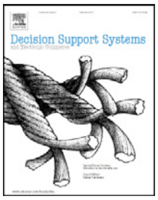
Decision Support Systems 57 (2014) 54–63

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss



IT security auditing: A performance evaluation decision model

Hemantha S.B. Herath [a], Tejaswini C. Herath [b,*]

[a] Department of Accounting, Goodman School of Business, 240 Taro Hall, 500 Glenridge Avenue, St. Catharines, Ontario L2S 3A1, Canada
[b] Department of Finance, Operations, and Information Systems, Goodman School of Business, 240 Taro Hall, 500 Glenridge Avenue, St. Catharines, Ontario L2S 3A1, Canada

ARTICLE INFO

Article history:
Received 6 September 2011
Received in revised form 18 June 2013
Accepted 29 July 2013
Available online 8 August 2013

Keywords:
Information technology management
Information technology audit
Information systems audit
Information security audit
Audit decision
Agency model

ABSTRACT

Compliance with ever-increasing privacy laws, accounting and banking regulations, and standards is a top priority for most organizations. Information security and systems audits for assessing the effectiveness of IT controls are important for proving compliance. Information security and systems audits, however, are not mandatory to all organizations. Given the various costs, including opportunity costs, the problem of deciding when to undertake a security audit and the design of managerial incentives becomes an important part of an organization's control process. In view of these considerations, this paper develops an IT security performance evaluation decision model for whether or not to conduct an IT security audit. A Bayesian extension investigates the impact of new information regarding the security environment on the decision. Since security managers may act in an opportunistic manner, the model also incorporates agency costs to determine the incentive payments for managers to conduct an audit. Cases in which the agency model suggests that it is optimal not to conduct an IT security audit are also discussed.

1. Introduction

The 2011 ISACA survey notes that compliance with ever-increasing privacy laws, accounting and banking regulations, and standards is a top priority for most organizations [30]. Accounting regulations have had a visible impact on information security practices in organizations. The Sarbanes–Oxley Act (SOX), emerging international accounting regulations such as the International Financial Reporting Standards (IFRS), and other accounting regulations affect computing practices in public organizations in the United States and worldwide [25]. Although the specific requirements of SOX and IFRS do not explicitly discuss information technology, the profound shift in business records from pen and paper to electronic media has significant implications for IT practices for the purposes of financial reporting. In addition to the external threats, an extensive dependence on technology may inadvertently provide sophisticated means and opportunities for employees to perpetrate fraud in rather simple and straightforward ways [12,29]. As IT controls have a pervasive effect on the achievement of many control objectives [26], regulations have implications for IT governance and controls [7,13,18]. In most organizations, since the data that is used in financial reporting is captured, stored, or processed using computer-based systems, achieving a sufficient level of internal controls means that controls have to be put in place for technology use in organizations [22].

From the accounting regulation perspective, public corporations, at least in theory, must go through information systems audits in order to obtain an auditor's report confirming that there are sufficient internal controls. However, this regulation-driven audit is not mandatory for public companies earning annual revenue of less than 2 million dollars or for many organizations that are not public companies. Security surveys show that security audits are the predominant approach in testing the effectiveness of security technologies. Almost 50–65% of companies surveyed report that they carry out security audits [34], but not all companies undertake these investigations. The question thus arises, if system audits are not mandatory, when should firms undertake security audits? IT systems are complex, which makes evaluating their performance and security a complex problem [25]. Audits are often very laborious and expensive [37]. Implementing an IT audit strategy that justifies its cost and which promotes the effective use of information systems is a challenging task [33]. Given the costs involved in carrying out these audits and the opportunity costs of not conducting such audits, the question becomes an important one.

Although literature in the area of the “economics of IT security” is burgeoning with papers dealing with the issue of whether or not to invest in IT security or how to establish the optimal level of investment in IT security [17,19,23], there is hardly any research that deals with the control aspects. Given budgetary constraints, firms often have to decide whether or not to spend resources on non-mandatory security initiatives such as IT security audits. Thus, it is important for a firm's management to have an objective basis and a sound decision model for deciding whether or not to undertake an IT security audit. The decision model we develop attempts to fill a gap in the literature and in practice in this area. More specifically, we consider the question of whether or not to carry out an IT security audit by developing a performance evaluation decision model. The model considers security investments and their relationship to IT audits.

* Corresponding author.
E-mail addresses: hemantha.herath@brocku.ca (H.S.B. Herath), teju.herath@brocku.ca (T.C. Herath).

0167-9236/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.dss.2013.07.010

Our approach is similar to the probabilistic variance analysis model in Bierman et al. [5]. The probabilistic variance analysis model [5] demonstrates the conditions under which a cost variance investigation is warranted in a single period setting. Applying this model to the IT security context, we extend Bierman et al.'s [5] model in several ways. First, from an application point, in order to demonstrate the IT audit decision model, we use an IT security investment setting. Second, we incorporate Bayesian decision theory to investigate the impact of new information regarding a security environment on the decision of whether or not to conduct an IT security audit. Lastly, in consideration that security managers may act in an opportunistic manner, we incorporate agency theory into the IT security audit decision problem to determine the incentive payments for audit managers that would motivate them to carry out an audit. We also discuss the efficiency loss of the agency model where an optimal decision may differ from the baseline model (i.e., without agency issues). Our approach is general and is applicable in a wide range of settings, including cyber security auditing and IT manager performance evaluation.

The paper is organized as follows. In the subsequent section, we review the background literature and discuss the security audit research problem. We then develop a decision model that explicitly considers the cost and benefit tradeoffs associated with a system audit with a view to deciding whether or not an IT audit should be performed. Further, we investigate the impact of new information on the IT audit decision. Recently, the cyber security literature has highlighted agency problems that may arise in the information security context. To address this issue, we apply agency theory to determine the incentive costs pertaining to an IT audit decision and extend the analysis to investigate the efficiency loss of the agency model. Finally, we conclude with a discussion of the model's limitations and avenues for future research.

2. Background literature

2.1. Information system trends and accounting information: internal controls and information security audits

The ability to capture and report financial and accounting information through computerized systems has evolved during the last few decades to the point that the key business processes that capture this information in many companies are entirely automated. Despite the significance of IS and technology to the accounting and financial reporting processes, relatively little is known about their impact on the frequency and types of financial misstatements [12]. Messier et al. [31] found that control problems are more prevalent in computerized environments. Problems arise even from relatively simple technologies such as spreadsheet applications, which are often used by small- and medium-sized businesses for accounting and finance purposes. This extensive dependence on technology may also inadvertently provide sophisticated means and opportunities for employees to perpetrate fraud [29] by rather simple and straightforward means [12].

Altered, incomplete, or inaccurate data, as well as a complete loss of data, have adverse implications for businesses and financial reporting. Internal and external information security threats represent a fundamental risk to a firm's operations as well as to the quality of its financial and non-financial information. IT systems managers are charged with protecting privacy and personally identifying financial information; they are responsible for building access controls capable of protecting the integrity of financial statements and safeguarding intellectual property in a strong and growing regulatory environment against an ever increasing worldwide threat. Automated systems such as general IT and application controls can test input accuracies to ensure the validity of transactions, thereby reducing the likelihood of misstatements [31]. Proper information systems controls can also mitigate the risk of certain frauds [12].

Regulations such as Sarbanes–Oxley require a sophisticated set of internal controls that guide the creation of financial documents and disclosure of financial information in a timely and accurate manner. In March 2004, the US Public Company Accounting Oversight Board (PCAOB) approved PCAOB Auditing Standard No. 2, entitled "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements," contending that IT controls have a pervasive effect on the achievement of many control objectives [26]. In addition to controls such as the segregation of duties, SOX has implications for other IT controls. To achieve these controls, the Securities and Exchange Commission (SEC) has mandated the use of a recognized internal control framework, specifically recommending the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework with regard to compliance with SOX.

General IT and application controls prevent input accuracies, which reduces the likelihood of misstatements [31] and mitigates the risk of certain frauds [12]. The COSO framework identifies IT control activities broadly in two categories: (1) application controls — designed within the application to prevent/detect unauthorized transactions, and (2) general controls — designed for all information systems supporting secure and continuous operation. The framework recommends monitoring activities to evaluate and improve the design, execution, and effectiveness of internal controls. It also recommends periodic separate evaluations such as self-assessments and internal audits that usually result in a formal report on internal controls. An organization may have different types of evaluations, including: internal audits, external audits, regulatory examinations, attack and penetration studies, performance and capacity analyses, IT effectiveness reviews, control assessments, independent security reviews, and project implementation reviews. IT audits can provide assurance that systems are adequately controlled, secure, and functioning as intended [33], and can play an integral role in enterprise risk management [2].

Under Sarbanes–Oxley Section 404, the annual external auditing of company financial records requires the inclusion of an assessment of the adequacy of the internal controls that impact public financial reporting. Management is required to report on the effectiveness of the internal controls and auditors are required to comment on the report. Thus, it is important to emphasize that it requires senior management and business process owners merely not only to establish and maintain an adequate internal control structure, but also to assess its effectiveness on an annual basis. Organizations must ensure that appropriate controls (including IT controls) are in place, in addition to providing their independent auditors with documentation, evidence of functioning controls, and the documented results of the testing procedures. The Auditing Standards Board's (ASB) Statements on Auditing Standards (SAS) No. 109 (effective in 2006) further increases the need for auditors to consider the effectiveness of their clients' internal controls, which in turn increases the need to evaluate automated as well as manual controls. Curtis et al.'s [12] research on the initial SOX Section 404, however, indicates that this goal may not have been achieved in a substantial number of public companies.

The attention to the issue of internal controls and their implications for systems security came about with the emergence of SOX-like mandates (e.g., HIPAA and the Gramm–Leach–Bliley Act, among others) since the regulations make these activities mandatory. To reach auditable compliance with the regulatory requirements, every documented node-to-node interface point where it can be demonstrated that adequate access and security controls are applied increases the probability of a positive audit report. The control issues surrounding compliance with these regulations, however, do not apply only to public companies. Governments at all levels, the nonprofit sector, and closely held companies all face the need to satisfactorily protect the integrity of their confidential information and provide adequate controls on access to data stores [2]. For some nonprofit organizations, the financial risk of litigation resulting from inadequate controls may be far greater than any harm from adverse audit findings.