SARBANES-OXLEY ACT: IT COMPLIANCE AND INFORMATION SECURITY

Dominique Louis, Pace University, 163 Williams Street, New York, N.Y. 10038, 212-346-1687
capital402000@yahoo.com

ABSTRACT

An important challenge to corporations and their leaders is a top management ethical conduct that permeates the corporate culture in every aspect. This issue of a strong, high quality leadership model projected by senior executives is illuminated by the Sarbanes-Oxley Act of 2002 that mandates public registrants to have corporate codes of ethics. Emphasizing the significant role of IT as the technical wherewithal to achieve law conformity, the paper examines the legislative impacts on IT and Information Security, highlights the effective strategies for Information Security Controls, analyzes the Regulatory Compliance, and concludes by offering some possible research questions for further study.

INTRODUCTION

The Public Company Accounting Reform Investor Protection Act of 2002, better known as Sarbanes-Oxley Act after its sponsors Senator Paul S. Sarbanes of Maryland and Representative Michael Oxley of Ohio, is a federal law that U.S. Congress passed in response to a number of acts of major corporate and accounting malfeasances - including those of Enron, Arthur Andersen, Tyco International, Peregrine Systems, World Com and Adelphia - that imposes responsibility on public companies operating in the U.S. to safeguard the integrity of the information that is used internally and released externally, aiming to protect investors from the possibility of fraudulent accounting activities by corporations. Thus, the Act is arguably considered the single most important piece of legislation affecting corporate governance, financial disclosure and practice of public accounting since the U.S. securities law of the early 1930's. The paper objectives align Information Technology Impacts, Information Security Impacts, Information Security Controls, Compliance, Guidelines for Secure Electronic Record, Enforcement Action to Information Security, Acceptance, and Resistance. The research type is purely descriptive.

METHODOLOGY

The literature includes information extracted from regular, financial, and computer magazine articles, journals, and organization websites. The type of sampling was based on novice and advanced users, as social implications of SOX compliance embrace all levels of publicly traded companies. Research activity was enticing, even though limited as to the extraction of statistical information.

BACKGROUND

Before the Act was incarnated, corporate executives engaged in the fictitious "*earnings management*" strategy - routinely releasing *invented or inflated* numbers that excellently concealed intrinsic corporate earnings - targeting to augment their stock prices and gain competitive advantage. As a result, between 1997 and 2002 public companies reported nearly one thousand financial earning restatements reflecting

the glaring inconsistency of their previously inaccurate statements.[15] In a frenzy so intense to establish credibility, reflect sales growth and thereby attract investors, fraudulent companies ventured forward into acquisitions, investments, and unnecessary employee hiring with later layoffs, that inevitably instigated their competitors to seek advancement through heavy investing in new technology, price wars, cost-cuttings, and layoffs. Given that a *public company* or *publicly traded company* is a company that has permission to offer its registered securities (stock, bonds, etc.) for sale to the general public, it is abundantly clear that this entire illicit activity caused hundreds of billions of dollars in shareholder value to evaporate, yet, more significantly with grave implications on the American economy at large. [15]

LAW OVERVIEW

In a comprehensive review, the Sarbanes-Oxley Act is a wide-ranging enacted legislation that directly impacts companies registered on New York Stock Exchange or NASDAQ, such as *CPAs, CPA auditing public companies*, and *publicly traded companies*, their owners, officers, employees, attorneys, financial analysts, investment bankers, brokers and dealers. The law establishes a **five-member Public Company Accounting Oversight Board (PCAOB)** appointed by the Securities and Exchange Commission (SEC), and subjected to SEC oversight, with duties to ***register*** *public accounting firms that prepare audit reports,* ***establish*** *or adopt auditing, quality control, ethics and independence standards,* ***inspect****,* ***investigate*** *and* ***discipline*** *public accounting firms, and* ***enforce*** *compliance with the Act*. [10] Important to compliance are Section 302 pertaining to *Corporate Responsibility for Financial Reports*, Section 402 pertaining to *Disclosures in Periodic Reports*, Section 404 pertaining to *Management Assessment of Internal Controls*, Section 409 pertaining to *Real Time Issuer Disclosures*, and Section 802 pertaining to *Criminal Penalties for Altering Documents*. [12] However, **Section 404** is considered **the most critical section** due to its IT impact, as it assigns the onus of effective internal control consistency and reliability on m*anagement* and *independent auditor*, where management is required to incorporate in their annual report a *statement providing immediate visibility as to the scope and adequacy of their internal control structure and procedures*, as well as *assessing the effectiveness of such internal controls and procedures for financial reporting*, whereas, independent auditors are required to *attest to management's assessment of its internal control over financial reporting*. [12]

INFORMATION TECHNOLOGY IMPACTS

The Act promotes IT impacts that stem from the use of the *COSO integrated framework*, identified by the Security Exchange Committee as a methodology for achieving compliance. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a private US organization that provides guidance to executive management and governance entities on organizational issues, such as governance, ethics, internal control, risk management, fraud, and financial reporting. [13] To facilitate its mission, COSO has established an *internal control model* that defines seven components with IT impacts. **Objective setting** specifies law expectations and reflects the organizational culture to avoid litigation. **Event identification** is the path to reconnoiter violation incidents and align the organizational response appropriately. [13] **Risk assessment** is the process to assess the *risks that directly or indirectly affect the successful completeness of financial reports*, evaluating the level of effectiveness of current systems, and the current level of accuracy of the existing documentation. **Risk response** is the action to

thwart or contain malicious attempts, aiming to mitigate their effects while ensuring business continuity. **Control activities** embrace creation of *audit trails* for financial information systems, deployment of *independent* design, implementation and quality assurance *testing teams, employee cross training on IT functionality(*system structure, software applications, operational procedures, and quality assurance), and discouragement of *manual operations* as prone to human errors.[13] **Information and communication** involve the role of IT management to *identify and address risks* based upon the communication of timely and reliable information, such as a comprehensive presentation to top executives proposing remedial projects for law conformity. **Monitoring** refers to frequent *auditing processes* that should be conducted within the IT area and enterprise-wide to determine the level of organizational preparedness against security abuses, with management's awareness and responsibility for their outcome. [13]

INFORMATION SECURITY IMPACTS

Albeit the Act does not, in fact, comprise any information security requirements, it essentially entails **information technology security** as the fundamental component for its fulfillment, precisely because enterprises need a powerful IT infrastructure enabled by a dynamic information security configuration, in order to ensure a rigorous process as to the *confidentiality, integrity,* and *availability* of their vital assets.[1] Since the primary concern of the Act engulfs *financial systems and where information and finances mee*t, organizations are driven to proactively safeguard their assets against illicit manipulation through a variety of security measures. A coherently integrated **security plan** with enforced, explicitly articulated *policies* (including a wireless policy) that reflect SOX compliance takes precedence. [1] **Security architecture** encompasses the *multiple layers of defense* that provide a much more reliable measure of security effectiveness, as they prevent, detect, and react when intrusions occur. **Identity management** is the method to constantly *qualify, quantify,* and *update user authenticating privileges,* assigning and revoking access levels in strict adherence to individual duty needs, because technological advancements enable *data accessibility* by various users from disparate locations.[1] *Integrity signifies a measure of quality*, thus, **data integrity** is achieved by embedding the *encryption* and *digital signatures* methods into business operations, where encryption protects data from security breaches, whereas digital signatures ensure unmodified data in transit. To meet law objectives of a *secure* and *impenetrable* IT architecture, **vulnerability management** espouses a detailed *risk analysis assessment including a penetration testing* to evaluate the depth of defense mechanisms, detect potential system vulnerabilities, and properly decide on the acquisition of new safeguards. Lastly, a**utomated audit capabilities** inherent in the software design, accelerate the process of *tracking access* to sensitive organizational resources to deliver the needed specificity without interfering with routine system performance. [1]

INFORMATION SECURITY CONTROLS

To guard against security attacks, *information security controls* must be appropriately configured to respond quickly and innovatively, thus maintaining operational efficiency, consistency, and flexibility. From the SOX perspective, Section 302 requires certified disclosures of issues having a material impact on company shareholder value, albeit the statutory language does not specify whether IP assets should be included. [6] Given that **intellectual property** assets, such as *patents, trademarks, copyrights, trade secrets, business know-how, customer lists, and brands*, account for the majority of the total value of

most companies, SOX and IP intersect in three ways. Initially, failure to properly identify and value IP assets violates Sections 302 and 401, failure to establish proper internal controls for monitoring and reporting changes in IP asset values violates Section 404, while failure to properly value the company IP assets could create an unrealistic market value for that company, empowering employees to report SOX violations according to SOX whistleblower protection provision. [6] Therefore, it is imperative that organizations maximize the value associated with their IP assets through an effective IT protection plan. **Spreadsheet applications** are powerful mechanisms used by accountants, auditors and clients that present promising targets for *unauthorized access, and/or unauthorized altering of formulas, data, or formatting.* Consequently, internal auditors play an invaluable role in this domain, by evaluating clients' operations versus spreadsheet using and providing viable solutions before abuses emerge.[2] ***Restricting access*** through password protection constitutes the fundamentally preventive and defensive measure over unauthorized access, where in the *Read-only* mode users *may view*, but *not alter* existing data, in the *Open* mode users *may read and write* to spreadsheets after entering a correct open password, while in the *Modify* mode privileged users are required to input *another password* as safeguard for saving freshly input data, otherwise the original document cannot be modified. [2] ***Locking workbooks and cells*** applied to the entire workbook document or to only those cells that contain sensitive formulas, is another feature to prevent unauthorized workbook updates. ***Modification controls*** provide the assurance that they are properly performed within the application framework as intended. However, it may not be practically efficient to formally modify the majority of spreadsheet applications across the organization, especially when each separate change may necessitate multiple concomitant approvals until it is entirely implemented. Lastly, ***evaluating built-in controls*** vigilantly is crucially important in determining the adequacy of security measures that predict the effectiveness of spreadsheet applications. [2]

COMPLIANCE

Regulatory compliance translates the management intent into an enforceable technical approach associated with organizational network security, data storage and content protections practices, with the admirable goal to achieve law conformity and thereby reduce liability. **Storage** capabilities constitute the core evaluation for legislative requirements that revolve around *what the data is saved with, how to identify and retrieve data, and how to ascertain that data has not been altered or tampered with.* [8] Therefore, it is critically important that storage technology is updated, and strategically assembled to implement security directives that ensure data retrieval, since audit data may not be retrievable in subsequent years due to outdated or obsolete storage equipment, not because of its degradation. **Content management** is the activity of effectively controlling and tracking the creation, sharing and archiving of business documents and their content across organizational boundaries. [8] **E-Mail and collaboration management** is the process that filters out outbound e-mail content to restrict unauthorized corporate disclosures while inhibiting spam and virus traffic, because an area where government regulations focus on for potential security breaches is corporate e-mail transactions. Strong and agile **security and vulnerability scanners** enhance regulatory requirements, but, they simultaneously provide the foundation for evaluating the architecture resilience when necessities emerge to lock down certain important networks, systems, and applications. **Systems and network management** controls are capable to detect changes and failures occurring on systems by tracking servers, systems and networks,

and thereby create custom reports producing real-time images on how the corporate IT infrastructure is law compliant. [8] In the corporate landscape, coordinating *collaboration and accountability* across the enterprise constitutes the fundamental driver that will provide the solid foundation for a fruitful operational efficiency. As system complexity encumbers efforts, **integrating the IT architecture** by consolidating redundant systems, platforms, and databases yields substantial benefits versus its significant investment requirement, including operational savings, reduced assets threats, reduced compliance costs, and better quality information. Compiling **portals** provides a clear view of refined information available to executives for strategic decision making and financial reporting. [5] **Control automation** enhances law compatibility, because from the auditor's perspective, a UNIX system or an Oracle database with inherent automated processes for provisioning, are considered organizational advantages. **Data standardization** by integrating entry points and formalizing data flaws substantially eliminates redundancy and superfluous information gathered from various sources. **IT governance** by structuring effective IT management and applicability articulates the benefit of the investment expense to secure the *confidentiality, integrity and availability of information,* as required. [5]

GUIDELINES FOR SECURE ELECTRONIC RECORD

A rigorous electronic record retention program is consolidated on organizational principles that involve: a) *electronic data management***,** b) *document-review, retention and destruction policies*, c) *records of all types of hardware/software used*, d) *data transmission channels*, e) *electronic "footprints"*, f) *employee technology-use training program*, g) *litigation response team*, and h) *routine audits*. [7]

ENFORCEMENT ACTION TO INFORMATION SECURITY

Enforcement of the Sarbanes-Oxley Act or any of its promulgated rules and regulations is deemed as a *violation of the Securities Exchange of 1934*, where the SEC is to issue a complaint for adjudication in federal court. Obviously, an *information security* violation is interpreted as a Section 404 violation [9]

ACCEPTANCE

In spite its tumultuous high-cost implementation, the Sarbanes-Oxley Act proves *cost-effective* as per Protiviti's 2010 first quarter survey where 70% of respondents assessed *benefits outweighed costs*, while *investor confidence in U.S. public companies remains strong*, per the September 2010 survey by the Center of Audit Quality. [3, 11, 4]

RESISTANCE

Conversely, law controversy produced convoluted implications, such as the *competitive disadvantage* of the U.S. financial market against its more attractive international counterparts, and the phenomenon of *stifling innovation* for smaller U.S. firms, by limiting their ability to enter capital markets. [14]

FUTURE DIRECTIONS

Issues for further investigation are: **Question 1**: *Does restricting access management privileges make organizational processes less wieldy?* **Hypothesis 1**: *When access management privileges are properly*

assigned, organizational processes will remain agile and resilient. **Question 3**: *What levels of storage protection are required to ensure impenetrable storage systems?* **Hypothesis 3**: *When organizations employ stringent storage protection measures, storage systems will remain impenetrable.*

CONCLUSION

Conformity with the Sarbanes-Oxley Act illustrates the strategic implementation that encapsulates balance between IT systems agility and rigorous operational controls. With its impact on information security, business strategy and society as well, the legislation promotes the foundation for a vigorous ethical behavior to flourish, and an archetype to be consistently followed, thus deterring social costs. Essentially, character involves not just doing the right thing, but doing the right thing for the right reasons. In addition, attitudes precede actions and leadership attitudes are ethical values.

REFERENCES

[1] Ali Pabrai, Uday O.IT's Role in Sarbanes-Oxley Compliance. *Certification Magazine*, (2005) 7, 3, 72-73, 2p. http://certmag.com/print.php?in=1097

[2] Bordelon, Paul L.Safeguarding spreadsheets: built-in software controls can protect the integrity of important financial data and formulas. *Internal Auditor Magazine*, (2006), 4, 63, i3, p29(3). http://infotrac.galegroup.com/itw/infomark/547/100/33536710w16/purl=rcl_GBFM_0_A147344388

[3] Brodkin, Jon. SOX: Five years of headaches. *Network World*, (2007), 24, 29, 1-16, 2p. http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=25985000&site=bsi-live

[4] Center for Audit Quality (2010), 4, 9. http://www.thecaq.org/emails/CAQ_Newsletter_2010-09.htm

[5] Dittmar, Lee. Governance and Compliance: Driving IT Priorities.*Financial Executive*, (2006), 22, 1, 48-51, 4p http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=19364060&site=bsi-live

[6] Johnson, James H. IP and SOX: Managing Intellectual Property Assets in Accordance with Sarbanes-Oxley. *Intellectual Property & Technology Law Journal*, 2009, 21, 2, 1-4, 4p. http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=36400528&site=bsi-live

[7] Lange, Michele C.S. Sarbanes-Oxley Has Major Impact on Electronic Evidence. *The National Law Journal* (2003) http://www.law.com/jsp/article.jsp?id=1039054510969

[8] Rapoza, Jim. Compliance is close at hand. *eWeek*, 2006, 23, 21, 33-36, 3p. http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=20943915&site=bsi-live

[9] Sabett, Randy V. (2004). The real deal with Sarbanes-Oxley: Perspectives for the security manager http://searchsecurity.techtarget.com/tip0,289483,sid14_gci956077,00.html

[10] Sarbanes-Oxley Act of 2002. http://www.nysscpa.org/oxleyact2002.htm

[11] 2010 Sarbanes-Oxley Compliance Survey. http://www.protiviti.com/soxsurvey

[12] Sarbanes-Oxley Act of 2002. http://www.soxlaw.com

[13] Sarbanes-Oxley Act of 2002. http://www.sox-online.com/coso_cobit_coso_cube-new.html

[14] Sarbanes-Oxley Has Not Put US at Competitive Disadvantage, Says Act Co-Author in New Gartner Podcast. Press Release (2007) http://www.gartner.com/it/page.jsp/id=515007

[15] Surowiecki, James. Sarboxed In?; The Financial Page Series: 5/5.*The New Yorker*, 2005, 81, 40, 46 http://www.newyorker.com/archive/2005/12/12/051212ta_talk_surowiecki