Received 15 June 2015
Revised 12 November 2015
13 January 2016
Accepted 13 January 2016

Developing a theory-based information security management framework for human service organizations

Sameera Mubarak
School of Information Technology and Mathematical Sciences, University of South Australia, Adelaide, Australia

Abstract

Purpose – This paper aims to identify organizations' information security issues and to explore dynamic, organizational culture and contingency theories to develop an implementable framework for information security systems in human service organizations (HSOs) based soundly in theory and practice.

Design/methodology/approach – The paper includes a critical review of global information security management issues for HSOs and relevant multi-disciplinary organizational theories to address them.

Findings – Effective information security management can be particularly challenging to HSO because of their use of volunteer staff in a borderless electronic environment. Organizations' lack of recognition of the need for staff awareness of information security threats and for training in secure work practices, particularly in terms of maintaining clients' privacy and confidentiality, is a major issue. The dynamic theory of organizational knowledge creation, organizational culture theory and contingency theory were identified as the most suitable theoretical perspectives to address this issue and underpin an effective information security management framework for HSOs.

Research limitations/implications – The theory-based framework presented here has not been tested in practice. Such testing will be carried out in further research.

Originality/value – Currently, there is no framework for information security systems in HSOs. The framework developed here provides a foundation on which HSO can build information security systems specific to their needs.

Keywords Information security, Human information behaviour, Computer crime, Human service organizations, Information security management, Organizational theories

Paper type Conceptual paper

1. Introduction

Information technology (IT) is considered a lifeline for organizations irrespective of their size and nature. Thus, information security crime is not just a concern for nations; it is a concern for business and non-business organizations and individuals. Rapid technological developments, the vast expansion of IT networks and the wide use of electronic commerce present enormous security challenges for many organizations. The scope of information security now stretches from the IT resources within an organization to beyond the organization's boundaries. The borderless electronic information environment affords anonymity and concealment and provides a constant stream of new tools for engaging in criminal activity. Wright (2008) stressed that the

Journal of Information, Communication and Ethics in Society
Vol. 14 No. 3, 2016
pp. 254-271

1477-996X
DOI 10.1108/JICES-06-2015-0018

internet and computer networks have created new types of threats that computer criminals can exploit for personal gain. Therefore, protecting and managing information within organizations is essential (Von Solms and Von Solms, 2004). Appropriate information security is needed to enhance the confidentiality, integrity and availability of data, helping to maintain the original form of information content without risk of modification or loss. Various disciplines involved in managing organizations and securing their information have shown intense interest in the field of information security management (Goo *et al.*, 2013), effectively preventing security breaches and using up-to-date information management strategies to meet the latest information security standards. This paper focuses on information security management issues for human service organizations (HSOs) and presents an information security management framework to assist them in reducing the threat of information security breaches.

2. Information systems and human service organizations

HSOs may be governmental, non-profit and even for-profit, but their key common goal is to transform people's lives by ameliorating, preventing or otherwise addressing problems such as child abuse, mental illness, substance abuse, homelessness and poverty. Hasenfeld (2009) describes the complex nature of HSOs, stating that they are characterized by the "extrinsic benefits but intrinsic rewards that come from helping people", coupled with the "frustration" of dealing with paper-based documents. Information systems' capability of storing easily retrievable client data over a long period of time has the capacity to reduce some of the frustration, particularly for hospitals, social welfare organizations and HSOs. Information and communication technology (ICT) has been advantageous for HSOs in terms of work process improvement, facilitating shared communication and increased efficiency.

Although the IT revolution has benefited HSOs, adapting technology to meet their needs has created unforeseen problems (Gillingham, 2011). The information systems within these organizations face many security threats from unpredictable sources because of the sensitive nature of their data. Often, these organizations collect confidential and legally sensitive client information, for example, health reports, psychological reports and family background and income details. Many individuals and organizations are interested in this information, including, for example:

- *The insurance industry*: May be interested in gaining access to current and prospective clients' medical records.
- *Parents*: May be interested in knowing more about the personal life of their children with addiction and other behavioural problems.
- *Careers of problematic adolescents*: May be interested in gaining access to sensitive information such as psychological reports to gain legal and other advantages.
- *Spouses considering divorce*: May be interested in gaining legal advantage by obtaining personal information related to their partner's health and/or mental health condition. If accessed by the wrong people, data collected on sensitive issues such as mental health can lead to potentially damaging long-term stigma for a person with mental health problems.
- *Patients who have undergone surgery*: May be interested in details of their surgical procedures when preparing their case for a lawsuit against their surgeon.

- *Employers*: May be interested in gaining access to sensitive information about job applicants' personal lives.
- *Other HSOs*: May be interested in information related to the financial management or mismanagement of a particular HSO.
- *Other organizations*: May be interested in information related to human resources when looking for trained personnel.
- *Disgruntled employees*: May have unauthorized access to sensitive information and misuse it.
- *Malicious hackers*: May not necessarily be interested in the information but can cause major damage to ICT systems, thereby threatening HSO information security.

As Hasenfeld (2009, p. 18) identified, multiple constraints are a drawback to applying ICT in an HSO:

> At the organization level, resource constraints, competing demands from key stakeholders, quality of staff and internal systems of monitoring and rewards are likely to affect how the technology is actually practiced.

In addition, threats to the security of information collected by HSOs have raised questions about the ethical integrity of these organizations' service provision. This must be of great concern for human service workers whose personal and professional integrity rely on maintaining client confidentiality in the interests of achieving the best possible outcomes for their clients. They need to be acutely aware of information security and possible threats to their organizations' ICT systems.

Lack of information security management facilitates information security threats in the form of "computer crime" or "e-crime", which involves offences using a computer as either the object of the offence or the tool for its commission. According to Cross (2008, p. 11), computer crime in the broader sense involves:

> […] any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network.

Content-related offences such as possession of child pornography, or the dissemination of hate or racist material, are becoming more common (Australian High Tech Crime Centre (AHTCC), 2005). Gaining illegal access to clients' information can lead to hackers disseminating such material under the guise of a client or an organization. Other offences particularly relevant to HSOs include computer trespass (manipulation or theft of stored or online data), computer abuse (sabotage of equipment and data), illegal interception, industrial espionage, software piracy, hacking, e-mail fraud, computer-related forgery (where false data are put forward as authentic) and computer-facilitated fraud (fraudulent interference with, or manipulation of, data to cause property loss), which increasingly includes web page hijacking and identity theft (Smith, 2007). Criminals use social engineering – manipulating human behaviour to gain confidential information such as user names/passwords – to launch outsider attacks (Whitman and Mattord, 2012), and electronic transactions can be converted to other crimes such as money laundering (Choo *et al.*, 2007).

3. Information security challenges for human service organizations

Six main challenges face HSOs in terms of information security. First, the environment within HSOs is significantly different from non-HSOs, and, as Remin and Osten (2001) argued, the two types of organizations attach different values to their information. This implies that there may be differences in the way the organizations understand the term "information". In the world of non-HSOs, information is a prized possession with millions of dollars invested in not only protecting their "intellectual property" but also developing information systems to enable the collection and effective use of data (knowledge). In contrast, information-based competition and cultures steeped in propriety are less intense in HSOs. Most HSOs are "non-profit oriented and community based, and processes may appear inefficient and disorganised" (Productivity Commission, 2010, p. 13), which can interfere with the protection of valued information from external threats.

Second, there has been a severe shortage of funding and constant pressure to cut costs within the HSO sector in recent years (Jackson and Donovan, 1999; Hasenfeld, 2009). This has led many of these organizations to focus on widening their customer base and improving service quality. Although IT is frequently used to achieve both of these goals, the funding situation has pressured HSOs into allocating less funding for information security. Limited resources have also affected governance within HSOs and not-for-profit organizations. According to Carey-Snith (2007), non-profit or HSOs are similar to small and medium enterprises in terms of limited resources. At times, there is a need for everyone in the organization to contribute to particular tasks to complete a job, resulting in poorly controlled segregation of duties. Directors may have to move from an oversight role into an operational role and, in so doing, need to recognize that they report to an executive while completing the particular task. Similarly, although all roles should have clear definitions and boundaries, the same person may sometimes fill more than one, or all, of these roles. This must be acknowledged overtly so that role definition remains clear and internal controls can be applied effectively at both the human and policy levels. Internal controls are needed to protect against fraud, particularly where individuals are performing more than one role. "Poor internal controls" and "poor segregation of duties" are seen as major reasons for fraud (BDO Australia, 2010, p. 21). Segregation of duties promotes internal control among HSOs by introducing checks and balances for actions, thus reducing the risk of inappropriate action. When there is less segregation of roles, there is more chance of fraudulent activities. For example, if the person who proposes and approves the budget also signs the cheques, they may fail to maintain accountability for the process. In the case of HSOs and small organizations, this and similar multi-role situations may arise because of lack of resources, resulting in serious fraud. Human level controls to address this issue take the form of separation of duties, whereby different people handle two related duties to reduce the likelihood of fraud. Roles and responsibilities should be clearly documented in organizational policies and procedures that explain who is responsible for each step of each action and who has authorization rights.

Third, HSOs have a wide range of users accessing their information systems, which increases their vulnerability to system insecurity. Professionals (permanent employees of the organization) and non-professionals (volunteers and interns) use the information systems within HSOs. Volunteers play a significant role in the success of HSOs (Jackson

and Donovan, 1999). Australian HSOs have been forced to rely on volunteers more heavily because of the tight funding situation, as evidenced by an increase in volunteers from 12 per cent in 2008 to 19 per cent in 2010 (BDO Australia, 2010). However, volunteers pose complex and peculiar challenges to HSO management (Jackson and Donovan, 1999), particularly in terms of information security. HSOs cannot afford to train volunteers in information systems security, and volunteers may pose a security threat if there are inadequate formal procedures for verifying their backgrounds. There is also a risk of permanent employees and volunteers sharing passwords and confidential information, leaving HSOs vulnerable to fraud.

Fourth, HSOs provide a flexible work environment for their employees, which particularly suits volunteers (New South Wales Council of Social Service, 2008). Recent developments in network and wireless technology permit easy communication via access to information systems from many locations, which may be a security threat (Liu, 2014).

Fifth, HSOs constantly receive a wide range of interns, for example, medical, nursing, social work and psychology students, who need access to the organizations' information systems. Although interns are vetted stringently before placement in HSOs, similar to volunteers, they may receive only minimal training in information systems security, which significantly increases their level of threat to the HSOs, as demonstrated by the significant increase in internal attacks from 8 per cent in 2008 to 27 per cent in 2010 (BDO Australia, 2008, 2010). As long as HSOs remain "embedded in a complex system of internal and external control mechanisms" (Hasenfeld, 2009, p. 23) to guard trustworthy and fair relationships with clients, record keeping and monitoring and to meet external demands such as competition, government accreditation and standardization, they need to develop and maintain a strong culture of individual and organizational responsibility.

Sixth, the effects of organizational culture should not be underestimated. Boards and senior management must ensure that they instil an ethical organizational culture, supported by appropriate policies and procedures. Although any changes to policies and procedures may be met with resistance, ignoring a poor organizational culture can have dire consequences, such as vulnerability to security breaches due to employees' inaccurate handling of information (Thomson *et al.*, 2006). In some instances, the need to "unlearn" existing practices may result in high levels of anxiety and resistance (Schein, 1999).

Most importantly, HSOs have adopted networked forms of governance, relying on technology for communication with clients, stakeholders and the public, with an increased likelihood of lack of security for sensitive data and communications (Smith and Jamieson, 2006). This lack of security can result in damage to employee morale, financial loss, litigation and loss of reputation (Kolb and Abdullah, 2009). All the challenges noted above indicate the need for strong organizational management.

4. Instances of information security breaches in human service organizations

Some of the information security breaches reported within HSOs in recent years pose a great danger to individual and organizational confidentiality and integrity. HSOs involved with health care store and process confidential patient information such as names, addresses, medical history and family information, which is shared through

non-secure or semi-secure ICT tools such as e-mail Kolb and Abdullah (2009). Other HSOs accept credit card donations online, with donor credit card details stored and processed electronically (Donohue, 2008), leaving them open to service provider security breaches. Recent examples of data security breaches at organizations storing the abovementioned types of information in Australia are:

- A Centrelink employee accessing records belonging to customers and co-workers on 124 separate occasions and misusing the agency's IT systems to benefit those people (Dearne, 2011).
- Australian and New Zealand charities (not-for-profit sector) losing a total of $2.9m in fraud cases involving cash theft, payroll fraud, credit card fraud and online fraud. Online fraud was reportedly close to $375,000 (BDO Australia, 2012).

These cases point to ineffective information management systems facilitating breaches of information security. It is not only HSOs in Australia that are affected by information insecurity problems, as emphasized by the following examples from the USA:

- In November 2007, Convio, a software provider for HSOs, reported a security breach in its "GetActive" software systems, which led to the theft of user accounts and passwords. The affected HSOs had to inform their patrons about the compromise to their donor accounts (Search Security, 2007).
- Two employees at Memorial Healthcare System in South Florida accessed 9,497 patient records with the intent to process fraudulent tax returns (McNickle, 2012).
- A stolen laptop at Indiana Internal Medicine Consultants resulted in a breach of 20,000 patient records (McNickle, 2012).
- Healthcare in Atlanta announced a data breach after the organization misplaced ten backup disks containing information about more than 315,000 patients treated between 1990 and 2007 at Emory University Hospital Midtown and the Emory Clinic Ambulatory Surgery Centre (Horowitz, 2012).

The above cases illustrate the urgency for all HSOs to implement effective and workable information security management systems, with a strong theoretical grounding, to meet their specific needs.

5. Theories relevant to addressing information security systems issues

Several organizational theories can be used to explain HSO contexts and their employee behaviour. These include Douglas McGregor's XY theory, systems theory, socio-technical systems theory, dynamic theory, organizational culture theory and contingency theory.

Douglas McGregor's XY theory, which proposes a positive management style and techniques, remains central to organizational development and to improving organizational culture and motivation, which allows people to grow and develop (Carson, 2005). Von Bertalanffy's (1928) the systems theory, on the other hand, states that all the components of an organization are interrelated, and that changing one variable may impact many others. Organizations are viewed as open systems, continually interacting with their environment. They are in a state of dynamic equilibrium as they adapt to environmental changes (Kast and Rosenzweig, 1972;

Scott, 1981). A central theme of the systems theory is that non-linear relationships may exist between variables. Small changes in one variable can cause huge changes in another, but large changes in a variable may have only a nominal effect on another (Senge, 1990). The socio-technical systems theory considers that every organization is made up of people (the social system) using tools, techniques and knowledge (the technical system) to produce goods and services valued by customers (who are part of the organization's external environment) (Appelbaum, 1997). The concept of the socio-technical system was established to emphasise on the two-way relationship between people and machines. Its role is to foster the programme of shaping both the technical and social conditions of work to prevent efficiency and humanity from contradicting each other.

The dynamic theory of organizational knowledge creation explains how the knowledge of individuals, organizations and societies can be enriched through amplification of tacit and explicit knowledge of each. The key to this process is the joint creation of knowledge by both individuals and organizations (Nonaka, 1994). The organizational culture theory provides a framework for describing a culture as a pattern of basic assumptions that are invented, discovered or developed by a given group as an organization learns to cope with problems of external adaptation and internal integration (Schein, 1988). The contingency theory proposes that management techniques should be dependent upon current circumstances because management effectiveness is contingent upon the interplay between the application of management behaviours and specific situations (Scott, 1981).

After reflecting on the above theories, the author concluded that the first three briefly discussed here did not suit the purpose of building an information security management framework. For example, Douglas McGregor's XY theory fails to address the fact that the workforce is changing rapidly, and the workplace is a dynamic mix of employees from different backgrounds, races and genders. Similarly, the systems theory is too complex to provide an easily understandable framework for use in HSOs. Any misunderstanding of this complexity may lead to fatal damage to the HSO's security management system. Although the socio-technical systems theory enables change, it does not explain how to design the technology to support performance of change initiatives. Based on these factors, the author considered only the dynamic theory of organizational knowledge creation, organizational culture theory and contingency theory as suitable for the creation of an information security management framework for HSOs. These three theories are discussed in depth in the following section.

6. Information security management framework for human service organizations – theoretical perspectives underpinning practice

In consideration of the unique nature of the organizational environment in HSOs, the author developed a new generic information security management framework based on the dynamic theory of organizational knowledge creation, organizational culture theory and contingency theory, as shown in Figure 1.

The framework's underpinning theories and how these are implemented in practice are explained in the following sections.

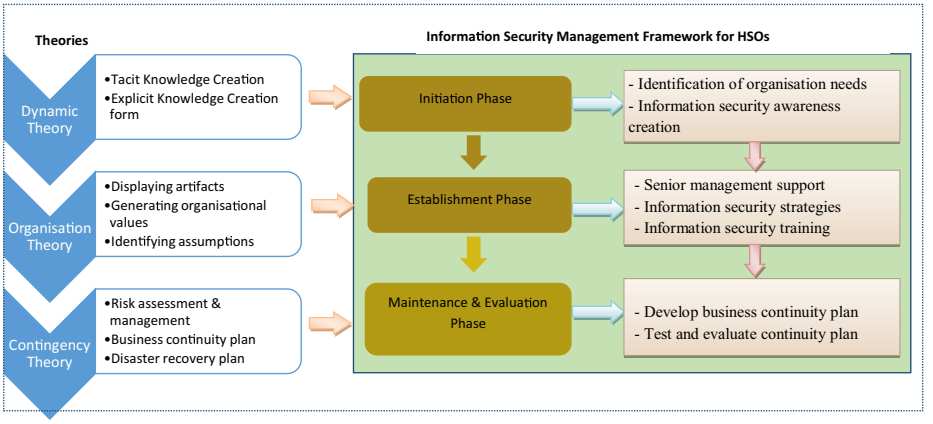

Figure 1.
Information security management framework for HSOs

6.1 Dynamic theory of organizational knowledge creation

The dynamic theory developed by Nonaka (1994, p. 17) explains:

> […] how knowledge held by individual organizations and societies can be simultaneously enlarged and enriched through spiral, interactive amplification of tacit and explicit knowledge held by individuals, organizations and societies.

New ideas and concepts are formed through individual interaction leading to "communities of interaction", resulting in the development of new knowledge (Nonaka *et al.*, 2000, p. 6). Applying this theory, it is clear that organizations, including HSOs, have great potential to expand their security awareness knowledge within their organization if they take information security management seriously. In addition, the dynamic theory emphasises that "new knowledge is developed by individuals; organizations play a critical role in articulating and amplifying that knowledge" (Nonaka, 1994, p. 17). Information shared by formal and informal means can become a great asset to an organization, for example, an induction programme on information security management for new staff will not only educate employees but also enable them to share their knowledge with others. The dynamic theory also emphasises on two dimensions of knowledge: "tacit knowledge", which is hard to formalize and communicate, and "explicit knowledge", which is codified and formal.

This theoretical foundation, in the form of an effective regular security awareness programme focused on information security threats and management, could help HSOs enormously. Facilitating informal communication opportunities between experienced and new employees would create an atmosphere conducive to discussing any past incidents of information security threats and the actions taken to overcome them. Thus, information security knowledge can be transferred informally.

The components of the dynamic theory have been used to establish the initiation phase of the HSO information security framework proposed in this paper. The outcomes of the initiation phase include:

- identifying the needs of the HSOs based on the organization's nature;
- information security awareness through informal exchange of tacit knowledge among staff; and

- formation of explicit knowledge in the form of security policies and the application of security standards to provide a clear structure for information security practices.

H1. Dynamic theory of organizational knowledge creation lays a foundation for the information security management framework for HSOs.

6.2 Organizational culture theory

Security culture is part of an organization's overall culture (Ruighaver *et al.*, 2007). According to George and Jones (1996), strong organizational culture functions under a cohesive set of values and norms, whereas in weak cultures, employees are left with minimum guidance. As noted by Carey-Snith *et al.* (2007), there are significant problems with information security culture and awareness and use of information security policies. Some organizations do not promote strong security awareness or monitor behaviour that could lead to potential risk. It is known that when senior management fosters a culture that promotes security, employees are more likely to exhibit the same behaviour (Wills, 2002). Properly trained, diligent employees can become the strongest link in an organization's security infrastructure (Henry, 2004, p. 664). According to Thomson *et al.* (2006), when employees understand information security, secure behaviour and actions should become second nature in their daily activities.

The organizational culture theory frameworks support many aspects of the dynamic theory. The most widely used framework is that of Schein (1988), who adopted a functionalist view. Schein described culture as a pattern of basic assumptions invented, discovered or developed by a given group as it learns to cope with its problems of external adaptation and internal integration. This pattern has worked well enough to be considered valid and taught to new group members as the correct way to perceive, think and feel in relation to the specified problems. Culture exists on three levels in Schein's (1988) model:

(1) Artifacts, which are difficult to measure. They deal with organizational attributes that can be observed. HSOs can openly display artifacts in the form of posters and information bulletins about information security. This may help people tune in to the concept of information security practices. Simple but important behaviour, such as protecting passwords securely or not opening suspicious e-mail attachments, can be communicated easily through artifacts.

(2) Values include the organizational values and missions around protecting client data from internal and external fraud. These values must be emphasised continuously, not only during induction programmes. The key step is senior management's recognition of the importance of information security and aligning that with the HSO management strategies. A top-down approach, involving senior management's recognition of, and support for, information security will result in other members of the organization absorbing and practicing security protocols. Security standards and policies in a simple form, updated in a timely manner, should be available to all employees. It is essential to stress that insider information security attacks can affect the organization's reputation and operation.

(3) Underlying assumptions include phenomena that remain unexplained when insiders are asked about the organizational culture's values. Information is

gathered at this level by carefully observing behaviours to identify underlying assumptions that are sometimes taken for granted and not recognized. According to Schein (1988), the essence of organizational culture lies at this level.

The organizational culture theory as described above underpins the establishment phase of the HSO information security framework presented in this paper. The establishment phase consists of:

- senior management support for establishing information security management practices as added value to the HSOs;
- inclusion of information security strategies included in the HSO core strategic direction;
- specific training in information security control mechanisms, such as password protection and protection from spam and viruses; and
- posters on information security practices, such as "not to share the password" and "importance of backup" to attract the attention of all staff.

H2. Concepts of organizational culture theory help establish an information security management framework for HSOs.

6.3 Contingency theory

In addition to awareness creation within HSOs, management has a major role to play in planning for any unforeseen situations such as natural disasters or power blackouts, which may damage the organization's information systems. This concept can be explained through the contingency theory, proposed by Scott (1981), who stated that "the best way to organize depends on the nature of the environment to which the organization relates". A wide range of external and internal factors must be considered, focusing on the action that best fits the given situation. The aim is to design an organizational structure that can handle uncertainties effectively and efficiently. Therefore, each organization's design must be tailored to its sources of environmental uncertainty. Given that every HSO is unique in terms of its function and organizational culture, managers must be able to analyze each organization individually and develop a pertinent contingency plan.

Guidelines, instructions, recommendations and considerations for establishing a contingency plan are outlined in the National Institute of Standards and Technology's (NIST) "Contingency Planning Guide for Federal Information Systems" (Swanson *et al.*, 2010). The NIST argues that a contingency plan is a living document that must be updated regularly. It is a basic requirement for any organization and provides key information and established procedures for system recovery following a disruption (Swanson *et al.*, 2010), including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures and system testing. The NIST recommends that organizations should use the following approach to develop and maintain an effective IT contingency plan (Swanson *et al.*, 2010):

> Develop the contingency planning policy statement and develop recovery strategies, stating roles and responsibilities of personnel. HSO need to have an effective contingency policy describing the responsibilities of key people in the team to take necessary action should such a situation arise. The contingency planning document should describe who has the authority to delegate and execute the recovery strategies.

Clear documentation and availability of the action plan during an emergency is equally important, as illustrated in the following instructions (Swanson *et al.*, 2010):

> Conduct the business impact analysis (BIA) to examine the critical components of the business and its impact on the business should there be any disruption. HSO must separate critical and non-critical areas of information, and quantify the loss in case of disaster. For example, details of client intervention processes will be critical for a counselling centre. Losing that information will impact the centre and rebuilding the system may be highly expensive or impossible.

Plan testing, training and exercises are also required (Swanson *et al.*, 2010). Staff need adequate training and live exercises to identify any deficiencies in the plan for the purpose of plan maintenance and updating. The updated contingency plan must be communicated regularly to all staff.

This discussion of the contingency theory and the practices needed to develop and implement a contingency plan are applicable to the maintenance and evaluation phase of the HSO information security framework presented in this paper. Specific steps to achieve this phase include:

- *Development of a simple business continuity plan (BCP) for the HSOs*: The plan will include a list of critical information assets, their value, possible threats to the assets and actions to overcome the threats. It will also list the person responsible for administering those actions.
- *Regular testing of the BCP to make sure it fits the HSO's current security needs*: Any changes made to the original plan should be documented clearly and any malfunctions noticed at this stage must be documented, communicated to the business continuity team and corrected.

H3. Theoretical components of contingency theory relate directly to the maintenance and evaluation phase of an information security management framework for HSOs.

7. Information security management for human service organizations – theory into practice

7.1 Initiation phase

The initiation phase consists of ensuring information security awareness and formulating information security policies and procedures.

7.1.1 Information security awareness from an human service organizations perspective. Addressing human aspects of information security is an important step from an organizational perspective (Furnell and Clarke, 2012). In implementing information security systems in accordance with this framework, it is essential to conduct user involvement and awareness programmes for administrative and professional staff such as social workers and psychologists. Spears and Barki (2010) suggested that although users are the greatest threat to information security, they can also contribute towards security compliance. Increased user awareness and participation in information security can positively affect security measures.

Awareness of international standards for information security and knowledge of how organizations can implement these is important (Tsohou *et al.*, 2010). Instituting a security awareness programme is an essential piece of the overall information security infrastructure (Kolb and Abdullah, 2009). It enhances good security practice (Wilson and Hash, 2003) by communicating mandatory IT security policies and procedures to all

staff and volunteers. Therefore, it is highly recommended that all levels of HSO employees participate in an awareness programme, followed by security management training. As identified earlier, awareness programmes need to be continuous to keep up with IT changes. Programmes must involve senior management as leaders to guide organization-wide information security education; information security policies and procedures, testing, documenting and acting on continuity and disaster recovery; and information security awareness from the employees' perspective.

Lacey (2010) emphasised on the importance in the current climate of embedding information security awareness in employee and organizational culture. Veiga and Eloff (2010) argued that a culture of information security awareness will minimise employee misbehaviour and harmful interaction with information assets. This is especially important because information security threats can come from insider attacks (Mubarak and Slay, 2009). A disgruntled employee may leak confidential information to unauthorized people. Similarly, ex-employees may remotely access confidential content and misuse it for personal gain.

7.1.2 Formulation of information security policies and procedures. There are four steps in an information security policy life cycle: plan; implement; monitor; and evaluate (Conklin *et al.*, 2004). If any of these steps are missed, an organization is open to information security threats. Every HSO can benefit from a sound information security policy that includes information security roles and responsibilities and definitions and explanations of the security controls that need to be installed in line with the organization's unique requirements (Bowen *et al.*, 2006). The specified roles and responsibilities provide guidance on employees' expected behaviour in a given situation or in accomplishing a specific task.

7.2 Establishment phase

Establishing information security management so it becomes part of organizational routine depends on senior management involvement and information security training for all of an organization's staff and professional colleagues.

7.2.1 Senior management involvement. It is important that managers/authorities understand the current state of security knowledge as a starting point for a larger programme. Senior management approval will ensure adequate resources for developing and implementing an HSO's awareness plan. Security awareness programmes must cover the entire user population (all levels of employees). Security management training, following successful dissemination of a security awareness programme, teaches necessary skills to the people directly involved with implementing it. Training is much more intensive than the awareness programme and may require several sessions. Enhancing security management through employee training and regular updates to organizational policies and procedures is essential. Training should focus on information security threats, such as threats to client details, and secure ways of using information processing facilities to minimise possible risks. Information security programmes for HSOs need to focus on a best practice guide for professionals and administrative employees who deal directly with client information.

Management cooperation is also essential when adopting security measures in any organization. In HSOs in particular, funding bodies may insist on information security systems as a core funding component, part of which is training all personnel. Management must ensure that funders' requests are met. Johnston and Hale (2009)

argued that organizational information security can be improved by adopting information security "governance". They found that when information security was addressed at the corporate level as part of an organization's planning process, it created an organization-wide culture of information security awareness. For example, non-technical employees should receive at least a basic orientation to information security management by understanding the importance of "not sharing their password with a co-worker when he/she does not have the same privileges" or "not replying to a phishing e-mail which includes his or her username" (Johnston and Hale, 2009, p. 127).

This discussion iterates findings from a survey of information security managers in various Norwegian organizations (Hagen *et al.*, 2008), which demonstrate that emphasising on policies and procedures in implementing information security measures while not emphasising on security awareness leads to less effectiveness of the measures. Hagen *et al.* (2008) showed that awareness measures are the most effective security strategies. Thus, it is important to emphasise on security awareness when adopting security programmes.

7.2.2 Information security training for everyone in human service organizations. All personnel need training in information security vocabulary. Knowing terminologies such as "spam" and "phishing" may impact greatly on personnel's understanding of information security. Kruger *et al.* (2010) argued that an information security system's vocabulary test is a good starting point from which to assess the security awareness of an organization's personnel. The vocabulary test provides a guide to which topics to include in security awareness programmes. Hagen and Albrechtsen (2009), who developed an e-learning tool for creating security awareness, noted that such a tool significantly improved the respondents' security knowledge, awareness and behaviour. Security awareness tools create an insight into employees' current knowledge and can prepare them to reflect on issues about which they are not confident. Generating security awareness is a proactive preventive programme for HSOs rather than a reactive strategy after a security breach.

7.2.3 Information security as part of professional human service organizations employees' responsibilities. Information security is a prime concern for human service workers because they generate vast amounts of sensitive client data daily and have a moral, legal, professional and organizational obligation to safeguard it. To do so, they need to be aware of IT security protocols and their role in safeguarding their agency's IT infrastructure. They have an obligation to respect their clients' privacy and to understand the following key IT security areas:

- the place where the data are stored and how safe they are;
- what protocols their agency is adopting to safeguard sensitive client data;
- who has access to these data and how they handle it; and
- the possibilities for breaches of IT security and the backup and contingency plans for dealing with a potential breach.

Human service workers also save their own sensitive data within the IT infrastructure. This may include their professional judgements about clients, colleagues, subordinates, supervisors and professionals from other agencies. Any breach in the security of this sensitive data will have negative implications for the workers. It is in their best interests

to ensure they understand the protocols for the safety of these data and their own role in keeping them secure.

Some human service professionals work in dangerous conditions, for example, in prisons and other correctional settings working with criminals, with people with complex mental health issues, and with drug addicts and drug dealers. The potential for these clients to commit offences such as sabotaging IT security is very high. Thus, it is crucial for human service professionals to be aware of ways in which their clients may breach their organization's IT infrastructure. Even where HSOs do not provide much training in IT security, human service professionals need to take a proactive stance. They need to learn and understand the technical aspects of IT security and human and technical reasons for possible IT security breaches and the role they can play in safeguarding their organization's IT infrastructure.

7.3 Maintenance and evaluation phase

Once information security management is well established, it is essential to maintain and evaluate it on a regular basis because of IT developments and employee turnover.

7.3.1 Developing a business continuity plan. A BCP ensures that critical business functions can continue if a disaster occurs (Whitman and Mattord, 2014). As a first step, an HSO must identify its internal critical systems and assets. For example, client data in a counselling centre's IT system are critical for running the organization. Thus, counselling centres should analyze the impact of data loss on their system, identify preventive measures such as back-up of critical data and develop a recovery plan that explains who is in charge and alternative strategies in emergency scenarios. The plan should be tested and reviewed regularly to identify gaps and keep it up-to-date.

7.3.2 Testing, documenting and evaluating continuity and disaster recovery. An HSO's contingency planning policy incorporates testing, documenting and acting on continuity and disaster recovery. A policy based on NIST (Swanson *et al.*, 2010) includes:

- clear demarcation of the roles and responsibilities of people in charge of IT security [and] provision of adequate resources for training in IT security;
- conducting a business impact analysis mainly to analyze the down time effect on the business/HSO to evaluate the maximum tolerable system down time. The down time effect on the organizations' computer systems must be analyzed from a technical point of view to enable backup preparations prior to any incidents. Organizations need detailed backup policies and procedures that should be communicated to personnel as part of their training. Contingency strategies must include data and information backup and recovery strategies, including offsite data storage;
- identifying preventive controls such as fire suppression or smoke detectors;
- documenting the plan, discussing the plan's scope and assumptions within the team, testing the plan and conducting training and exercises;
- ensuring plan maintenance – maintaining data security, integrity and back-up; and
- securing plan appendixes: items such as contact information, equipment tests, service agreements and any other related contingency plans.

Following the NIST guidelines is a good generic starting point for HSO to test, document and evaluate their continuity and disaster recovery plans. However, each organization's specific characteristics, such as type of employees and clientele, will require management to implement some practices specific to their organization's work context.

8. Conclusion

Information security remains unrecognized in many HSOs, creating risk to the organizations, their staff and their clients. This paper highlights the importance of addressing this issue by providing and unpacking a new theory-based generic framework of how to embed information security management into organizational culture. Adopting the framework (Figure 1) may be a useful step in beginning the process of developing an HSO-sector culture of awareness of the responsibilities and risks of working in an electronic information storage and sharing environment and instituting information security systems within each organization. If all HSOs work together from the same plan, building in features unique to each organization's situation, they may regain client confidence in the areas of privacy and confidentiality of information and securely share information with each other. Establishing partnerships with the IT industry to keep up to date with technological developments would also be advantageous for HSOs.

References

Appelbaum, S.H. (1997), "Socio-technical systems theory: an intervention strategy for organizational development", *Management Decision*, Vol. 35 No. 6, pp. 452-463.

Australian High Tech Crime Centre (AHTCC) (2005), *High Tech Crime Brief: Concepts and Terms, Australian Government*, Australian Institute of Criminology, Canberra, available at: www.aic.gov.au/documents/6/B/6/%7b6B679000-637F-4A27-9229-3C42928B364B%7dhtcb001.pdf (accessed 5 October 2013).

BDO Australia (2008), "BDO not-for-profit fraud survey 2008", available at: http://resources.news.com.au/files/2011/04/03/1226032/860218-fraud.pdf (accessed 6 July 2013).

BDO Australia (2010), "BDO not for profit survey", available at: https://eprints.usq.edu.au/18580/1/Howard_Best_PV.pdf (accessed 6 July 2013).

BDO Australia (2012), "Not-for-profit fraud survey 2012", available at: www.bdo.com.au/__data/assets/pdf_file/0006/137706/FraudSurvey2012_A4_FINALPRINT.pdf (accessed 22 July 2013).

Bowen, P., Hash, J. and Wilson, M. (2006), *SP 800-100: Information Security Handbook: A Guide for Managers*, National Institute of Standards and Technology, Gaithursburg, MD.

Carey-Snith, M., Nelson, K. and May, L. (2007), "Improving information security management in non-profit organization with action", *Proceedings of 5th Australian Information Security Management Conference*, *Perth*.

Carson, C.M. (2005), "A historical view of Douglas McGregor's Theory XY", *Management Decision*, Vol. 43 No. 3, pp. 450-460.

Choo, K.K.R., Smith, R.G. and McCusker, R. (2007), *Future Directions in Technology-enabled Crime: 2007-09*, Australian Institute of Criminology, Canberra.

Conklin, A., White, G., Cothren, C., Williams, D. and Davis, R.L. (2004), *Principles of Computer Security: Security+ and Beyond*, McGraw-Hill, Illinois.

Cross, M. (2008), *Scene of the Cybercrime*, 2nd ed., Syngress Publishing, Burlington.

Dearne, K. (2011), "Centrelink cracks down on misconduct", available at: www.theaustralian.com.au/australian-it/government/centrelink-cracks-down-on-misconduct/story-fn4htb9o-1226221128140 (accessed 23 July 2013).

Donohue, M. (2008), "States push to encrypt personal data", available at: www.thenonprofittimes.com/news-articles/states-push-to-encrypt-personal-data/ (accessed 2 July 2013).

Furnell, S. and Clarke, N. (2012), "Power to the people: the evolving recognition of human aspects of security", *Computers & Security*, Vol. 31 No. 1, pp. 983-988.

George, J.M. and Jones, G.R. (1996), *Understanding and Managing Organizational Behaviour*, Addison-Wesley Publishing Company, Reading, MA.

Gillingham, P. (2011), "Computer based information systems and human service organizations: emerging problems and future possibilities", *Australian Social Work*, Vol. 64 No. 3, pp. 299-312.

Goo, J., Yim, M.S. and Kim, D.J. (2013), "A path way to successful management of individual intention to security compliance: a role of organizational security climate", paper presented at the 46th Hawaii International Conference on System Sciences (HICSS) 2013, Urbana, IL, IEEE, pp. 2959-2968.

Hagen, J.M. and Albrechtsen, E. (2009), "Effects on employees' information security abilities by e-learning", *Information Management & Computer Security*, Vol. 17 No. 5, pp. 388-407.

Hagen, J.M., Albrechtsen, E. and Hovden, J. (2008), "Implementation and effectiveness of organizational information security measures", *Information Management & Computer Security*, Vol. 16 No. 4, pp. 377-397.

Hasenfeld, Y. (2009), *Human Services As Complex Organizations*, Sage Publications, London.

Henry, K. (2004), *The Human Side of Information Security, Information Security Management Handbook*, 5th ed., Auerbach Publications, Boca Raton.

Horowitz, B.T. (2012), "Emory healthcare data breach in Atlanta affects 315,000 patients", available at: www.eweek.com/c/a/Health-Care-IT/Emory-Healthcare-Data-Breach-in-Atlanta-Affects-315000-Patients-704506/ (accessed 5 May 2013).

Jackson, A.C. and Donovan, F. (1999), *Managing to Survive: Managerial Practice in Not for Profit Organizations*, Allen & Unwin, Sydney.

Johnston, A.C. and Hale, R. (2009), "Improved security through information security governance", *Communications of the ACM*, Vol. 52 No. 1, pp. 126-129.

Kast, F.E. and Rosenzweig, J.E. (1972), "General systems theory: applications for organizations and management", *Academy of Management Journal*, Vol. 15 No. 4, p. 451.

Kolb, N. and Abdullah, F. (2009), "Developing an information security awareness for a non- profit organization", *International Management Review*, Vol. 5 No. 2, pp. 103-108.

Kruger, H., Drevin, L. and Steyn, T. (2010), "A vocabulary test to assess information security awareness", *Information Management & Computer Security*, Vol. 18 No. 5, pp. 316-327.

Lacey, D. (2010), "Understanding and transforming organizational security culture", *Information Management & Computer Security*, Vol. 18 No. 1, pp. 4-13.

Liu, C. (2014), "The enemy within: the inherent security risks of temporary staff", *Computer Fraud & Security*, Vol. 2014 No. 5, pp. 5-7.

McNickle, M. (2012), "Ten of the largest data breaches in 2012 […] so far", available at: www.healthcareitnews.com/news/10-largest-data-breaches-2012-so-far?page=,0,1 (accessed 10 December 2013).

Mubarak, S. and Slay, J. (2009), "Protecting clients from insider attacks on trust accounts", *Information Security Technical Report*, Vol. 14 No. 4, pp. 202-212.

New South Wales Council of Social Service (2008), *NCOSS News*, Vol. 35 No. 9.

Nonaka, I. (1994), "A dynamic theory of organizational knowledge creation", *Organizational Science*, Vol. 5 No. 1, pp. 14-37.

Nonaka, I., Toyama, R. and Konno, N. (2000), "SECI, Ba, and leadership: a unified model of dynamic knowledge creation", *Long Range Planning*, Vol. 33 No. 1, pp. 5-34.

Productivity Commission (2010), "Contribution of the Not for profit sector", Research Report, Canberra.

Remin, D.G. and Osten, M. (2001), "Information as an organizational asset", *Technology Planning*, 14 December 2001.

Ruighaver, A.B., Maynard, S.B. and Chang, S. (2007), "Organizational security culture: extending the end-user perspective", *Computers and Security*, Vol. 26 No. 1, pp. 56-62.

Schein, E.H. (1988), *Process Consultation*, Addison-Wesley, Reading, MA, Vol. 1.

Schein, E.H. (1999), *The Corporate Culture Survival Guide*, Jossey-Bass Publishers, San Francisco, CA.

Scott, W.R. (1981), *Rational, Natural, and Open Systems*, Prentice-Hall, Englewood Cliffs, NJ.

Search Security (2007), "Convio acknowledges security breach", available at: http://searchsecurity.techtarget.com/news/1281717/Convio-acknowledges-security-breach (accessed 11 January 2013).

Senge, P. (1990), "The art & practice of the learning organization", in Ray, M. and Rinzler, A. (Eds), *The New Paradigm in Business: Emerging Strategies for Leadership and Organizational Change, 1993*, World Business Academy, Jeremy P. Tarcher, New York, NY, pp. 126-138.

Smith, R.G. (2007), *Consumer Scams in Australia: An Overview*, Australian Institute of Criminology, Canberra.

Smith, S. and Jamieson, R. (2006), "Determining key factors in e-government information systems security", *Information Systems Management*, Vol. 23 No. 2, pp. 23-32.

Spears, J.L. and Barki, H. (2010), "User participation in information systems security risk management", *MIS Quarterly*, Vol. 34 No. 3, pp. 503-522.

Swanson, M., Bowen, P., Phillips, A.W., Gallup, D. and Lynes, D. (2010), "Contingency planning guide for federal information systems (NIST Special Publication 800-34)-Revision 1", available at: http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-3rev1_errata-Nov11- 2010. Pdf (accessed 29 January 2014).

Thomson, K.L., Solms, R.V and Louw, L. (2006), "Cultivating an organizational information security culture", *Computer Fraud & Security*, Vol. 2006 No. 10, pp. 7-11.

Tsohou, A., Kokolakis, S., Lambrinoudakis, C. and Gritzalis, S. (2010), "A security standards' framework to facilitate best practices awareness and conformity", *Information Management & Computer Security*, Vol. 18 No. 5, pp. 350-365.

Veiga, A.D. and Eloff, J.H. (2010), "A framework and assessment instrument for information security culture", *Computers & Security*, Vol. 29 No. 2, pp. 196-207.

Von Bertalanffy, L.K. and Mattord, H.J. (1928), "Theorie der formbildung, Gebrüder Borntraeger", in Woodger, J.H., *Modern Theories of Development: An Introduction to Theoretical Biology*, Oxford Clarendon Press, Berlin.

Von Solms, R. and Von Solms, B. (2004), "From policies to culture", *Computers & Security*, Vol. 23 No. 4, pp. 275-279.

Whitman, M.E. and Mattord, H.J. (2012), *Principles of Information Security*, 4th ed., Cengage Learning, Boston.

Whitman, M.E. and Mattord, H.J. (2014), *Management of Information Security*, 4th ed., Cengage Learning, Boston.

Wills, L. (2002), "Security policies: where to begin", available at: www.sans.org/reading-room/whitepapers/policyissues/security-policies-919 (accessed 29 January 2014).

Wilson, M. and Hash, J. (2003), "Building an information technology security awareness and training program", NIST Special publication, 800-50, National Institute of Standards and Technology, Technology Adminstration, US Department of Commerce.

Wright, C. (2008), *The IT Regulatory and Standards Compliance Hand Book*, Syngress, Burlington.

Corresponding author
Sameera Mubarak can be contacted at: sameera.mubarak@unisa.edu.au