SOPHOS

Laws, regulations and compliance:
Top tips for keeping your data under your control

The challenge of complying with a growing number of frequently changing government, industry and internal regulations designed to protect data is becoming harder and more expensive to manage. This paper outlines the rules, looks at the main threats to security compliance and highlights how a well-defined strategy, backed up by powerful technology can provide the solution.

A Sophos white paper

December 2008

Laws, regulations and compliance:
Top tips for keeping your data under your control

The rise of compliance as an issue

High-profile losses of confidential data from TJ Maxx, the US Department of Veterans Affairs, the UK's Child Benefit department, and other large organizations have raised awareness of the need to protect information. Governments and industry worldwide have responded with an increasing number of more complex and frequently changing regulations. This has made compliance more expensive to manage and has raised it as a significant issue for organizations today.

IT departments have become increasingly tasked with protecting their organizations not only from security risks, but from compliance risks such as failed audits, steep regulatory fines and criminal penalties, loss of credit card processing privileges, and adverse publicity. The importance compliance now has can been seen in figure 1, which shows how respondents to a SearchSecurity.com survey answered the question "What are key drivers of data protection at your organization?"[1]

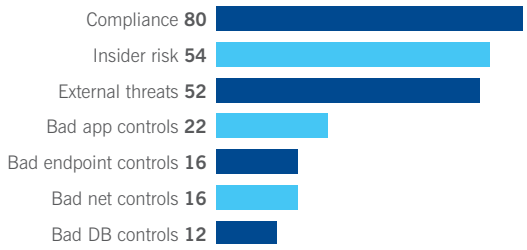

Figure 1: Data protection drivers

What is compliance?

In this paper, "compliance" refers to the need for organizations to meet

- government
- industry and
- internal

laws, regulations and policies

A well-orchestrated IT security strategy protecting your servers, endpoint computers and data goes a long way to helping you achieve compliance with the myriad laws and regulations that now exist. However, the challenge comes not so much in creating the strategy but in ensuring that all managed, guest and mobile computers connecting to your network adhere to that strategy 24/7, and that internal policies relating to employees' responsibilities for protecting data are understood and adhered to.

External legal and regulatory requirements

Many people think of government regulations when they think of compliance, but in fact regulations from outside the organization come not just from government but also from industry. Each has its own requirements but the driving force for all of them is the need to stop the intentional or unintentional exposure of two key types of confidential data:

- Personal – customer, partner and employee
- Business – plans, intellectual property and financial.

Government regulations

Over the past decade a raft of government regulations have introduced requirements, some more specific than others, for protecting and retaining corporate information over time. Many address specific areas of business.

- **Healthcare** HIPAA (Health Insurance Portability and Accountancy Act standards) established national standards in the US in 1996 for electronic healthcare transactions.
- **Government** CoCo (Code of Connection) is a UK government standard to be used when connecting to government networks.
- **Financial** Sarbanes-Oxley Act (SOX) (passed in 2002 in the wake of the Enron and WorldCom financial scandals) introduced major changes to the regulation of financial practice and corporate governance. All US public company boards, management and accounting firms must comply.

The Payment Card Industry (PCI) Data Security Standard

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks
- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications
- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security

- **Banking** Gramm-Leach-Bliley Act allowed commercial and investment banks to consolidate in 1999 and includes provisions to protect consumers' personal financial information held by financial institutions.
- **Information** EU Data Protection Directive protects the privacy of all personal data collected for or about EU citizens, especially as it relates to processing, using, or exchanging the data.

> *The challenge is in ensuring that all managed, guest and mobile computers connecting to your network adhere to your security strategy 24/7.*

Industry standards

In response to high-profile security breaches certain industries have also come together to create their own sets of guidelines, as demonstrated in the following examples. Several of the standards have an international remit, highlighting the extent of the problem.

- **Credit cards** The PCI DSS (Payment Card Industry Data Security Standard) is one of the most well-known standards (see box) governing the handling of information relating to credit card transactions. It was created by major credit card companies, including MasterCard and Visa, in response to increasing credit and debit card security threats, and is designed to prevent credit card fraud, hacking, and other risks.
- **IT governance** CobiT (Control Objectives for Information and related Technology) is an internationally accepted set of best practices for developing appropriate IT governance and control in a company.
- **Financial** Basel II is an international business standard that requires financial institutions to maintain enough cash reserves to cover risks incurred by operations.
- **Security** Center for Internet Security (CIS) is a not-for-profit organization that helps enterprises reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls. CIS Benchmarks is a set of system hardening configuration settings and actions accepted by many auditors for compliance with a number of regulations, including HIPAA and Sarbanes-Oxley.
- **Standards** ISO (International Organization for Standardization) forms a bridge between the public and private sectors and is the world's largest developer and publisher of International Standards with 157 member countries.

> *Stupidity, malware and lack of organizational rigor can knock even the most well-thought out strategy off course.*

Internal guidelines

Many organizations also have their own internal guidelines, partly to ensure compliance with external regulations and partly to protect them from conflicts of interest, lawsuits, and loss of credibility with their partners, customers, and employees. Some have additional sets of guidelines customized for certain departments and business units.

Acceptable use policies set out the rules for accessing and using company systems and information, and define the responsibilities employees have for maintaining security. These policies can – and should – raise awareness of the risks employees create if they turn off security settings, such as the firewall, or of the vulnerabilities that arise from so-called "configuration drift" where computers fall behind in their security patches and updates.

In addition these internal policies can cover every aspect of data protection including:

- What types of document can be emailed outside (and, indeed, within) the organization
- What data can be stored on mobile laptops and removable media
- Which applications can and cannot be installed
- Any websites or types of website that must not be visited
- The consequences for violating the policy.

Web use in particular has become a top priority, because:

- Huge security vulnerabilities are created by the rapidly expanding number of infected websites
- Music downloading, video sharing, gaming, pornographic, and social networking sites reduce employee productivity, and consume bandwidth and data storage space
- Downloaded content might be offensive to other employees making the organization liable to legal action.

Compromising compliance

Organizations can find themselves out of compliance with these regulations in a number of ways but in every case non-compliance risks the loss of data that the rules are designed to protect.

Ignorance/stupidity

It is worth pointing out that while a large number of data leakage incidents are intentional, the overwhelming majority, up to 98 percent[2], are actually unintentional, based on user error or ignorance of corporate policy. Furthermore, many of the largest and most publicized security breaches have involved lost or stolen laptops and USB memory sticks full of confidential customer or employee information, rather than infiltration of the corporate network.

Malicious software

That said, the threat from malicious software is significant. Although the cause of only 2 percent of lost data, that data had been deliberately stolen with the express intention of exploiting it for financial gain. Today's malware campaigns, unlike the mischief making sport of five years ago, are targeted, profitable exploits for secretly monitoring, stealing and selling confidential information. In December 2008, for example, the accounts of 21 million German bank customers were being offered for sale on the black market for 12 million euros by a hacking gang.[3]

Other campaigns are focused on harnessing thousands or millions of computers as botnets for spreading spam and popup ads or redirecting search results.

Hackers use a variety of methods to get spyware onto an organization's computers. By far the most likely way today is via a hijacked website. Spammers send out emails containing links to the compromised website, from where a keylogging or other Trojan is downloaded onto the unwitting visitor's computer. These spam campaigns mutate rapidly in an attempt to avoid being detected and blocked.

Other methods for getting company data include spyware being delivered by an external device, such as a USB memory stick, by infected email attachments and through unsecured wireless connections. Data can also be compromised by rootkits that embed themselves in the operating system.

Just a few statistics indicate the scale of the problem:

- In the US the average cost of data breaches in 2008 was just under $300,000, or $500,000 where the breach meant financial data was compromised.[4]
- In the UK, online banking fraud losses from January to June 2008 totaled £21.4m ($31.3m) – a 185 per cent rise on the 2007 figures, and 20,000 fraudulent phishing websites were set up – an increase of 186 percent.[5] 20,000 new samples of suspect code are analyzed every day by SophosLabs.
- A new infected webpage is discovered every 4.5 seconds.[6]
- One new spam-related webpage is discovered every 15 seconds.[6]

Unmanaged or disconnected computers

Laptops used by telecommuters and "road warriors" who have been working from home or connecting to the internet at airports, hotel rooms and the like, might well be out of compliance with your company's security policy when they next connect to the corporate network, and, indeed, might be infected and their data compromised. In one instance 81 percent of corporate computers tested had missing Microsoft security patches, disabled client firewalls, or missing endpoint security software updates.[7]

Similarly, compliance threats come from non-compliant guest users, such as contractors or business partners, who connect to your corporate network to access email or information.

Security policy

Security technology without clear policy is a strategy doomed to failure, since people are often the weakest link in any security strategy.

A security policy is important both strategically and educationally as it gives you an intimate knowledge and understanding of your organization's mission-critical business units, systems, applications, and data, and lets you

- organize
- summarize
- communicate

your organization's security goals, rules and mechanisms.

Your policy should also include assessing for compliance, fixing non-compliance, enforcing when not compliant, and reporting compliance issues.

Enforcing compliance

Because today's blended threats to the network are so numerous and come from so many different sources, the only viable way to remain compliant with the multiple regulations for protecting data is to create a detailed security policy backed up by powerful integrated technology. You need to ensure that the protection you have covers the endpoint and gateway and that it enables you to track, monitor and enforce:

- compliance
- access control
- anti-malware and anti-intrusion protection
- encryption
- authentication.

Endpoint protection

Endpoint protection should consist of centralized server-based management software that takes care of policy, installation, management and updating.

Anti-malware protection Every desktop, laptop and device that has access to your network needs to have proactive protection against zero-day threats for which signatures do not as yet exist. They also need to be constantly up to date with the latest security patches and updates – be it your own organization's or belonging to a visitor, and no matter what operating system it supports. Malware protection needs to go hand-in-hand with centrally managed endpoint firewall protection, which will let you control internet and other connections to and from each computer.

- **Encryption** Hard disk encryption renders data on stolen or lost laptops, USB devices, optical disks and smartphones useless to anyone outside the organization as it can only be read by someone with authorized access and encryption keys.
- **Device control** By preventing employees from writing to CDs, USB drives and other removable media, you can stop confidential information from leaving your organization. Device control can also block wireless connections to ensure they are not used to take confidential information outside the organization.
- **Application control** Centralized monitoring and management of applications that you might not want your employees using, such as Instant Messaging, lets you plug both the security and productivity hole that they create.
- **Authentication** By checking and validating the computers logging on to your network, you can manage and control access to your network, servers, applications and data, and restrict access to only those that need it.

Endpoint compliance and access control

Endpoint compliance and vulnerability management software is the key to ensuring, and enforcing, your endpoint security strategy. It performs the crucial checks that security applications like client firewalls, anti-virus and anti-spyware software, and the latest security updates and patches are installed, enabled and up to date and fully compliant with the corporate security policies at all times.

Non-compliant systems can be brought into compliance by installing necessary applications, patches and updates, or preventing a guest system from accessing anything but the internet. Once connected, these solutions allow access only to applications and data the user is authorized to access.

Endpoint compliance and vulnerability solutions can also provide comprehensive reports on network connections and the compliant posture of devices that have connected in the past, which can be invaluable when preparing for a compliance audit.

Gateway protection

Data protection and policy compliance for email and web traffic is critically important. Protecting the gateway where this traffic leaves and enters is not only the most efficient and effective solution but is also the most transparent to end users. This enables sophisticated centralized organization-wide policy and security that does not impact productivity.

- **Email filtering** By inspecting outgoing email, sophisticated policy options can be used to block, warn, or quarantine sensitive data and unwanted file types while alerting management, administrators, and users of violations. In addition, policy settings can be employed to enforce encryption rules and legal disclaimers. Incoming emails can also be inspected and scanned to eliminate productivity-draining spam as well as malicious content, links or attachments.
- **Email encryption** Encrypting sensitive email at the gateway ensures that confidential or proprietary data is protected from unauthorized access by anyone other than the intended recipient. Central policy management can be applied to ensure complete compliance across the entire organization or particular groups.
- **Web content and URL filtering** By scanning all web traffic for malware and violations of acceptable use policy, you can protect your organization from today's web threats coming from known malicious websites, hijacked trusted websites, malicious web mail, and potentially unwanted applications. It's equally important to filter and control outbound information whether it's being posted by users to forums, sent via webmail, or is the result of a transmission from an infected system on your network.

Conclusion

As new threats arise and new working practices evolve, government, industry and organizations continue to create new regulations to protect sensitive business and personal data. Complying with all relevant regulations and guidelines can seem overwhelming, but with the right combination of policies, technologies, and strategy, you can achieve a fully secure network and enforce compliance.

Sophos solution

Sophos products enable you to comply with security regulations and guidelines comprehensively. Our endpoint, web, email and encryption solutions simplify security to provide integrated defenses against malware, spyware, intrusions, unwanted applications, spam, policy abuse, data leakage. Our network access control technology enables effective endpoint compliance and vulnerability management, providing simple-to-use, pre-packaged policies and helping you to easily meet government, industry and internal regulations.

Sources

1 SearchSecurity.com
2 www.networkworld.com/news/2007/091107-data-leak-prevention.html
3 www.sophos.com/blogs/gc/g/2008/12
4 Computer Security Institute's 2008 CSI Computer Crime & Security Survey
5 www.apacs.org.uk
6 SophosLabs research
7 www.sophos.com/pressoffice/news/articles/2008/06/endpoint-vulnerability-results.html

Boston, USA | Oxford, UK

SOPHOS
WWW.SOPHOS.COM