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.

© 2013 Elsevier B.V. All rights reserved.

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.

2.2. Security and audit costs

To put the general and application level IT controls in place requires substantial investments. Security evaluations such as internal audits, external audits, attack and penetration studies, or any other types of assessments also have cost implications for businesses. Gordon and Loeb [17] have argued that the allocation of funds to information security should be similar to or at least based on cost and benefit terms due to the irreversibility of investment costs and the uncertain nature of the outcomes. Security investments are difficult to justify due to difficulties in defining and measuring the full array of benefits. Research is scant, but some of the security investment literature has tried to address this issue [10,17,19,23,24]. Security investments that allow putting various IT controls in place are likely to have an impact on the achievement of positive audit reports. However, due to the evolving nature of information security threats, the effectiveness of these controls needs to be audited regularly. Related questions then arise, such as: When should businesses carry out security evaluations? And what is the relationship between these security investments and evaluation?

In this regard, the cost variance investigation literature in accounting and the emerging literature in cyber security management control design can provide us some insights. After the investments in security technologies are made, the effectiveness of these investments can be studied through the lens of variance investigation. Prior cost variance analysis literature in accounting that has examined whether a cost variance investigation should be undertaken or not is analogous to research into the decision of whether or not to carry out an IT audit. Investigation of cost variances involves the expenditure of effort and funds. The underlying criterion for investigating cost variances invariably is that an investigation should be undertaken if and only if the expected benefits exceed the cost of investigating and correcting the source of the cost variance. Numerous articles have appeared that deal with this management control problem (e.g. [5,14,27]).

Research into the variance investigation problem can be broadly categorized into single verse multi-period models. Kaplan [27] developed a probabilistic model using discrete dynamic programming techniques to determine optimal policies governing when to investigate variances. Demski [14] has classified the sources of cost deviations and developed an algorithm to determine the minimal expected time to discover the source of a variance. Bierman et al. [5] were the first to incorporate the costs and benefits of an investigation into the cost variance investigation decision. They developed the criteria for when to carry out a cost variance investigation. Kaplan [27] provided an excellent survey which summarizes techniques that are potentially useful for assessing the significance of cost variances under these two categories.

More recently, the cyber security literature has also highlighted the agency problems that may arise in the information security context [20]. Gordon et al. [20] discuss that information security managers may have an incentive to request more funding than is justified on an economic basis as it is more risky for them from a career point of view when security breaches occur. An auditing process which allows the measuring of the cost effectiveness of security activities can play an important role in reducing agency problems. In this context, Gordon et al. [20] have developed an analytical model that shows that firms can use an information security audit as part of a management control system designed along with incentive contracts and investment decision rules to discourage a Chief Information Security Officer (agent) from using resources for empire building. To address the above two concerns, we develop an IT security performance evaluation model that can be used to decide when to undertake an IT security audit and what incentive payments are needed to ensure that the manager will perform the audit.

3. System audit decision model

The model developed in this article addresses the basic decision problem of whether or not a firm should conduct an IT system audit. As in Bierman et al. [5], the model considers two measures to decide whether or not to conduct an IT system audit: (1) the amount of the unfavorable loss deviation and (2) the probability of unfavorable loss deviation resulting from uncontrollable factors.

3.1. The two period security investment problem

Consider a firm planning to make IT security investments in two periods. The firm will initially invest in Period 1 and then, based on the ex-post outcome of first period decision, it will decide whether or not to invest in Period 2. The investment cost associated with securing information may include the software costs, hardware costs, and a one-time IT labor cost for configuration and system set up. The model assumes that the IT manager can partially control computer equipment and software failures through investment in IT security and the implementation of IT security policies. If the investment is ineffective, it will result in controllable costs or losses.[1] Thus, when undertaking the first investment in IT security, the manager will estimate the expected loss (mean loss) due to IT security breaches from uncontrollable factors, assuming the investment is effective. The expected loss because of uncontrollable factors is set assuming that favorable and unfavorable deviations from the mean are equally likely under practical levels of effectiveness and efficiency. As such, a normal distribution for the losses from uncontrollable factors can be assumed for the upcoming period (Period 2). This normal distribution assumption makes it possible to determine the probability of a loss deviation of any magnitude resulting from uncontrollable factors, which can be used along with the amount of the unfavorable deviation to determine whether or not to conduct an IT security audit. The two-period setup is shown in Fig. 1.

The rationale is that an IT system audit should be conducted if the unfavorable loss deviation due to an IT security breach is significant and the deviation is due primarily to controllable causes. The model compares the cost of conducting an IT security audit, such as a "penetration" test, against the benefits of cost avoidance in the case of an erroneous decision: for example, making a further investment in IT security when the unfavorable loss deviations due to controllable factors are large (i.e., original investment was ineffective) and an IT manager is paid an incentive based on planned loss reduction.

The model uses following notations for the model variables:

t	time subscript ($t \in (0,1,2)$)
I_0	base level of information security investment cost
I_t	information security investment cost at time t
s_t	level of information security (expressed as an index, i.e., $s_t = \frac{I_t}{I_0}$)
Ω	estimated loss with no IT security investment
θ_i	state of nature (i.e., $i \in (1,2)$)
a_i	possible acts or decisions (i.e., $i \in (1,2)$)
p	probability associated with state θ_2 (thus probability associated with state θ_1 is $(1-p)$)
C:	cost of a IT security audit
ε	opportunity cost associated with not conducting an IT security audit
Δ_t	deviation in losses due to a breach in period t
L_t^P	planned loss in $ in period t
L_t^A	actual losses in $ in period t
σ_t^2	variance of the loss distribution in period t
C_{IDS}	cost of configuring an IDS (excluding investment costs)
v_t	probability of a security breach
β	benefit (or income) to the firm regardless of the state of nature.

[1] The notion of controllable events/costs and uncontrollable events/costs for evaluating a manager's performance is standard in the management control literature in accounting. Uncontrollable costs tell nothing about a manager's decisions and actions because, by definition, nothing a manager does affects such costs.

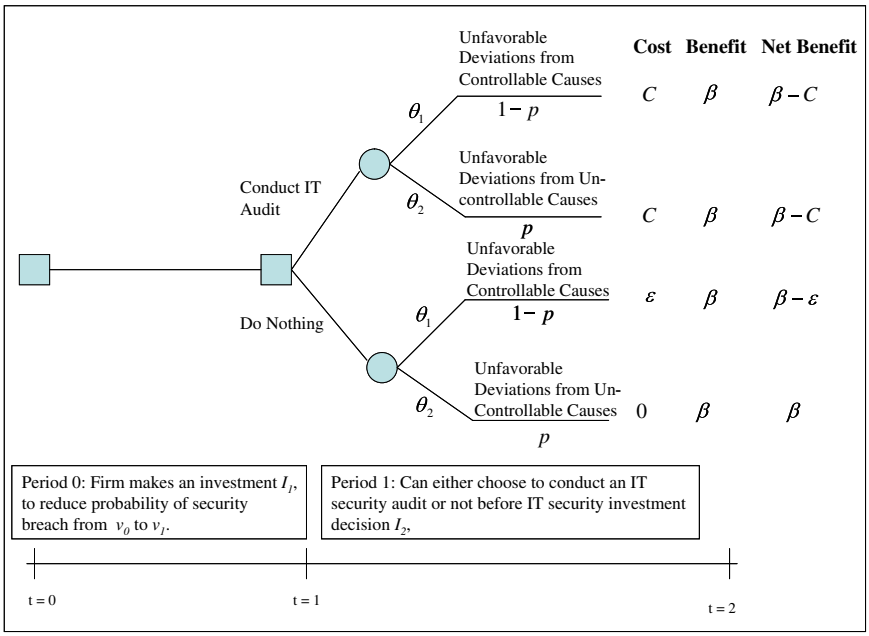

Fig. 1. Two period setup.

The decision regarding whether to conduct an IT security audit is modeled in the following scenario. At the beginning of the period (i.e., $t = 0$), the IT security manager is asked to identify, in the event of a breach, what amount of loss would be expected due to uncontrollable factors in the event of a breach. For example, the IT security manager believes that making an IT security investment I_1 is likely to reduce breach probability and result in a planned loss L_t^P due to a reduction in breach probability. Thus, the expected losses in Period 1 would be given by $E(\text{loss}) = L_1^P$. In order to identify the amount of unfavorable deviation (Δ_1 = Actual Losses − Planned Losses) from the planned loss of L_1^P due to uncontrollable factors, we need an estimate of the standard deviation σ_1 to specify the loss distribution at the time of undertaking the IT security investment I_1.

The standard deviation σ_t of loss distribution can be estimated by the following subjective procedure for a normal distribution [5]. We could ask the IT security manager to come up with a 50:50 odds bet on what range the Period 1 loss would likely fall into due to uncontrollable (random) causes, say $10,000. Assuming a normal distribution for the $ losses, since one half of the area under a normal curve lies within ± 0.67 standard deviations of the mean, σ_t can be computed as $\frac{2}{3}\sigma_1 = 10,000$, and thus, $\sigma_1 = \$15{,}000$. Now, the firm can decide whether or not to do a cyber audit based on the audit performance evaluation model shown in Fig. 2. The critical region of whether or not to conduct a cyber audit can be derived as the optimal act of minimizing the expected costs. Thus, we define the following two acts as a_1 : Do an IT security audit and a_2 : Do nothing. We define the two states of nature as θ_1 : Unfavourable deviation resulted from controllable causes, and θ_2 : Unfavourable deviation resulted from uncontrollable causes.

Suppose there is an unfavorable deviation Δ_1 (actual losses are greater than the planned losses); then the decision whether or not to do a cyber audit to investigate the causes will depend on the probabilities of the above two states of nature. If the true state is θ_1, then the unfavorable deviation was caused by factors within the control of the IT security manager, such as not configuring the system properly despite making an investment to do so and not implementing the security policies of the firm to minimize the computer equipment and software failures. Then conducting an IT security audit is worthwhile because the firm can benefit from future cost savings. More specifically, the firm will not invest in Period 2 and not incur Period 2 IDS configuration costs. Thus, the firm will incur an opportunity cost due to not conducting an IT security audit given by $\varepsilon = I_2 + C_{IDS}$, which can reasonably be assumed to be greater than the cost of an IT security audit C (i.e. $\varepsilon > C$). The cost of an

Acts

States	a_1 : Do an IT security audit	a_2 : Do nothing	Probability
θ_1 : Unfavorable deviations resulting from controllable causes.	C	ε	$1-p$
θ_2 : Unfavorable deviations resulting from uncontrollable causes.	C		p

Fig. 2. State-Act-Conditional costs.

IT security audit will be incurred if an audit is performed but not otherwise. If the true state is θ_2, where the unfavorable deviation is due to factors beyond the control of the IT security manager, then conducting a security audit is not worthwhile and the cost incurred is zero. The State-Act-Conditional Payoff table for the decision problem is shown in Fig. 2.

Given an unfavorable deviation, the probability that the deviation resulted from uncontrollable factors θ_2 is p and the probability associated with state θ_1 is $(1 - p)$. Note that p and $(1 - p)$ are the conditional probability of the two states given that an unfavorable variance has occurred. We can now compute the expected cost of an investigation as

$$E(\text{Cost of Audit}) = Cp + C(1-p) = C. \quad (1)$$

The expected cost of not conducting an IT security audit is

$$E(\text{Do nothing}) = \varepsilon(1-p). \quad (2)$$

If $C < \varepsilon(1 - p)$, the firm should conduct the IT security audit, and if $C > \varepsilon(1 - p)$, the firm should not conduct an IT security audit. Notice that $\varepsilon(1 - p)$ is analogous to the expected future cost savings. By equating the expected cost of the two acts (i.e., $C = \varepsilon(1 - p)$) and solving for the probability, one can find the critical probability p_c which separates the decision space into when it is worthwhile to conduct an IT security audit, given as

$$p_c = \frac{\varepsilon - C}{\varepsilon}. \quad (3)$$

By substituting $\varepsilon = I_2 + C_{\text{IDS}}$ in Eq. (3), we obtain the following expression for the critical probability in terms of IT security variables

$$p_c = \frac{I_2 + C_{\text{IDS}} - C}{I_2 + C_{\text{IDS}}}. \quad (4)$$

If the probability is $p < p_c$ (critical probability), then $C < \varepsilon(1 - p)$ and an IT security audit is warranted; however, if the probability is $p > p_c$ (critical probability), then $C > \varepsilon(1 - p)$ and a security audit is not warranted. In the model given in Eq. (4), the firm's management must estimate the various cost parameters that make up the opportunity cost ε. For simplicity, we assume that the cost of conducting the IT security audit is a fixed amount.

The configuration costs C_{IDS} of an intrusion detection system will vary with different levels of investment I_t. The approach for determining the configuration cost C_{IDS} follows the receiving operating characteristic (ROC) approach outlined by Cavusoglu and Raghunathan [11], Ulvila and Gaffney [36], and Herath and Herath [23]. The expected cost of an intrusion detection system configuration as a function of the quality parameters of a detection system, vis-à-vis the probability of detection and the probability of false positive, is elegantly explained in Cavusoglu and Raghunathan [11].

3.2. Determining the separation curve

The firm can now determine the separation curve that indicates the "region" of whether or not to conduct an IT security audit. It has to estimate the cost of conducting the IT security audit C and, assuming C remains constant, it can further estimate the cost that can be avoided if an IT security audit is conducted by using the expression for $\varepsilon = I_2 + C_{\text{IDS}}$. For a fixed C and assuming $\varepsilon = I_2 + C_{\text{IDS}}$ is a linear function of the unfavorable deviations Δ_t, the following separation curve can be plotted (see Fig. 3) by equating $\Delta_t = I_2 + C_{IDS}$ and computing $p_c = \frac{I_2 + C_{\text{IDS}} - C}{I_2 + C_{\text{IDS}}}$ for different levels of security investments and configurations. Notice that the equivalence $\Delta = \varepsilon$ is used only for the purpose of plotting the separation curve. The conditional probability shown in Fig. 3 is conditional on an unfavorable loss deviation having occurred. Also, both the probability and size of an unfavorable loss deviation are used in deciding whether or not to audit.

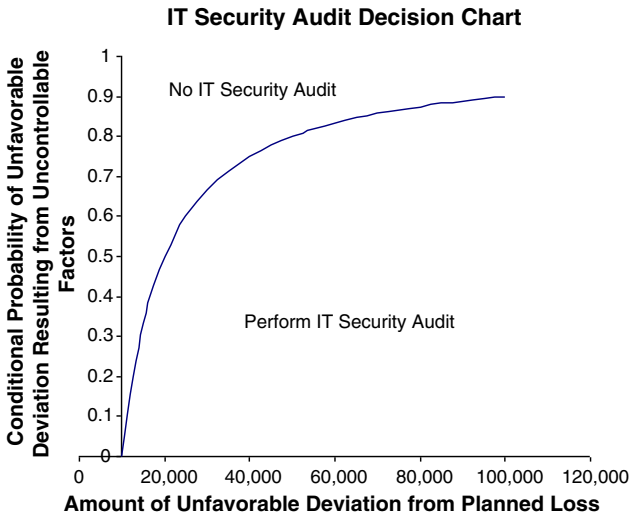

Fig. 3. Plot of critical probabilities and unfavorable deviations.

Suppose we model the breach risk as a decay function; then, at a given security spending level s_t, the probability of a breach occurring is $v_t = \Pr(o|s_t) = e^{-\alpha s_t}$ where the adjustment parameter α represents an expert's subjective assessment of the effectiveness of the system. More specifically, after making the investment I_1 (i.e. $s_1 = \frac{I_1}{I_0}$), the firm can compute the probability of breach as $v_1 = \Pr(o|s_t) = e^{-\alpha s_1}$. If the expected loss without any investment is $s_0 = 0$, and thus $v_0 = \Pr(o|s_0) = e^{-\alpha s_0} = 1$ is estimated as Ω, then the mean of the expected loss distribution is given by $L_1^P = \Omega v_1$. Accordingly, it is assumed that the investment reduces the probability of a breach and in turn the magnitude of the loss.

If the manager's subjectively assessed standard deviation is σ under the normal distribution assumption, then the loss distribution is given by $N(\Omega v_1, \sigma^2)$. If the actual loss is L_1^A, we can compute the unfavorable loss deviation $\Delta_1 = L_1^A - \Omega v_1$. Define the event (X) as a loss deviation of amount Δ_1 or more. Using the normal distribution, the probability of an unfavorable loss deviation Δ_1 or more can be computed as $\frac{\Delta_1}{\sigma} = \frac{L_1^A - \Omega v}{\sigma}$ standard deviations from the mean. The probability of an unfavorable loss deviation of this scale or larger can be determined from the normal distribution tables, as $\hat{p}$.

In Fig. 3, the scale of the y-axis is from 0 to 1, which is the conditional probability of an unfavorable deviation resulting from uncontrollable factors. Define the event (Υ) as the event in which an unfavorable loss deviation has already occurred. From the normal distribution, $N(\Omega v_1, \sigma^2)$, we know that $P(B) = 0.5$, since this is the total area under the normal curve where the actual loss deviation is greater than the expected loss deviation (mean) because otherwise the deviation is favorable. Therefore, the required conditional probability that the unfavorable loss deviation of Δ_1 or more results from uncontrollable factors can be computed as $P(X|\Upsilon) = \frac{\hat{p}}{0.5}$. When the un-scaled probability $\hat{p}$ is from 0 to 0.5, the computed conditional probability, which is scaled from 0 to 1, is the applicable probability and can be used with the separation curve in Fig. 3.

Once the combination of the conditional probability of an unfavorable deviation resulting from uncontrollable factors $P(X|\Upsilon)$ and the amount of the unfavorable deviation is available, we can see in which region of Fig. 3 the point with the combination (unfavorable deviation, probability) given by $(\Delta_1, P(X|\Upsilon))$ falls. If it is in the "Perform IT Security Audit" region, only then is it worth conducting the audit. Notice that both the unfavorable loss deviation as well as the probability are due to uncontrollable factors.

4. The impact of new information

Suppose more information is gained about the states from an external information source (an expert). The expert predicts that when the state is (θ_1:deviations resulted from controllable causes), there is the possibility of a favorable security environment (G) with a probability p_1 and an unfavorable security environment (B) with a probability $1 - p_1$. Similarly, for the state (θ_2:deviations resulting from uncontrollable causes), there is the possibility of a favorable security environment (G) with a probability p_2 and an unfavorable security environment (B) with a probability $1 - p_2$. The additional information, which may affect the decision whether or not to conduct a security audit, should be combined with the prior information about the states. This can be done using the Bayesian formula to obtain the posterior probabilities as given in Table 1.

In order to determine the critical region after incorporating the new information, one needs to determine the Bayesian strategies. The idea is to solve the decision problem twice, once for the favorable security environment condition (G) and then for the unfavorable security condition (B). We illustrate the Bayesian strategies and the derivation of the resulting critical probability p_c^G for the favorable security environment (G) below in Fig. 4.

As before with the no new information case, we can compute the expected cost of an investigation conditional on the security environment being favorable (G) using the posterior probabilities as

$$E[V(a_1)|G] = C. \tag{5}$$

The expected cost of not conducting an IT security audit conditional on the security environment being favorable (G) is

$$E[V(a_2)|G] = \frac{\varepsilon p_2(1-p)}{p_1 p + p_2(1-p)}. \tag{6}$$

If $C < \frac{\varepsilon p_2(1-p)}{p_1 p + p_2(1-p)}$, the firm should conduct the IT security audit, and if $C > \frac{\varepsilon p_2(1-p)}{p_1 p + p_2(1-p)}$, the firm should not conduct an IT security audit. By equating the expected cost of the two acts (i.e., $C = \frac{\varepsilon p_2(1-p)}{p_1 p + p_2(1-p)}$) and solving for the probability, one can find the critical probability p_c^G for the favorable security environment (G) as

$$p_c^G = \frac{p_2(\varepsilon - C)}{C(p_1 - p_2) + p_2\varepsilon}. \tag{7}$$

Similarly, we can find the critical probability p_c^B for the un-favorable security environment (B) as

$$p_c^B = \frac{(1-p_2)(\varepsilon - C)}{\varepsilon(1-p_2) + C(p_1 - p_2)}. \tag{8}$$

In Fig. 5, we show the plot of the security audit/no security audit region without (base case) and with additional information (favorable/unfavorable security environment assuming $p_1 = 0.8$ and $p_2 = 0.4$). As expected, additional information about the prior states has an influence on the security audit/no security audit region. If the security environment is favorable, then the "perform IT security audit" region is smaller. Alternatively, if the security environment is unfavorable, then the "No IT security audit" region reduces, which increases the "perform IT security audit" region.

Table 1
Posterior probabilities.

	G	B
θ_1	$\frac{p_2(1-p)}{p_1 p + p_2(1-p)}$	$\frac{(1-p)p_1}{(1-p_1)p + (1-p_2)(1-p)}$
θ_2	$\frac{p_1 p}{p_1 p + p_2(1-p)}$	$\frac{(1-p_2)(1-p)}{(1-p_1)p + (1-p_2)(1-p)}$

5. Incorporating incentive costs

Agency problems in a cyber-security context arise between principals (the owner or a Chief Executive Officer (CEO) who empowers cyber-security managers to make decisions) and agents (IT security managers who are in charge of the information security of firms) [20]. These agents operate as internal auditors who may have incentives and opportunity that influence their evaluations. Previous research shows that opportunities to receive incentive compensation result in less reliance by external auditors on internal auditors' work where tasks are subjective [15]. Their study finds that if the tasks are objective, such as a test of internal controls, incentive compensation is effective in mitigating excess consumption of leisure and perquisites.

In line with the agency theory literature, we assume that the principal (owner or CEO) is risk-neutral (seeks to maximize expected cash flows) and the agent (IT Manager) is risk averse (has a disutility for acts or effort). The agent's utility function for a net benefit (or cash flow) ω and effort a is given by $U(\omega,a) = F(\omega) - G(a)$. A reservation utility denoted by $\overline{U}$ is required to make the offer attractive to the agent. Both the agent and the principal assess identical state probabilities $\varphi(\theta)$. The total net benefit under the state $\theta \in \Theta$ and the act $a \in A$ is denoted by $x = f(\theta,a)$. The agent and the principal are assumed to jointly observe only the net benefit (or cash flow). The payment to the agent if $x = f(\theta,a)$ is observed is given by $\omega = \omega(x)$. Therefore, if a net benefit (or cash flow) x is observed, the agent receives $\omega(x)$ and the principal receives $x - \omega(x)$. The principal's problem is given by:

$$\max_{\substack{a\in A \\ \omega(x)\geq \overline{w}}} \sum_{\theta\in\Theta} [f(\theta,a) - \omega(f(\theta,a))]\phi(\theta) \tag{9}$$

$$\text{Subject to}: \quad \sum_{\theta\in\Theta} F(\omega(f(.)))\phi(\theta) - G(a) \geq \overline{U} \tag{10}$$

$$a \in \arg\max \sum_{\theta\in\Theta} F(\omega(f(.)))\varphi(\theta) - G(a) \tag{11}$$

where $\overline{\omega}$ is the minimum feasible payment. The above model ensures a self enforcing effort supply and a payment schedule that maximizes the principal's expected utility. We next develop the principal-agent model specific to the IT security audit setting.

In the model, β is defined as the benefit (or income) to the firm regardless of whether state θ_1 or θ_2 occurs. Notice that the uncertainty pertains to the unfavorable deviations (planned vs. actual losses from a security breach) resulting from controllable and uncontrollable causes and not from uncertainty that affects the benefit (or income) β.[2] Suppose the agent's effort levels pertaining to the two acts a_1 and a_2 are respectively e_1 and e_2. The outcomes (net benefit or cash flow) conditional on the act and the state $x = f(\theta,a)$ and the effort levels are given in Fig. 6.

Suppose we define the following decision variables: let ω_1 be the agent's payment if outcome $\beta - C$ is observed; let ω_2 be the agent's payment if outcome $\beta - \varepsilon$ is observed; and let ω_3 be the agent's payment if outcome β is observed. To keep the model simple, we assume a square root utility function for the agent. Therefore, the agent's utility for the net benefit (or cash flow) ω and effort a is $U(\omega - e) = F(\omega) - G(e) = \sqrt{\omega} - e^2$. Since both parties only observe the outcome, if effort $a_1 = e_1$ is supplied, we have the following model:

$$\max_{\omega_1,\omega_2,\omega_3\geq 0} \{(1-p)[(\beta - C) - \omega_1] + p[(\beta - C) - \omega_1]\} \tag{12}$$

$$\text{Subject to}: \quad (1-p)\sqrt{\omega_1} + p\sqrt{\omega_1} - e_1^2 \geq \overline{U} \tag{13}$$

[2] The uncertainty pertaining to β (for example, uncertainty due to product demand — increased θ^u and decreased θ^d) can be incorporated. In this case, the state's space will consist of all the possible combinations of uncertain states due to both the demand and deviations (i.e., there will be four states $\theta^u\theta_1$, $\theta^d\theta_1$, $\theta^u\theta_2$ and $\theta^d\theta_2$).

Acts

States	a_1 : Do an IT security audit	a_2 : Do nothing	Probability
θ_1 : Unfavorable deviations resulting from controllable causes.	C	ε	$\frac{p_2(1-p)}{p_1 p + p_2(1-p)}$
θ_2 : Unfavorable deviations resulting from uncontrollable causes.	C		$\frac{p_1 p}{p_1 p + p_2(1-p)}$

Fig. 4. State-Act-Conditional cost for security environment condition (G).

$$(1-p)\sqrt{\omega_1}+p\sqrt{\omega_1}-e_1^2 \geq (1-p)\sqrt{\omega_2}+p\sqrt{\omega_3}-e_2^2. \quad (14)$$

If effort level $a_2 = e_2$ is supplied, then we solve the following model:

$$\max_{\omega_1,\omega_2,\omega_3 \geq 0} \{(1-p)[(\beta - C)-\omega_2]+p(\beta-\omega_3)\} \quad (15)$$

$$\text{Subject to}: \quad (1-p)\sqrt{\omega_2}+p\sqrt{\omega_3}-e_2^2 \geq \overline{U} \quad (16)$$

$$(1-p)\sqrt{\omega_2}+p\sqrt{\omega_3}-e_2^2 \geq (1-p)\sqrt{\omega_1}+p\sqrt{\omega_1}-e_1^2. \quad (17)$$

In the above two models, the first constraint is the individual rationality constraint, which ensures that the incentive arrangement is attractive to the agent. The second constraint is the incentive compatibility constraint, which ensures the self-enforcing property. In a situation where there is new information about the uncertain states, then the above agency models can be directly applied if the combination of (Δ_1, P($X|\Upsilon$)) falls in the shifted "Perform IT security audit" region as a result of the resolution of uncertainty. If an audit is required, then the incentive payment which ensures that the agent will perform the audit can be determined using the agency model.

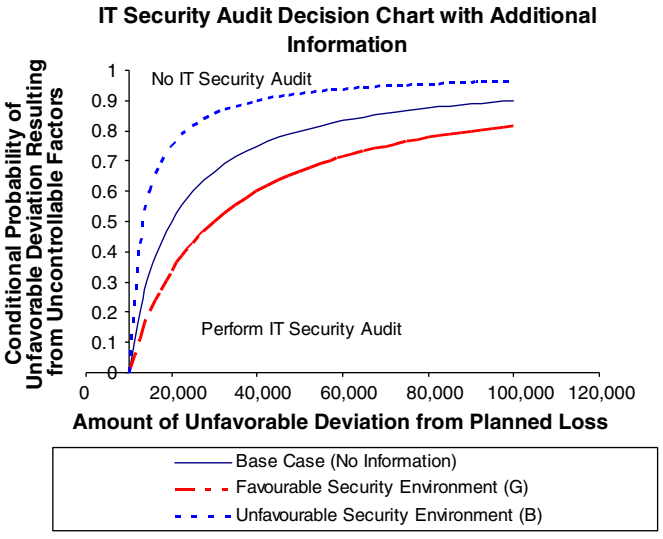

Fig. 5. Plot of critical probabilities and unfavorable deviations with additional information.

5.1. Numerical example

In order to illustrate the model, we use the following example. Suppose the form estimates the expected loss without any investment to be $\Omega = \$75{,}000$, base level investment $I_0 = \$10{,}000$, period 1 investment $I_1 = \$25{,}000$, an adjustment parameter $\alpha = 0.925$, and the cost to conduct a IT security audit is \$10,000. The probability of a breach, and hence the expected loss, can be computed as $v_1 = e^{-\alpha s_1} = e^{-0.925(2.5)} = 0.10$ and $L_1^P = v_1\Omega = \$7,500$. Suppose the managers' subjectively assessed standard deviation is $\sigma = \$200{,}000$; then loss distribution due to uncontrollable factors is given by N(7500,200000^2). If the actual loss at the beginning of period 2 is found to be $L_1^A = \$72,500$, then the unfavorable loss deviation is $\varepsilon = \Delta = \$65{,}000$. The probability of an unfavorable loss deviation of \$65,000 or more is calculated as $\frac{65{,}000}{200{,}000} = 0.325$ standard deviations from the mean. From the normal probability tables, the probability of 0.325 standard deviations or more is found to be 0.375. Thus, the required conditional probability is P($X|\Upsilon$) = 0.75. In the baseline model without any agency issues, the point (Δ_1,P($X|\Upsilon$)) falls in the "Perform IT Security Audit" region as $p_c(0.85) > p(0.75)$.

Suppose that the jointly observed benefit (or cash flow) to the firm is $\beta = \$80{,}000$, and the agent's reservation utility is $\overline{U} = 100$. The agent has two options: either conduct an IT security audit (act a_1 at cost of productive effort $e_1 = 5$) or do nothing (act a_2 at cost of productive effort $e_2 = 0$). Without the ability to observe the agent's choice of ($a \in A$) and without a completely trustworthy agent, the principal must offer an acceptable contract that ensures the agent will supply the desired effort (i.e., a_1).

Next we define the following: let ω_1 be the agent's payment if outcome $\beta - C = \$70{,}000$ is observed; let ω_2 be the agent's payment if outcome $\beta - \varepsilon = \$\,15{,}000$ is observed; and let ω_3 be the agent's payment if outcome $\beta = \$80{,}000$ is observed. We use the Microsoft Excel solver tool to solve the agency models. If we consider the scheme to supply effort $e_1 = 5$, the optimal solution is found as $\omega_1 = \$15,625$, $\omega_2 = 0$, and $\omega_3 = 0$, and the principal's expected benefit (or cash flow) is \$54,375. Similarly, for the scheme to supply effort $e_2 = 0$, the optimal solution is found as $\omega_1 = 0$, $\omega_2 = \$10{,}000$, and $\omega_3 = \$10{,}000$, and the principal's expected benefit (or cash flow) is \$53,750. The agent's expected utility in both situations is $E(U) = 100$. In the above example, it turns out that the agent is indifferent regarding supplying either effort e_1 or e_2. When faced with a multiple optima, we assume that the agent will settle for the act most desirable to the principal. That is, act a_1 at cost of productive effort $e_1 = 5$ since the expected value to the principal is \$54,375 > \$53,750. The agent would receive \$15,625 to conduct an IT security audit if the net benefit (or cash flow) is \$70,000. Through conducting the IT security audit at an incentive cost of \$15,625, the firm avoids an opportunity cost of \$65,000 that pertains to the second period investment and configuration cost.

	Acts		
	a_1 : Do an IT security audit Effort $=e_1$	a_2 : Do nothing Effort $=e_2$	Probability
θ_1 : Unfavorable deviations resulting from controllable causes.	$\beta - C$	$\beta - \varepsilon$	$1 - p$
θ_2 : Unfavorable deviations resulting from uncontrollable causes.	$\beta - C$	β	p

Fig. 6. Net benefits (or cash flow) and effort levels.

5.2. Efficiency loss of the moral hazard

In this subsection, we further compare the baseline case with no moral hazard with that of the agency model. Interestingly, in the above example, both the baseline model and the incentive contract which maximized the principal's payoff resulted in a recommendation that an IT security audit be conducted (act a_1). In order to investigate whether the baseline case and the incentive model solution result in different outcomes, we performed sensitivity analyses of the effort level and the reservation utility. The efficiency loss of the moral hazard when the effort level is varied and the reservation utility is varied (with effort level held constant $e_1 = 5$) is shown below in Figs. (7) and (8) respectively. In Fig. 7, when the effort level is increased above 5 units, the optimal act under the incentive contract is act a_2, "do not perform IT security audit." Similarly, in Fig. 8, for a constant effort level $e_1 = 5$ when the reservation utility is above 110, the optimal act under the incentive contract is act a_2, "do not perform IT security audit," contrary to what the baseline model suggests. This example provides an interesting case of hysteresis in the agency model as applied to an IT security audit situation.

Although the agency model provides a useful framework for mitigating motivational problems pertaining to cyber-security, the above example highlights its limitations. The principal agency model's emphasis is on internal consistency and optimality. As such, it takes a restricted view of the environment in which an organization operates [3]. In practice, however, knowing these limitations is important since contrary to the no audit optimal decision, conducting an IT security audit may have benefits that are not considered in the model setup. For example, conducting an IT security audit has the potential to reduce cyber insurance premiums [35], demonstrate due care and due diligence for the organization, and minimize the likelihood of litigation, as well as highlight any IT control weaknesses, thereby enhancing IT governance.

6. Conclusion, limitations, and future research avenues

Although the current regulatory environment tries to advocate a controlled environment, it is not imperative for all businesses. Given the budgetary constraints organizations face, non-mandatory security initiatives such as security audits are often overlooked. Motivated by the above, in this paper we develop a performance evaluation decision model that allows firms to decide whether it is worthwhile conducting an IT security audit.

The model developed in this paper makes contributions both to theory and practice. We draw upon the literature in investments in security technologies and cost variance investigation, as well as agency theory. Our model extends Bierman et al.'s [5] cost variance analysis by incorporating a two period IT security investment setting. The model is applicable in a wide range of situations but is especially useful for small firms where SOX requirements do not apply since firms can compare the amount of the unfavorable loss deviation and the probability that the unfavorable loss deviation resulted from uncontrollable factors as a basis for conducting the audit. If the deviations are small and the probability that they are from uncontrollable factors is large, then it is not worth conducting the IT security audit to assess the performance of the IT security manager. We also discuss a case in which an expert opinion is sought regarding the need for more information about the uncertain states. Thus, our model also incorporates the impact of having additional information. More specifically, using Bayesian decision theory, the model allows us to investigate the impact of new information on the IT audit decision. We show that the security audit/no security audit region area shifts depending on the addition of new information.

Regarding agency issues, the model also permits the determination of incentive payments for managers that can motivate them to carry out an audit. Our approach is general and is applicable in a wide range of settings including cyber security auditing and IT manager performance evaluation. The agency model pertaining to the audit decision model allows the determination of the optimal incentive costs that guarantee goal congruence. We also discuss the efficiency loss of the moral hazard, where the optimal decision of the agency model results in a different outcome from what the baseline model suggests. These

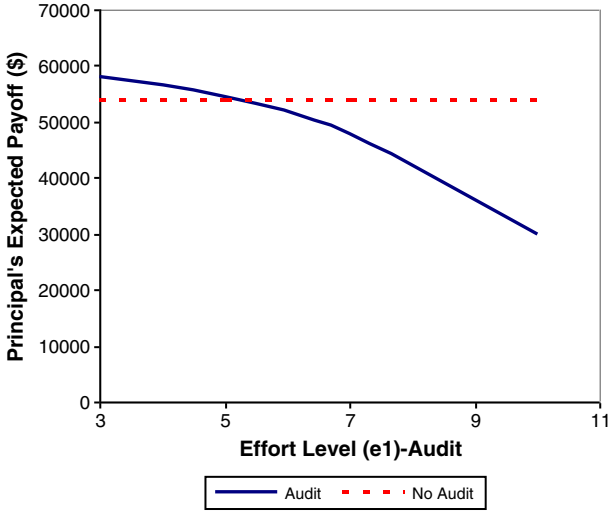

Fig. 7. Efficiency loss of moral hazard as a function of effort.

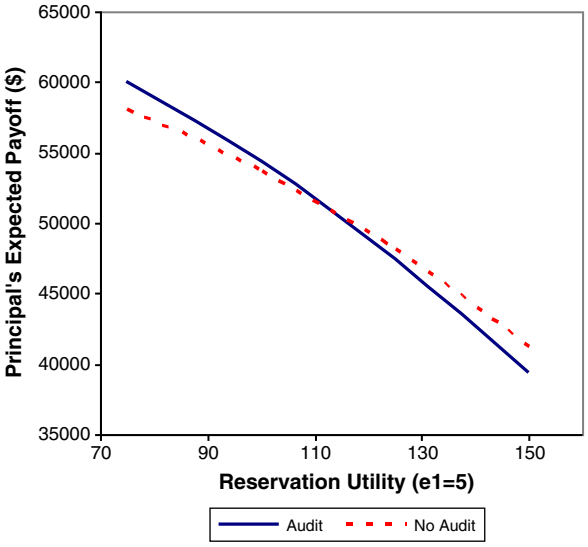

Fig. 8. Efficiency loss of moral hazard as a function of reservation utility.

findings provide useful information for designing managerial incentives in an IT security context.

There are several limitations of the model which provide avenues for further research. First, the loss deviations or the unfavorable variance that is investigated in this paper pertains to a single observation. If the losses occur in several sub-periods and a sequence of observations is available, then a multi-period approach may be more appropriate, which may be determined through future research. The second limitation pertains to the estimation of the parameters of the model, which includes the state probabilities, the opportunity costs associated with future savings, and the cost of manager effort pertaining to conducting an IT security audit. Although these limitations are common in many analytical models, the advantage of the IT security audit model with the agency extension is that it provides a clear criterion based on two parameters, the magnitude of the loss deviation and the probability of losses due to random factors. The model addresses an important management control issue in IT security.

The model considers agency issues commonly observed in in-house audit situations. However, the outsourcing of IT security audits is a common practice today [34], which may result in other issues. While outsourcing an internal audit can provide many advantages such as greater cost savings and improved quality, it can also result in disadvantages such as the lack of loyalty and business knowledge and the loss of a "valuable training ground" [4,6]. Firms offering outsourced audit services benefit from economies of scale, while audits done internally can provide benefits due to familiarity with the firm's operations and procedures [8]. In settings where the activities to be controlled are technically specific and complex [1] or in industries that face substantial regulatory scrutiny [9], the employment of in-house internal auditors with industry knowledge may be more cost-efficient. An interesting set of questions for future research includes what factors—for example, the size of the company, the industry in which it operates, and the regulatory effect—would impact the decision of whether to perform in-house or outsourced IT audits? Given the known risks in IT outsourcing [6], which control strategies would be most suited if IT audits are outsourced [32]? What would be an optimal contractual mechanism if the IT audits are outsourced? Finally, what would be the impact on the evaluation of IT security risks if the security audits are outsourced versus performed in-house?

IT security audit setting in this article pertains to classic IT infrastructures. Security becomes challenging in the new cloud computing environments due to factors such as the various models of cloud computing, shared resources, scalability, and third-party hosting [16,21,28]. In this regard, new questions arise as to how the audit decision model would change in cloud environments, what additional factors have to be considered, and could cyber-insurance be an alternative to IT security auditing? These questions create a fertile platform for future research in IT security auditing.

Acknowledgements

The authors would like to thank two anonymous referees for their valuable suggestions. The authors acknowledge the research funding support from IIIA (Grant 336-332-033). Dr. Hemantha Herath acknowledges research funding from the Social Sciences and Humanities Research Council (SSHRC) of Canada (Grant no: 410-2009-1398) and Dr. Teju Herath acknowledges research funding from the Social Sciences and Humanities Research Council (SSHRC) of Canada (Grant no: 410-2010-1848). The authors thank the participants at the AAA-MAS Annual Conference 2011 and WISP 2010 for their valuable input on an earlier version of this article. The usual disclaimers apply.

References

[1] M.B. Adams, Agency theory and the internal audit, Managerial Accounting Journal 9 (8) (1994) 8–12.
[2] U.L. Anderson, M.H. Christ, K.M. Johnstone, L.E. Rittenberg, A post-SOX examination of factors associated with the size of internal audit functions, Accounting Horizons 26 (2) (2012) 167–191.
[3] S. Baiman, Agency research in managerial accounting: a second look, Accounting, Organizations and Society 15 (4) (1990) 341–371.
[4] R.H. Barr Jr., S.Y. Chang, Outsourcing internal audits: a boon or bane? Managerial Auditing Journal 8 (1) (1993) 14–17.
[5] H. Bierman Jr., L.E. Fouraker, R.K. Jaedicke, The use of probability and statistics in performance evaluation, The Accounting Review 36 (3) (1961) 409–417.
[6] J. Blaskovich, N. Mintchik, Information technology outsourcing: a taxonomy of prior studies and directions for future research, Journal of Information Systems 25 (1) (2011) 1–36.
[7] D.C. Brewer, Security Controls for Sarbanes–Oxley Section 404 IT Compliance: Authorization, Authentication, and Access, Wiley Publishing, Inc., Indianapolis, USA, 2006.
[8] D.H. Caplan, M. Kirschenheiter, Outsourcing and audit risk for internal audit services, Contemporary Accounting Research 17 (3) (2000) 387–427.
[9] J.V. Carcello, D.R. Hermanson, K. Raghunandan, Factors associated with U.S. public companies' investment in internal auditing, Accounting Horizons 19 (2) (2005) 69–84.
[10] H. Cavusoglu, B. Mishra, S. Raghunathan, The value of intrusion detection systems in information technology security architecture, Information Systems Research 16 (1) (2005) 28–46.
[11] H. Cavusoglu, S. Raghunathan, Configuration of detection software: a comparison of decision and game theory approaches, Decision Analysis 1 (3) (2004) 131–148.
[12] M.B. Curtis, J.G. Jenkins, J.C. Bedard, D.R. Deis, Auditors' training and proficiency in information systems: a research synthesis, Journal of Information Systems 23 (1) (2009) 79–96.
[13] M. Damianides, Sarbanes–Oxley and IT governance: new guidance on IT control and compliance, Information Systems Management 22 (1) (2005) 77–85.
[14] J.S. Demski, An accounting system structured on a linear programming model, The Accounting Review 42 (4) (1967) 701–712.
[15] F.T. Dezoort, R.W. Houston, M.F. Peters, The impact of internal auditor compensation and role on external auditor's planning judgements and decisions, Contemporary Accounting Research 18 (2) (2001) 257–281.
[16] F. Doelitzscher, C. Reich, M. Knahl, N. Clarke, Understanding Cloud Audits, Privacy and Security for Cloud Computing, Springer, 2013. 125–163.
[17] L.A. Gordon, M.P. Loeb, The economics of information security investment, ACM Transactions on Information and System Security 5 (4) (2002) 438–457.
[18] L.A. Gordon, M.P. Loeb, W. Lucyshyn, T. Sohail, The impact of the Sarbanes–Oxley act on the corporate disclosures of information security activities, Journal of Accounting and Public Policy 25 (5) (2006) 503–530.
[19] L.A. Gordon, M.P. Loeb, W. Lucyshyn, Information security expenditures and real options: a wait and see approach, Computer Security Journal 19 (2) (2003) 1–7.
[20] L.A. Gordon, M.P. Loeb, T. Sohail, C.-Y. Tseng, L. Zhou, Cybersecurity, capital allocations and management control systems, The European Accounting Review 17 (2) (2008) 215–241.
[21] B. Grobauer, T. Walloschek, E. Stocker, Understanding cloud computing vulnerabilities, IEEE Security and Privacy 9 (2) (2011) 50–57.
[22] D.A. Haworth, L.R. Pietron, Sarbanes–Oxley: achieving compliance by starting with ISO 17799, Information Systems Management 23 (1) (2006) 73–78.
[23] H.S.B. Herath, T.C. Herath, Investments in information security: a real options perspective with Bayesian post-audit, Journal of Management Information Systems 25 (3) (2009) 337–375.
[24] K.J.S. Hoo, How Much is Enough? A Risk Management Approach to Computer Security, (Ph.D. Dissertation) Stanford University, 2000.
[25] S.M. Huang, W.H. Hung, D.C. Yen, I. Chang, D. Jiang, Building the evaluation model of the IT general control for CPAs under enterprise risk management, Decision Support Systems 50 (4) (2011) 692–701.
[26] IT Governance Institute, IT Control Objectives for Sarbanes–Oxley: the Importance of IT in the Design, Implementation and Sustainability of Internal Control Over Disclosure and Financial Reporting, IT Governance Institute, 2004.

[27] R. Kaplan, The significance and investigation of cost variances: survey and extensions, Journal of Accounting Research 13 (2) (1975) 311–337.
[28] J.M. Kizza, Cloud computing and related security issues, Guide to Computer Network Security, Springer, 2013, pp. 465–489.
[29] A. Lynch, M. Gomaa, Understanding the potential impact of information technology on the susceptibility of organizations to fraudulent employee behavior, International Journal of Accounting Information Systems 4 (4) (2003) 295–308.
[30] T. McCollum, Regulations' top IT audit concerns, Internal Auditor 68 (3) (2011) 14–15.
[31] W.F. Messier, A. Eilifsen, L.A. Austen, Auditor detected misstatements and the effect of information technology, International Journal of Auditing 8 (3) (2004) 223–235.
[32] P. Nagpal, K.J. Lyytinen, R.J. Boland, Which control strategies and configurations affect performance? Evidence from large scale outsourcing arrangements, AAA (2012) Management Accounting Section (MAS) Meeting Paper, 2011.
[33] M. Petterson, The keys to effective IT auditing, The Journal of Corporate Accounting & Finance (2005) 41–46.
[34] R. Richardson, CSI computer crime and security survey, Computer Security Institute 1 (2008) 1–30.
[35] S. Romanosky, Are Firms (and consumers) Investing Enough in IT Security?, Comments to the Department of Commerce on Incentives to Adopt Improved Cybersecurity Practices: Docket Number 130206115-3115-01, 2013.
[36] J.W. Ulvila, J.E. Gaffney, A decision analysis method for evaluating computer intrusion detection systems, Decision Analysis 1 (1) (2004) 35–50.
[37] W. van der Aalst, K. van Hee, J.M. van der Werf, A. Kumar, M. Verdonk, Conceptual model for online auditing, Decision Support Systems 50 (2011) 636–647.

Hemantha S. B. Herath is a professor of Managerial Accounting in the Goodman School of Business at Brock University. Previously, he was an assistant professor at University of Northern British Columbia and a consultant in the Oil and Gas Division of The World Bank, Washington D.C. His research interests include real option analysis, management accounting and economics of information security. He has published articles in a variety of journals including *Journal of Economics and Finance*, *Journal of Management Information Systems*, *Journal of Accounting and Public Policy*, *Advances in Management Accounting*, and *The Engineering Economist*. He was twice a recipient of the Eugene L. Grant Best Paper Award (2001, 2008) from the American Society of Engineering Education (ASEE). He currently serves as an area editor of The Engineering Economist. He is also a member of Sigma Xi-research honor society. His research has been funded by SSHRC Canada and other grants.

Tejaswini C. Herath is an assistant professor of Information Systems in the Goodman School of Business at Brock University, Canada. She received her Ph.D. in Management Science and Systems from the State University of New York at Buffalo. She holds an MMIS and MSCE from Auburn University, and a B.Eng. from Pune University, India. She also holds Advanced Certification in Information Assurance from the University at Buffalo (USA) and is a Certified General Accountant (CGA—Canada). Her work has been published in the *Journal of Management Information Systems*, *Decision Support Systems*, *European Journal of Information Systems*, *Information Systems Journal*, *Information Systems Management*, among others. Her research interests are in Information Assurance and include topics such as information security and privacy, diffusion of information assurance practices, economics of information security and risk management. Her research has been funded by SSHRC Canada and other grants.