

## Ensuring Information Security: New Regulatory Challenges



How Websense Helps Organizations  
Achieve Regulatory Compliance

## Safeguarding security, mitigating liability

*It has always been good business practice for companies the world over—whether in financial, educational, health care, business, or retail organizations—to protect their customers’ privacy and control access to sensitive information. In recent years, the inadequacy of policies and controls at companies such as Enron, WorldCom, and Arthur Andersen has led to the creation of new regulations. Some of the strictest regulatory controls have come from the US, with regulations such as Sarbanes-Oxley. In the UK, lawmakers have initiated the Higgs Review to examine the role and effectiveness of non-executive directors. These new regulations impose new requirements on organizations, establish standards for compliance, and institute penalties—some extremely harsh—for noncompliance.*

Regardless of where the regulations originate or the organizations to which they apply, these new laws set forth the need for companies to do the following for their employees, stockholders, and customers:

- Protect the security of the company’s network infrastructure. This includes establishing controls to prevent intruders from placing unauthorized files and programs in the company network, accessing and capturing private or proprietary information, and transferring that information to unauthorized destinations.
- Control access to customer records and personal information. This includes setting and enforcing policies on who should have access to different types of information.
- Monitor communications going into and out of the organization, including email and file transfers.
- Institute an auditing system to verify compliance with regulatory standards and establish a process for identifying issues (such as security breaches).
- Report compliance status to designated company management and the pertinent regulatory agency.

Organizations face a complex challenge in securing the computing environment they rely upon to conduct business. The employee computing environment offers access to rich content and tempting new applications on the internet. Due to the complexity of the computing environment, organizations must deal with new security risks and challenges every day. IT managers are under tremendous pressure to provide an open, collaborative networking environment. At the same time, they are responsible for protecting the organization from financial losses and legal liabilities that may result from security breaches.

In recent years, there has been a series of new and increasingly alarming web-based threats which can impact not only the IT department, but executive management as well. Seemingly every day a new threat emerges, whether through web-based attacks, spyware, malicious mobile codes, phishing, or hacking attacks. These threats cost organizations an estimated \$12.5 billion worldwide in 2003<sup>1</sup>. Remote internet access and wireless devices have also expanded the network perimeter and the potential for attacks.

Consider the following:

- 1 in 3 companies have detected spyware on their network. (Websense UK Survey, 2003)
- Nearly 80% of instant messaging (IM) in companies is done over public IM services such as AOL, MSN, and Yahoo, exposing companies to security risks. (Radicati, 2003)
- The number of malicious code attacks with backdoors, which are often used to steal confidential data, rose nearly 50% in the last year. (Symantec, 2003)
- 45% of businesses have reported unauthorized access by insiders. (CSI/FBI, 2003)

This white paper summarizes some regulatory requirements that have been enacted to ensure information security and their associated challenges, and explains how Websense® software and services can help companies achieve compliance.

## Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) became Public Law 106-102 when it was signed into law by President Clinton on November 12, 1999. The GLBA dictates how financial institutions are to manage and protect personal consumer information and applies to all companies that offer financial products or services, such as loans, financial or investment advice, or insurance to individuals. The GLBA includes three sections:

- The Financial Privacy Rule governs the collection and disclosure of customers' personal financial information by financial institutions. This rule also applies to companies that receive this information, whether or not they are financial institutions.
- The Safeguards Rule, enforced by the Federal Trade Commission, requires financial institutions to have a security plan in place to protect the confidentiality and integrity of personal consumer information. This rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions such as credit reporting agencies that receive customer information from other financial institutions.
- The Pretexting provisions of the GLBA protect consumers from individuals and companies that obtain their personal financial information under false pretenses, a practice known as "pretexting."

The Act also requires financial institutions to give customers written privacy notices that explain their information-sharing practices. All affected businesses were to be in full compliance by July 1, 2001.



The final rule, adopted May 23, 2002, added language targeted specifically to information security. The Commission added "network and software design" to the examples of information systems a financial institution should examine; it also added the term "detecting" to the requirement that each financial institution consider means of "preventing and responding" to attacks, intrusions, and other systems failures.

*For affected companies, compliance is mandatory. Institutions found to be noncompliant with these rules are subject to liability suits and regulatory enforcement measures ranging from corrective action to fines or other penalties.*

### THE CHALLENGE... AND THE SOLUTION

From an IT perspective, the GLBA requires that companies restrict access to their networks and implement controls to protect sensitive information and prevent malicious or inadvertent disclosure of nonpublic personal information. The Act also requires financial

services organizations to perform regular assessments of risks to the security of customer information to identify foreseeable threats, assess the likelihood of potential damage from these threats, and judge the sufficiency of implemented controls in mitigating threats. Results of these assessments are to be reported to corporate leadership.

New web-based threats such as spyware, keylogging applications, and internet-borne viruses are particularly worrisome for the insurance and financial services industries. These malware applications may be inadvertently installed by employees and can go undetected for extended periods of time, resulting in a continuous, long-term outflow of confidential customer, personal, or organizational data to unknown third parties. By using Websense software and services, companies can protect proprietary information and ensure compliance with these important GLBA provisions.

#### Restrict access to the company network

With Websense software and services, companies can define the applications that are allowed to access the network and the ports by which they can access it. Websense restricts network access to only authorized categories of programs, denying access to unknown or unauthorized programs.

#### Protect the security of customer records and customers' nonpublic information

The first step toward compliance in this area is to understand clearly the threats a company is facing. The next step is to control the flow of information into and out of the organization. The final step is to report information back to company management so that corrective action can be taken as needed.

#### Step 1: Understand threats

Websense software and services help companies identify potential problem areas by using monitoring and reporting tools that offer real-time and historical views of company risks related to employee web activities. Several features in the Websense solution give management insight into how employees are using their computers – the applications they

are running, attempts to perform unauthorized transactions, websites they are visiting, etc. Administrators can drill down on reports of network usage by protocol signature, username, user group, and by destination IP or hostname.

#### Step 2: Control the flow of information

Using Websense software and services, companies set appropriate application use policies for any combination of users, groups of users, workstations, or networks. One key feature also restricts application use by "white listing" only approved applications. This feature ensures that only approved applications are allowed to run; applications that are unknown, known to be malicious, or unclassified (like mass-mailing worms) are prevented from launching entirely. The approved list can be created automatically through a software inventory process and can be updated on a scheduled basis. With Websense software, companies can control the use of unsafe applications like instant messaging (IM), peer-to-peer (P2P), hacking tools, and the like. Once the policies are in place, even employees who are running their laptops remotely will not be able to launch restricted applications.

In addition, since employees should not be allowed to circumvent the corporate email system, managing the appropriate protocols can prevent proprietary information from being distributed via other methods such as IM. Because proprietary information can easily be sent to or accessed by unauthorized individuals via IM, companies may choose to allow its use but prohibit the use of file transfers using IM. If the company chooses to deny use of certain applications altogether (IM, P2P, and chatting, for example), Websense software will also block access to the websites from which these client applications are downloaded. Websense software can also prevent employees from accessing sites infected with malicious code or those identified with phishing or other hazards.

#### Step 3: Report results

The same tools used to identify potential threats can be used on an ongoing basis to report results back to management.



### CASE IN POINT – PENN NATIONAL INSURANCE

Penn National Insurance, a leading insurance company based in Harrisburg, PA, relies on Websense to help the company comply with GLBA requirements by safeguarding confidential consumer financial data from new web-based attacks. Founded in 1919, Penn National Insurance offers property-casualty insurance through 750 independent agencies.

Penn National Insurance selected Websense to enable the company to meet the privacy and security regulations of the GLBA, as well as provide protection from online security threats for nearly 1,000 of its employees, all of whom are managed by Websense products.

"Deploying Websense products was part of a rigorous four-year plan to bolster internet security, boost productivity, and comply with industry regulations including the Gramm-Leach-Bliley Act," said Thomas Miele, manager of information security/security management at Penn National Insurance. "As we continue to rely on our employees' use of internet technology to improve efficiency, we see Websense as an essential solution in defending the security of our customers' confidential information, while at the same time improving overall employee output and optimizing our network bandwidth.

Websense protects personal customer data from web-based attacks in several ways. Websense prevents employees from inadvertently accessing sites that are infected with mobile malicious code or distribute spyware. Should spyware find its way to the corporate desktop, Websense stops the transmission of sensitive information, such as consumer financial records, to external spyware host servers.

Websense also blocks employees from accessing websites such as internet radio and TV, streaming media, and P2P file sharing. In addition to the bandwidth drain, P2P file sharing applications are potentially dangerous in the workplace because they connect users directly to each other to download and swap files. P2P networks bypass traditional security barriers and are easily exploitable by hackers to spread viruses, worms, and spyware, as well as transfer confidential information.

"As malicious applications such as spyware and keylogging become more prevalent with the increased use of unmanaged peer-to-peer file sharing networks, organizations are taking action to proactively protect their corporate assets as well as comply with important industry regulations," said Leo Cole, vice president of marketing for Websense, Inc. "The Websense implementation at Penn National Insurance is an example of our commitment to providing a robust solution that offers a solid defense for corporate networks, intellectual property, and employees from online dangers."

*For Penn National Insurance, employee internet management using Websense makes perfect sense as it helps safeguard confidential consumer financial data from new web-based attacks. Penn National Insurance relies on Websense to help it achieve full compliance with GLBA and other regulatory requirements.*

## Sarbanes-Oxley Act

With President George W. Bush's signature on July 30, 2002, the Sarbanes-Oxley (SOX) Act of 2002 became Public Law 107-204. The stated purpose of the Act is "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the security laws, and for other purposes." SOX was written to address some of the issues revealed during the incidents with Enron, WorldCom, and Arthur Andersen. SOX aims to prevent corporate mismanagement by requiring better controls and accountability for corporations.

SOX affects companies that report to the Securities and Exchange Commission (SEC). Public companies with a market capitalization of \$75 million or more were required to meet the November 15, 2004 compliance deadline. Companies whose market cap is less than \$75 million have until July 15, 2005 to demonstrate compliance.

The Act covers a wide range of issues, many covering the types of trade that are allowed within a company, with an emphasis on ensuring the integrity of the company and its officers. Some key provisions are:

- The Chief Executive Officer (CEO) and Chief Financial Officer (CFO) must personally certify that financial reports are accurate and complete. They must also assess and report on the effectiveness of internal controls around financial reporting.
- All communications must be archived and transparent, and auditable systems must be created for recording transactions and business correspondence.
- Whistleblowers—individuals who report violations of this law or any other SEC or federal violation—are protected from being fired, demoted, suspended, threatened, harassed, or otherwise discriminated against.

### THE CHALLENGE... AND THE SOLUTION

Although information security is not specifically addressed by the SOX Act, tight internal controls rely on information security. An insecure system cannot be trusted as a source of reliable financial information because of the inherent potential for manipulation of numbers and unauthorized transactions.

The SOX Act points to three key areas for ensuring the security and integrity of financial information:

- Control access to systems and data.
- Ensure the security of the company's network infrastructure.
- Monitor activities and log events that might indicate security breaches.

*SOX penalties are harsh.*

*A CEO or CFO who knowingly submits a false certification faces a \$1 million fine and up to 10 years in prison.*

*If the false certification is found to have been submitted willfully, the penalty is increased to up to \$5 million and 20 years in prison.*

Data security breaches could indicate weaknesses in controls that must be disclosed under Section 404 of the SOX Act. If material assets are compromised and not sufficiently protected, the internal controls over financial reporting may not be effective, and management would be required to disclose material weaknesses to their audit committee and outside auditors. The SOX Act does not require that a company's systems be impenetrable; however, the company must protect against reasonably foreseeable vulnerabilities.

The amount of security should be commensurate with the level of importance to the company of the assets being protected. For example, customer data, proprietary information, significant intellectual property, financial reporting information, HR information, and other such matters will likely be high on the security priority list. Other statutes, such as California S.B. 1386, may also require disclosure to customers or employees if their personally identifiable, unencrypted information has been improperly accessed.

### Control access

To ensure compliance with the SOX Act, controls must be in place to ensure that only those people who are authorized to use the system or to access specific types of information are able to do so. With Websense software and services, companies can accomplish this goal by setting appropriate application use policies. Companies can also restrict application use to only those on an approved list. Using this feature, unsafe applications like IM, P2P, and hacking tools can be blocked entirely. Even employees who are running their laptops remotely are protected.

Instant messaging can be a useful way to share appropriate information within an organization. However, since sensitive information can be transmitted during IM sessions, many companies are opting to prevent—or at least restrict—the use of IM clients. Because many IM clients allow users to attach files to send to one another, IM introduces the risk of employees sending confidential company information as IM attachments. With Websense software and services, companies can establish and enforce the IM use policies that make sense for them: allow unrestricted IM use, allow only certain users or groups of users to use IM clients, allow IM use for only a specific amount of time each day, allow IM use but prevent IM file attachments, and so on. Companies can also rely on Websense software to block access to IM websites from which IM clients can be downloaded if they have adopted a no-use policy on instant messaging.

Employees need to visit websites to get their jobs done. Websense software and services ensure that employees are protected while they

do so, and that companies' web access policies are continually enforced. When an employee requests to visit a website, the website's URL is checked against the Websense Master Database to ensure that it is an approved and safe site, free of malicious code or phishing.

### Ensure network security

Traditional corporate security measures typically include a combination of one or more firewalls and antivirus software. Although these security components are critical, they are no match for the sophisticated, blended web attacks that have recently been unleashed. Additional security defenses and technologies are needed to supplement these traditional technologies.

Websense URL filtering can help protect against web-based attacks by blocking access to malicious websites (with phishing, spyware, malware, etc.), managing the use of personal storage sites and personal email accounts, and limiting access to hacking portals.

Websense software and services supplement antivirus protection on all company computers with security technologies that have lockdown features, allowing companies to deny network access to unauthorized applications.

### Monitor activities and events

Companies need to implement monitoring technology that tracks and records invalid login attempts, port scans, and requests for inappropriate access, all examples of attempted security breaches. Since a great deal of event information can be generated, several Websense reporting and analysis tools should be used to ensure effective monitoring. Reports show real-time network statistics on application usage and help administrators identify the specific computers involved. Administrators can also drill down on reports of network usage by protocol signature, username, user group, and by destination IP or hostname. Reports can be predefined and formatted and sent to the administrators via email, ensuring that administrators have up-to-date information. The results of the monitoring activity should be early identification of security issues that need to be addressed.



### CASE IN POINT – GOLDEN STATE FOODS

Golden State Foods (GSF) based in Irvine, CA is a \$2 billion manufacturer and distributor in the foodservice industry with 2,500 employees worldwide. Founded in 1947, the firm is the largest full-line supplier to the fast-food giant, McDonald's, providing it and other food industry customers with hundreds of products. GSF has 10 distribution centers in the US and Egypt, and operates five food processing plants worldwide (in City of Industry, CA; Conyers, GA; Cairo, Egypt; Sydney, Australia; and Kuala Lumpur, Malaysia).

Golden State Foods chose Websense to address security, bandwidth management, and productivity concerns related to internet use. Employees can unknowingly expose their companies to security risks by using the internet for personal or non-work-related reasons. GSF was no exception to this trend.

"Security was a major concern, spyware was a problem, and we needed to be able to lock down desktops in the event of a virus; Websense gave us that ability. Using Websense brought security threats to our attention and helped us to reduce them," said Mike Bourque, Technical Services Manager at Golden State Foods.

Websense products provide Golden State Foods with zero-day protection against unknown security threats, including sophisticated malware, by preventing them from spreading across the network. Websense products stop the execution of unauthorized applications, such as spyware, P2P file sharing, and hacking tools. Complementing traditional firewall and antivirus tools, Websense closes the window of exposure to unknown security threats that often bring down networks before the appropriate actions can be taken to correct them.

Websense reporting tools have provided GSF with capabilities for tracking, analyzing, and reporting on internet activity and overall risks associated with employee computing. "With the Websense reporting tools, we learned that P2P file sharing with programs like Kazaa was more prevalent than we originally thought," Bourque said.

With employees at far-flung distribution and manufacturing centers, Golden State Foods also needed controls for the internet kiosks it installed in lunchrooms so workers could do personal business during breaks. GSF takes advantage of Websense's flexibility by activating the quota option, "We give employees 90 minutes of quota time for shopping and banking and other personal things," said Bourque.

*Golden State Foods relies on Websense to help manage employees' web activities, thus helping to protect the company and its network infrastructure from threats like malicious code, hacking, and phishing.*

## Health Insurance Portability and Accountability Act



The Health Insurance Portability and Accountability Act of 1996 (HIPAA) became Public Law 104-191 on August 21, 1996, with some regulations still being finalized today. It was enacted by Congress to improve the efficiency of the health care system by standardizing electronic data interchange and to protect the confidentiality and security of health data. HIPAA establishes standardized mechanisms for electronic data interchange, security, and confidentiality of all health care-related data. It consists of two sections:

- Title I deals with protecting health insurance coverage for people who lose or change jobs.
- Title II deals with the standardization of health care-related information systems.

HIPAA was finalized and formally adopted as of April 2003 and affects virtually all health care providers, health plans, public health authorities, health care clearinghouses, and self-insured employers, as well as life insurers, information systems vendors, various service organizations, and universities. All health care organizations that maintain or transmit health information in electronic form must comply by April 2005. Smaller health care organizations have until April 2006 to achieve compliance.

*HIPAA provides for significant civil and criminal penalties for violations of its provisions, ranging from \$100 per violation up to \$250,000 and 10 years in prison. The harshest penalties are for deliberate misuse, particularly for sale or use of information for personal gain, commercial advantage, or malicious harm.*

### THE CHALLENGE... AND THE SOLUTION

As more hospitals connect their databases to the public internet, new security questions similar to those plaguing the financial services and banking industries have arisen. These concerns are primarily about the control of access to proprietary health information and monitoring and reporting security events.

Malicious spyware applications, such as keystroke logging software, are particularly dangerous in the health care environment because they may be inadvertently installed by employees and can go undetected for extended periods of time, resulting in a continuous, long-term outflow of confidential patient, personal, or organizational data. Websense software and services help protect patient data from unauthorized access and prevents unauthorized employees from launching patient data applications or hacking tools to gain access to restricted information.

### Control access to proprietary information

To ensure compliance with HIPAA, health care agencies must ensure that only authorized personnel can use the system or access sensitive information. With Websense software and services, agencies can accomplish this goal by setting appropriate application use policies which can restrict the use of applications by user, group, workstation, or network. Agencies can also elect to prevent employees from using applications that are not on an approved list. These policies can even be enforced on computers that are disconnected from the network.

Since instant messaging and chatting can be used to transmit unauthorized information, Websense software enables agencies to restrict their use to only authorized personnel and to disable the use of IM attachments altogether if that is the organization's policy.

With very few exceptions, P2P applications have no use in a business environment. Since P2P is often used to surreptitiously download unwanted, malicious piggyback programs, Websense suggests that P2P applications be restricted, as well as access to websites from which P2P applications can be downloaded.

Websense software and services prevent employees from visiting harmful websites, thus protecting them from acquiring malicious code or becoming victims of phishing or hacking. Websense software also helps protect patient data from unauthorized access by allowing IT administrators to block the launch of software applications by category, such as spyware, hacking tools, or games, while allowing free access to all other categories of software previously defined as allowable by the organization.

### Report security events

Several Websense reporting and analysis tools can be used to ensure effective monitoring. With real-time network statistics on application usage and knowledge of the specific computers involved, administrators have the information they need to understand the threats facing the organization. Administrators can also drill down on reports of network usage by protocol signature, username, user group, and by destination IP or hostname to find more detailed information. Reports can also be defined and scheduled for automatic distribution to administrators via email.

The monitoring activities help identify security issues that need to be addressed.

### CASE IN POINT – SHARP HEALTHCARE

Sharp HealthCare, San Diego's most comprehensive health care provider and a recognized leader in the use of internet-based technologies, uses Websense to protect the computing environment and confidentiality of its patients' health information from emerging threats such as spyware, keystroke logging programs, employee internal hacking, and internet-borne virus outbreaks. Sharp HealthCare's implementation of Websense helps enable the company to comply with HIPAA's privacy and security rules.

"Sharp HealthCare has been honored for the fifth year in a row as one of the nation's most wired health care systems. As we continue to increase our use of internet technology to improve efficiency and patient care, it becomes both more important and more difficult to protect the privacy of our health information," said Patric Thomas, vice president, enterprise architecture and support, Sharp HealthCare. "Caring for our patients is at the heart of every technology initiative we implement, and we see Websense as an essential solution to defending the security of our patients' and employees' confidential information."

Websense also enables the highest degree of end-point security with its "lockdown mode." This feature enables IT administrators to easily create an approved "white list" of software applications for each desktop and prevent the launch of any application not included on the list. In the health care environment, Websense also prevents unauthorized employees from launching patient data applications or hacking tools to gain access to restricted information.

"Malicious spyware applications pose a rapidly growing privacy and security threat to companies, especially for health care organizations where keeping patient information confidential is absolutely critical," said Bill Goldbach, vice president of sales, North America, for Websense, Inc. "Sharp HealthCare's use of Websense products is an example of our commitment to providing best-of-breed technology solutions that can be utilized to help health care organizations meet HIPAA regulations."

*Websense is helping Sharp HealthCare work toward its goal of HIPAA compliance by enforcing appropriate application use policies and providing reporting and analysis tools that give Sharp HealthCare insight into potential security weaknesses.*

#### About Websense, Inc.

Websense, Inc., the global leader in web filtering and a premier provider of web security software, is preferred by leading Fortune 500 and FTSE 100 customers, as well as government agencies. Websense's employee-centric software and services increase employee internet productivity and secure organizations from emerging internet threats by providing a proactive web security component that complements traditional security solutions. Only Websense delivers flexible, integrated policy enforcement at the internet gateway, on the network, and at the desktop. Websense is trusted to provide solutions to over 18 million employees worldwide. For more information, visit [www.websense.com](http://www.websense.com).

© 2005 Websense, Inc. All rights reserved. Websense and Websense Enterprise are registered trademarks of Websense, Inc. in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other logos and trademarks are the property of their respective owners. BR-SLLUS R.01.06.05



Websense, Inc.  
10240 Sorrento Valley Road  
San Diego, California 92121  
USA  
Tel: 800.723.1166 or 858.320.8000  
Fax: 858.458.2950  
[www.websense.com](http://www.websense.com)