IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITB12705

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2* edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

Increasing Governmental Regulations and Their Impact on IT: SOX and HIPAA

Amita Goyal Chin & Sushma Mishra
Dept of Information Systems, School of Business, Virginia Commonwealth University, Richmond, VA,
T: (804)828-7131 [Chin], -7091 [Mishra], F: (804)828-3199, amita@saturn.vcu.edu, mishras@vcu.edu

ABSTRACT

Given the recent monumental events including the September 11th attack on the World Trade Center and the Pentagon as well as the Enron and MCI Worldcom debacles, people have witnessed, and more readily accepted, a significant increase in governmental authority, leading to a dramatic upsurge in the number of governmental regulations imposed on business organizations and society. This paper identifies two of the most significant of these governmental regulations – SOX and HIPAA — and discusses their considerable impact and implications on information technology, both from a technical and managerial perspective.

INTRODUCTION

IT infrastructure, processes, and security have been thrust to the forefront due to colossal catastrophes such as the September 11th attack on the World Trade Center and the Pentagon, illegal corporate activities, identity theft, and cyber crime. The plethora of governmental regulations successfully passed ensuing these recent events hold business organizations unmistakably accountable, with serious consequences, including fines and imprisonment, for noncompliance. While such legislation may not directly be aimed at corporate IT, the omnipresence of information technology along with the indisputable gravity of these governmental regulations has forced business organizations to revisit and subsequently revamp their IT infrastructure and processes in order to achieve legislative compliance. This paper discusses two of the most significant of these governmental regulations – SOX and HIPAA — including their considerable impact and implications on information technology, both from a technical and managerial perspective.

GOVERNMENTAL REGULATIONS

Sarbanes-Oxley Act (SOX)

In the aftermath of the Enron and MCI WorldCom fiascos, the Sarbanes-Oxley Act (SOX), also known as the Public Company Accounting Reform and Investor Protection Act of 2002, was enacted in response to public anger with accounting fraud and corporate governance and reporting failures, and protects investors from fraudulent reporting by corporations (Moore 2005). SOX, applicable to public traded companies, mandates that companies employ stringent policies and procedures for reporting financial information accurately and in a timely manner.

SOX contains eleven titles, each of which contains multiple "Sections," which itemize the mandatory requirements (SEC, 2003). Several of these Sections have grave implications for key corporate executives, including the CEO, CFO, and CIO. Perhaps the most serious of the SOX Sections are Sections 302 and 906, which require signatures from the CEO and the CFO attesting that the information provided in the company's quarterly and annual reports is authentic and accurate (Volonino, 2004). Furthermore, these key company executives bear the responsibility for any inaccurate representation of the reports, whether or not they possessed a priori knowledge of such errors. Section 906 holds CEOs, CFOs, and corporate directors both accountable and liable for the accuracy of financial disclosures. Unlike Section 302, Section 906 penalizes officers only if they knew of a possible problem or error when certifying a report (ITGI, 2004). Sections 103 and 802 specify audit record retention and security requirements (ITGI, 2004).

Section 401 requires the company to disclose not only balance sheet transactions, but also transactions not normally shown on the balance sheet. Additionally, all arrangements, obligations (including contingent obligations) and other relationships that might have a material current or future effect on the financial health of the company (ITGI, 2004) must be divulged. Section 401 restricts the use of pro forma information and directs companies to represent financial information in a manner consistent with generally accepted accounting principles (GAAP).

Section 404 requires that executives attest not only to the company's financial statements, but also to the control processes for the collection of the data supporting the financial statements (SEC, 2003; Gallagher, 2003). Section 409 requires real time disclosure of financial and operating events, requiring companies to disclose any events that may have material impacts on their financial condition or operations on a rapid and current basis (Volonino, 2004). Technological progress may soon define "rapid and current basis" to be within 48 hours following the occurrence of an event. Compliance with Sections 404 and 409 requires that each step in a business transaction — order, payment, storage of data, aggregation into financial reports, etc. — must be audited, verified, and monitored.

Section 802 requires the retention and protection of corporate records and audit documents and expressly includes e-records in the mandate (ITGI, 2004). This Section institutes criminal penalties for unauthorized document alteration or destruction.

Health Insurance Portability and Accountability Act (HIPAA) of 1996

HIPAA safeguards the privacy of medical records of patients by preventing unauthorized disclosure and improper use of patients' Protected Health Information (PHI) (CMMS, 2005). With a significant emphasis and monetary investment in the 1990s on the computerization of health services operations, the possibility of data manipulation and nonconsensual secondary use of personally identifiable records has tremendously increased (Baumer, 2000). HIPAA declares PHI "privileged," protecting individuals from losses resulting from the fabrication of their personal data. Businesses subjected to HIPAA are directed to protect the integrity, confidentiality, and availability of the electronic PHI they collect, maintain, use, and transmit.

Three major components of HIPAA are:

- **Privacy:** the privacy of individuals' health information in written, oral and electronic form must be protected. Health information includes medical records, claims, and payment information, and almost all additional information related to patient health care.

- **Security:** private information of individuals must be kept safe from damage of any kind. The purpose of this clause is to protect electronic patient information from alteration, destruction, loss, and accidental or intentional disclosure to unauthorized persons.
- **Transaction:** various participants in the healthcare industries must effectively and electronically communicate patient information. Successfully meeting this requirement necessitates the privacy and security covenants also be met.

DISCUSSION

Sarbanes-Oxley Act (SOX)

With a cost of compliance for 2005 estimated at $5.8 billion (AMR, 2005), SOX significantly depletes available organizational resources (Bennett & Cancilla, 2005). SOX forces organizations to reevaluate IT governance practices (Fox, 2004), since both managerial and technical commitment is required to create the necessary organizational infrastructure necessary for compliance. This means that management must establish and exercise considerable internal control assessment measures in order to be prepared to cope with the demands of SOX, such as quarterly reporting, security policies, cost management, and external audits.

Technical issues (see Table 1) that must be revisited and subsequently modified due to the enactment of this regulation include: data management (Volonino et. al., 2004; Farris, 2004, Yugay and Klimchenko, 2004), which impacts data and systems security (Bertino, 1998); software development methodologies, which should now incorporate compliance issues as a component of the development lifecycle; and documentation and recordkeeping, which should now be strengthened to include versioning and audit ability (Peterson and Burns, 2005; Volonino et. al., 2004).

Health Insurance Portability and Accountability Act (HIPAA) of 1996

The cost of compliance with HIPAA to healthcare organizations, just for 2002, was $270 million (NetWorkWorld, 2003). This regulation has forced companies to revisit and reorganize their business processes. Compliance with HIPAA is not just a matter of technical products ensuring safe and secure data collection, transaction, and storage; rather, compliance is an issue of "organizational change management." It requires instituting new structures and patterns for health care companies to coordinate efficiently, trust other's intentions, and responsibly maintain and protect sensitive data (Huston, 2001). Success depends on how well each organization develops a "management infrastructure with well defined roles that will address administrative, physical, and technical safeguards" (Mercuri, 2004). HIPAA compliance requires companies to constantly evaluate and test their internal controls over all business units and functional areas (Farris, 2004). Additionally, organizations must provide audit trails which are subject to external evaluation (Peterson et al., 2005), implement proper planning, institute privacy policies (Mercuri, 2004), and ensure controls in all data access points (Mercuri, 2004).

Table 1. Impact of Legislations on various domains of Information Systems

Legislation	Impact on Information Technology	
	Technical	Managerial
Sarbanes-Oxley Act (SOX)	▪ Database Systems (data integrity, data quality, database architecture) ▪ Software development methodologies ▪ Security ▪ Versioning and auditing of electronic record retention ▪ Extensive documentation	▪ IT Governance (effective internal control) ▪ Systems Audit ▪ Quarterly reporting ▪ Cost management ▪ Policy evaluation
Health Insurance Portability and Accountability Act (HIPPA)	▪ Data Security ▪ Data integrity ▪ Transaction processing ▪ Disaster recovery ▪ Real-time data access ▪ Encryptions and authentication ▪ Network communications	▪ Privacy policy for health information access ▪ Audit control planning ▪ Privacy policy implementation at all information collection points

HIPPA impacts healthcare organizations at the basic infrastructure level, thus demanding reevaluation at all levels, including the creation and implementation of technical solutions. Employing and adapting to technical solutions requires not only proper planning but also an overhaul in organizational processes. Data integrity (Mercuri, 2004), data security (Huston, 2001; Mitrano, 2003), transaction processing (Huston, 2001; Peterson et.al, 2005), real time accessibility (Peterson et.al., 2005), encryption and authentication techniques (Knorr, 2004), network communications (Huston, 2001), and disaster recovery techniques must all be investigated and modified in order to guarantee private patient data storage and interchange.

CONCLUSION

The ubiquitous Internet has yielded a marketplace of global proportions. In juxtaposition with this atmosphere of global connectivity is the responsibility for information safety, security, privacy, and accuracy. Numerous governmental regulations have and are continuing to force organizations to revamp their IT infrastructures. IT has become a central organizational function and thus, governmental regulations often radically impact IT and business processes, particularly in terms of the cost of compliance, preparedness for external audit, organizational restructuring, sharing of data amongst enterprises, enhanced technical support and regular monitoring, and the assessment of business processes.

Governmental regulations are usually proposed in reaction to growing public dissatisfaction and concerns (Milberg et. al., 1995). While they may be expensive and arduous to fulfill, these regulations present an opportunity for organizations to restructure and improve their information technology operations.

REFERENCES

1. AMR Research. (2005). http://www.amrresearch.com/ Retrieved on 05/10/05.
2. Baumer, D., Earp, J. B. and Payton, F. C. (2000). Privacy of Medical Records: IT Implications of HIPAA. *Computers and Society*.
3. Bennet, V., and Cancilla, B. (2005). IT responses to Sarbanes-Oxley. *IBM*. http://www-128.ibm.com/developerworks/rational/library/sep05/cancilla-bennet/index.html. Retrieved on 09/30/05.
4. Bertino, E. (1998). Data Security. *Data & Knowledge Engineering*. Vol. 25 (199-216).
5. Farris, G. (2004). Mitigating the Ongoing Sarbanes-Oxley Compliance Process with Technical Enforcement of IT Controls. *DM Direct Newsletter*. DMReview.com
6. Fox, C. (2004). Sarbanes-Oxley- Considerations for a Framework for IT Financial Reporting Controls. *Information Systems Control Journal*, Vol. 1.
7. Gallagher, S. (2003). Gotcha! Complying with Financial Regulations. Baseline Magazine. http://www.baselinemag.com/article2/0,1397,1211224,00.asp. Retrieved on 10/02/05.
8. Huston, T. (2001). Security Issues for Implementation of E-Medical Records. *Communications of the ACM*. Vol. 44. No. 9.

9. (ITGI) Information Technology Governance Institute. (2004). IT Control Objectives for Sarbanes-Oxley.
10. Klimchenko, V. (2004). SOX Mandates Focus on Data Quality and Integration. DM Review, February 2004.
11. Knorr, E. (2004). The Bitter Pill: Regulation has come to town, and IT will never be the same. *CIO Magazine*. http://www.cio.com/archive/. Retrieved on 09/20/05.
12. Mercuri, R.T. (2004). The HIPAA-potamus in Health Care Data Security. *Communications of the ACM.* Vol. 47. No. 7.
13. Milberg, S.J., Burke, S.J., Smith, H.J. and Kallman, A. (1995). Values, Personal Information Privacy and Regulatory Approaches. *Communications of the ACM.* Vol. 38. No. 12.
14. Mitrano, T. (2003). Civil Privacy and National Security Legislation: A Three-Dimensional View. *Educause review*. November/December.
15. Moore, C. (2005). The Growing Trend of Government Involvement in IT Security. *Proceedings from InfoSecCD Conference '04, October*.
16. NetWorkWorld. (2003). http://www.networkworld.com/research/2003/0901regs.html?page=1. Retrieved on 09/29/05.
17. Peterson, Z. and Burns, R. (2005). Ext3cow: A Time-Shifting File System for Regulatory Compliance. *ACM Transactions on Storage*. Vol. 1, No. 2 (190-212).
18. (SEC) U.S Securities and Exchange Commission. (2003). Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports. http://www.sec.gov/rules/final/33-8238.htm Retrieved on 09/30/05.
19. Volonino, L., Kermis, G., Gessner, G. (2004). Sarbanes-Oxley links IT to Corporate Compliance. *Proceedings of the Tenth Americas Conference on Information Systems*. New York, New York.
20. Yugay, I. and Klimchenko, V. (2004). SOX Mandate Focus on Data Quality and Integration. *DM Review Magazine*. Dmreview.com Retrieved on 09/30/05.