

# Effective Compliance Practices: Information security, email security, proof of control

A Sophos white paper

May 2005

## SUMMARY

To ensure compliance with current and future legislation, organizations must establish a comprehensive IT security policy that addresses virus protection and email policy enforcement.

---

## Introduction

Major legislation is forcing organizations to change the way they manage information. Regulations like the Sarbanes-Oxley Act, Gramm-Leach Bliley Act, Health Insurance Portability and Accountability Act, and California Security Breach Information Act mandate that organizations must enact stringent policies to safeguard paper-and computer-based data.

Organizations are responding to these regulations, trying to determine what data to keep, how long to keep it, and when to divulge it. However, they can't ignore the underlying need to guard the data itself, and the right data at that.

As email passes through the gateway and across servers, it brings unique challenges to the issue of compliance. IT teams must implement information security mechanisms for protecting their networks against email-borne threats, including viruses and phishing. They must also develop and enforce email security rules in order to ensure collection and dissemination of the right information. Finally, they must have systems in place to verify that they are satisfying legal obligations.

## The need for legislation

Recent legislation is the first step in addressing a range of problems, such as corporate fraud and violations of privacy, which arise when organizations abuse the way they manage information.

---

*Non-compliance can do substantial damage to an organization's credibility and competitive position.*

---

## Corporate fraud

The news is filled with instances of overstated profits, fraudulent accounting practices, private use of company funds, and insider trading. According to SEC Commissioner Cynthia

Glassman, "Much of the behavior we have witnessed recently – greed, sacrificing strategic interests for instant gratification, promoting self-interest over fiduciary responsibility, suspension of rational investment decision-making, and loose lending practices coupled with rampant speculation – have plagued business and the markets throughout recorded history."

The effects of this level of fraud are astronomical. Countless individuals have lost jobs and retirement savings. Investigations have implicated bankers, analysts, auditors, and corporate officers. By 2003, the Association of Certified Fraud Examiners estimated annual losses at \$600 billion. In addition, fraud had dealt a blow to economic growth, which depends on investor confidence.

## Violations of privacy

The computerization of business transactions and record keeping has increased the risk of accidental disclosure. The question has become, what kind of information can companies collect about someone, how can they use it, and how is it protected?

In the healthcare arena a desire to provide better patient care and cost-cutting measures encourages doctors, employers, and insurance organizations to accumulate – and share – personal health information. These practices contribute to healthcare quality and efficient reimbursement but also create more opportunities for inadvertent or malicious disclosure. As attention around these privacy issues increases, patients are becoming more aware of the potential risks and are demanding effective protection from their healthcare providers.

Similar risks are present in the corporate world, where softening of anti-trust laws has permitted banks, insurance companies, and investment firms to consolidate and increase the number of inter-industry mergers. Again, the distributed nature of the data in business creates opportunities for individuals to incorrectly transmit sensitive information, both intentionally and unintentionally.

---

## The legislative response

Federal and state agencies are implementing a range of legislation to address corporate fraud, violations of privacy, and identity theft. SOX, GLB, HIPAA, and SB 1386 provide sets of industry- and domain-specific guidelines, regulations and recommendations.

### SOX

Overseen by the Securities and Exchange Commission (SEC), the Sarbanes-Oxley Act (SOX) has established the Public Company Accounting Oversight Board. This private, non-profit corporation watches over financial audits and holds corporate officers responsible for the accuracy of financial statements. In particular, the act says that management must prevent – or detect in a timely manner – unauthorized acquisition, use, or disposition of systems that could affect financial data. It also specifies the kinds of records companies must keep and how long they must keep them.

---

*Forrester Research believes that micro-sized companies will spend up to \$4.7 million – and large companies will spend up to \$45 million – just to comply with SOX.*

---

### GLB

Under the Gramm-Leach Bliley Act (GLB), the Federal Trade Commission has enacted policies to prevent entities from obtaining personal information under false pretenses. The guidelines cover administrative, technical, and physical safeguarding of personal information. Provisions of GLB require

---

*Organizations that fail to meet GLB regulations face criminal penalties and fines of up to \$11,000 per violation.*

---

financial institutions to verify identities before they provide protected information, and must report suspected identity theft to affected customers and law enforcement. They are also required to monitor their environment in order to protect against “reasonably foreseeable” threats.

### HIPAA

The original intent of the Health Insurance Portability and Accountability Act (HIPAA) was to guarantee portability of coverage. To realize portability in an efficient and secure

manner, HIPAA standardizes the electronic transactions that health plans, healthcare providers, third-party administrators, insurers, and other vendors use to exchange personal data. Because electronic transmission opens the door to violations, HIPAA requires companies to prevent unauthorized access, alteration, deletion, and transmission of electronically stored and transmitted Protected Health Information (PHI). The act defines policies for protecting this information and for notifying consumers of the regulation and allowing them to opt out as desired.

---

*CxOs, auditors, and the like face HIPAA penalties of \$100 to \$25,000 per person ... per year ... per incident of unintentional disclosure; or ten years in jail for wrongful disclosure of medical information; or both.*

---

### SB 1386

The California Security Breach Information Act – also called the California Privacy Act – (SB 1386) requires organizations that maintain personal information about California residents to inform those individuals if the security of their information is compromised. It requires that agencies maintain accurate records of disclosures, and stipulates that businesses must destroy customers’ personal information when it is no longer in use.

## Satisfying compliance regulations

The development of SOX, GLB, HIPAA, and SB 1386 have been driven by different needs and circumstances. However, the acts have much in common.

### Collective challenges

SOX, GLB, HIPAA, and SB 1386 present similar challenges. Organizations have not seen this number of business-focused legislative acts for sixty years. Most companies are aware of the financial penalties of non-compliance. Unfortunately, these costs may turn out to be negligible as the media and investor communities begin to scrutinize non-compliant firms.

The language of all of the acts is vague. For example, Sarbanes-Oxley holds officers of the company responsible for establishing “internal controls”, without defining them. Auditors are working without a rulebook, looking for early cases to establish legal benchmarks.

Moreover, even as the windows for compliance are closing quickly, specific requirements change daily. Organizations must make a long-term commitment – both cultural and technical – to conform to evolving regulations.

To make matters worse, companies are under a deluge of “compliance helper” products. Unfortunately, these single-purpose tools do not offer the kind of comprehensive solutions required to address broad security issues, rather than just discrete compliance issues, across the organization.

---

*“Compliance efforts to meet these regulations could be coordinated, using a highest common-denominator strategy. This would include assigning common project management for all relevant regulations, identifying common points of risk or vulnerability, developing auditable security processes, and evaluating vendor solutions that best integrate the components of a solution.”*

Adrian Bowles, ITCi

---

## Shared requirements

As you begin to establish a strategy for compliance, you have at least one thing in your favor. You can meet many requirements of SOX, GLB, HIPAA, and SB 1386 by achieving the same three goals:

- *Information security:* At the heart of the acts is the need to protect information. Nothing should alter original data, and there must be a clear alert in the event of any attempt to modify or destroy information.
- *Email security:* There are three key aspects to protecting email. Organizations should maintain the confidentiality of important content; all email should include consistent legal information across recipients; and, to succeed fully, email policy enforcement must ease retrieval and monitoring efforts.
- *Proof of control:* Key to satisfying regulations is the ability to prove that compliance efforts are working. Event logs, audit trails, and reporting are critical to meeting this goal.

## Information security

Incorrect, lost, and corrupt data is a major focus of all the legislation. A compliance infrastructure must both prevent data corruption and offer a window into network security, including unauthorized attempts to damage or alter data.

### *Protecting data integrity*

Viruses, malicious spyware, and other malware can compromise the most carefully managed data. HIPAA requires that you prevent even new, unknown email-aware worms from

entering your business. GLB stipulates a formal framework of administrative, technical, and physical safeguards to protect against anticipated threats or hazards to such records.

---

*A Midwestern college effectively quarantines 30-50 virus-infected emails a day, using a quarantine digest for more efficient handling of suspicious email. The anti-virus and email policy protection systems run on Linux, multiple flavors of Windows, UNIX, and Mac OS.*

---

The current state of “blended threats” is exacerbating the problem. A blended threat can combine worms, viruses, Trojans, and/or spam. It usually causes more than one kind of problem, such as damaging an operating system, installing a backdoor, and/or corrupting a data source. It employs multiple attack methods: infecting EXE files, modifying registry keys, and altering HTML files, for example. Finally, it replicates and spreads through several routes, including email, IRC channels, file-sharing, and downloading.

### **How can you prevent data corruption?**

Some anti-virus solutions clean out threats as they come in via email. Others detect viruses on external data sources such as CDs, mobile phones, network servers, and online downloads. To be effective, your data security schemes must take a multi-tiered approach to protecting gateways, servers, and desktops.

Make sure any solution you consider addresses all parts of your network. It is not enough to protect your workstations and desktops; it is also critical that you guard your gateway to contain threats at the network gateway. As the velocity of attacks increases, preventing viruses from getting to your network should be a top priority. For example, the SQL Slammer virus spread to 250,000 servers in ten minutes.

Your efforts must also acknowledge the inherent vulnerabilities of network servers, especially UNIX/Linux platforms. A UNIX or Linux file server can be a “carrier” that passes viruses along the network, infecting more susceptible Windows systems. Legislation seeks prudent protection to foreseeable threats such as the increase of viruses affecting UNIX/Linux platforms. Many companies have determined that SOX requires anti-virus protection on every server that manages financial data.

### *Observing network security activities*

Compliance is not just a matter of end-of-quarter reports. You need real-time check-and-balance mechanisms to confirm that technology and procedures are actually protecting data.

### How do you verify information security?

First of all, to maintain information security, you must have a way to recognize breaches of security. Anti-virus solutions must alert supervisors immediately of any viruses, worms, Trojans, malicious spyware, and malware affecting the network.

In addition, you need a real-time view of the status of every device in the network. You must be able to ascertain which devices are protected, which need updating, and which, if any, have been attacked. Automatic updates and centralized installation ensure continuous protection.

### Email security

There are several aspects to controlling data distribution. Firstly, information should not go to the wrong entity. Secondly, the correct information – together with any standard language – must go to the required entity. Finally, as the volume of email and spam rises daily, it is imperative that companies find ways to identify and save compliance-related

---

*A drugstore chain needed to prevent inadvertent release of private patient information. The solution blocks outbound messages if they are addressed to recipients that are outside the company's extended network. In addition, the software notifies the sender of the appropriate mechanisms for sending information.*

---

communication while filtering out other messages and attachments.

### Securing data transmission

Gateway protection policies should prohibit the distribution of inappropriate content and attachments. They also must not permit unauthorized parties to view any of the following:

- Protected health information and diagnostic codes (HIPAA)
- Personal and financial information (GLB)
- Financial disclosure (SOX et al)
- Intellectual property and trade secrets (SOX, GLB, SB 1386)
- Confidential internal memos (SOX, GLB).

An article in the Sarbanes-Oxley Compliance Journal states, "As people increasingly send and receive email using multiple devices ... the potential for information to fall into the wrong

hands is a very real risk." Data can be stolen; it can be misrouted; or it can simply be addressed to the wrong person.

### How can you make sure email doesn't get into the wrong hands?

Policy enforcement, or the ability to manage email, helps enable organizations to define rules that expedite email traffic while protecting the organization.

Email management applications support a range of business requirements. One may require that email with a particular subject line or header is always encrypted – for example, when transmitting patient information to a trusted partner. Some may indicate that certain functional roles should never see or send email with certain content. Another may specify that the recipient's address must match stored information about the client named in the email. Or it might route all mail destined for a particular organization – perhaps an investment house, law firm, or insurance company – through the appropriate VPN.

Moreover, since different departments deal with more confidential information than others, any filtering mechanism must enforce policies at a granular level. That is, filters may act differently on email depending on a message's source or destination. Finally, all of this enforcement must take place with minimal impact on legitimate business email.

### Using templates

Incorrect handling of proprietary or personal information via email can result in non-compliance and litigation, so most companies are instituting requirements for wording, copyright and trademark statements, legal disclaimers, and

---

*A state agency uses a web console that allows multiple users to manage spam and anti-virus rules. Its IT department has found it simple to build custom rules that act on the subject or header of email, regardless of the brand of email system. This feature has made it easier to handle email exchange with citizens.*

---

confidentiality clauses. To satisfy GLB, for example, organizations that release confidential financial data are including a statement that they keep records related to the engagement but do not disclose client information to anyone without permission.

As e-commerce lawyer Jo Brook of Sprecher Grier Halberstam says, "These kinds of disclaimers are placed on business emails because businesses simply cannot monitor all the communications that leave the confines of the company ... Email is so instantaneous it can lead to problems, and a

disclaimer can rein in some of the enthusiasm and excesses that it is prone to.”

### **What can you do to ensure the inclusion of standard verbiage?**

In an effort to comply with regulations, organizations are writing policies that specify the format and legal statements that must be part of every email. Unfortunately, it is impossible to guarantee that every member of an organization presents data in a consistent format with the correct legal language.

Policy enforcement at the gateway is an ideal mechanism for achieving compliance in these areas. The software can scan email for particular keywords or attachment types and apply formatting and text per company-specified rules. More complex scenarios can be covered through the administration and control of virtually every aspect of an email message.

### ***Saving the right data***

How do companies decide what information will be necessary to ensure compliance, particularly in the case of email? IT sees the problem in terms of storing and retrieving bits and bytes. Corporate sees email as legal documents. Compliance officers think about preservation and control. End users want easy access to the email they need to be productive.

One approach is “if in doubt, save it all”, and many companies are forced to adopt this strategy due to inadequate systems. There are risks to storing everything, as Michele Lange of the National Law Journal points out: “Outdated email, antiquated files, and data are often kept past their useful life. Case law reveals that unwieldy preservation of all electronic data can come back to haunt a corporation when litigation ensues.” Excessive storage places an unnecessary burden on scanning, archiving, and encryption systems. There is also the difficulty of retrieval; given voluminous databanks, the right document can be like a needle in a haystack. It can actually be more expensive to keep all email than to enforce an email storage policy.

### **How can you ensure that you store the right email and attachments?**

Unfortunately, most email programs just don't have the granularity of control to address specific regulatory requirements efficiently. Their drawbacks include generalized junk email rules, mailbox size limitations, and duplicate storage on servers and personal PCs.

Again, policy enforcement at the gateway provides an effective way to separate business-critical messages – email concerning business proceedings, operations, obligations, and financials – from spam, personal correspondence, thank you notes, and other short-lived items.

By looking for patterns, including sender/recipient paths and keyword combinations, the email gateway can provide even

finer-grained control to help you isolate the most important and highest risk messages. When the software finds these characteristics, it can tag the email as per company-specific rules, intercept and re-route the message, or log the transaction for later audit.

### **Proof of control**

In the world of compliance, record keeping and maintenance are key parts of the process. SOX requires public companies to establish, document, and assess the effectiveness of their internal controls and procedures over financial reporting. GLB not only says that banks must protect customer privacy – it demands that they prove compliance. SB 1386 mandates that organizations must disclose any breach of the security of systems that contain personal information.

HIPAA requires formal documentation of “routine and nonroutine receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information”. In fact, HIPAA mandates that organizations prove that there have been no unauthorized alterations or destruction of electronically stored confidential information, and to describe the mechanisms they use to accomplish this.

You cannot prove compliance unless you have captured the proof first. As one organization writes, “If it isn't documented... if we cannot prove compliance to HIPAA procedures, it [simply] did not happen.”

To prove your use of internal controls, you must log transactions and events. To verify that you are protecting information, you must detect and record exceptions. Finally, you must output comprehensive, well-organized statements that prove control.

### **How do you capture every email and anti-virus transaction?**

Some organizations are capturing the content and header information for each email transmission that comes in and goes out from their email servers. You must record all real or intended breaches of security and policy. Compliance requires the capture of metadata:

- Who didn't follow which policy on what date?
- How many times did filters capture inappropriate content?
- What caused an unintentional or undesired disclosure of financial or personal information?
- When was this file corrupted and what was the source of the virus?

Detailed transaction logs can provide the information you need to meet internal control documentation requirements.

## Detecting exceptions

Compliance is not just a matter of end-of-quarter reports. CxOs need real-time check-and-balance mechanisms to verify that technology and procedures are actually preventing security leaks via viruses and email.

---

*The IT group at a 270-person software development firm appreciates how easy it is to administer the network, thanks to a web console that presents both current and historical event tracking.*

---

“Part of the \$1.4 billion settlement in April between the SEC and ten of the nation’s top Wall Street firms was for, among other things, ‘failure to supervise’ employee communications,” writes David Greene in AIIM E-DOC Magazine. “Regulations such as NASD 3010 and NYSE 342 require organizations to establish and maintain a system of supervision, demonstrate that their system is complete, evaluate it on a regular basis, and ensure that it remains effective.”

### What do monitoring and audit trails entail?

Clearly, virus protection software can monitor and clean systems to assure data integrity. Also, email programs can maintain copies of all incoming and outgoing messages. But that is not enough.

Anti-virus solutions must alert supervisors immediately of any infections in hardware, software, and data across the network. In the same manner, supervisors need to receive instant notice of email security breaches.

Graphical displays of current filter activity can clarify message streams and quarantine contents. At the same time, measurable feedback on message-filtering activities helps IT teams to track progress and justify procurement and processes.

To feed compliance reports, the protection mechanisms should also create an audit trail of every virus scan and its results, anomalies detected, and instances of damage. Real-time journals must record all email activity, including incidences of – and reasons for – all enforcement activities such as quarantining files, verifying senders or receivers, adding standard disclaimers, and deleting compromised and unnecessary data.

## Generating compliance reports

Regulations dictate that organizations must be able to demonstrate proof of control for any point in time. In addition, proof-of-compliance documentation must use clear and concise language and demonstrate a common organization

and format. Given the over-abundance and complexity of required compliance-specific data, generating consistent, systematic output is no mean feat.

### What is the best way to produce compliance-specific reports?

A variety of applications maintain information about viruses and email. Per Jeffrey Plotkin, former Assistant Regional Administrator of the SEC’s New York Regional Office, “Companies that take advantage of such third-party software may significantly reduce their costs and anxieties related to necessary email retention/destruction policies.”

The first step in effective reporting is collecting the right data around email traffic. Email gateway security systems should be able to trigger and log different events for both illegitimate and legitimate mail. The tools should also allow automatic handling of suspicious messages, including simple discarding, complex routing and multi-stage reviews. Finally, this step should include both basic reporting of policy violation and detailed reporting on specific instances.

The second step in effective reporting involves detailed analyses of virus attacks across your network. This allows you to isolate infected machines and provides a starting point for a detailed investigation of the impact of the virus. Your solution should include individual and aggregated virus reports for all devices on networks of virtually unlimited systems, and analytical tools to explore trends.

## Choosing a compliance solution

New regulations put a stronger focus on the broad range of security risks facing IT departments. Like most security risks, these threats will continue to evolve and broaden in scope, compelling organizations to seek partnerships with vendors that have the necessary expertise and proven track record of adapting to constant changes in the security environment. There are several overarching strategies for finding a security solution that meets your organization’s compliance needs:

- 1 Use compliance projects as an opportunity to bolster your existing security infrastructure. There are many points of similarity between security and compliance architectures. The right security system can help you detect threats and manage privacy risks in a single, consistent environment.
- 2 Plan for change across all your compliance projects. A powerful policy environment can deliver the flexibility and agility you need to respond quickly to evolving best practices and requirements.
- 3 Find ways to simplify ongoing management of the solution. Using multiple elements from a single vendor can help to ease the technological side of system management. Vendors that maintain their own threat detection labs can provide greater visibility into emerging threats, and more consistent detection of existing threats.

## Compliance solution in action

Anti-virus and email policy enforcement solutions are already helping companies comply with SOX, GLB, HIPAA, and SB 1386 legislation. These companies are choosing solutions that “go the extra mile”.

The following case study involving Virginia Mason Medical Center provides an example.

---

**Virginia Mason Medical Center (VMMC)** – a private, integrated health services organization based in Seattle, Washington – recently purchased Sophos PureMessage to combat viruses, spam, and other email-borne threats. The solution’s email policy enforcement capabilities are ensuring best practices for legislative compliance.

---

*“The last thing we want to do is compromise or disclose our patients’ private information, so we need to be compliant with legislation like HIPAA. There are mandates that define how we interact with insurance companies, and securing email is crucial to that. Without Sophos PureMessage, we would be putting our business and our patients at risk.”* Michael Spohnholtz, Senior Technology Consultant, VMMC

---

With nearly 4,000 email users, VMMC processes more than 1.5 million email messages each month. Before deploying PureMessage™, 75% of all email received was either spam or messages containing viruses.

“Prior to the Sophos implementation, the hospital was hit by a virus that generated thousands of infected messages and took us eight hours to get back on track. Two weeks later, a month’s worth of email flooded in that took us 12 hours to clean up,” said Michael Spohnholtz, Senior Technology Consultant at VMMC.

“Ensuring quick response without downtime is critical, as our first priority is to provide safe patient care. Before using PureMessage, we really didn’t have a clear picture of just how big a problem viruses and spam caused since we didn’t have the tools to eradicate the problem. Right out of the box, PureMessage is identifying a high rate of spam and blocking viruses from hitting our network.”

Spohnholtz continued: “VMMC also wanted a solution with a low rate of false positives, as we needed to ensure that legitimate emails with medical terms and medical product names, such as Viagra and other drugs, got through the filters.”

Going a step further, Sophos is working with VMMC to use

PureMessage to ensure secure messaging for the hospital’s patient base. Patients will be assigned a Virginia Mason email address – accessible through webmail via their home email address – that will enable them to communicate directly with their doctor. “Deploying PureMessage directly to our patients ensures that no email will leave VMMC’s infrastructure and get into the wrong hands,” Spohnholtz concluded.

---

## Conclusion

Legislation such as SOX, GLB, HIPAA, and SB 1386 all aim to prevent the misuse of information across different industries. While they specify a multitude of varying regulations, there are three core requirements around information security, email monitoring, and proof of control that are common across multiple acts.

No matter which legislative requirements you are striving to meet, you must implement a comprehensive approach to compliance that affects all areas of your business. The combination of a multi-layer security architecture, powerful policy tools and strong vendor support can go a long way to expediting your success.

Recognized as a world leader in protecting businesses against viruses and spam, Sophos is the ideal partner for addressing compliance issues. Our anti-spam, anti-virus and email policy enforcement software delivers an integrated solution that helps you overcome the challenges of compliance legislation.

**Sophos Anti-Virus™** protects your network, desktop, and even remote laptop computers from the latest viruses, Trojans, worms, and spyware. The quality of its award-winning technology has been confirmed time after time by independent bodies such as West Coast Labs, ICSA Labs, and Virus Bulletin.

**Sophos PureMessage** is a secure email gateway solution that delivers the best protection over time, against a broad variety of security risks. Built upon a mature and robust pattern-matching engine, Sophos PureMessage performs real-time filtering, analyzing all aspects of each message, including the message source, header, body, source, layout, organization, and content – even handling multiple languages. Based on the results of the analysis solution, Sophos PureMessage applies company-defined rules that can sort, delete, route, add confidentiality statements, and manipulate messages in many other ways that facilitate compliance. Sophos Anti-Virus and PureMessage employ Genotype™ virus and spam detection technology which provides proactive protection against families of viruses and spam campaigns even before specific detection becomes available. Sophos solutions are also backed up by SophosLabs™, a global network of threat analysis centers.

If you would like to learn more about how Sophos solutions can contribute to realizing compliance, please visit [www.sophos.com](http://www.sophos.com) or email [nasales@sophos.com](mailto:nasales@sophos.com).

---

## Sources

- 1 AICPA; Gramm-Leach-Bliley Act—Full Compliance Required by July 1, 2001. (<http://www.aicpa.org/pubs/tpcpa/june01/gramm.htm>)
- 2 AIIM E-DOC Magazine; Eye on IM: Look Into Your Compliance Strategy, David Greene. ([http://www.edocmagazine.com/article\\_new.asp?ID=27565](http://www.edocmagazine.com/article_new.asp?ID=27565))
- 3 BDO Seidman; Financial Reporting, Definition of Internal Controls Over Financial Reporting. ([http://www.bdo.com/about/publications/assurance/fr\\_mar\\_2003/def.asp](http://www.bdo.com/about/publications/assurance/fr_mar_2003/def.asp))
- 4 California State Senate; Bill SB 1386. ([http://info.sen.ca.gov/pub/01-02/bill/sen/sb\\_1351-1400/sb\\_1386\\_bill\\_20020926\\_chaptered.html](http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html))
- 5 CFO Magazine; How Audits Must Change, Kris Frieswick. ([http://www.cfo.com/article.cfm/3009752/c\\_2984781?f=archives&origin=archive](http://www.cfo.com/article.cfm/3009752/c_2984781?f=archives&origin=archive))
- 6 Computerworld; ID Theft Law Keeps Low Profile, Jaikumar Vijayan. (<http://www.pcworld.com/news/article/0,aid,116420,00.asp>)
- 7 CPA Journal; The Sarbanes-Oxley Act and the Evolution of Corporate Governance, Jorge E. Guerra (IMA). (<http://www.nysscpa.org/cpajournal/2004/404/perspectives/nv5.htm>)
- 8 Federal Register: Department of Health and Human Services; 45 CFR parts 160, 162, 164 Health Insurance Reform.
- 9 IT Compliance Institute; Compliance Strategies: From CYA to ROI, Adrian Bowles. (<http://www.itcinstitute.com/display.aspx?ID=38>)
- 10 IT Week; Keeping Email Woes at Bay, Mark Street. (<http://www.webactivemagazine.co.uk/features/1131151>)
- 11 KVC; White Paper: Corporate Governance – The Impact on Your IT Staff, Jeffrey Plotkin LLP. ([http://www.kvsinc.com/\\_filelib/FileCabinet/PDFs/white%20papers/KVS%20WP%20Plotkin%20Corporate%20Governance.pdf](http://www.kvsinc.com/_filelib/FileCabinet/PDFs/white%20papers/KVS%20WP%20Plotkin%20Corporate%20Governance.pdf))
- 12 Midwest Technology Journal; HIPAA, GLB, Sarbanes-Oxley, FISMA. ([http://www.pjournal.com/modules.php?name=News&new\\_topic=14Smoke and Mirrors](http://www.pjournal.com/modules.php?name=News&new_topic=14Smoke%20and%20Mirrors))  
or Information Security Best Practices? (<http://www.pjournal.com/modules.php?name=News&file=article&sid=225>)
- 13 The Sarbanes-Oxley Compliance Journal; Email: The Appliance of Compliance, Alex Shipp. ([http://www.s-ox.com/features/f2004\\_10/f\\_email\\_compliance.html](http://www.s-ox.com/features/f2004_10/f_email_compliance.html))
- 14 Transform Magazine; What You Should Know About E-Mail Archiving, Julie Gable. (<http://www.transformmag.com/compliance/showArticle.jhtml;jsessionid=XREBNTAYHNUJ3YQSNDBCSKHOCJUMEKJVN?articleID=23905110>)
- 15 US Securities and Exchange Commission; Sarbanes-Oxley and the Idea of "Good" Governance, Cynthia A. Glassman, SEC Commissioner. (<http://www.sec.gov/news/speech/spch586.htm>)
- 16 Washington University, HIPAA Privacy Procedures. ([http://www.neuro.wustl.edu/HIPAA/Procedure\\_1\\_Neurology.pdf](http://www.neuro.wustl.edu/HIPAA/Procedure_1_Neurology.pdf)).