

Ensuring Information Security: New Regulatory Challenges



How Websense Helps Organisations
Achieve Regulatory Compliance In The UK

Regulatory agencies in the UK and abroad have recognised the need for strong controls in managing proprietary customer and financial information. This paper addresses some information security requirements common to many of these regulations and explains how Websense® software and services can help companies ensure the security of their corporate networks and achieve and demonstrate compliance.

The Role of IT Security in Compliance

While the first five years of the so-called Noughties saw the corporate world rocked by scandal and fraud, the next five could ultimately be remembered for ushering in an era of openness and transparency in corporate governance.

Never has regulatory intervention been so high on the boardroom agenda with new legislation emerging at alarming speed and with rapid frequency. Since the financial scandals of Enron, WorldCom and Arthur Andersen, several major regulations have been introduced—the Sarbanes-Oxley Act, Companies Act, Data Protection Act, Basel II, and Combined Code (to name a few)—that impose new restrictions on organisations, establish standards for corporate governance, and institute penalties for non-compliance.

The list of regulations might not seem relevant to the everyday activities of most employees, let alone trip easily off the tongue, but this legislative drive is feeding investment levels in technology and processes not seen since the heights of Y2K. Compliance is the buzzword of the Noughties and companies would be foolish to ignore the pressures of regulatory intervention.

While each law has its own agenda, there are some overriding issues that this new legislation collectively addresses: audit controls, information management, financial reporting, risk management and security.

Security has a significant role to play, given that some of these regulations are designed to prevent security breaches—from viruses, spyware and malware, for example—and make companies more accountable in how they protect both corporate and customer data.

Collectively, this new breed of regulations sets forth the need for companies to do the following for their employees, stockholders and customers:

- Protect the security of the company's network infrastructure—establishing controls to prevent intruders from placing unauthorised files and programmes in the company network, accessing and capturing private or proprietary information, and transferring that information to unauthorised destinations;
- Control access to customer records and personal information—setting and enforcing policies on who should have access to different types of information;
- Monitor communications entering and leaving the organisation, 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 relevant regulatory agency.

In theory this shopping list of requirements is clear in its demands, but in reality, many organisations are still hazy about their timeframe of compliance and the security controls they need to enforce.

Organisations face a complex dilemma in securing the computing environment they rely upon to conduct business. Never before has the employee computing environment offered such easy access to rich content and tempting new applications on the internet. Yet each of these brings with it a new security risk and a potential backdoor for unwanted visitors.

At the same time, IT managers are under tremendous pressure to provide an open, collaborative networking environment and to allow employees to benefit from developments in technology that enable them to work outside of the office, on site with customers, or implement flexible working practices. Yet the current security environment brings with it challenges that lead many companies to shy away from implementing new working policies, or worse, taking a gamble and risking it regardless of the potential dangers it presents to their organisation.

In recent years, there have been a series of new and increasingly alarming web-based threats, which threaten to impact not only the IT department, but executive management as well. A new threat appears to emerge every day, whether through web-based attacks, spyware, malicious mobile code, phishing, or hacking. These threats cost organisations an estimated \$16.7 billion in 2004, according to Computer Economics. Remote internet access and wireless devices have also

expanded the network perimeter and the potential for attacks.

Consider the following:

- 99% of companies use antivirus software but 78% of them were hit by viruses, worms and so on (2004 CSI/FBI Computer Crime and Security Survey);
- A survey of three million corporate computers found 83 million instances of spyware (Gartner Group, September 2004);
- 90% of businesses suffered hacker attacks in the last year (Websense, February 2005);
- 55% of large European companies have suffered from IT security breaches of one sort or another—the worst affected country is the Netherlands, where 73% of companies have been attacked (Stress of Security report, February 2005).

This white paper summarises some of the 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.

Sarbanes-Oxley Act

BACKGROUND

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." While this might not sound too complicated on paper, SOX is, according to PricewaterhouseCoopers, "the single most important piece of legislation affecting corporate governance, financial disclosure and the practice of public accounting since the US securities laws of the early 1930s."

SOX was written to address some of the issues revealed during the incidents involving Enron, WorldCom, and Arthur Andersen. As such, it aims to prevent corporate mismanagement by requiring better controls and accountability for corporations. Non-compliance will typically result in fines, but if the stock market reaction to Enron or WorldCom is any indication, a loss of shareholder trust and market status is also highly likely.

SOX affects companies that report to the Securities and Exchange Commission (SEC), hence it primarily affects US companies. But any

European company listed on a US stock exchange, any European subsidiaries of US companies, or even foreign auditors on US-listed companies are also affected by its regulations.

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

Public companies with a market capitalisation 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 unauthorised transactions. Few CEOs or CFOs will also want to



sign off their company data if they have any concerns that internal controls could have been compromised.

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.

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.

Control access

To ensure compliance with the SOX Act, controls must be in place to ensure that only those people who are authorised 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 instant messaging (IM), peer-to-peer networks (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 organisation. 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 such as AOL, Yahoo, and MSN. Many IM clients allow users to attach files to send to one another, introducing the risk of employees sending confidential company information as IM attachments.

With Websense software and services, companies can establish and enforce 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 do their jobs effectively. Websense software and services ensure that employees are protected while they do so, and that those 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.

Ensure network security

Traditional corporate security measures typically include a combination of one or more firewalls and antivirus software. Although these security tools are critical, they are no match for the sophisticated, blended web attacks that have recently been unleashed. Additional security defences 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, malicious code and so on), 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 unauthorised 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 of which could be 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 the up-to-date information they need. The results of the monitoring activity can provide early identification of security issues that need to be addressed.

The Companies Act

BACKGROUND

On 10 July 2003, the UK Government announced its plans for reforming company law. Their plans consisted of three elements:

- Early legislation to implement changes to the law following recent major corporate failures and to help restore investor confidence in companies and financial markets;
- The introduction of a statutory Operating and Financial Review (OFR) for large companies;
- Programme of comprehensive reform of company law, following the independent Company Law Review and the Modernising Company Law White Paper, with the aim of providing a modern, cost-effective, fair and transparent framework for business, shareholders, creditors and others.

To give it its full name, the Companies (Audit, Investigations and Community Enterprise) Act 2004 was the result of the first element of the Government's review and came into force at the beginning of the year. According to Mike Davis, senior research analyst at Butler Group, it "will have as radical an impact on UK companies as the Sarbanes-Oxley Act in the US."

The Companies Act follows in the wake of corporate scandals at Enron, WorldCom and, more closer to home, Parmalat. As such, its aim is to prevent similar corporate scandals happening in the UK by improving the reliability of financial reporting and strengthening investor confidence in corporate governance, company accounting and auditing practices in the UK. Specifically, the Act makes the following demands of companies:

- Directors must make a statement in the directors' report about the disclosure of relevant information to their auditors;
- Large and quoted companies need to publish details of non-audit services provided by their auditors;
- Professional accountancy bodies that supervise auditors need to sign up to independent auditing standards, monitoring and disciplinary procedures.

In addition, the Government aims to improve checks and balances in reporting and auditing financial information by:

- Giving the Financial Reporting Review Panel (FRRP) new powers to demand documents and broadening its scope;
- Allowing the Inland Revenue to pass information about suspect accounts to the FRRP;
- Improving investigators' access to relevant information;
- Reducing the possibility of delay or obstruction by companies under investigation;
- Removing a possible deterrent to individuals volunteering information when complaints are vetted for possible investigation;
- Introducing more effective sanctions.

The Companies Act does not directly refer to information security, but it demands that companies put in place proper checks to ensure all data relating to trades and accounting practices is auditable, requires organisations to ensure their data is secure and they have established comprehensive security policies.

THE CHALLENGE... AND THE SOLUTION

The Companies Act does not directly refer to information security, but it demands that companies put in place proper checks to ensure all data relating to trades and accounting practices is auditable, requires organisations to ensure their data is secure and they have established comprehensive security policies.

The integrity of financial reporting, accounting and auditing can be demonstrated through three areas of information security:

- Reducing company exposure to security breaches, whether from inside the organisation or an external threat;
- Preventing unauthorised access to data to ensure key data is not compromised by malicious attacks or viruses;



- Improving security policies to identify whether a company is at risk of non-compliance.

The aim of the Companies Act is to help restore investor confidence in financial markets, auditing practices and corporate governance within companies. As with the Sarbanes-Oxley Act, directors need to ensure that no information has been disclosed that could put them in breach of accounting and auditing practices, otherwise they risk criminal charges and heavy fines.

Ensuring the independence of auditors and providing them with access to any information they request, demands organisations to monitor all forms of communication—whether through traditional means or new internet-based



communication, such as instant messaging (IM) or web chat—and be able to show that they are abiding by the Act.

Reduce exposure to security breaches

No matter how compliant an organisation is with the Companies Act, they are putting their organisation at risk of non-compliance if their systems are insecure. Despite 99% of companies using antivirus software, 78% were still hit by viruses, worms and other malicious attacks, according to the 2004 CSI/FBI Computer Crime and Security Survey.

This statistic alone suggests that antivirus software is not enough to protect the corporate

infrastructure. In addition to the usual armoury of firewalls, VPNs and access management systems, companies need tools to tackle internet-based security threats, such as spyware, phishing and P2P-borne malware. Research has shown that 92% of organisations with more than 100 employees have been contaminated with spyware, yet ignorance amongst employees about what spyware is or how it can infect their systems runs almost as high.

Websense software and services can help organisations reduce the risk of having their systems attacked. For example, Websense can protect an organisation from a malicious code outbreak, preventing a new worm, virus or Trojan horse from destroying all or some of the data regulated under the Act. Websense provides industry leading internet filtering and the Websense Master Database contains the most frequently accessed sites and protocols on the web. Organisations can set custom policies to prevent harmful applications from executing—such as spyware, a phishing email or malcode from a peer-to-peer application—and also log any systems involved in an attack so companies know exactly which data might have been compromised.

Prevent unauthorised access to data

Taking control of information lies at the heart of the Companies Act, and Websense software and services can help organisations meet this requirement by preventing wrongdoing and reporting on sources of attacks. An Employee Internet Management policy enables companies to enforce internet usage policies by preventing access to certain sites and applications, such as IM. Policies can be set to always block these applications or access, or they can be customised to allow employee access at set times, such as after 6pm or during lunchtime.

This prevents not only attacks from entering the network through external means—such as spyware, keyloggers and phishing—but also malicious employees from trying to launch an attack from the inside. Even if an employee tries to bypass the corporate email system by using a web-based email service, such as Hotmail, the system can be configured to prevent this application from loading. An additional benefit of

using Websense is that it protects companies from the threat of litigation from employees exposed to inappropriate, obscene or illegal content, which could in turn lead to a knock in consumer confidence or drop in the company's share price.

A central tenet of the Companies Act is that key stakeholders can regularly access information on a company's performance. The Websense Explorer reporting tool can be configured to provide relevant information relating to employees' use of the internet and related risks to the necessary people securely, thereby increasing the integrity of any data being passed to third parties.

Improve security policies

Given the penalties directors face for non-compliance, it is vital that companies can ensure they have in place proper internal checks for their auditable data and can demonstrate they are continually improving these to ensure future compliance as well. Websense Enterprise includes reporting and analysis tools that offer real-time and historical views of company risks and employee computing, which can be used to review and build upon security existing policies.

The Data Protection Act



BACKGROUND

The Data Protection Act 1998 seeks to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal information. One of the oldest laws relating to IT, it gives individuals certain rights regarding information held about them and places obligations on those who process information (data controllers), whether it relates to facts or opinions about the individual.

The Act is all encompassing and anyone processing personal information must notify the Information Commissioner's Office that they are doing so, unless their processing is exempt. Given that most organisations store information about individuals, it has implications for the majority of UK businesses. For example, under the Act, individuals can find out what information is held about them on computer, ask a data controller not to process information about him or her that might cause distress, and claim compensation if a data controller has breached the Act.

There are eight principles of good practice that anyone processing personal information must comply with. These say that data must be:

1. Fairly and lawfully processed;
2. Processed for limited purposes;

3. Adequate, relevant and not excessive;
4. Accurate and up-to-date;
5. Not kept longer than necessary;
6. Processed in accordance with the individual's rights;
7. Secure;
8. Not transferred to countries outside European Economic area unless the country has adequate protection for the individual.

Anyone failing to comply faces the possibility of criminal sanctions and the Act has created a number of new criminal offences that organisations need to be aware of.

Anyone failing to comply faces the possibility of criminal sanctions and the Act has created a number of new criminal offences that organisations need to be aware of, covering actions such as failing to notify the Commissioner if data is being processed; disclosing personal

information without the consent of the data controller (except where it relates to crime prevention/detection); and sending out unsolicited electronic marketing communications.

The challenge for organisations is that although the Act might seem clear on paper, data protection issues are complex and areas of the Act continue to be modified by the Information Commissioner's Office.

THE CHALLENGE... AND THE SOLUTION

Information security is highlighted as one of the eight principles of good practice under the Act and, on the whole, the Act makes more explicit reference to IT than other recent legislation. For example, with regards to security, the law states, "appropriate technical and organisational measures should be taken against unauthorised or unlawful processing of data, as well as against accidental loss, destruction, or damage to such data." The challenge for organisations lies in determining how far their "technical and organisational measures" will extend and what systems they have in place to maintain the integrity of personal data.

Compliance with the Data Protection Act can be demonstrated through three areas of information security:

- Ensure the security and integrity of IT systems;
- Control access to proprietary information;
- Protect the organisation from other companies breaching the Data Protection Act.

Organisations need to take a two-pronged approach to the Data Protection Act: firstly, they must ensure that the information they hold on individuals is accounted for, registered with the Information Commissioner's Office, and meets the regulatory commitments. Secondly, they must ensure that they are not a victim of another company's violation of the Data Protection Act, which could potentially open up their systems to unwanted security breaches.

Ensure the security and integrity of IT systems

One of the biggest hurdles for organisations in complying with the Act lies in demonstrating the integrity of their data and its security. Ensuring that a company's network is secure is one of the first steps to accomplishing this goal. Spyware, keyloggers, Trojan horses, internal hacking, instant messaging (IM) and peer-to-peer (P2P) usage could all directly impact the integrity of a company's data if it bypasses their security systems. Using Websense software and services, organisations can stop these malicious threats in their tracks, thereby ensuring that personal information is secure.

Websense Enterprise works by blocking spyware, phishing sites and other malicious mobile code, even if the attempt is from within an organisation by an employee innocently trying to access one of these sites, share files using P2P or chat on IM, for example. Network administrators can also set policies that block the sending and receiving of IM attachments, thereby minimising the possibility of viruses or worms being imported via IM applications, and reducing the overall danger that personal data could be leaked out to an unknown party or corrupted.

Control access to proprietary information

Ensuring that personal information does not get into the wrong hands is key to complying with the

Data Protection Act. After all, what happens if personal customer information is leaked as a result of a spyware infection? The company in question could end up facing not only criminal charges, but also a loss of shareholder trust and drop in customer confidence.

In addition to protecting systems from internet-based threats, Websense software and services can help organisations extend control to laptops being used remotely by staff, which might also contain personal information. Websense Client Policy Manager (CPM) prevents malware from infecting an organisation when reconnected to the corporate network by stopping unauthorised applications from running or accessing the network, and blocking application network access to specific ports and protocols by application category. In particular, it helps safeguard data held on corporate systems during a virus outbreak—before patches and antivirus updates can take effect—by blocking the launch of malware, spyware, keyloggers, etc.

Specific provision is made under the Act for processing sensitive personal information—such as racial or ethnic origin—and organisations must demonstrate at least one of several extra conditions to ensure compliance with the Act. Websense works with several prominent customers responsible for large amounts of sensitive information. Using Websense software and services, these organisations have been able to demonstrate the security of their network in protecting the integrity of personal data.

Protect the organisation from other companies breaching the Act

As well as ensuring their own compliance with the Data Protection Act, organisations also need to put in safeguards to ensure they do not fall victim to another company's non-compliance. For example, a key provision included in this Act refers to unsolicited electronic marketing communications. The Act expressly says that "unsolicited marketing emails or SMS should not be sent to any individual subscriber who has not consented unless the email address or phone number was collected in the context of a commercial relationship."

Otherwise known as spam, unsolicited marketing

emails are not only a nuisance to network managers, but also pose a security threat. It has been suggested that around 40% of all spam received by companies can be attributed to spyware/adware. More worrying still, many pieces of malicious code contain the capability to take control over systems and act as spam mail relays. Websense software and services can help reduce the amount of spam—obviously any breach of the Act should also be referred to the Information Commissioner—by blocking spyware from running. It can also reduce the possibility of corporate systems—and the data held on them—being compromised by stopping malicious web sites or malware executing on the corporate network.

Basel II Accord

BACKGROUND

If there is one piece of new legislation keeping IT directors at financial services providers awake at night, it is Basel II—one of the most important changes in financial services legislation in the last 15 years.

The purpose of Basel II—otherwise known as the second Basel Accord—is to ensure that financial institutions manage risk so that they have the capital to cover exposure to debt. The original Basel Accord was agreed in 1988 by the Basel Committee on Banking Supervision. According to the Financial Services Authority (FSA), the 1988 Accord, now referred to as Basel 1, “helped to strengthen the soundness and stability of the international banking system as a result of the higher capital ratios that it required.”

It continues, “Basel II is a revision of the existing framework, which aims to make the framework more risk sensitive and representative of modern banks’ risk management practices.” In an industry already heavily regulated, the aims of Basel II are to increase transparency, reduce the risk of fraud and prevent consumer loss or market disruption from the imprudent management of risk.

Crucially, Basel II brings operational risk into its definition of risk as a factor in determining capital requirements. It is not enough for organisations to know their risk within separate business units; they must also be able to assess, manage, control and quantify operational risk across the whole organisation.

Herein lies the challenge for organisations because enterprise-wide risk management is a significant undertaking. Little wonder then that Metrica Research estimates hundreds of millions of pounds will be spent in the UK alone on technology to comply with Basel II. Management consultancy McKinsey puts the cost between \$100 million and \$250 million, depending on the organisation’s size.

The FSA has outlined below the four main components of the new framework:

- It is more sensitive to the risks that firms face—the new framework includes an explicit measure for operational risk and includes more risk sensitive risk weightings against credit risk;

- It reflects improvements in firms’ risk management practices, for example by the introduction of the internal ratings based approach (IRB) that allows firms to rely to a certain extent on their own estimates of credit risk;
- It provides incentives for firms to improve their risk management practices, with more risk sensitive risk weights as firms adopt more sophisticated approaches to risk management;
- The new framework aims to leave the overall level of capital held by banks collectively broadly unchanged.

The new Basel Accord will be implemented in the EU via the Capital Requirements Directive (CRD). The FSA will be responsible for ensuring compliance with the Accord in the UK by January 1, 2007. However, Basel II dictates that companies need to show five years’ worth of historical data, which means that financial service providers need to either be collecting the data already, or able to backfill their data sets. Furthermore, from January 1, 2004, finance organisations need to demonstrate that they have been using a rating system for risk in line with the Basel requirements.

Compliance with Basel II requires financial services providers to conduct a fundamental review of their business processes and IT systems to ensure that they can control and monitor credit risk exposure.

The new framework consists of three ‘pillars’:

- Pillar 1 of the new standards sets out the minimum capital requirements firms will be required to meet for credit, market and operational risk;
- Under Pillar 2, firms and supervisors have to take a view on whether a firm should hold additional capital against risks not covered in Pillar 1 and take action accordingly;

- The aim of Pillar 3 is to improve market discipline by requiring firms to publish certain details of their risks, capital and risk management.

While the legislation might seem onerous, there are also incentives for organisations to comply. If an organisation can demonstrate that it knows what its risk are and has processes in place to support that risk, the authorities might be willing to reduce the amount of capital a financial services provider is required to maintain. Compliance could, therefore, give one organisation a lead, or competitive advantage, over another.

THE CHALLENGE... AND THE SOLUTION

Compliance with Basel II requires financial services providers to conduct a fundamental review of their business processes and IT systems to ensure that they can control and monitor credit risk exposure. Under Basel II, operational risk is defined as “the risk of losses resulting from inadequate or failed internal processes, people and systems or external events.” The Accord identifies a range of operational risk types including:

- Internal fraud;
- External fraud;
- Clients, products and business practices;
- Business disruptions and system failures;
- Execution, delivery and process management.

Many of these risks relate to information systems, so there is clearly a strong role for information security to play in minimising risks from threats inside and outside the organisation. Specifically, organisations can address compliance with Basel II by putting in place the following procedures:

- Control access to corporate systems and information to reduce risks associated with fraud, wrongdoing or attempts to circumvent company policy;
- Enforce and monitor company policy on employee internet use to prevent employees inadvertently or maliciously providing a backdoor to unwanted risks;
- Keep risk management policies current and fresh by regularly reviewing new and emerging threats.



Financial organisations are probably most at risk from current and emerging threats such as phishing, spyware and keylogging. They are also the primary targets of internet hackers and fraudsters and, as such, routinely have to deal with security compromises. Take the example of Japanese bank Sumitomo Mitsui, which was targeted by cyber criminals in October 2004 intent on stealing £220 million from its London offices after hacking into the bank's systems using keylogging software. This is just one example of the threats organisations face in managing risk across their organisation in line with Basel II requirements.

Control access to corporate systems and information

Organisations face several types of fraud in the current environment. The first type is phishing, which primarily affects end users but has a knock-on effect for the financial institutions, responsible for reimbursing duped end users. As an evolution of phishing, there are an increasing number of cases taking place now where people are gaining access to loans via deception. This is similar to identity theft where fraudsters capture details of end users—via phishing, keylogging and other means—to obtain loans and finance based on the identity of the victims.

A third type of fraud is the malicious employee who gains access to internal systems and then uses this level of access to steal funds or attempt to

corrupt the business in some form. The employee does not necessarily require elevated levels of access—he or she could have obtained access by using hacking tools or keylogging software. In each case, controlling access to corporate systems and information is a significant way of reducing the risk of falling victim to fraud or wrongdoing.

Websense software and services provide enterprise-wide internet filtering at multiple points at the gateway, on the network and on the desktop to protect against threats such as phishing, keylogging, spyware and malicious mobile code (MMC). According to industry data, nearly half of all MMC can be embedded on web sites that many companies would normally allow employees to access freely, such as travel sites and search engines.

Using Websense software and services, organisations can also prevent peer-to-peer file sharing, employee hacking and manage instant messaging securely. In addition, network administrators can set policies that block the sending and receiving of file attachments, minimising the possibility of viruses or worms being imported via IM applications.

Enforce and monitor company policy on employee internet use

Websense solutions can be used to help the IT department automatically enforce a company's

internet usage policy which governs what employees can and cannot access online. Even if an employee is mobile and using a laptop to connect to the network at sporadic times, organisations can prevent network access by application type, and stop the execution of any unauthorised applications. This prevents mobile workers from jeopardising compliance with Basel II.

Keep risk management policies current

One of the challenges organisations face in complying with Basel II is keeping up-to-date with its regulations. A second challenge is ensuring that their systems are complying at all times with the legislation. Websense specialises in delivering internet monitoring and policy enforcement capabilities to help organisations tackle the threat of new and emerging technologies. Using Websense, companies have the ability to perform regular risk analysis activities to ensure they fully understand the current risk they are exposed to.

Combined Code

BACKGROUND

Unlike other legislative Acts mentioned in this paper, companies not adhering to the Combined Code will not be breaking the law or face heavy penalties. The Combined Code is based on instilling good practices within organisations around corporate governance, accounting and auditing. However, listed companies not complying must be prepared to state in their Annual Report their reasons for doing so.

Corporate governance has been a feature of regulation since the Cadbury Committee published its Code in May 1991. The Committee, which was set up by the Financial Reporting Council (FRC), London Stock Exchange and accountancy profession, proposed the following recommendations:

- The board should meet regularly, retain full and effective control over the company and monitor the executive management;
- There should be a clearly accepted division of responsibilities at the head of a company;
- Directors should report on the effectiveness of their system of internal control, and the auditors should report on their statement;
- Directors' service contracts should not exceed three years without shareholders' approval;
- The board should establish an audit committee of at least three non-executive directors with written terms of reference that deal clearly with its authority and duties.

The Code was strengthened in relation to directors' remuneration in 1995 by a study group led by Sir Richard Greenbury, then chairman of retailer Marks & Spencer. Three years later, the Combined Code was issued and included recommendations from the Cadbury and Greenbury committees. Some of its proposals included:

- Companies should publicly justify a decision to combine the posts of chairman and chief executive officer in one person;
- Boards of directors should set up remuneration committees of independent non-executive directors to make recommendations to the board on the company's framework of executive remuneration;
- The directors should, at least annually, conduct

a review of the effectiveness of the group's system of internal control and should report to shareholders that they have done so. The review should cover all controls, including financial, operational and compliance controls and risk management.

A year after the Combined Code was published the Internal Control Working Party of the Institute of Chartered Accountants in England and Wales published the Turnbull Report to assist listed companies in implementing the requirements in the Code relating to internal control.

In July 2003, a revised version of the Combined Code was published by the FRC, incorporating many of the recommendations of the Higgs Report, which reviewed the role and effectiveness of non-executive directors, and the Smith Report, which gave guidance on audit committees. The revised Code came into effect in November 2003 and some of its key requirements include:

IT governance clearly has a valuable role to play in helping organisations manage risk effectively and demonstrate that they have in place internal controls covering "financial, operational and compliance controls and risk management systems."

- Non-executive directors should scrutinise the performance of management in meeting agreed goals and objectives and monitor the reporting of performance. They should satisfy themselves on the integrity of financial information and that financial controls and systems of risk management are robust and defensible;
- The roles of chairman and chief executive should not be exercised by the same individual;
- Except for smaller companies, at least half the board, excluding the chairman, should comprise non-executive directors determined by the board to be independent;
- The directors should explain in the annual report their responsibility for preparing the accounts

and there should be a statement by the auditors about their reporting responsibilities;

- The board should, at least annually, conduct a review of the effectiveness of the group's system of internal controls and should report to shareholders that they have done so. The review should cover all material controls, including financial, operational and compliance controls and risk management systems.

THE CHALLENGE... AND THE SOLUTION

With an emphasis on internal controls and risk management in the revised Combined Code, IT governance clearly has a valuable role to play in helping organisations manage risk effectively and demonstrate that they have in place internal controls covering "financial, operational and compliance controls and risk management systems."

In particular, information security can assist organisations in complying with the Code in three ways:

- Enforce internal controls around network security;
- Monitor and record internet use to meet transparency requirements of the Code;
- Test and review the security of the IT environment with a view to making continual improvements.

Enforce internal controls around network security

The Turnbull Report made some key recommendations on internal controls that companies need to have in place to fulfil their business objectives, safeguard shareholders' investment and minimise the possibility of being unnecessarily exposed to avoidable financial risks.

Preventing fraud is a key part of the preventative measures companies need to have in place to comply with the Code. However, the challenge for organisations is that the web-based threats they face today are growing in number, complexity, and cost. Traditional security products, such as antivirus software and firewalls, play a significant role in combating these security threats, but have inherent time and technology gaps that leave organisations vulnerable. Websense Web Security Suite complements existing security products by offering organisations a comprehensive internet



security solution that protects them from both internal and external web-based threats.

One of these new threats comes from phishing emails, which having been growing in number each month by 26% since July 2004 (according to the Anti-phishing Working Group). Websense software and services can help organisations protect their IT network from such threats by blocking phishing emails and malicious mobile code (MMC) from launching, as well as spyware and keylogging transmissions being sent back to their host sites. It also controls the sending and receiving of instant messaging (IM) clients, which many employees use to send information around and outside their organisation.

Organisations also worried about employee activity away from the office can rest assured that Websense Client Policy Manager will stop laptops from infecting the network when they are re-connected by preventing unauthorised applications from executing.

Monitor and record internet use

As with most regulations around corporate governance, a key aim of the Code is to make today's organisations even more open and transparent in their financial dealings, auditing and accounting practices. An Employee Internet Management policy can help enforce auditable and transparent working practices by controlling employee access online.

Websense software and services ensure that employee and management actions carried out on the internet are logged centrally. This means that if an employee unwittingly responds to a phishing email or maliciously tries to hack into corporate systems, IT administrators can identify who has caused the security breach and then act to stop any damage being inflicted.

Test and review the IT security environment

The risks and challenges an organisation faces are constantly evolving. As such, any risk management strategy and system of internal controls need to be continually evaluated and monitored. As the Turnbull Report points out, "since profits are, in part, the reward for successful risk-taking in business, the purpose of internal control is to help

manage and control risk appropriately rather than to eliminate it."

Websense recognises that a virus-free world will never exist and its software and services can be used by organisations as part of a wider risk management / risk analysis framework. Its collection of analysis and reporting tools provide IT administrators with the ability to identify, analyse and report on internet and desktop application activity and the risks associated with employee computing.

As a leading authority on the latest web-based security threats, Websense can offer organisations up-to-date information on the security risks they face. It is also continually striving to improve and build on its existing product base to safeguard organisations and help them meet their compliance goals now—and in the future.

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 organisations 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 protect over 24,000 organisations worldwide.

For more information, visit www.websense.co.uk.

DISCLAIMER: This Document is provided "as is" without any express or implied warranty. While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with a lawyer. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by Websense.

© 2005 Websense, Inc. All rights reserved. Websense, Websense Enterprise and Websense Web Security Suite 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-SLLUK R.06.05



Websense UK Ltd.
3000 Hillswood Drive
Chertsey, Surrey KT16 0RS
United Kingdom
Tel: 01932 796001
www.websense.co.uk