A Guide to the Sarbanes-Oxley Act and Email Security

I - Introduction

Motivated by corporate scandals, the Sarbanes-Oxley Act (SOX)[1] has profoundly changed the way corporate America does business and redefined the law of securities more than any statutory change since the original 1933 and 1934 securities laws. It addresses perceived shortcomings in the ability for the law to deal with abuses such as false financial reporting, auditors failing to blow the whistle on shady accounting practices, and the destruction of evidence. The real-world examples of these abuses were corporate scandals in companies such as:

- Enron, which used off-the-books partnerships to inflate earnings and conceal debt;
- Arthur Anderson, which failed to stand up to Enron's aggressive accounting techniques and later destroyed documents relevant to the investigation; and
- WorldCom, which overstated its revenue and understated its losses.

SOX addresses the threat of fraud in the finance departments of public companies[2] by placing great emphasis on companies establishing reliable "internal controls" for gathering, processing, and reporting financial information with the ultimate goal of ensuring accurate reporting of public companies' finances for the benefit of investors. Taken to its logical conclusion, however, implementing reliable internal controls means more than just avoiding human manipulation of revenue and cost figures. Internal controls relate to the entire system of running a finance department and the infrastructure that funnels financial information to the finance department. Moreover, given the critical role played by information technology in finance operations, a focus on internal controls inevitably will involve some scrutiny over assurances of the integrity, reliability, effectiveness, and performance of information systems used by finance or, in other words, information security.

Email communication policy is an integral part of controls to safeguard information from unauthorized use, disclosure, modification, damage, or loss. Email communications is an important means of moving revenue and cost information to those analyzing it, a means of circulating financial reports internally, and communicating information to those who will report it to the public. At the same time, email security vulnerabilities create the risk of the unauthorized disclosure, loss, destruction, or corruption of financial information, thereby thwarting the SOX goal of accurate financial reporting. The interception and unauthorized access to email can lead to leaks of financial information. Malicious code, including viruses, worms, Trojan horses, certain kinds of spyware, may infect workstations with code allowing for later unauthorized access or tampering with financial records. A deluge of spam may overwhelm corporate email servers, reducing the effectiveness and availability of this vital resource.

The bottom line is that internal controls rest on a foundation of system-wide mechanisms, policies, and procedures that include IT security and particularly email security, and given the critical role played by email, as well as the considerable security vulnerabilities plaguing email, securing email within public companies must be a high priority.

This guide shows how Sarbanes-Oxley compliance and email security relate to each other

II - What SOX Says About Internal Controls

SOX contains a variety of provisions to strengthen the reliability of financial reporting by public companies. One of the most important reforms called for by SOX is a thorough revamping of the infrastructure, called "internal controls," that public companies put into place to gather, process, and report financial information. The idea is that if companies establish good internal controls, it will be harder for rogue executives and personnel to cook the books.

Section 404 of SOX calls for new rules requiring public companies to report on the effectiveness of their internal controls in their annual reports. Internal control reports must acknowledgement management's responsibility to establish and maintain "an adequate internal control structure and procedures for financial reporting."[3] Internal control reports must also contain an assessment of the effectiveness of the internal control structure and financial reporting procedures.[4] Congress required the U.S. Securities and Exchange Commission to issue these new rules. SOX also places the responsibility on public accounting firms to attest to and report on public companies' internal control reports. These attestations must be done in accordance with Public Company Accounting Oversight Board (PCAOB) standards.[5]

To make sure that companies meet these new rules, Congress placed personal responsibility on executives to clean up internal controls. Section 302 requires public company CEOs and CFOs to make certifications to the SEC (and the investing public) about their financial reporting and the strength of their internal controls. Specifically, CEOs and CFOs must certify in reports to the SEC that they:

- are responsible for establishing and maintaining internal controls;
- have designed internal controls to ensure internal reporting of material information;
- have evaluated the effectiveness of internal controls;
- have included in the reports their conclusions about the effectiveness of internal controls;
- have disclosed to auditors and the board of directors audit committee significant deficiencies in internal controls or fraud; and
- have included in the reports significant changes in internal controls, factors affecting internal controls after the last evaluation, and corrective actions.

The purpose of these disclosures is to ensure that the investing public knows the true strength or vulnerabilities in the internal controls of the company.

III - SEC Regulations and Guidance on Internal Controls

Congress handed rulemaking responsibility to the SEC, and the SEC responded with regulations that flesh out the internal controls requirements. The SEC's SOX regulations require public companies to maintain internal controls over financial reporting.[6] The rules also say that management, including CEOs and CFOs, must evaluate internal control effectiveness each quarter.[7] Part of the reporting must include a statement about material changes in internal controls since the last report,[8] such as improvements or new vulnerabilities.

The SEC regulations define "internal controls" by saying they involve a process to provide "reasonable assurance" regarding the reliability of financial reports, including policies and procedures for:

- maintaining records that accurately and fairly reflect transactions and asset transfers;
- providing reasonable assurances that transactions are recorded properly and that receipts and expenditures are authorized by management; and
- providing reasonable assurance of preventing or detecting unauthorized acquisition, use, or disposition of assets.[9]

Having required public companies to establish "internal controls" so defined, and required periodic reports on their strength, the next natural questions is, "what are the things a public company must do to have sound internal controls"? The regulations do not answer this question. They do, however, provide guidance on where they can find the answer. Management must use a "suitable, recognized control framework" for assessing internal controls.[10] The regulations do not call for any particular industry-standard assessment methodology framework to judge internal controls, but rather leave some discretion to public companies themselves to choose one that is "suitable" and "recognized."

The SEC and PCAOB, however, have identified one particular framework as acceptable: the Committee of

Sponsoring Organizations of the Treadway Commission's (COSO) *Internal Control – Integrated Framework* (1992).[11] The SEC stated in a release that COSO "satisfies our criteria" as an appropriate evaluation framework. PCAOB called COSO "a suitable and available framework for purposes of management's assessment."[12] The acceptance by SEC and PCAOB reflects the reality that COSO had been, for some time, the de facto industry standard for assessing internal controls and recognized as such by professional accounting associations and standard setting organizations.

IV - Frameworks for Evaluating Internal Controls and IT Security

The SEC opened the door, through regulation, to an evaluation of a company's "internal controls." "Internal controls" is a broad term, and to be thorough, a company will need to evaluate its financial reporting infrastructure holistically, and not simply focus on phony transactions, changing earnings numbers, or similar individual focused manipulations. The call for evaluating internal controls affects all phases of the financial reporting infrastructure's operations.

For some time, auditing professionals have been aware of the critical role played by information technology in the establishment of sound internal controls. The American Institute of Certified Public Accounts acknowledged this realization in SAS 94,[13] which tells auditors how to consider the ways in which a company's IT systems affect internal controls consistent with generally accepted auditing standards. Auditors, however, are not only aware of the role of IT systems in financial reporting, they are also specifically concerned about IT security and the effect of security vulnerabilities on internal controls.

Consequently, companies recognizing the role of IT security in establishing sound internal controls have searched for frameworks to assess internal controls that contain more control objectives relevant to IT security. Because COSO predated much of the information revolution, it contains little discussion of IT security. Since COSO, companies have turned to two newer frameworks for evaluating controls for IT systems used for gathering, processing, and reporting financial information:

- *Control Objectives for Information and related Technology* (COBIT), published by the Information Systems Audit and Control Association (ISACA); and
- *IT Control Objectives for Sarbanes-Oxley*, published by the IT Governance Institute.

Both COBIT and *IT Control Objectives for Sarbanes-Oxley* contain control objectives that cover not only IT controls, but more specifically IT security controls.

V - Internal Controls Cover E-Mail Security

COBIT and *IT Control Objectives for Sarbanes-Oxley* contain a series of control objectives on IT subjects. The control objectives set high-level goals. These goals cut across types of technology and, in practice, are highly relevant to email, web, IM and ftp traffic.

For instance, both COBIT and *IT Control Objectives for Sarbanes-Oxley* call for controls to safeguard information from unauthorized use, disclosure, modification, damage, or loss. Thus, access controls necessarily must extend to email to prevent interception and disclosure of confidential financial information. Technology solutions are available to address confidentiality concerns, namely solutions for confidentiality encryption. These solutions can ensure that communications are encrypted so that only authorized, intended recipients can read the communication. Likewise, integrity controls to prevent modification or damage of information should include measures to prevent tampering with or corruption of emailed information. Digital signature technology can address email integrity issues to ensure that any changes in the email after the sender sends it will be detected.

Other control objectives address other email security concerns. The table below shows some of the email security issues addressed generally by COBIT and *IT Control Objectives for Sarbanes-Oxley*. The appendix to this guide contains specific COBIT and *IT Control Objectives for Sarbanes-Oxley* control objectives that apply to email security. Please see the appendix for more details.

Examples of Control Objectives Applicable to Email in COBIT and *IT Control Objectives for Sarbanes-Oxley*	**Applicable Email Security Solutions**
Access control to provide assurances against unauthorized use.	End to End encryption is needed to provide assurances against interception and unauthorized disclosure. Companies may also need to perform other boundary services such as archiving and content scanning. Therefore, the optimal system must be able to provide desktop-to-desktop encryption with outbound policy gateway. Solutions that use webmail, symmetric or solely gateway approaches are not ideal for this scenario.
Assurances against modification or damage of information.	Digital signatures on email provide assurances of integrity to detect any tampering or corruption.
Provide assurances of authorization and authentication for electronic transactions.	A digital signature on an email associated with a public key-private key pair bound to the identity of a particular authorized user provides assurances that the email came from that authorized user, and not from an imposter.
Refresh credentials periodically to maintain the effectiveness of authentication.	By policy, companies can require users to generate or obtain a new key pair periodically to minimize the risk of key compromise. Such a policy can ensure continued effectiveness of email digital signatures for authentication.
Procedures to govern issuing, suspending, and closing user accounts.	Solutions exist to manage not only email accounts but also the identity credential to ensure, for instance, that only authorized users receive accounts and credentials, and that the email accounts and credentials of departing personnel are terminated.
ontrols to deter parties from falsely denying that they originated a certain transaction or communication.	Digital signatures on emails, supported by credential binding a key pair to an authenticated user, can provide strong evidence tying that user to a particular transaction or communication.
Prevent, detect, and take corrective measures in response to malicious software, such as viruses and Trojan horses.	Antivirus solutions can prevent, detect, and respond to malware. Email is a key vector for introducing viruses into systems. Consequently, AV solutions must secure email.
Ensure that systems meet performance and availability business needs.	One of the most significant challenges facing email systems is the deluge of spam hitting email systems. Antispam solutions are critical to ensure the continued availability of email as a viable means of communication and to ensure the effective performance of email systems. Encryption systems must be highly available and should be able to operate in offline mode.

As is apparent from these examples of email-related control objectives, email security comprises a critical component of any IT internal controls program, which in turn is a key element of a program of internal controls for the accurate financial reporting that SOX demands.

The market offers many email security solutions. Some focus on encryption and others on protection from viruses and spam and content scanning. The control objectives in the frameworks for SOX IT internal controls are broad. Consequently, a broad solution that provides end-to-end encryption with a policy-based gateway offering anti-spam, anti-virus, content scanning and configurable policies to automate encryption will be necessary to optimize IT internal controls for SOX compliance.

VI - Conclusion

Since its enactment, SOX has dominated the corporate governance landscape. SOX reaches deep into organizations by requiring the thorough reform of internal controls to create reliable company systems to report financial results. It also imposes personal accountability on management by requiring CEOs and CFOs to certify that financial reports are accurate and to certify the effectiveness of internal controls.

Any thorough evaluation of internal controls for financial reporting will involve a comprehensive examination of finance-related systems. General accepted auditing standards acknowledge the effect of IT on internal controls. Security vulnerabilities point to areas that internal controls must address. Moreover, given the importance and vulnerability of email communications, a comprehensive email security program will prove vital to a program of sound internal controls.

While neither SOX nor the SEC's implementing regulations impose specific requirements for email security or IT security in general, the frameworks commonly used for assessing internal controls set control objectives applicable to email security and IT security generally. Companies that fail to implement email or other components of IT security, run the risk that auditors will be unable to attest to the internal controls or to the accuracy of their financial statements.

Turning a blind eye towards email and other IT controls also carries the risk of SEC enforcement actions to impose civil sanctions, or possibly even criminal penalties for willful conduct. False certifications that internal controls are effective may lead to securities fraud claims. By contrast, a sound program of email security and other IT security controls will reduce security vulnerabilities to finance-related systems and help establish the controls needed to keep the regulators at bay.

While there are many types of email protection and security products available, not all of them can provide the capabilities needed to enforce internal controls. Encryption solutions must offer desktop-to-desktop encryption with a fully integrated policy-based gateway that can provide other critical services for regulatory compliance and email protection such as anti-spam, anti-virus, archiving and content and content scanning.

Bottom Line: Email security is an integral part of effective internal controls that are critical for Sarbanes-Oxley compliance in public companies.

Appendix

The table below maps control objectives in COBIT and *IT Control Objectives for Sarbanes-Oxley* to email technology solutions that help companies implement these control objectives.

Requirement	**Applicable Law or Guideline**	**Role of Email Technology Solutions**
I. COBIT Control Objectives Relevant to Email Security		
Safeguard information against unauthorized use, disclosure, modification, damage or loss.	COBIT Control Objective DS5.	End to end encryption fully integrated with policy-based gateway at the network edge
Restrict logical access by	COBIT Control Objective DS5,	Companies can provision authorized

authentication mechanisms, linking users and resources with access rules.	Detailed Control Objective 5.2.	and identified users with public-private key pairs used in the creation and verification of digital signatures.
Management should establish procedures for requesting, establishing, and closing user accounts. Central management of identification and access rights of users.	COBIT Control Objective DS5, Detailed Control Objective 5.4, 5.9.	Solutions can help to automate and enforce policies for user enrollment, credential provisioning, and credential revocation.
Where appropriate, implement non-repudiation measures, such as through digital signatures, time stamping, and trusted third parties.	COBIT Control Objective DS5, Detailed Control Objective 5.15.	A digital signature provides evidence tying the signing party to a particular transaction, which can be used in litigation to enforce the transaction.
Implement procedures to manage cryptographic keys through generation, use, change, revocation, and other lifecycle functions. Distribute information about compromised keys, such as through certificate revocation lists.	COBIT Control Objective DS5, Detailed Control Objective 5.18.	Traditional PKI systems have these characteristics – however are impossible to manage in B2B and B2C scenarios, therefore an Identity-Based Encryption approach is preferable as it has all the benefits of a PKI without the need for CRLs and other PKI infrastructure. These benefits include the ability to generate key pairs, permit policy-based enforcement of periodic rekeying, and revoke keys. Information concerning compromised keys can be made available in real time.
Management should establish a framework of adequate preventative, detective, and corrective control measures, and occurrence response and reporting concerning malicious software, such as viruses or Trojan horses.	COBIT Control Objective DS5, Detailed Control Objective 5.19.	Antivirus solutions can prevent, detect, and respond to malware and spyware, including spam carrying malicious code.
B. Managing Performance and Capacity Ensure that adequate capacity is available and that best and optimal use is made of it to meet required performance needs.	COBIT Control Objective DS3.	Encryption system must be highly available and must continue to work offline in the case of a disaster. Backup, redundancy and disaster recovery must be easy to implement without the need for restoring multiple databases and key stores.
Ensure continuous monitoring of the performance of IT resources and timely reporting of exceptions.	COBIT Control Objective DS3, Detailed Control Objective 3.3.	Tools exist to monitor the performance of resources, such as mail servers, and to alert administrators of possible overloads.
Management should identify IS availability and performance business needs. Management should prevent resources from being unavailable.	COBIT Control Objective DS3, Detailed Control Objectives 3.1, 3.8.	Solutions can help maintain the availability of resources. In the email context, solutions can help protect against overload or overuse, such as in the case of filtering spam to minimize email traffic.
II. IT Governance Institute's IT Control Objectives for Sarbanes-Oxley		

A. Ensure Systems Security Controls provide reasonable assurance that financial systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.	IT Control Objectives for Sarbanes Oxley, page 68.	
Managing systems security includes physical and logical controls to prevent unauthorized access. Controls typically support authorization, authentication, non-repudiation, data classification, and security monitoring.	IT Control Objectives for Sarbanes Oxley, page 68.	For authorization and authentication, see solutions addressing COBIT Control Objective DS5, Detailed Control Objective 5.2 above. For nonrepudiation, see solutions addressing COBIT Control Objective DS5, Detailed Control Objective 5.15 above.
For authorization and authentication, see solutions addressing COBIT Control Objective DS5, Detailed Control Objective 5.2 above. For nonrepudiation, see solutions addressing COBIT Control Objective DS5, Detailed Control Objective 5.15 above.	IT Control Objectives for Sarbanes Oxley, page 69.	For authorization and authentication, see solutions addressing COBIT Control Objective DS5, Detailed Control Objective 5.2 above.
Procedures are followed to maintain the effectiveness of authentication and access mechanism.	IT Control Objectives for Sarbanes Oxley, page 69.	Solutions can enforce routine rekeying of cryptographic keys coupled with possible policies relating to re-authentication to ensure proper binding of authentication credentials with identity over time.
Procedures exist and are followed to ensure timely requesting, establishing, issuing, suspending, and closing user accounts.	IT Control Objectives for Sarbanes Oxley, page 69.	For user account management, see solutions addressing COBIT Control Objective DS5, Detailed Control Objective 5.4, 5.9 above.
Controls exist to ensure that neither party can deny transactions and non-repudiation controls are implemented.	IT Control Objectives for Sarbanes Oxley, page 70.	For non-repudiation, see solutions addressing COBIT Control Objective DS5, Detailed Control Objective 5.15 above.
B. Availability		
Controls provide reasonable assurance that all IT components, as they relate to security, processing and availability, are well protected. Controls provide reasonable assurance that authorized programs are executed as planned, including controls over system availability. End-user computing policies and procedures concerning security, availability and processing integrity exist and are followed.	IT Control Objectives for Sarbanes Oxley, pages 72, 76.	For a discussion of availability, see solutions addressing COBIT Control Objective DS3, Detailed Control Objective 3.8 above.
IT has procedures to protect systems	IT Control Objectives for	For a discussion of malware, see

from viruses.	Sarbanes Oxley, page 72.	solutions addressing COBIT Control Objective DS5, Detailed Control Objective 5.19 above.

Footnotes

[1] Sarbanes-Oxley Act of 2002, Public Law No. 107-204, 116 Statutes at Large p. 745.

[2] SOX also affects some private companies. Private companies will also want to begin SOX compliance work if they anticipate an event like an IPO or acquisition, since they will need to comply after the event.

[3] Title 15 United States Code (U.S.C.) Section 7262(a)(1).

[4] 15 U.S.C. § 7262(a)(2).

[5] 15 U.S.C. § 7262(b).

[6] Title 17 Code of Federal Regulations (C.F.R.) Sections 240.13a-15(a), 240.15d-15(a).

[7] 17 C.F.R. §§ 240.13a-15(b), 240.15d-15(b).

[8] 17 C.F.R. §§ 240.13a-15(d), 240.15d-15(d).

[9] 17 C.F.R. §§ 240.13a-15(f), 240.15d-15(f).

[10] 17 C.F.R. §§ 240.13a-15(c), 240.15d-15(c).

[11] SEC Release 33-8238, Management's Report on Internal Control over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, Vol. 68 Federal Register (Fed. Reg.) pages 36636, 36642 (Jun. 18, 2004).

[12] Public Company Accounting Oversight Board, Auditing Standard No. 2 – An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements, Section 14, 69 Fed. Reg. 20672 (Apr. 16, 2004), approved by SEC Release 34-49884, 69 Fed. Reg. 35083 (Jun. 17, 2004).

[13] AICPA, The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit – SAS No. 94 (2001).

All information in this document is subject to change without notice. This document is provided for informational purposes only and Voltage and CipherTrust make no warranties, either express or implied, in this document. Voltage SecureMail, SecureFile, SecureIM and SecurePolicy Suite are trademarks of Voltage Security, Inc. CipherTrust IronMail is a registered trademark of CipherTrust, Inc. All other company and product names may be trademarks of their respective owners.

About Voltage Security

Voltage Security is a new information security company focused on developing innovative solutions to address the challenges of securing business critical communication. Voltage is the first to use identity to bring confidence to business communication. Voltage solutions make anytime, anywhere business communication easy to use and painless to deploy. Voltage Security is based in Palo Alto, California.

About CipherTrust, Inc.

CipherTrust, Inc. is the leader in messaging security. The company's powerful, award-winning IronMail appliance combines the five critical e-mail security components of spam and fraud prevention, virus and worm protection, policy and content compliance, e-mail privacy, and secure e-mail gateway capabilities into a single easy to deploy and manage platform IronMail protects the messaging systems of more enterprise e-mail users than any other solution, including 30 percent of the Fortune 100. CipherTrust is based in Atlanta, Georgia.