sub networks (subnets) so only traffic addressed to a computer on another subnet makes it to that other subnet. The sniffer solution then requires you to build a complicated array of sniffer computers - one on each subnet.

The third approach is a client-server solution. Here, a program or "agent" is securely installed on each machine and the program communicates with a central administration computer (server) in order to receive Internet access policies that have been designed for that specific user or machine. The workstation software is also responsible for logging Internet activity back to the central administration server for subsequent data analysis and reporting. The benefit of this approach is that it is highly secure with the monitoring and control function bound to the machines on which the software is installed. The monitoring and control polices follow the user, even if the user is mobile with his or her laptop or off the network in a remote office or teleworking environment. Another benefit is that there exists no single point of failure to cripple network communications. No policy misses are created as mentioned in the sniffer/pass by solution and since all of the monitoring and filtering work is distributed to the client computers, no bottle-

necks are created as described in the proxy/pass through solution. The downside is that each computer and mobile device must have software installed on it and many IT employees like to take the path of least resistance when it comes to deploying new solutions. Leading EIM solutions now alleviate this pain by providing automated mechanisms for installing software on devices across your network. The client-server approach continues to gain in popularity as the concept of "securing the endpoint" takes on new meaning as users continually become more mobile and more attached to their personal computing devices.

- Duty of Care -

Many years ago, the Philadelphia Inquirer interviewed one of our customers to create a news piece portraying Employee Internet Monitoring as the coming of "big brother." It was interesting how the journalist's thoughtful concerns for employee privacy issues were quickly quelled by the very people that were being monitored. The employees were clear that so long as they understood what was expected of them with regards to personal use of the Internet - the rules of the road - then they were fine with the company's policy to monitor their use. Potential customers frequently ask us if it's legal to monitor their employee's Internet access. The presumption being that the company owns the computers provided to the employee, the employee is on company time and the company may be held liable for illegal acts perpetrated by the employee using company resources while on company time. The Federal law agrees: The Federal Electronic Communications Privacy Act (ECPA)

affords employers the right to "monitor an employee's conversations if the monitoring occurs in the ordinary course of business or with the employee's implied consent."[5] However, as individual states vary in their privacy laws and their own versions of the Federal ECPA, as a course of practice we recommend that corporate council be consulted to render an opinion on specific privacy issues. For example, in Connecticut the law provides that "each employer who engages in any type of electronic monitoring shall give prior written notice to all employees who may be affected, informing them of the types of monitoring which may occur." The statute goes on to state that "[e]ach employer shall post, in a conspicuous place which is readily available for viewing by its employees, a notice of the types of electronic monitoring which the employer may engage in. Such posting shall constitute such prior written notice." In general, however, an employee that brings suit must show that he or she had a reasonable expectation of privacy in the communication at issue. As common sense dictates, most cases have allowed employers to monitor employee's use of the Internet.

For US Government agencies and their contractors, the Office of Management and Budget requires administrators to monitor employee Internet communications. In both the public and private sectors, management shoulder-shrugging and ignorance to their employees' Internet actions is not a defensible argument. Duty of Care requires that all reasonably practicable measures be taken to control risks against negligent practices in the workplace. As EIM tools are readily available, their lack of

5. Information Week, "The Privacy Lawyer: Monitoring Employees' Internet Communications: Big Brother Or Responsible Business?", June 2004

use does not hold up as a defense against libelous employee behavior.

- Consent -

Regardless of latitudes in the law, our company has always advised customers against monitoring employee Internet access by surreptitious means or methods. You need to monitor Internet access in a consistent manner and adopt a policy that works for your corporate culture. A formal Internet Acceptable Usage Policy (AUP) should be created and communicated to your entire workforce (a sample policy is available at www.pearlsoftware.com). Your AUP should include notice and consent language so that the employee is aware that if he or she uses company resources to access the Internet, the employee is aware of and consents to the company's review and monitoring of Internet communications as outlined in the policy. Your AUP should warn employees that if they make use of the Internet to transmit personal messages or documents, those items will be treated no differently than other employer documents. The AUP should state plainly that employees should not use the company provided Internet to send or to receive any messages or documents that they wish to remain private.

Your AUP should be part and parcel of your overall company handbook. Your policy should make it very clear that the company will treat Internet communications as any other business communication. This includes transmitting any defamatory, offensive or harassing messages. This language should be part of your overall harassment and non-discrimination poli-

cies. An employee's failure to comply with the company's AUP should have specific penalties for clear policy violations. These policies should be enforced consistently. Creating and communicating a clear AUP will go a long way towards avoiding inappropriate Internet usage and it will be less likely that you will face right-to-privacy litigation in the future.

Part Four

What am I Looking for, Specifically?

People want economy and they will pay any price to get it.

-Lee Iacocca

There are a host of affordable EIM solutions available today. The cost of a solution is usually based on product feature sets and the number of licenses required. Taken in the context of how much time is being wasted on personal use, return on investment is much less than the two or three year payback you might require on a capital equipment expenditure. How about a two or three day payback? A salaried employee earning $40,000 per year earns roughly $20.00 per hour. If employees are spending an hour a day on personal internet use, you can easily see your initial investment recouped. Though cost from an ROI perspective will most likely not be an issue, be sure you are comparing apples to apples in evaluating competing solutions. Some EIM providers charge a subscription on an annual basis. Others provide a one-time perpetual license fee. Some providers require Maintenance Agreements to be purchased for their products to continue to func-

tion. Others provide Maintenance Agreements as an option. In addition, feature sets vary widely among EIM providers so be certain to understand what capabilities are being offered by each solution. The remainder of this section highlights some of the key features to consider when evaluating an EIM solution. Included at the end of this book is a detailed criteria matrix your company can use when comparing competing solutions.

Leading EIM tools offer a combination of monitoring and filtering capabilities. Web Filtering is the method of blocking Web page access based on content classification techniques. Web Filtering is typically done either by contextual word analysis, flesh tone analysis, maintenance of a database of categorized Web sites or a combination of all three. Checking the context in which a word is used (e.g. sex as a verb versus sex as an adjective) and flesh tone analysis - looking for images that have flesh colors and thus a higher probability of nudity - provide the greatest incidence of false positives and thus tend to over-filter or over-block. The most prevalent and accurate form of Web Filtering is the maintenance of a database of categorized Web sites. A comprehensive and accurate list of unacceptable Web addresses is a powerful approach to Web Filtering. EIM companies build their databases by having their computers crawl the Web and apply custom logic to identify and categorize content. This is similar to how search engines like Google and Yahoo! crawl the Web for indexing purposes. A Web Filtering list should be created with a blended approach of category based content analysis - what is the topic of the site's pages - , link analysis - what sites lead to and from the site un-

der review - and domain analysis - who owns the site and what other sites fall under the same owner's purview. Each EIM provider creates its own rules for properly categorizing Web content. Because an artificial intelligence approach is not foolproof, a quality Web Filter will incorporate human site review in order to ensure proper evaluation and classification of sites that cannot be done in an automated fashion. The Web Filter database should be maintained by the EIM provider and frequent updates to the database automatically applied. When evaluating a Web Filter database, be leery of size claims. EIM providers may try to impress you with an excessive amount of Web site categories which you can purchase to configure your access rules and may boast of an inordinate number of Web sites included in their databases. For example, the pearlsoftware.com Web site has roughly 500 pages and can be categorized as a business-to-business Web site. Some EIM providers will count pearlsoftware.com as a single entry in their database because all rules that apply to the root Web site, pearlsoftware.com, also apply to all pages contained within the site (e.g. pearlsoftware.com/about/). Other EIM vendors may maintain each page in their database and thus boast a filtering database 500 times larger than their competitors. The 80-20 rule is a good rule of thumb to use when evaluating filtering capabilities: 80 percent of your employees will visit 20 percent of the most popular Web sites in each category. EIM providers will have the twenty percent covered and are battling at the edge to categorize less popular sites visited by fewer people.

As you know by now, the Web is only one aspect of the In-

ternet and so Web Filtering is only one aspect of managing employee access to the Internet. A complete EIM solution will also include in depth monitoring capabilities. Not only should you be able to prevent access to certain categories of Web sites, you should be able to discern habits regarding employee e-mail, chat, IM, blogging, Web 2.0 and file transfers. For those that are concerned with security compliance and identity theft, monitoring software is more appropriate. Compliance and Security Officers are more concerned with leaked information rather than inbound communications being blocked. Monitoring software allows your employees to send files or e-mail, for example, and then captures data from these transmissions and provides reports of Internet activity. A complete EIM solution will allow you to recover the text of these e-communications and set audit flags that are triggered when certain risk criteria are met. In-depth monitoring solutions will not only monitor the content of e-mail but will also audit and control the real time communications of e-mail attachments like Word documents and Excel spread sheets. Suppose you are concerned with the potential leak of financial data from someone in your accounting department. It is not sufficient to monitor only the content of an e-mail message body for potential infractions while ignoring the spreadsheet that is attached to the e-mail.

A good EIM solution should provide a high level of flexibility. It should be flexible in terms of the environments in which it will work and it should be flexible in allowing you to set access privileges that are directly in line with your Internet Acceptable Use Policy. For instance, suppose your company cul-

ture and your AUP are such that you would like to permit unmonitored, online shopping on the Web during lunch hours and after 6 pm. Your EIM solution should include time controls that allow you to sync your AUP with your actual Internet access restrictions. You should also consider the environment in which your employees work today and you anticipate they may work in the future. Do you provide flexibility in allowing users to work from home? If you don't, chances are you eventually will. Telecommuting has been shown to lead to increased employee retention. Technologies such as inexpensive or free video communication and online collaboration tools are making possible remote work scenarios while maintaining the benefits of face-to-face communications. An AT&T survey of active telecommuters revealed that 36 percent would quit or find another home-based job if their employer decided they could no longer work at home. Telecommuting has been shown to lead to lower costs for the employee and for the employer. Do your sales people and executives take laptops on the road? If telecommuters and road warriors are part of your company's landscape, you will want the flexibility of having the same rules that govern Internet access while employees are at the office to apply while the employee is using your company's laptop on the road or at home. It is a common misconception that it is not possible to monitor and control Internet access of machines that are not on your network.

Another key requirement in your EIM evaluation is that Internet monitoring be reported by the employee's login name and not just on the machine name or ID that accessed the 'Net.

One of our customers told us of an employee of his that had a grudge against a co-worker. Knowing that the company was monitoring Internet access, the employee used his coworker's machine to access porn with the intent of getting his coworker fired. The devious employee had to log into his coworker's machine to access the Internet. Because our EIM solution logs the user's login name as well as the machine that was being used, the employee's plot backfired and it was the employee and not the coworker that was terminated. It is likely that if your company has a server, your IT group has set up a directory system. Simply put, a directory system allows IT administrators to define company-wide computer usage policies, deploy programs to many computers and manage user login accounts and credentials in a centrally organized database. IT administrators use directory systems to assemble users into groups that have common properties such as available network login hours or access to specified network resources like printers, databases and files. The two most common directory systems are Microsoft's Active Directory and Novell's eDirectory. A comprehensive EIM solution will integrate with your company's existing directory system in such a way that new user logins and groupings need not be created in order to define and implement Internet usage rules. For example, suppose you would like employees in your shipping department to have Web access to fedex.com and ups.com and not have access to e-mail, chat, IM, etc. For the sake of this example, your IT administrator has already set up a group called "Shipping Employees" in your company's directory system. The EIM solution should allow

you to apply your new Internet policy directly to the Shipping Employees group so that when employees in your shipping department login, the new policy is seamlessly applied.

The preceding example also demonstrates the need to customize the EIM solution's Internet access control lists. In the Shipping Employee example, an "Allow List" or "White List" needs to be defined as opposed to relying on the large database of blocked sites provided by the Web Filtering feature. Using Allow Lists, users or groups of users are confined to specific resources on the Internet. Be sure your EIM solution provides Allow Lists not only for Web access but also for e-mail, IM, news groups, etc. It is quite often that our customers want to restrict e-communications between employees and designated vendors or subcontractors. Nowhere is this more true than in call centers where telephone operators have access to other companies' costumer information while simultaneously having little management oversight and no allegiance to the company for which they act as subcontractor.

As an owner or manager of your business you already know how important it is to dot your "i's" and cross your "t's" before terminating an employee for misconduct. The more documentation you have, the more likely you will be to prevail should an ex-employee file a wrongful termination suit against you. It may be required that the data used as a basis for your decision to terminate an employee withstand a defense assessing that the data had been altered. The EIM solution that you deploy should include data verification mechanisms on captured and stored content that can withstand chain of custody require-

ments. A unique time-stamped event record should be generated for every Internet session that is attempted by an employee. This identifying record should include the Internet address or site, subject or title of the site, date and time of the transaction, the reason if a restriction occurred, the user name, machine name, physical machine address and a file signature (or fingerprint) on the logged event record. These unique identifiers improve the evidentiary integrity of each record and produce forensic quality data that can be used to support compliance auditing and investigative activities on specific employees.

Your EIM solution should also give you the flexibility to be as circumspect in your monitoring as you desire. For example, you may want to log all e-mail transactions including the e-mail's subject without actually providing details of actual content. Alternatively, you may want to have full access to the content of all communications including the ability to decode encoded file attachments. You may want the flexibility to receive only summary access to e-communication transactions and have full access to content on highly suspect transactions. In addition, there may be times when you would like to provide an employee with complete confidentially in certain communications. For example, an employee may need to communicate with her or his doctor or lawyer and you may want to extend the privileged and confidential nature of the communications through your own network.

In our early product releases back in the mid 1990s, we provided an extensive log of data which served as a complete audit trail of user Internet activity. We provided no reports; just raw

data. This would never fly today given the amount of data being captured and the sheer volume of users using our solutions within a single organization. A comprehensive reporting module is now a "must" with any EIM solution. The reporting module's purpose is to synthesize raw data and turn it into information and trends that can be easily understood and used to manage your employees. The amount of time and labor cost a user spends at sports related Web sites is an example of an informative report. The number of violations to your AUP is another. Reports should provide information graphically and numerically and should be able to be scheduled to be run and distributed automatically. Advanced features like report customization and distributed reporting can be beneficial. In large or growing organizations you may want to have managers run their own reports however you may want to limit your manager's visibility to data of only those employees for which they are responsible.

Total cost of ownership, or TCO, is something that is thrown about fairly regularly in the IT world. TCO refers to all the costs for selecting, purchasing, installing, maintaining and updating an application, piece of hardware or network device in your environment. The last thing your IT administrator wants is to baby-sit an EIM system and become your company's Internet police. Your EIM solution should be easy to configure, automatically maintain its list of Web Filters, update itself with new program patches and automatically generate and distribute reports to managers and key stakeholders. In addition, your solution should not be tied to a specific piece of hardware. For

instance, there are parasitic solutions in which you can plug in a basic Web Filter database to an existing network choke point like a firewall. Your network, for the most part, is a dynamic entity. It changes with changing requirements and performance expectations. When you tie your EIM solution to an existing network component, that component becomes rigid and more difficult to change or upgrade.

The EIM solution you select will undoubtedly be deployed and managed by your IT administrator. Many of the IT folks that evaluate our products will make the same joke, "This is great…so long as my boss can't see what I'm doing." Make sure you can see what they are doing! As stated previously, your Internet AUP should be applied clearly and consistently throughout your organization. As the principal of your organization, libelous activity rests with you – make sure you have visibility into everything – even what the watchers are up to.

Part Five

How Will This Change in the Future?

Where is the wisdom we have lost in knowledge? Where is the knowledge we have lost in information?

-T. S. Eliot

Internet evangelists speak of a day when your refrigerator will create its own shopping list and use the Internet to coordinate a pickup at your local grocery store; or the day when your car will use the Internet to check your PC calendar and automatically schedule your next maintenance check with the car dealer; or the day when you lease your extra computer CPU capacity to researches trying to solve problems that require massive computations. Whether or not these ideas fully materialize, it is true that the Internet and the way in which we use it are in a constant state of change. When we first started Pearl Software, there was no IM or broad band; phishing was spelled with an "f" and tweeting was for the birds. The sentiment of change on the Internet holds true today.

The Internet of today uses a communications language or protocol called Internet Protocol Version 4 (IPv4). There is a growing shortage of IPv4 addresses, which are needed by all

new machines and electronic devices added to the Internet. IPv4 supports 4.3 billion unique addresses. The next generation of the Internet Protocol, Version 6, (IPv6) supports enough addresses for each person alive today to have fifty octillion devices on the Internet[6],

Why does IPv6 matter? In addition to supporting more addresses, IPv6 will support more efficient routing of data and therefor higher "quality of service" (QOS) of data transmission. With higher QOS will come the increased adoption of technologies where high quality data transmission is required. Think of a leading surgeon in Philadelphia remotely operating on a patient in California where the quality of the remote video and correctness of commands that drive robotic actuators must be free from error. In a less daunting scenario, the same doctor checks the Internet to monitor a patient's vital signs which are displayed in real time over a secure Web site. Today, early adopters are sending telephone calls over the Internet – voice over IP or VOIP. Currently VOIP has the quality of a good mobile phone connection. With the availability of large amounts of bandwidth and guaranteed QOS, there will be no reason to maintain traditional telephone services when voice calls can be routed over your Internet connection. Next, combine the increased QOS with increased availability of wireless hotspots and we will see the emergence of mobile devices that will bypass today's cell phone networks enabling you to place VOIP calls over the Internet with computer mobile devices.

Coinciding with the explosion of PC use in the 1980's came the migration away from large central servers to one of distrib-

6. IPV6 supports 340,000,000,000,000,000,000,000,000,000,000,000,000,000 addresses.

uted computing. Today we have multiple devices - work pc, home pc, laptop, smart phone - and we want to have access to one copy of our data instead of trying to synchronize data across all devices. This requirement combined with increased mobility, increased connectivity, decreased storage costs and increased vigilance over data security has put server-centric computing back in vogue. We will continue to see the prevalence of server-centric computing architectures like Microsoft's Terminal Services and Citrix's access solutions. As when we first started our company, EIM solutions must adapt to this changing environment. EIM solutions must accommodate the mobile workforce. They must accommodate the use of multiple devices that access data. They must accommodate changing network architectures and they must accommodate the continually evolving technologies that are the very foundation of that which makes up the Internet.

And how do your employees fare in all of this? Ultimately we would like to see the always-on employee become more efficient. As EIM solutions become a knowledge base of company specific e-communications content, EIM solutions will have the capability of supplying sought after information to employees in a predictive manner. Tomorrows EIM should make it easier for employees to do their jobs and provide a self-monitoring component in order to help employees manage their own time in a responsible manner.

Part Six

What Should My Managers Know?

It is better to know some of the questions than all of the answers.

- James Thurber

Since you are the one exposed to risk, the following are some pointed questions that your managers should be able to answer with certainty.

* Are our employees aware that salacious e-mail sent from our company legally exposes our company?

* Can we easily and quickly identify inappropriate Internet use without calling in forensic specialists?

* Do our employees have an expectation of privacy in their Internet communications? Do we have an Internet AUP in place? Has it been communicated? Have employees signed an AUP acknowledgement form?

* Are our computers backed up in case a machine is

seized by law enforcement and we need to figure out what we are defending ourselves against?

* Do we allow personal e-mail usage? If so, to what extent and how do we quantify and audit this?

* Can we easily identify inappropriate use and excessive personal use of the Web and IM?

* What do we have codified in case we detect illegal activity by one of our employees? What law enforcement agency do we contact? Are our lawyers versed in these issues?

* Are our computers secure from unauthorized use after hours? Do our employees have login names and passwords? Do their computers secure themselves if left idle or if employees forgot to logout?

* What is our e-mail and monitoring data retention policy?

As your company begins to evaluate various EIM solutions, the selection criteria matrices that appear on the following pages will provide a guide in comparing product features, capabilities and costs.

- EIM Selection Criteria Matrices -

Protocol Filtering, Monitoring and Control	Product 1	Product 2	Product 3
Web			
FTP			
E-mail			
POP-3			
SMTP			
IMAP			
Exchange Mail			
Web-Mail			
Other			
News (NNTP)			
Chat			
Internet Relay Chat			
Web-Chat			
Blog Content			
IM			
AIM			
MSN Messenger			
Microsoft Messenger Service			
Yahoo!			
ICQ			
ICQ Lite			
Other			

Access Controls	Product 1	Product 2	Product 3
Web Filter Database			
Administrator Defined Allow/White Lists			
Administrator Defined Block/Black Lists			
Administrator Defined Keyword Controls			
Block Content Transmission			
Audit Content Transmission			
Real-time Document Decoding and Scanning			
PICs Rating System			
Access Rules tied to Active Directory Objects			
Time Controls Configured for:			
Controlled and Monitored Access			
Blocked and Monitored Access			
Free and Unmonitored Access			
Free and Monitored Access			

Reporting	Product 1	Product 2	Product 3
Enterprise-Class Report Manager			
Report Categories			
General Statistics			
Frequent Activity			
Time Online			
Cost Online			
User Statistics			
Machine Statistics			
Bandwidth Utilization			
Custom Reports			
Distributed Reporting Console			
Reports based on Active Directory Objects			
Reports based on Custom Groups			
Interactive Report Generation			
Automatic Report Distribution			
Reports Posted to Intranet			
Reports auto-Emailed to Managers			
Configurable Report Format (Word, PDF, etc.)			

Configuration	Product 1	Product 2	Product 3
Server-Centric User-Level Management			
Terminal Server			
Citrix Server			
Desktop Applications			
Published Applications			
Mobile Workforce Management			
Laptop Users			
Telecommuting Users			
Roaming Users			
System Maintenance			
Automatic Patch Management			
Automatic Installation			
Automatic Web Filter Database Update			
Data Maintenance			
Internet Content Restoration			
Privileged Data Protection			
Data Validation			
Data Archive			
Data Purge			
Database Integration			
Built-in Database			
SQL Server			
Oracle Server			
Active Directory Integration			
Novell User Detection			
Administration Console			
Administrator Level Logon			
User/Restricted Level Logon			

Cost	Product 1	Product 2	Product 3
Year 1			
License Cost			
Maintenance & Support			
Web Filter Database Subscription			
Other Costs			
Year 2			
License Cost			
Maintenance & Support			
Web Filter Database Subscription			
Other Costs			
Year 3			
License Cost			
Maintenance & Support			
Web Filter Database Subscription			
Other Costs			
Year 4			
License Cost			
Maintenance & Support			
Web Filter Database Subscription			
Other Costs			
Year 5			
License Cost			
Maintenance & Support			
Web Filter Database Subscription			
Other Costs			
Additional Hardware Costs			
Five Year Total Cost			

About the Author

David A. Fertell is the CEO and co-founder of Pearl Software, a leading Employee Internet Management software company. He was an active participant in the Clinton Administration's efforts to protect children from the dangers posed by the Internet. His professional background spans disciplines in robotic imaging, avionics design, manufacturing operations, enterprise information systems and entrepreneurial start-ups.

He has a master's degree in Electrical Engineering from the Georgia Institute of Technology and Executive Studies at Stanford Graduate School of Business.

David lives in Chester Springs, Pennsylvania with his wife and two children.