

The Top Six Risks of Employee Internet Use and How to Stop Them

An Essential Guide for HR and Compliance Managers

When it comes to your employees' use of the Internet, it isn't wise to underestimate the potential for damage to your organization.

From a network used by dedicated scientific intellectuals devoted to honest research, the Internet has grown to become the world's biggest clearinghouse for information of all kinds. At the same time, it has become a haven for inappropriate behavior and systems attacks, as well as posing a liability for any company that doesn't appropriately manage their employees' Internet use.

Due to the serious nature of many threats, the Internet use of even one unmonitored employee on a single unmanaged system can ravage a company's internal network, irrevocably delete critical data, and ultimately ruin the company's ability to conduct business. Situations like this aren't works of fiction, but actual everyday occurrences for organizations with unprotected networks.

Moreover, the potential for liability and subsequent lawsuits resulting from employees' inappropriate surfing habits are very real. Litigation from just one incident can entangle a successful business in resource-draining legal procedures that can drag on for months. That's just one person, one machine, and one lawsuit. Now multiply this by several employees and several incidents of Internet abuse. It's easy to see how destructive unmanaged Internet access can be.

It's clear that employees in today's businesses have come to rely on the Internet for everyday workflow and that removing that access could easily cause productivity to suffer. Because of this, companies must rely on the Internet to maintain the successful flow of business while seeking to mitigate the threats associated with employee Internet abuse.

This paper will discuss the risks involved with unmanaged Internet access specifically focusing on the needs of HR and Compliance Managers, and describe the controls your company can put in place to alleviate them. We will also discuss Internet-based threats and the resulting legal issues and regulatory compliance requirements with which you must contend in order to protect your business.

The Top Six: Unmanaged Internet Access is a Gateway for Threats

If you've ever attempted to recover your home computer from an accidental infestation of Spyware, you're familiar with how easily it can corrupt your entire computer. Imagine that single instance propagated across every computer in your organization. It isn't difficult to realize that a single infestation can lead to a substantial loss of productivity and ultimately, revenue. Similarly, anyone who has ever accidentally released personal information to an illegitimate website, knows that the unintentional disclosure of sensitive information can have serious consequences.

Before you can understand how to protect your organization's systems from these dangerous possibilities, you need to understand the types of threats lurking on the Internet. In the section below we identify six different types of Internet-based threats and explain their negative impact on your organization.

1. Inappropriate Surfing

Classifying what is “inappropriate surfing” can be extremely difficult. What one employee considers appropriate may be considered offensive or even harassment by another employee. Supreme Court Justice Potter Stewart famously said in *Jacobellis v. Ohio* (1964) that pornography was hard to define, but “I know it when I see it.” He later went on to recant that statement in a following case, *Miller v. California* (1973) when he realized that this view was, “simply untenable.”

Because of the subjectivity inherent in determining what is offensive content, many companies restrict the use of the Internet to business purposes only. From a legal standpoint, this limits the liability of the company. However, implementing controls on Internet use cannot be effective without a technical means of enforcement. A typical technical solution could involve the implementation of a device to permit or block traffic to certain websites based on content. It could be argued that implementing a device that makes the determination of content inappropriateness as part of managing Internet access moves the burden of liability from the company to the solution provider.

Additionally, a technical solution can also help prevent downloaded, copyrighted content from coming into your network. This data, should it reside on your internal computers, can open the possibility of copyright infringement litigation. One example of such an occurrence that was widely reported in the media involved the Recording Industry Association of America’s (RIAA) clear intent to seek prosecution of any entity found in violation of copyright laws governing artists’ music. According to the RIAA web site, “Online infringement of copyrighted music can be punishable by up to 3 years in prison and \$250,000 in fines.”

In any case, inappropriate surfing can have a deleterious affect on employee morale as well as productivity. Technical solutions to monitor and manage employee surfing habits are necessary in order to establish a consistent baseline of what is considered “appropriate”.

2. Spyware

Although the term Spyware is often used to describe bad software downloaded to a user’s computer, the term Spyware has a very specific meaning. Spyware actually describes a subset of Malware that is specifically coded to monitor and report on activity on an infected system.

Spyware comes in many varieties, and combinations of different types of these malicious intruders can be used to create what is called a “blended threat”. Many types of Spyware, often called Key Loggers, are used to compromise data and steal personal or proprietary information. Key Loggers monitor computer users’ every keystroke, hoping to encounter a series that will turn out to be a password or a credit card number. When such a keystroke series is identified, it is uploaded through a silent background process to a central location where it can be retrieved and used. Once installed, Key Loggers can copy any data entered into the infected computer and are often a major component in identity theft.

Other types of Spyware, often called Adware, are used to monitor the Internet surfing habits of users so they can market alternate sites to them. These applications run in the background and are often used to deliver “pop-up” advertisements. If you’ve ever had a pop-up advertisement appear even though you took no action on your computer, you are experiencing the result of a Spyware stealth application. These types of Spyware do not necessarily involve data compromise, but can slow down a system and reduce worker productivity.

3. Instant Messaging

Instant Messaging (IM), also known as Internet Relay Chat (IRC), can be a useful tool for communications between employees but it can also be a major distraction if employees are having non-work related conversations with others either inside or outside your organization. Employees with unsupervised IM access could conceivably spend large amounts of time communicating with friends and family during work hours, or chatting with other employees, taking away from their ability to be productive. They can also circumvent internal corporate controls for data protection, easily transferring sensitive data outside the network.

The protocols that serve Internet-based IM can also be a vector for a type of attack known as a Zombie Attack. In a Zombie Attack, an attacker utilizes IM protocols to infest multiple machines with an application controlled by a central console. Through this application, the perpetrator instructs all infected Zombies to attack a specified Internet site. This type of attack is called a Distributed Denial of Service (DDoS). DDoS attacks involve hundreds or thousands of Zombies attempting to send massive quantities of data to the attacked site, preventing it from operating.

If your company is seen to be the source of a Zombie attack, you could be liable for the loss of service by the entity being attacked. This introduces a risk of litigation from the attack destination, and can occur even if you are only the unsuspecting medium through which the attack is enabled.

4. Phishing

Phishing is a relatively new tool used by criminals to drive unsuspecting email users to fake sites for the purpose of retrieving personal information. Phishing exploits use emails designed to mimic legitimate sites such as well-known banks, or popular sites like eBay, Amazon, and others. These official looking emails instruct the user to login to a website in order to enter or confirm a data request. When the user clicks on the email link, they are directed to a website that in many cases is hardly distinguishable from the legitimate site. Because of this, the unsuspecting user may feel safe in entering personal information such as login identity passwords, credit card information, or bank account numbers.

Phishing tactics have gotten more sophisticated since their first use in 1996 with websites that deftly clone legitimate sites right down to the web address. Although phishing exploits have mainly targeted consumers as individuals, it isn't hard to imagine how they could damage businesses too. A highly-directly version of these attacks could entice an employee to submit sensitive business data to illegitimate sites, potentially compromising proprietary corporate data as well.

5. Malware

Malware is short for Malicious Software, and is a superset of Spyware. Malware describes any piece of software designed to damage a computer system, delete data, or interrupt the normal processing of the infected computer. Malware comes in many classifications, including Viruses, Worms, and Trojan horses. All of these are software that can be inadvertently downloaded onto an employee's computer simply by clicking a link on a web site. Or, when browser security is not configured securely enough, some Malware can be automatically installed without the user's awareness.

Viruses and Worms are particularly insidious because both are types of software with a programmed drive to replicate. When a worm is introduced into a network, it can do two things: First, it begins replicating itself to other unprotected machines on the internal network. It also typically begins processing what is called its "payload", which is the code intended to be run on every infected machine. This payload can involve information disclosure to an outside entity, data deletion, or operating system corruption.

Modern infections often incorporate multiple Malware downloads packaged together into a “drive-by download”. This multiple packaging increases the impact of infection and enhances the difficulty with removing the software from the affected system. In many cases, the only way to remove the Malware is to rebuild the system. As with Spyware, the only way to prevent a malware attack is to stop the intruder at the network perimeter through a network scanning device before it can reach your internal servers.

6. Peer-to-Peer Applications

Peer-to-Peer applications have grown in popularity in recent years because they offer users an easy and convenient way to share files, applications, and data among many others within their peer-to-peer networks. Unfortunately, these types of applications are often used to share copyrighted data like music or video, and due to the ease of distributing material once it has been shared, P2P can rapidly transfer data from one location to another through a series of meshed networks. This illegal sharing of copyrighted data can cause daunting legal liability for corporations as well as individuals. Business networks that do not prevent P2P applications from running on their networks open themselves to liability if the illegally-obtained files are being stored on corporate hard drives.

Many peer-to-peer applications are also configured to share a person’s hard drive on the Internet. This characteristic opens the possibility that sensitive business files within the sharing location can be made available for others to view and download. This creates the possibility for proprietary or sensitive business or customer data to be transmitted to outside parties, leading to legal and financial problems that can seriously damage an organization.

The Business Impact of Unmanaged Internet Access

According to a statistic referenced recently in InfoWorld Magazine , “...Spam, Spyware, Malware, and other unwanted agents account for at least a 20% productivity drain in the workplace per year.” This 20% loss in productivity can be traced to several factors; one is the reduction in machine performance due to Malware infection; another is the inability of employees to accomplish daily tasks because an infection event renders a workstation inoperable; and third, the distraction associated with Spam and Spam removal.

The same InfoWorld Magazine article references a recent Gallup Management Journal report that labeled “[at work] 56% of American workers are ‘not engaged’ – that is, more interested in surfing YouTube than doing their jobs. Another 15% are ‘actively disengaged.’” These statistics reflect an inability on the part of management to direct employees away from unproductive tasks like web surfing and towards their assigned job duties. Implementation of a threat management system with web content filtering is the only way to insure that employees are not misusing time at work with inappropriate surfing.

The following section discusses the critical factors that drive the need for businesses to implement Internet threat management. These factors include the risk of legal liability; the regulatory compliance requirements faced by all businesses; the need to manage bandwidth; the threat of productivity loss; and the potential for security breaches.

Legal Liability & Your Acceptable Use Policy

An Acceptable Use Policy (AUP) is a document used by businesses to establish and enforce the company’s rules regarding use of the network. This document is used as legal protection for corporations when they require that employees use the corporate network only for policy-sanctioned corporate purposes. As a business’ network is often connected in some way to the Internet, the AUP ensures legal recourse in the case of an employee whose inappropriate surfing or use causes litigation to be served against the company.

AUP’s are typically written in one of two ways. The first method specifies that the business network is to be used for business purposes only. In this version of the AUP, employees are forbidden to use the Internet for personal reasons. The benefit of this type of AUP is that it applies a broad restriction over what can and cannot be done on the company Internet. However, it can be difficult to enforce as it places the onus of defining “business purposes” on the business.

Some companies choose a less all-or-nothing solution to the problem of Internet use. These companies implement an AUP that proscribes limited Internet use during the workday, not to interfere with the official duties of business. By allowing limited access to employees for personal use, the onus of defining appropriate use is partially moved from the employer to the employee.

Compliance Regulations

In either situation, corporations utilizing an AUP must have auditable technical controls in place to manage and monitor for violations. Numerous compliance regulations exist which – based on the industry – mandate the types of controls put in place. These controls can have a number of objectives such as preventing personal data disclosure, protecting financial data ,and protecting children.

The table below discusses some of the major compliance regulations, their associated industries, and their risk area of focus:

Compliance Regulation	Affected Industry	Risk Area of Focus
Sarbanes-Oxley Act (“SOX”)	All publicly-traded companies.	Risk of data disclosure that could negatively impact shareholder value.
Gramm-Leach-Bliley Act (“GLBA”)	All financial institutions. This includes any institution that handles personal financial information.	Risk of personal financial data disclosure.
Health Insurance Portability and Accountability Act (“HIPAA”)	All medical institutions.	Risk of personal medical data disclosure.
Children’s Internet Protection Act (“CIPA”)	All educational institutions.	Risk of child exposure to obscene, pornographic, or harmful data.

As you can see from the table above, most of the regulatory requirements assigned to corporations in almost all industries deal specifically with the risk of data disclosure. From a network perspective, these types of risks address exposure from the opposite direction of many of the Internet threats previously discussed. Whereas reducing the threat of Internet attack prevents external attacks from impacting the Internal network, compliance litigation demands that same risk reduction also prevent internal data from being distributed outside the network.

Bandwidth & Productivity Loss

Another business driver towards managed Internet access involves the problem of excessive bandwidth consumption. If your business uses a narrow bandwidth connection to the Internet, a single employee streaming excessive media into your network can monopolize available bandwidth, which effectively prevents others from using it for work-related purposes.

Network bandwidth is typically purchased based on the needs of each business. If those needs cannot be resolved through available bandwidth, employee overuse of the Internet could drive the need to purchase additional bandwidth unnecessarily, in order to resolve the problem. Continuously increasing the size of the pipe to the Internet, however, is not a sustainable solution as unmanaged employee Internet use has the tendency to fill any available bandwidth, even as it increases.

In many cases, the only sustainable solution is to implement a business policy that mandates and limits employee use of the Internet. At the same time, implementation of a network control is needed to enforce that policy. Your network control should monitor for inappropriate high-utilization traffic like video and audio streaming and large file downloads to limit or prevent them from consuming available bandwidth.

Security Breach

One component of GLBA defines the need for financial institutions to secure their data. FTC Section 314.1 discusses the need to establish standards to develop, implement, and maintain administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

It is the responsibility of the compliance manager to ensure appropriate procedural and technical controls during data storage and transfer to prevent its misuse or inappropriate disclosure. Lack of these controls can cause significant financial damage to a company. One example of this is the DSW Shoe Warehouse, where, in 2005, there was a lapse in network security compromising 1.4 million customer credit and debit cards and 96,000 checking accounts. According to the Federal Trade Commission, DSW's exposure for breach-related losses ranges from \$6.5 million to \$9.5 million. DSW settled the matter out of court.

This single security incident exemplifies the need for good internal controls on network traffic and threat management. Even a single security incident could incur millions of dollars in legal and remediation costs and irreparably damage corporate goodwill.

Three Components of Internet Filtering

The St. Bernard iPrism Internet Filter is the award-winning access management solution that protects against external attack while protecting internal networks against inappropriate data disclosure. This appliance-based solution ensures enforcement of your business' AUP while monitoring and blocking Internet-based threats by filtering the URL traffic coming into your network. The iPrism Internet Filter is designed to be implemented between the internal network and the Internet. Positioning the iPrism in this manner ensures that all traffic going to and from the Internet is scanned, evaluated, and blocked according to your AUP.

The iPrism Internet Filter is easy to install, administer, and maintain. As a hardware device, implementing the iPrism involves little more than connecting the device to the company Internet and power, completing an initial configuration, and enabling the device. The device can be configured in one of two modes. The first, proxy-mode, makes optional the use of the iPrism and requires configuration at the client to use the device as a proxy server. In proxy-mode, the iPrism can monitor and filter certain, but not all, types of traffic.

In its other mode, bridge-mode, all traffic to and from the Internet will flow through the iPrism device. In bridge-mode all types of Internet-bound traffic can be monitored and filtered, and use of the iPrism is not optional. In this configuration, there is the added benefit that no client configuration is necessary to use the device.

In either configuration, the device will accomplish three critical tasks in support of reducing the risks of employee Internet use: Stopping threats, mitigating risk, and supporting your AUP.

Stopping Threats

Unlike workstation-based threat management systems that rely on individual workstation configurations to enable the threat filtering, iPrism is a single (or dual-redundant) device that sits at the connection between your internal network and the Internet. By locating a device between the inside and the outside, all inbound Web traffic can be effectively filtered by the device. With software based workstation threat management systems, each workstation must be configured to employ the software. However, because iPrism is appliance-based and resides at your network's perimeter, it works seamlessly with any workstation configuration and is transparent to end-users.

The administrator configures the types of traffic to watch for (web, IM, Malware, etc.) and configures the system to automatically receive regular updates through a St. Bernard's update subscription. This ensures that the device is always looking for and stopping the most up-to-date threats from the Internet. New updates are automatically pushed to the iPrism daily, with critical spyware, malware, and phishing sites updated hourly.

Mitigating Risk

By stopping threats before they enter the internal network, the iPrism can mitigate the risk associated with employee Internet use. For all threats, the iPrism incorporates the highly-accurate iGuard database. The iGuard database includes dozens of profiles that can restrict entire classifications of potentially inappropriate surfing such as pornography, gambling, and drug use. The iGuard database is renowned for its accuracy because each and every site is human-reviewed for its categorization.

Combining the quick updates to the iPrism device with the accuracy of the iGuard database means the iPrism ensures the least risk to your internal network.

Supporting Acceptable Use Policies

Obviously no technical solution works well without supporting policies that enable and enforce its use. Combining in-place policies with its granular categorization of appropriate and inappropriate Internet use, iPrism is the technical control that supports your Acceptable Use Policy.

The iPrism enhances the auditing needs for your AUP by providing a comprehensive reporting engine, detailing the types and destinations of all your Internet-bound traffic. Email alerts can be configured to notify management or human resources when attempts to connect to inappropriate sites occur. Administrators can be notified when external entities attempt to launch attacks against the internal network. When inappropriate activity occurs, iPrism can display a customized web page notifying the offender of the inappropriate activity. If the destination site is deemed necessary to be allowed, a user-specific override can be enabled for that site.

The Return on Appliance-based Security

Using an appliance as a security device brings to the table some intelligent features. Network appliances are typically single-use machines that are highly optimized to perform their task. This single-minded focus on security and threat filtering means the device can incorporate a hardened by design architecture, a reduced need for maintenance and patching by systems administrators, and enhanced performance.

Hardened by Design

Many Unified Threat Management systems are software-based, which involves their installation onto a pre-existing operating system. This installation onto a full operating system rather than a dedicated appliance means an increased responsibility on the part of the administrator to manage, patch, and harden the underlying operating system. Full operating systems may have multiple open network ports and process more than one application. This has the tendency to make that full operating system less secure than a hardened appliance. It is, after all, the full operating systems inside your network that you are trying to protect.

Utilizing a single-use appliance as a security device means only the necessary connections with the outside network are enabled. Hardened by design also means that the appliance can only accomplish one task rather than a multitude of tasks. That appliance runs only the necessary pieces of code to accomplish its assigned task.

Supportability & Patch Management

The iPrism appliance incorporates a hardened by design architecture that requires far less patching than full operating systems. To enhance that network protection, if the iPrism does require a patch or an update, that patch is automatically downloaded as a part of the daily signature download. This feature means less daily monitoring on the part of already overworked systems administrators.

Additionally, with full operating systems conflicts with installed software can cause a patch installation to crash the system. This is not the case with network appliances. The device's known configuration virtually ensures that any downloaded patches will not negatively impact its availability.

Performance

Lastly, a highly optimized appliance also means better performance than a software-based one installed onto a full operating system. With software-based solutions, any filtering logic must go through multiple operating system layers away from the low-level "kernel" before the high-level filtering code can act. This has the tendency to slow down that device's capability to process inbound and outbound traffic and ultimately do its job.

With the iPrism, the device is the filter. In this case, the filtering happens at a level very close to that device's core, which means fewer operating system layers to traverse for each request and substantially improved performance.

Managed Internet Access & iPrism are a Best-in-Class Approach to Mitigating Business Risks & Increasing Employee Productivity. Internet threats really do exist. But with today's Internet threat filtering technology, best represented by a hardened and optimized appliance such as iPrism, you can keep them out of your internal network.

With its appliance-based architecture, the iPrism is your best choice for a highly secure and high- performance Internet access management. With its human-reviewed content filtering, the iPrism is your best choice for the most accurate threat filtering. And with its built-in network update capability and fast turn-around for threat signature recognition, the iPrism is your best choice for reducing the risks of your employees' Internet use.

All it takes is one unmonitored employee on one unmanaged computer. It's iPrism's job to prevent that from happening. For more information on the iPrism and St. Bernard's other solutions, visit www.stbernard.com.