



828 West Taft Avenue
 Orange, CA 92865
 714-282-6111
 714-282-6117 Fax
www.8e6.com

Use or Abuse? Why Your Company Needs A Web Policy

By The Forsite Group

Web-Use Policies: Protect, Preserve, Prevent

What is the primary purpose of corporate Internet or Web-use policies? Prevention would appear to be a perfectly logical answer. After all, these policies typically detail what employees and end-users can't do such as access adult content from company owned PCs and laptops.

But prevention is only part of the picture. The ultimate goal of Web-use policies is protection. They safeguard the companies that implement and enforce them from legal actions, investigations, HR problems, and much more.

How? By defining rules and guidelines that address every aspect of an organization's Internet-based activities. That can range from acceptable and unacceptable Web surfing, Instant Messenger (IM) exchanges, and FTP (file transfer protocol) uploads and downloads to the length of time server logs and e-mail messages should be retained.

E-mail policies are particularly important. One of the many lessons of the Microsoft antitrust suit (and subsequent civil and criminal actions involving other companies) is that e-mail can be very embarrassing (or even damaging). Having four or five years worth of messages stashed on a SAN (storage area network) is an open invitation to a fishing expedition. If a company is involved in a legal battle or a regulatory investigation, that e-mail can-and will-be subpoenaed.

None of this is to suggest that companies that implement and enforce Web-use policies have done anything wrong or have anything to hide. A corporate policy stipulating that e-mail must be dumped after 90 days is far more efficient than trying to explain the intent of an ambiguous message sent several years ago.

No One Under 18 Admitted: Dealing with Adult Content

How do companies formulate effective Web-use and acceptable-use policies (AUPs)? This task has become more complicated of late, since regulations like the Sarbanes-Oxley Act (SOA) of 2002 can affect these guidelines, even if only indirectly.

Policies that attempt to forbid all personal use of company PCs are a waste of time. They may even be bad for business. They make the company into a villain, breed resentment, and turn the IT department into the Internet police, which wastes their time and talents.

Having an explicit, enforced no-porn policy in place, however, can help keep a company from becoming embroiled in expensive and embarrassing sexual

harassment suits. Whether or not an employee decides to follow this rule is immaterial. The policy itself indicates a company's philosophy and intent. In this instance it helps make it clear that accessing adult content while at work is directly at odds with its stated policy.

Without such a policy, it's hard to imagine even the best corporate attorney convincing a judge that ogling porn at the office doesn't contribute to "a hostile work environment," a litmus test for virtually all harassment rulings. What's more, even when a company wins in court, it still winds up losing. It's impossible to put a dollar value on the damage that harassment cases can inflict on a company's reputation.

Policies and Products

Once a Web-use policy has been developed, how do companies implement and enforce it? That's the job of one of the Internet reporting tools now on the market. It's essential to select a tool that has the horsepower to get the job done without degrading network performance, as well as the ability to scale as corporate Internet access climbs.

Implementing an AUP can be tricky. A vendor that's willing to put in the requisite time, and has the expertise to do things right, is an invaluable asset. Committing overstretched IT resources to Internet reporting and then not configuring the equipment or implementing policies correctly is more than a waste of money. It can be very dangerous.

The Ministry of Porn

Just how dangerous can be seen from the recent scandal that rocked the U.K.'s Department for Work and Pensions. An investigation, launched after a staff member reported a co-worker for surfing Internet porn, revealed that employees had accessed up to 2 million pages of adult content within the past year—all from the departments' PCs. More than 18,000 images and sites involved child pornography. The embarrassment and public outrage are easy to imagine.

A total of 19 civil servants were fired as a result of the investigation, with more than 200 others subjected to disciplinary measures. The Department Secretary resigned twelve days after the story broke in the press.

Amazingly enough, the Internet-filtering tool the department had deployed failed to trigger on any of these illicit sites. Similarly, Web-usage reports didn't offer a clue as to what was going on.

This is obviously an extreme example. But it does help highlight how vulnerable companies are when they believe—incorrectly—that the tools and policies they've implemented will protect them.

Mastering the Art of Making Policy

There's no magic formula for creating an effective Web-use policy. The effort, at least some of the time, is going to feel like an exercise in frustration. The goal is to cover as many situations as possible, without knowing what some of them will be.

Some of the policy-making process comes down to common sense—along with the ability to see the larger ramifications of a particular problem or policy. That's

one of the reasons that policy makers should be drawn from as broad a base across the company as possible. Three must-have members for any Web-use committee are HR, corporate counsel, and IT management.

Tools and Trends: Admissible Evidence

When a Web-use policy is combined with Internet reporting, it becomes a very powerful tool. For one thing, reporting can reveal who's in violation of various policies and whether these are isolated incidents or a regular occurrence. If the latter turns out to be true, a company has hard evidence to take whatever actions its HR policies permit.

Web reporting also protects companies—and employees—in other ways. Consider a case in which an employee says a coworker regularly surfs the Web for porn, a habit he or she finds objectionable. When questioned about his behavior, the employee admits to having done so once or twice—out of curiosity or even by accident.

Without Web reporting, a company may have little choice but to suspend the employee and then go back through its server and firewall logs to recreate his online behavior. This can take weeks. What happens if at the end of the investigation the company can find no evidence of improper behavior. It apologizes to the employee and asks him to come back.

But the employee wants more than an apology. He claims this incident has humiliated him, tarnished his professional reputation, and caused his fiancée to break off their engagement. He hires a lawyer and hits his former employer with a \$5 million dollar lawsuit.

Web reporting prevents this situation from ever arising. Once a charge has been brought against an employee, IT can analyze and print out a report about his Web use within minutes. No lengthy log searches. No embarrassment. No six-figure lawsuit.

Setting Limits on Surfing

As noted, Web-use policies that are too strict are ineffective. Moderation should be the guiding principle, as long as the company is not being put in harm's way. Rather than barring employees from shopping online, the activity can be limited to lunch hours and coffee breaks. Here again, Web reporting makes it easy to see if employees are following policy.

Similarly, employees who visit sports-related sites several times a day are hardly undermining corporate productivity. The same holds for eBay and other consumer sites. Occasional visits are probably best ignored. What a company wants to know is if an employee is running a business on eBay when he or she is supposed to be working.

Knowing when employees access the Web and where they're going is invaluable. In one case, Web reporting revealed that a group of contractors working on a mission-critical project regularly logged on toward the end of the business day.

This pattern was immediately apparent to the Web-reporting tool, which flagged the activity and brought it to an administrator's attention. It turns out the contractors were uploading each day's work to their own FTP site. This not only violated the contract but also put sensitive information at risk. Data wasn't encrypted in transit, while security on the site was spotty.

The Quest for Compliance

Web reporting also can help companies prove they're in compliance with regulations or reveal problems that must be rectified before auditors discover them—which could result in fines, loss of contracts, damage to reputation, and even a drop in stock prices.

For example, the Sarbanes-Oxley Act (SOA) requires all financial systems and related reporting systems to be locked down to prevent insider information from being illegally shared. Web mail, IM exchanges, and FTP activity all qualify as reporting systems. IT professionals who want to ensure compliance should look for Web-reporting tools that can track all Internet activity.

SOA also imposes blackout periods when companies are being sold or large blocks of stock are being offered to the market. Sharing insider information during these periods is a violation of Securities and Exchange Commission regulations. Unfortunately, if a crooked employee does this, the entire company suffers. Here again, effective Web reporting makes it possible to spot these transactions, shut them down immediately, and make the SEC aware of the problem.

Throwing Out the Mail

As mentioned, a truly effective Web-use policy needs to address basic issues, such as how long e-mail and server logs should be retained. Most likely, corporate counsel will argue in favor of preserving just enough data to keep the business running. In some instances, this could be a 30- or 90-day period.

There are several advantages to this less-is-more approach. One is financial. E-mail and server logs are maintained on SANs. The smaller the amount of data that's being preserved, the less a company has to shell out for storage.

Another advantage is legal. If a company can show that its established policy is to dump data after 90 days, then investigators and auditors can't demand older records. In contrast, when companies maintain massive amounts of e-mail, it's almost an open invitation for investigators to go on a fishing expedition to see what they can turn up.

Companies that set a cut-off date for data need to be sure of two things: First, that the policy is implemented correctly and that data is being eliminated on schedule. Second, they need to make sure they're not overlooking anything. There's no point in eliminating e-mail and server logs after 90 days, if firewall logs are going to be left untouched for several years. This sort of oversight can have serious repercussions, since the courts can demand that an accurate picture of all activity be recreated from those logs.

Tools Not Tears

As the debacle at the "Ministry of Porn" demonstrated, even the best Web-use policy won't offer any protection if it's implemented incorrectly. Thus, choosing the right Web-reporting tool is critical.

Essentially, Web-reporting tools can be divided into three categories: on-box, off-box, and stand-alone. The first two are software-based schemes; the third approach uses dedicated hardware.

On-box reporting, as the name suggests, runs on top of another device—usually a firewall. In most cases the reporting software is free with the purchase of a vendor's product.

The drawbacks to an on-box approach should be immediately apparent. Essentially, a device built to do one thing is now doing two. Inspecting incoming packets, detecting viruses and worms, and deflecting DoS attacks are processor-intensive tasks. Most firewalls don't have many spare CPU cycles. When they're asked to add Web reporting to their to-do lists, something has to give. That "something" is usually firewall processing, which slows in proportion to the number of cycles it has to dedicate to reporting. This introduces latency (which can play havoc with delay-sensitive traffic) and degrades network performance. For many IT managers, that's too high a price to pay for Web reporting.

Off-box approaches introduce a server into the equation. Once packets clear the firewall, they're shunted to a proxy server running Web-reporting software. Once the server has collected the data it needs, it sends the packets back to the firewall, which then forwards them onto the network.

With an off-box scheme, Web reporting no longer burdens the firewall. Thus it doesn't impede that device's performance. But it does add latency to the network, since packets now have to make a round trip between the firewall and server before they actually hit the network.

It should be noted that neither software-based scheme scales effectively. With on-box Web reporting, as the traffic load climbs, so does the number of cycles the reporting software needs to borrow from the firewall. In other words, the Web-reporting tool slows the firewall down just when it needs to speed up to handle the increased traffic. At some point the reporting software will overwhelm the firewall. The solution is to deploy another firewall, which also is running an on-box reporting package. The bottleneck will be relieved, at least in the short term. If the reporting software seriously degrades the second firewall, then a third must be deployed, and so on.

With off-box reporting, the way to deal with higher traffic levels is to deploy more servers. While this doesn't put a drag on the firewall, the amount of latency added to the network increases with every new server.

The Standalone Solution

At present, only one vendor offers a standalone, hardware-based Web reporting appliance—8e6 Technologies. The dedicated 8e6 Enterprise Reporter 3.0 is built to do one thing and do it well—reporting. What's more, the ER 3.0 reports on all essential traffic: Web access and destination, IM, P2P, Webmail, and FTP. Thus, there's no traffic type that can escape its vigilant scrutiny.

The ER 3.0 is built on a MySQL database. As a standalone appliance, it never compromises the filtering speed or performance of any other networked device. Further, its unique architecture lets it generate reports far faster than its closer competitor.

Some of the speed and flexibility of the ER 3.0 stems from its proprietary, preprocessing technology. Since it only captures and indexes unique data elements, the ER 3.0 can handle very high quantities of Internet traffic—2.5 million hits/hour or 60 million hits/day.

The speed at which the ER 3.0 captures data is paralleled by the rate at which it can generate reports. This task, no matter how complex the material being

analyzed, takes minutes or even seconds. In contrast, competing devices can take hours, days, or weeks to create just one report.

The ER 3.0 also eliminates scaling problems. Standard internal storage is 600 Gbytes, which can be increased to several terabytes. It also comes with links to external NAS (network-attached storage). This gives it the ability to retain historical data for reports and reference, regardless of how much traffic is traveling over the network. In addition, the unit's high-performance Intel Pentium 4 processor (and 3 Gbytes of RAM) ensures that it won't be overwhelmed by high-bandwidth traffic flows.

Finally, the ER 3.0 is loaded with features that increase its flexibility and ensure that IT managers get the reports they need, without delay. On-screen reports can be massaged in numerous ways, simply by clicking on a column header. Pie and bar charts also are only a click away. In addition, it can "memorize" a view or report that end-users find particularly helpful.

8e6 is committed to making sure its products are deployed correctly and operating at peak performance. It can help customers deploy their equipment in a third-party environment, allowing the ER 3.0 to be a fully empowered member of any networking environment.

What's more, 8e6 has its roots in the ISP space, so it's perfectly comfortable deploying products in high-demand environments. It also understands the difficulty of what customers are trying to do. Implementing a system that reports on thousands or tens of thousands of end-users is a complex task, one that can quickly consume resources earmarked for other equally important projects. To prevent that from happening, and to ensure that its customers take full advantage of its products, 8e6 is ready to share its expertise and experience wherever and whenever necessary.



For more information on 8e6 Technologies and 8e6 appliance-based solutions for Internet Filtering, Web-use Reporting, Bandwidth Management and Spam Control, visit www.8e6.com.