CONF-IRM 2008 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2008

Information Security Policy Development for Caribbean Financial Institutions

Kevin H. Duncan
The University of the West Indies, kevin.duncan@uwimona.edu.jm

E. W. Duggan
The University of the West Indies, evan.duggan@uwimona.edu.jm

52F. Information Security Policy Development for Caribbean Financial Institutions

Kevin H. Duncan
The University of the West Indies
kevin.duncan@uwimona.edu.jm

E. W. Duggan
The University of the West Indies
evan.duggan@uwimona.edu.jm

Abstract

Governments of English-speaking Caribbean countries have begun to place greater emphasis on e-government to reduce bureaucratic inefficiencies and are encouraging, through legislation and other inducements, the expansion of e-commerce operations in order to enhance global competitiveness. This has expectedly led to a greater movement of data and with it information security risks. Information security managers continue to grapple with the difficulty of re-engineering policies and standards to meet this new reality. Hence many Caribbean organizations have become more vulnerable to security risks that are initiated internally. This is of grave concern to the Financial Institutions of the Caribbean as they prepare to offer extended services in order to exploit the opportunities expected from the introduction of the Caribbean Single Market and Economy. In addition, these institutions attempt to increase their share of both remittances from the Caribbean Diaspora and foreign direct investments which also serve to exacerbate these issues. These organizations are less capable of stemming the tide of fraud through identity theft and by other means, which are on the rise globally. In most cases these acts are facilitated (inadvertently or deliberately) by the actions of insiders. This paper proposes an approach to the development of context-based information security policies for Caribbean Financial Institutions aimed at mitigating insider risks.

Keywords

Information security, Agency Theory, Institutional Theory, Social Learning Theory, and Deterrence Theory.

1. Introduction

The internet has provided organizations with additional alternatives for structuring their business interests and operations. Businesses worldwide leverage this effective medium to distribute information related to products and services and to complete transactions in order to extend their global reach (Chang and Arnett, 2000). The financial sector in particular, has aggressively adopted the use of internet-based applications, primarily to provide Electronic Banking (e-banking) services to their customers on one hand, and to derive efficiency benefits for their internal processes on the other (Dewan, 2001; Liao, 2003).

E-Banking is an effective medium for funds transfer for many Caribbean Financial Institutions (CFIs) that are vying for an increasing share of the increasing movement of dollars between the Caribbean and other areas of the world, and within the region itself. The services sector in the

English-speaking Caribbean (ESC), as is the case in many other countries, continues to account for a progressively larger share of GDP - over 67 per cent in 2006 (CIA, n.d.). The economic pillars of ESC countries are tourism, foreign direct investments, and remittances from members of the Caribbean Diaspora. In addition, the Caribbean Single Market and Economy (CSME) is poised to become a reality and will also contribute to an increase in the funds transferred within the region. CSME is an integrated development strategy aimed at: (1) concretizing economic integration among CARICOM members (2) leveraging the economic resources of these nations, and (3) making the CARICOM region a viable trading block (CARICOM, n.d.).

Consequently, CFIs are engaging more in E-banking (Xu and Bowrin, 2005), which allows customers to conduct financial transactions electronically, (primarily) over the Internet, using personal or handheld computers or the telephone. CFIs seek the benefits of increased service accessibility and availability afforded by e-banking, which in turn force them to deploy these services as a competitive necessity.

The commitment of CFIs to E-banking and to other online transactions and the attendant proliferation of the traffic of digitized data (both within and across organizational boundaries) further heighten the need for guaranteeing the security of these transactions. However, for many ESC countries this is either new territory, new scale, or both (Xu and Bowrin, 2005); many of these organizations have struggled to protect purely internal transactions. The sensitivity and the myriad risks associated with data movement over the Internet have exacerbated what was already a growing concern, and have served to constrain the growth of e-commerce (Shelly et al., 2006). The slow pace of the development of Government legislation to protect Internet transactions, despite the commitment to the CSME, is yet another reason for CFIs to focus more keenly on security issues.

The foregoing provides the impetus for this conceptual paper, which examines the imminence of the explosion of e-banking services in the CARICOM region, for all the reasons indicated, against the less than robust information security policies and practices that now exist or are contemplated. In this analysis, we survey the literature to identify support for prescriptions for bolstering information security in this domain. Many researchers have long subscribed to the fact that effective information security policies ought to be cognizant of behavioural, deterrence, and security awareness educational concepts (Siponen, 2006; Straub, 1998). Additionally, because of the low perceived importance and the general lack of prescriptive approaches for the implementation of information security regimes within the region, we believe that Learning, Deterrence, Managerial Control, Agency and Institutional theories will provide the bases for a framework for understanding the issues and for generating a plausible baseline for remedying this situation for CFIs. We will use this framework ourselves and contribute it for use in future research.

In the remainder of this paper we undertake a literature review, discuss the theoretical pillars that support our proposed solution, and offer a conclusion.

2. Background Information

Scott (2001) defines an institution as a highly resilient social structure comprised of cultured-cognitive, normative and regulative elements that in conjunction with activities and resources provide stability and meaning to social life. This definition is reflected in the institutional carriers (symbolic systems, relational systems, routines and artifacts) that he identified. Björck (2004) posit that symbolic systems typically are rules, laws, values, expectations, categories, typifications and schema. Relational systems speak to governance systems, regimes, authority systems, structural isomorphism, and identities. Routines refer to protocols, standard operating procedures, jobs, roles, obedience to duty, and scripts, while artifacts are considered to be objects complying with mandated specifications, objects meeting conventions, standards, and objects which possess symbolic value.

Typically, open system organisations contend with both an external and an internal operating environment. The conditions of the external environment are dictated by the legal and regulatory framework - Symbolic Systems; the internal environment is driven largely by relational systems, routines and artifacts. The information security climate at the national level, to a large extent influences the information policies developed at the organizational level, for example the types of organizational information security policies developed post Sarbanes-Oxley implementation (Francoeur, 2004). Similarly, information security legislation within the ESC also influences the policies developed for local firms. As depicted in Figure 1, these distinct environments can impose their own influences on an organization's information security policy.

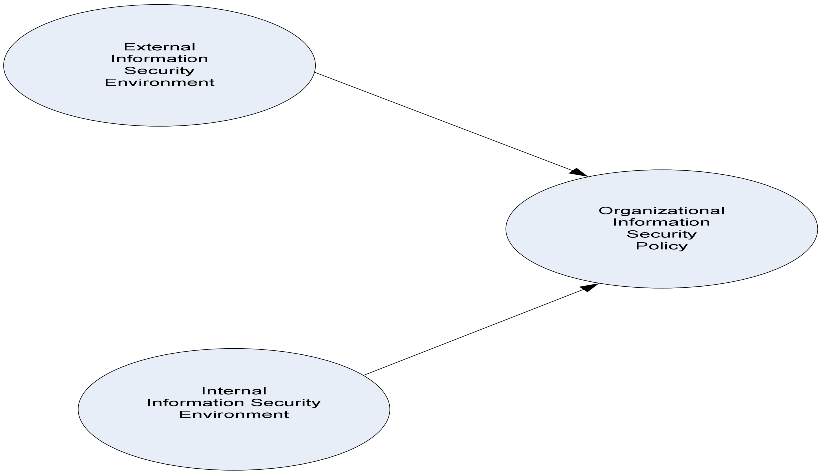

External Information Security Environment
Organizational Information Security Policy
Internal Information Security Environment

Figure 1: The existing Information Security Policy Development Process.

Smith and Jamieson (2006) posit that information security is the ability to ensure that the confidentiality, availability, and integrity of information are effectively maintained by way of policies and technological assets. For example, the adoption of e-commerce as a business channel by many modern firms has heightened information security concerns for both financial institutions, governments and other organizational units (Baskerville, 2002; Dewan, 2001). Cyber crime reports recently published by the FBI/CSI suggest that these fears are not unfounded. Recent statistics on identity theft estimated the losses due to information theft and acts of fraud at over JMD$1.2 billion (approximately USD$17.1Million) in Jamaica alone between 2000 to 2006 (Williams, 2006).

Stemming the upsurge of these incidents is very important for most countries but more so for the ESC, which is attempting to establish itself as regional trading block. Based on its location, it is expected to experience high traffic in financial transactions primarily from Trans-Atlantic trade, tourism and increased foreign direct investments within the region. Organizations in the developing world have largely bought into the need for effective IT governance (Weill and Woodham, 2004), which according to Sambamurthy and Zmud (1999) is the means of establishing decision rights and, ultimately, lines of accountability for and control of key IT decisions. However, in the Caribbean a new mindset is required to safeguard these transactions as most Caribbean firms rely almost entirely on their Information Systems departments to lead the effort in securing their information assets (Xu and Bowrin, 2005).

IT Governance structure provides an all-encompassing framework for enforcing compliance with information security controls; however, the controls are generally implemented using any one of the industry's widely accepted Information Security Management Standards (ISMS) such as, the control objectives for information and related technology (CobiT). This combination of governance and ISMS is required to create an environment which fosters confidentiality and security of the data for which the FIs have custodial rights (Francoeur, 2004; Xu, 2005).

However, while these ISMSs provide excellent guidelines for the creation of information security oriented processes, they offer very little implementation content and information related to achieving success from ISMSs. Current information security management standards offer very little prescriptions for ensuring congruence between objectives and outcomes (Siponen, 2006) or benchmarks for determining implementation success. According to (Eloff, 2003), security managers have to grapple with both social and technical issues in order to develop effective security solutions. Unfortunately, a holistic solution is not so easily defined. Security concerns related to technical issues can often be resolved by implementing technology-based solutions. In an organizational context there are myriad variables (including social behaviours) that are at play which, according to (Hilbert, 2003), are influenced by the macro culture and political climate in which the firm operates. However, finding a solution to incorporating these variables into an information security policy is not as simple.

In the ESC, the financial institutions continue to lead the charge towards incorporating ecommerce into business strategy (Xu, 2005). However, current security plans can be restrictive, expensive, time consuming, and, in some cases, cannot be implemented on the Internet (Hagyavati and Hicks, 2003). In addition, information security and business objectives are often conflicting, and in some cases mutually exclusive. For example, there is an increasing desire on the part of organizations to use the Internet as another channel for conducting business activities (Baskerville and Siponen, 2002). The pitfall is that the Internet is based on openness and flexibility and not necessarily for security. These conflicting ideals have often contributed to the difficulty in aligning business and information security objectives (Hamill et al, 2004).

Given this need for carefully crafted security policies with appropriate content which is cognizant of social context, we will appeal to Learning, Deterrence, Control, Agency and Institutional theories in order to explicate the complex relationships, provide a framework for understanding them and assisting with the generation of a plausible approach to developing a comprehensive policy with content relevant to both the technical and social contexts. The security policies so developed will be used to inform the ISMS implementation in ESC countries. These are discussed in the next section with a brief explanation of how each theory will be used and why. We envision information security management within a firm as the joint responsibility of the information security managers and the other internal stakeholders.

3. Theoretical Pillars

Siponen and Kukkonen (2007) identify four elements that an effective information security management strategy should encompass. These include: controlled access to information systems, secure communication, security management, and the development of secure information systems. Of these four objectives, controlled access to information and assurances for the security of data in storage and in motion relate directly to the security of electronic transactions. Many researchers contend that the human element is the most challenging variable to manage in the context of information security (Adams, 1999; Gonzales, 2002; Siponen, 2000). They further suggest that solutions to this problem lay in the realm of behavioural/motivational theories.

By Hewitt's (1986) definition, Financial Institutions that engage in e-banking are typical of open system organisations, which consist of both internal and external operating environments. The effectiveness of the external environment in the context of information security is determined by the macro information security policy (government legislation, industry standards and regulations). The effectiveness of the internal information security environment on the other hand is determined by how well the security regime is defined and articulated. Acharya (2001) defines security regime as the principles, norms and rules which regulate state behaviour. In the context of information security, a security regime encompasses the principles, norms and rules which regulate information security behaviours.

3.1 Agency Theory

Agency theory has been used to study contractual arrangements in a wide range of disciplines including accounting, sociology and organizational behaviour (Eisenhardt, 1989), primarily for describing the driving forces which determine the nature of the relationship between a principal and an agent, both in the case of a firm with external contractors and the firm, and the fiduciary arrangements between the management of the firm and its owners (Basu and Lederer, 2004). Eisenhardt (1989) suggested that the issues related to agency relationships stems from goal incongruence between principal and agent and also from the inability of the principal to determine if the agent has acted in the best interest of the principal.

Researchers have classified agents' behaviours into two types, adverse selection and moral hazard. According to Eisenhardt (1989) the former occurs when the agent misrepresents his abilities and operates in a manner which makes it difficult for the principal to falsify his/her claims. Moral hazard manifests in situations where the agent does not expend the agreed effort in completing the assigned task(s). This translates to six variables upon which agency type relationships are premised: shirking (agents not expending enough effort towards the goals of the principal); information asymmetry (agents withholding vital information from the principal); goal conflict, task programmability (the extent to which the appropriate behaviour of the agent can be predetermined); contract type (behaviour based and outcome based); and monitoring (Eisenhardt, 1989; Mahaney and Lederer 2003).

Walsh and Schnieder (2002) demonstrated that in contrast to the classical depiction of a single principal/agent relationship, Agency theory may well involve multiple relationships (e.g., in software development teams). Additionally, Adams (1994) believed that a firm can be viewed as an arrangement of contracts between resource owners (principals) and those dependent on the resource (agents) (Adams, 1994). The way in which these contracts are initiated and subsequently executed is determined by available information and the influence of incentives (Basu and Lederer, 2004). These conditions create an environment that facilitates the development of agency relationships.

We will use the Adams (1994) approach to explicate the nature of the controls that are needed to govern the principal-agent relationship which exists between the information security managers (principals) and other internal stakeholders (agents) with the context of information security function of a CFI.

3.2 Management Control Theory

Simons (1995) define management control systems as the formal information-based routines and procedures manager use to maintain or alter patterns in organizational activities. He identified four control systems as related to business strategy: belief systems (based on core values); boundary systems (to limit opportunistic behaviours); interactive control systems (to stimulate organisational learning); and diagnostic control systems (to measure output and performance). Duane and Finnegan (2000) extended this list of controls by including internal controls (procedural checks and balances to ensure data integrity). Das and Teng (2001) then identified three approaches to internal control within the context of a principal/agent relationship. These controls are behaviour-based, output-based and social controls. Behaviour-based controls measure behaviours to ensure compliance with the desired behaviour while Output-based controls measure outcomes to ensure that they are in accordance with desired outcomes. In both cases the metrics are formally declared and agreed upon by the principal and the agent. Social controls are far more informal and rely heavily on the organisation's culture and shared goals to bring about compliance with the desired behaviours or outcomes (Rasmusson, 1996).

In terms of information security, Baskerville (1988) advocated the existence of four categories of controls, namely deterrent controls (reflection of the strength/enforceability of the organisational information security policies), detective controls (threat identification), corrective controls (reactive threat mitigation), and preventative (proactive threat mitigation). We believe that the formulation of information security policies should span all four categories in order to be effective. We will use this expanded view of management control theory to elucidate the relationships between these types of controls and the internal information security environment and hence their role(s) in the formulation of effective organizational information security policy for CFIs.

3.3 Deterrence Theory

Deterrence theory emerged from military strategy utilized during the Cold War era, in which contending sides invoked strategies to convince the other that the success of an attack would pale in comparison to the consequences of retaliatory response. This disincentive includes deterrence by punishment or by denial. Deterrence by denial in the context of information security would be the implementation of security policies with explicitly stringent (and enforceable) punitive measures. Deterrence by punishment is the enforcement of these punitive measures once a breach has occurred and the guilty party is identified. In the Caribbean, information security is still given a relatively low priority. This is evident in the fact that only four of the twenty-six Caribbean countries have enacted electronic transaction legislation to promote accountability for information security breaches (Corbin, n.d.), and very few firms employ information security specialists.

3.4 Social Learning Theory

Perceptions about learning have undergone significant shifts in emphasis from mere focus on behaviour change to the modern view of learning as a process. This process view has facilitated the development of the Learning Theory (Smith, 1999). Merriam and Caffarella (1991) had posited three categories of learning: behavioural, cognitive, and humanistic-oriented learning. However, Smith (1999) added social- or situational-oriented learning. The behavioural view of learning is aimed at producing behavioural change in a desired direction; the cognitive view is aimed at developing capacity and skill to learn better; the humanistic view is aimed at attaining self actualization and autonomy; The social/situational view is where the acquisition of new knowledge causes the subject to interact with his/her environment.

In order to implement an effective information security regime in a CFI, information security content must contain a learning component. This component could then be the catalyst for effecting lasting change(s) in attitudes of the individuals within the organisation towards information security. The expected outcome of this change is the development of an information security aware workforce. This educational component would be based on learning theory aimed at engendering the desired behaviours and attitudes towards information security within the firm. The impact of this would be the development of a workforce which proactively manages the firm’s exposure to information security risks.

3.5 Institutional Theory

Björck (2004) describes Institutional Theory as a rich theoretic lens which allows us to explicate the factors affecting social behaviour within an organisation. Some of the underlying principles of institutional theory are isomorphism, structuration, cultural persistence and legitimacy. Organizations often go through many changes throughout their years of operation; these changes may be due to coercive forces (because of the need to comply with industry best practice, legislation, regulation and mandates), mimetic forces (due the need to reduce uncertainty) or normative forces (due to the need to conform to the organization’s view of normal practices). Within an industry, these forces often result in organizational homogeneity or isomorphism (DiMaggio and Powell, 1983). Giddens (1979) define the process of structuration as the relationship between the institutional properties of social systems and human action. Zucker (1987) describe cultural persistence as emerging from three processes: habitualization (patterned problem solving of new problems); objectification (a shared ontology of problems and their treatment) and sedimentation (the adoption of the shared ontology as the norm). Legitimacy refers to the process of weaving behaviours into the social fabric of the organization and in so doing legitimize their existence (DiMaggio and Powell, 1983).

The institutional view of a firm allows for a more holistic view of the factors influencing how the firm operates within its environment. Applying this theoretic lens to the firm helps to explain how the organization is influenced by internal and external factors (Zucker, 1987). For the purposes of this study institutional theory will be used to illustrate relevant internal and external environmental factors which warrant consideration when organizational information security policies are being developed.

4. Towards a Solution

The establishment of a viable information security regime is no longer considered to be predominantly technology-related and the purview of IS/IT departments (Dhillon, 2000). Deeper consideration is given to what strategies will be needed to allow for the indiscriminate acceptance of these technologies by end users (Arief, 2003; Aytes, 2004). According to Xu and Bowrin (2005), this phenomenon is gradually becoming the norm within the Caribbean.

This paper proffers a model (figure 2) which represents a synthesis of these theories in establishing a framework which information security practitioners can use in the development of information security policies specific to their organizations. We also will contribute the findings of this research to the research community as a means of providing extensions to the boundaries of the theories used. This model can be useful in providing prescriptions for the development of information security policies based on the internal and external information security environments within which the target firm operates. The external information security environment is driven by macro information security issues – government legislation, industry standards and regulations, while the internal information system security environment is largely influenced by the security regime implemented within the firm. Currently, researchers are of the view that the security regime will typically entail the combination of managerial, technological and physical controls. Here we propose that this view be extended to include a social learning component in order to effect the wholesale and sustained behavioural change towards information security with CFIs.

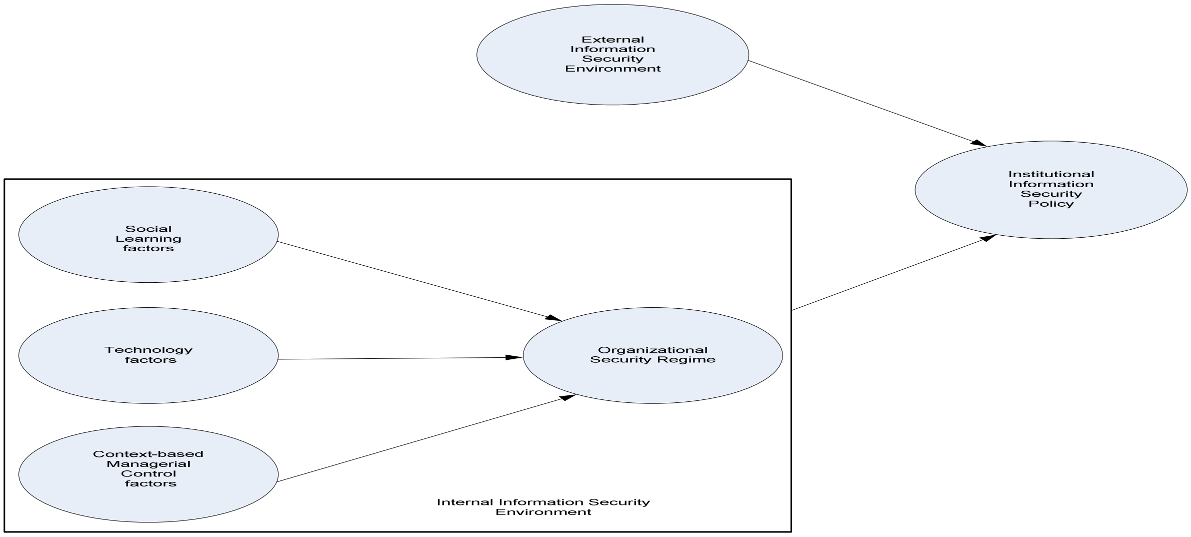

External Information Security Environment
Institutional Information Security Policy
Social Learning factors
Technology factors
Organizational Security Regime
Context-based Managerial Control factors
Internal Information Security Environment

Figure 2: The Contextual Information Security Policy Development (CIPD) Model

There exists a reflective relationship between context and behaviour (Scott, 2001). As a result, the process of developing information security policies using this model begins with an assessment of the situational factors relevant to the organization. These situational factors stem from social learning and managerial control factors.

Initially, we will engage in a process of seeking to identify the factors which facilitate learning in the organizational context for firms in ESC countries. Similarly, we will then validate what are the factors that positively affect the other situational factors (technology, managerial controls) within the targeted firm. In so doing we will derive the organizational security regime variables relevant to that firm. At the secondary level, we will then seek to elucidate what are the internal and external information security factors which influence the institutionalization of information security policies.

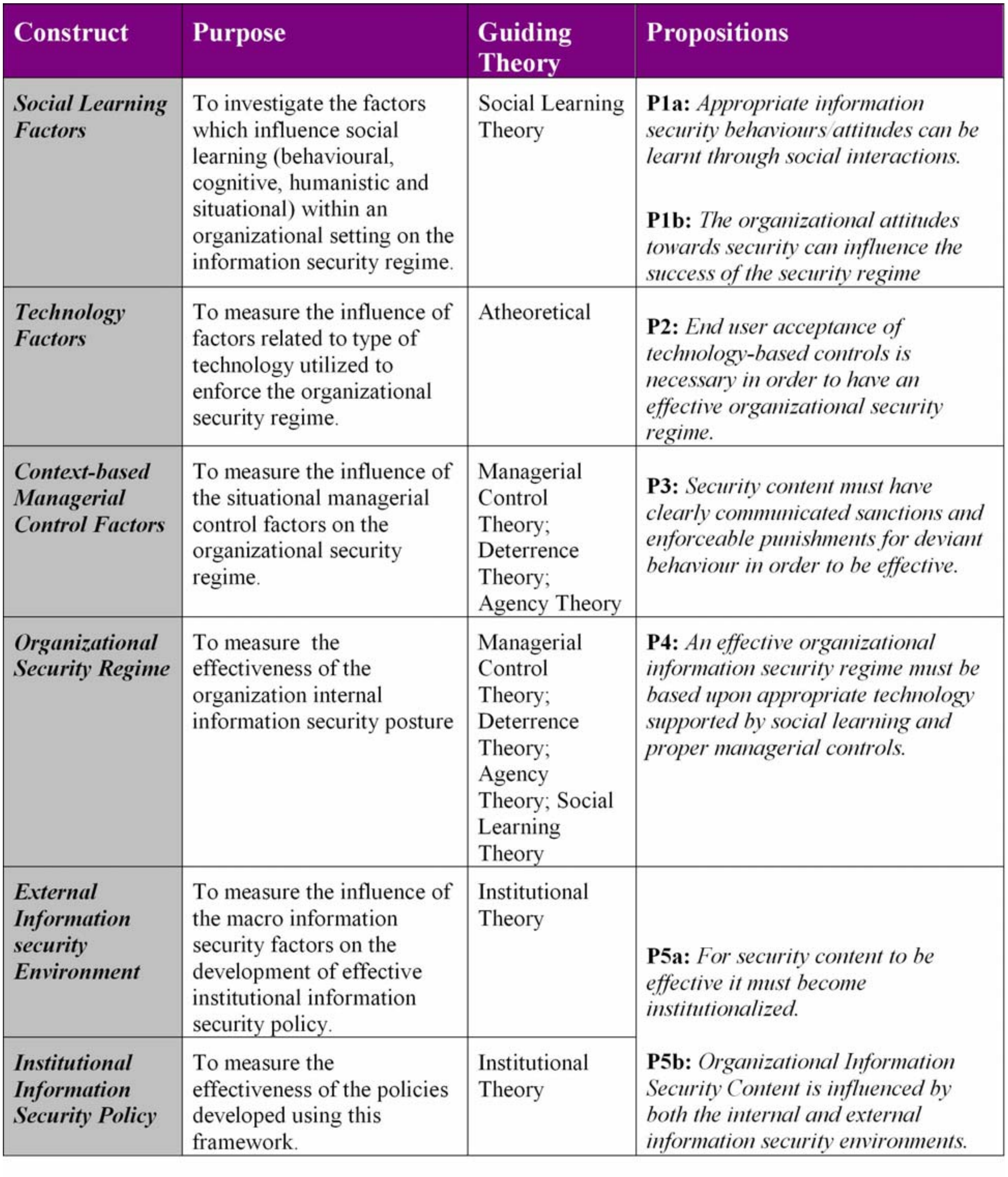
Though the CISPD model provides a comprehensive framework for the development of a contextually aware information security policy, we recognize that is need for further refinement of the theoretic base of the model in order to reduce the number of variables by identifying a set of critical factors. Kim and Mueller (1978a) recommended the use of exploratory factor analysis (EFA) only in cases where there exists a minimum of three (3) input variables. Also, EFA would provide a means for us to gain a better understanding of the underlying structure of the relationship between the variables implied by each theory used.

Our proposed model suggests the existence of a number of causal relationships. The next stage of this research will be to test the validity of the model by first examining the set of propositions presented in table 1.

5. Conclusion

The current approaches to information security within firms in ESC countries are not as mature as those in developed countries (Xu and Bowrin, 2005). However, the pressures of globalization on the competitiveness of regional firms will serve as a catalyst for motivating an awakening to the importance of information security and its role in achieving competitive advantage. Information security policies are typically designed to secure information systems and their outputs. However, these systems or outputs are ultimately used by people (Aytes, 2004). Acceptance of this fact implies the need for social and psychological controls to be central to the development of information security policy. Due to the issues influenced by culture and know-how as well as the trust and risk climates that exist in the application domain, these controls need to be very specific.

We have therefore contributed the proposed model, which synthesizes several relevant theories in an attempt to explicate relevant socio-technical relationships that bear on an effective information security regime for the ESC. Eventually we hope to test the validity of the model and to use it ourselves, and to offer it to the research community for refinement, to advance research in this area in order to provide information security practitioners within CFIs with rich insights that are tailored to the idiosyncrasies of their internal and external operating environments, which in turn will help them to create contextually conscious information security policies.



Construct	Purpose	Guiding Theory	Propositions
Social Learning Factors	To investigate the factors which influence social learning (behavioural, cognitive, humanistic and situational) within an organizational setting on the information security regime.	Social Learning Theory	**P1a:** *Appropriate information security behaviours/attitudes can be learnt through social interactions.* **P1b:** *The organizational attitudes towards security can influence the success of the security regime*
Technology Factors	To measure the influence of factors related to type of technology utilized to enforce the organizational security regime.	Atheoretical	**P2:** *End user acceptance of technology-based controls is necessary in order to have an effective organizational security regime.*
Context-based Managerial Control Factors	To measure the influence of the situational managerial control factors on the organizational security regime.	Managerial Control Theory; Deterrence Theory; Agency Theory	**P3:** *Security content must have clearly communicated sanctions and enforceable punishments for deviant behaviour in order to be effective.*
Organizational Security Regime	To measure the effectiveness of the organization internal information security posture	Managerial Control Theory; Deterrence Theory; Agency Theory; Social Learning Theory	**P4:** *An effective organizational information security regime must be based upon appropriate technology supported by social learning and proper managerial controls.*
External Information security Environment	To measure the influence of the macro information security factors on the development of effective institutional information security policy.	Institutional Theory	**P5a:** *For security content to be effective it must become institutionalized.* **P5b:** *Organizational Information Security Content is influenced by both the internal and external information security environments.*
Institutional Information Security Policy	To measure the effectiveness of the policies developed using this framework.	Institutional Theory	

Table 1: The Contextual Information Security Policy Development (CISPD) Model propositions

References

Acharya, A. (2001). *Constructing a Security Community in Southeast Asia*. New York: Routledge.

Adams, A., and Sasse, M. A. (1999). Users are not the Enemy. *Communications of the ACM, vol. 42*(No 12), 41- 46.

Adams, M. B. (1994). Agency Theory And Managerial Audit. *Managerial Audit Journal*, *9*(8), 8 -12

Arief, B. andBesnard, D. (2003). Technical and human issues in computer – based systems security. . *CS-TR-790*.

Aytes, K., and Connolly, T. (2004). Computer Security and Risky Computing Practices:A Rational Choice Perspective. *Journal of Organizational and End User Computing, 16*(3), 22-40.

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179-211.

Baskerville, R. (1988), Designing Information Systems Security, John Wiley Information Systems, John Wiley & Sons, NJ.

Baskerville, R., and Siponen, M. . (2002). An Information security meta – policy for Emergent organizations. . *Logistics Information Management, 15*(5/6), 337-346.

Basu, V.,and Lederer, A.L. (2004). An Agency Theory Model of ERP Implementation. *SIGMIS-ACM*, 8-13

Björck, F. (2004). Institutional theory: A new perspective for research into IS/IT security in organisations. *Proceedings of the 37th Hawaii International Conference on System Sciences - 2004*.

Chang, L., and Arnett, K. P. (2000). Exploring the factors associated with Web site success in the context of electronic commerce. *Information & Management, 38,* 23-33.

CARICOM (n.d.). The CARICOM Secretariat. Retrieved July 31, 2007

http://www.caricom.org/jsp/single_market/single_market_index.jsp?menu=csme

CIA (n.d.). The World Fact Book . Retrieved July 31, 2007 from https://www.cia.gov/library/publications/the-world-factbook/geos/jm.html#Econ

Corbin, J. (n.d.). E-Commerce: Issues and Challenges. Retrieved March 13, 2007 from

http://unpan1.un.org/intradoc/groups/public/documents/CARICAD/UNPAN006943.pdf

Das, T. K., and Teng, B. (2001). Trust, Control, and Risk in Strategic Alliances: An Integrative Framwork. *Organizational Studies, 22*(2), 251-283.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-339.

De-Silva, M. S. P., D.J.; Sandford, P.; Sandford, J.M. (2007). Automated Detection of Emerging Network Security Threats. *Sixth International Conference on Networking, 2007. ICN '07.*, 98-98.

Dewan, R., and Seidmann, A. (2001). Current Issues in E-Banking. *Communications of the ACM, 44*(6), 31-32.

Dhillon, G. andBackhouse, J. (2000). Information System Security Management in the New Millennium. *Communications of the ACM*, *43*(7), 125-128

DiMaggio, P. J., and Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review 48: 147-160.

Duane, A. and Finnegan, P. (2000). *Managing Intranet technology in an organizational context:toward a "stages of growth" model for balancing empowerment and control* Paper presented at the International Conference on Information Systems, Brisbane,Queensland, Australia.

Eisenhardt, K. (1989). Agency Theory: An Assessment and Review. *Academy of Management Review, 14*(1), 57-74.

Eloff, J. (2003). Information security management – a new paradigm. *Proceedings of SAIGSIT* 130 - 136.

Fusilier, M. and Durlabhji, S. (2005). An exploration of student internet use in India the technology acceptance model and the theory of planned behaviour. *Campus-Wide Information Systems, 22*(4), 233-246.

Francoeur, J., and Rothke, B. . (2004). It's time for e-goverance. *EWeek*, 43.

Giddens, A. (1979). Central Problems in Social Theory: Action, Structure and Contradiction in Social Analysis, University of California Press, Berkeley, CA.

Gonzales, J. J., and Sawicka, A. (2002). A Framework for Human Factors in Information Security. *Proceedings of the WSEAS International Conference on Information Security*.

Hagyavati, B., and Hicks, G. . (2003). A Basic security plan for a generic organization. *The Consortium for Computing Sciences in Colleges*, 248-256.

Hamil, J., Todd, D., Richard, F., and Kloeber, J. M. .(2004). Evaluating information assurance strategies, Decision Support Systems, Vol 39, pp. 463 – 484.

Hewitt, C. (1986). Offices are open Systems. *ACM Transactions on Information Systems, 4*(3), 271-287.

Hilbert, M., and Katz, J. (2003). *Building an Information Society: a Latin American and Caribbean Perspective*: United Nations.

Kim, J., and Mueller, C. W. (1978a). Introduction to factor analysis: What it is and how to do it. Thousand Oaks, CA: Sage Publications, Quantitative Applications in the Social Sciences Series, No. 13.

Liao, Z., and Cheung, M. T. (2003). Challenges to Internet E-Banking. *Communications of the ACM, 46*(12), 248-250.

Mahaney, R. C., and Lederer, A. L. (2003). *AN AGENCY THEORY ANALYSIS OF INFORMATION TECHNOLOGY PROJECT SUCCESS.* Paper presented at the Ninth Americas Confrenece on Information Systems, Tampa, Florida.

Merriam, S. and Caffarella (1991, 1998) *Learning in Adulthood. A comprehensive guide*, San Francisco: Jossey-Bass. 528 pages.

Rasmusson, L. andJansson, S. (1996). Simulated Social Control for Secure Internet Commerce. *Proceedings of the 1996 workshop on New security paradigms NSPW '96*.

Sambamurthy, V., Zmud, Robert (1999). Arrangements for information technology governance: a theory of multiple contingencies. MIS Quarterly, 23 (2), 261 – 290

Scott, W. R. (2001). *Institutions and Organisations* (second ed.). Thousand Oaks, California: Sage Publications.

Simons, R. (1995). *Levers of Control*. Boston: Harvard Business School Press.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Siponen, M. T. (2006). Information Security Standards focus on the Existence of Process, Not its Content. *Communications of the ACM, 49*(8), 97-100.

Siponen, M. T., and Oinas-Kukkonen, H. (2007). A Review of Information Security Issues and Respective Research Contributions. *ACM SIGMIS Database, 38*(1), 60-80.

Smith, M. K. (1999). Learning Theory. *The Encyclopedia of Informal Education*, www.infed.org/biblio/b-learn.htm.

Smith, S., and Jamieson, R. (2006). Determining the key factors in E-Government Information System Security. *Information Systems Management, 23*(2), 10.

Straub, D. W., and Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, 29.

Venkatesh, V. andDavis, F. D. (2000). A Theoretical Extension of the Technology AcceptanceModel: Four Longitudinal Field Studies. *Management Science, 46*(2), 186-204.

Walsh, K. R., and Schnieder, H. (2002). The role of motivation and risk behaviour in software development success. *Information Research, 7*(3).

Wand, Y., and Woo. C. C. (1991). An Approach to Formalizing Organizational Open System Concept. *ACM*, 141-146.

Weill, P., and Ross, J.W. (2004). *How Top Performers Manage IT Decision Rights for Superior Results*. Boston: Harvard Business School Publishing Corporation.

Weill, P., and Woodham, R. (2004). Don't Just Lead, Govern: Implementing Effective IT Governance. *MIS Quarterly Executive, 8*(1)

Williams, L. (2006, Sunday May 21). White-collar criminals, networks rake in millions annually from sophisticated scams. *The Jamaica Observer*.

Xu, H., and Bowrin, P. (2005). Information Security in the Caribbean Banks. *Issues in Information Systems, VI*(2), 210-216.

Zucker, L. G. (1987). INSTITUTIONAL THEORIES OF ORGANIZATION. *Annual Review of Sociology, Vol. 13.*, pp. 443-464.