Exploring Security Strategies for Enterprise Data Protection in Organisations

Olusegun Ademolu Ajigini
School of Computing, University of South Africa, Florida, South Africa
ajigioa@unisa.ac.za

Abstract: Due to the rise of data breaches, organisations constantly need to develop new strategies and security architectures to protect their data assets. This must be done to prevent further breaches, financial losses and a tarnished reputation. In recent years, organisations have focused on perimeter security to protect their data assets; however, since about 50 per cent of most security breaches are perpetrated internally, perimeter defences are no longer adequate for securing organisational data. This further emphasises the importance of developing strategies that can provide adequate data protection measures for organisations. This paper presents an overview of security strategies that can be utilised by organisations to safeguard and protect their data assets. The paper explores various aspects of data protection measures such as classification of sensitive data, defining a security policy around identified data, determining a mode of data privacy implementation, and cyber security awareness. A security strategy model for the protection of organisational data assets in organisations is proposed from the literature review. The paper provides valuable information on how organisational data can be handled safely and protected against both internal and external threats. The paper aims to assist organisations to protect their data as part of the contributions toward community engagement.

Keywords: data protection, security strategy, information classification, sensitive data, security model, cyber security

1. Introduction

Enterprise data protection strategy includes the implementation of policies for the processes, people and technology of organisations so as to avoid data security breaches (ITNoob, 2010). Enterprise data are now much more vulnerable, because it is transferred more frequently and stored on more devices than ever before. This is due to globalisation and is the result of using widely networked devices over wireless networks, and an increase in the mobile storage or computing power through cloud computing as well as server virtualisation. The view of Day (2010) is that data leakage is a primary business challenge since, as organisations store more data, their risk of a breach increases.

Information is a resource that has strategic value to an organisation and exists in many forms, like written or printed documents, electronic files, microfilms and videotapes (Fung & Jordan, 2002). Information has been regarded by Duri, Elliott, Gruteser, Liu, Moskowitz, Perez, Singh and Tang (2004) as the new currency of the global economy. Correct information is expected to support decision making or to provide service at the appropriate time. Therefore, the integrity of the information cannot be compromised, and data protection is vital for the users to be assured both of their privacy and that the data meets the service provider's integrity requirements (Duri et al, 2004).

Some of the hardest challenges that security researchers and professionals are faced with today include the prevention, detection and response to data leakage by authorised users or insider threats (Huth, Chadwick, Claycomb & You, 2013). Thus, information in organisations has to be protected in accordance with how sensitive, critical and valuable it is. However, this should not depend on the storage media, the processing manual or automated systems, or the methods of information distribution. The protection of information is in accordance with its sensitivity, and is substantiated by section 5 of the ISO17799 standard, which stipulates that information should be classified according to its actual value and level of sensitivity so that the appropriate level of security can be deployed. ISO 27002 Newsletter Issue 9 (2007) maintains that, ideally, a system of classification should be easy to understand and manage, able to be used to define the level of protection the information is given, and possible to use uniformly throughout the whole organisation. Organisations need to protect the confidentiality and privacy of their sensitive information using document security technologies (Deshmukh & Pande, 2014).

Because of the increase in data breaches, organisations constantly need to develop new strategies and security architectures to protect their data assets (Tumulak, 2010). Thus, organisations need to adopt an enterprise data protection strategy to safeguard their data from the core to the periphery of their enterprise. They also need to provide an end-to-end encryption solution across their databases, networks, applications and endpoint devices

(Tumulak, 2010). Thus, the paper will assist organisations to safeguard their data assets as part of a community engagement initiative.

In this paper, a security strategy model for the protection of organisational data assets in organisations is proposed in security strategies from Tumulak (2010), RSA (2010) and ITNobb (2010). The layout of the paper is as follows: The first section highlights the importance of the management of sensitive information in organisations and provides a definition of sensitive information from a synthesis of definitions given by different authors. This is followed by sections exploring the importance of protecting sensitive information and how information can be classified according to its sensitivity levels. The next section is about cyber security awareness and how cybercrimes can be prevented in organisations. The last section presents a proposed security strategy model that can be used to protect organisational data assets. The paper concludes with suggestions for future work in this area of research.

2. Management of sensitive information

The management of sensitive information related to their business ought to be very important to all organisations (Rakers, 2010). A new challenge for management is to keep secure the vast amounts of information contained within computer-based information systems in organisations (Taylor, 2006). This problem is exacerbated by the advent of big data (i.e. excessively voluminous or complex sets of data). There is also a special sensitivity surrounding any personal health data and medical records. The role of sensitive information as well as trust in decreasing the concerns about privacy of medical information have been investigated by Rohm and Milne (2004), who conclude that consumers are concerned about their medical history and records. Also, storing data in the "cloud" has not yet countered all user fears of security, especially public cloud. In South Africa, legally, no financial institution is allowed to store financial information outside the geographical borders of the country, and with public cloud, it could be located anywhere, unknown to the owner of the data (FATF/OECD, 2009).

Arai and Tanaka (2009) have highlighted the importance of avoiding information leakage when a computer system handles a company's sensitive information. They, furthermore, suggest that sensitive information should be encrypted and technology should make it possible to share the decryption key between the users dealing with that sensitive information. This process of encrypting and decrypting data forms part of the management framework on information sensitivity during software migrations.

The complexity of the information systems required for its safe-keeping increases as the amount of personal data stored and processed by companies' increases (Acquisto, Friedman & Telang, 2006). Internal employees of organisations might try to gain unauthorised access to the information, while others might unintentionally put organisational information at risk (Taylor, 2006). This is why information security problems due to the integration of organisations into the worldwide web draw considerable attention from investigators and experts (Ma & Pearson, 2005b).

Sensitive information from US government networks is being gathered by well-funded Chinese groups (Graham, 2005). This has led to national security concerns in the USA, and the extent of these intrusions as well as the nature of data exposed is not fully known (Casey, 2006). Sensitive information is kept by the social spontaneities defined by social interactions and it has to be protected, because lack of protection affects the organisational image. This is why the security of IT software and the network controls must be taken into consideration when designing and implementing new software systems (Scholz, 1990).

The definitions of sensitive information by different authors are highlighted in Table 1 below. This table can be used to identify sensitive information as part of the process of modelling security strategies for enterprise data protection in organisations.

Table 1: Definitions of sensitive information (Source: Ajigini et al, 2012)

Definitions of sensitive information	
Authors	Definitions of sensitive information by each author
Gennotte and Trueman (1996)	Protected information used to increase the prospect of the result for the organisation, group, or person handling the information.

Definitions of sensitive information	
ALRC (2000)	Information pertaining to a person's race or ethnicity, political orientation, religious relationship, philosophical inclination, profession, trade union or association, sexual orientation or criminal practices.
Thompson and Kaarst-Brown (2005)	Information about the owner that is concealed by the owner. It is also information known to a person about an organisation that the person does not want to reveal outside the organisation.
TJNAF (2007)	Information that can cause damage to the government, laboratory or persons if such information is made known to people who do not require knowledge of such information in the discharge of their duties.
McCullagh (2007)	The European Union defines sensitive data as information that exposes the ethnicity, political orientation, religious or philosophical affiliation, health, sexual beliefs and membership of trade union.
NIST (2008)	Sensitive information is defined as any information that, if lost, misused, modified by unauthorised persons, will result in undermining the national interest, federal programmes performance, individual privacy entitlement as enshrined in the Privacy Act, that is not approved by an Executive Order or Congress Act and which is expected to be hidden in line with national defence interest or foreign policy. According to the US Computer Security Act of 1987, agencies are required to categorise and distinguish their sensitive systems, train their employees in computer security and create computer security plans.
NIH (2008)	Sensitive information is when the loss of confidentiality, availability, or integrity of such information could have a disastrous unfavourable effect on individuals as well as organisational belongings.
Nawafleh et al (2013)	Sensitive data is any information which, if leaked, can lead to the destruction of the person or the organisation and may include personal information as well as the organisation's information.

In this paper, our definition, synthesised from Table 1 above, is that sensitive information is protected information that is concealed by the owner, and when the loss of such information can lead to the destruction of the organisation.

3. Protection of sensitive information

Corporations have been motivated to invest in information security by safeguarding their confidential data and their customers' personal information (Acquisto et al, 2006). The non-protection of sensitive information can damage an organisation's reputation (Rasmussen 2008). He maintains that organisations must protect their sensitive information throughout its lifecycle. This has led Taylor (2006), in carrying out research using case studies and intergroup bias theory, to investigate the current strategies to protect organisational information.

Proceeds from information theft were estimated at $105 billion US worldwide in 2004 (Swartz, 2005). Similarly, the cost of electronic crimes was estimated by the FBI to be approximately US$10 billion a year (Ma & Pearson, 2005b). Due to the high level of cybercrimes, the United States Congress passed a series of bills in November 2002 to allocate one billion dollars for research on cyber security with the aim of combating terrorist attacks on private and government computer systems (Ma & Pearson, 2005a). Moreover, Diffie (2008) indicates that information security is a vast field that involves vast amounts of money, publications and practitioners when compared to all computer science areas a half-century ago.

Information theft can also have non-financial implications. This view is shared by Bruce (2003), who points out that breaches of information systems can have non-financial implications, such as, a negative impact on a company's status, trust and goodwill, or a deficit in potential sales and competitive advantage. Also, losing sensitive information by organisations may cause confidential information leakage that can lead to financial loss (Sarrab & Bourdoucen, 2013).

In recent years, there has been wide media coverage of many incidents involving the disclosure of sensitive information due to leakage (Ahmad, Bosua & Scheepers, 2014). Ahmad et al (2014) stress that sensitive information leakage through unknown avenues is a serious problem for management, mostly caused by mobile devices, cloud computing, network technologies and social media. They maintain that due to leakage, organisations may suffer from reputational damage, revenue loss and loss of productivity. According to them, the leakage can be prevented by using technical measures to control information access, for example,

passwords, encryption, logging mechanisms, firewalls and intrusion detection systems. Organisations ought to have a data protection strategy as part of a data leak prevention solution (Gupta, 2010).

Data leakage includes different types of crimes perpetrated by insiders, theft of personally identifiable information, theft of intellectual property, an insider passing sensitive or classified information to an unauthorised third party (Huth et al, 2013). McCormick (2008) divides data leakage and theft into three stages: (a) obtaining access, (b) downloading data and (c) sharing data. Database privacy has to be maintained (Olivier, 2002). Olivier (2002) expresses the importance of database privacy and maintains that the challenge of database privacy is how personal information is enabled in databases in a way that balances society's needs with those of the individual. Database level encryption is considered when protecting data by using keys, and organisations use database-level access to control types of information that can be shared among users (Bayuk, 2009).

The majority of security incidents are caused by organisational employees who violate IS policies. Therefore, a proper working environment should be created to enhance employee compliance with organisations' IS policies (PWC, 2008; Whitman & Mattord, 2008; Kolkowska, 2011). This has called for the establishment of environments that ensure good security behaviour, by transforming the culture of the organisation and setting up an information security culture (Knap, Marshall, Rainer & Ford, 2007; Thomson, Von Solms & Louw, 2006). As part of protecting sensitive information, Rasmussen (2008) maintains that the detail of how sensitive information is labelled, stored, distributed and destroyed must be contained in organisations' data security policies. Security scholars have identified lack of awareness of security policies among users to be a major cause of failure (Abraham, 2011).

4. Information sensitivity and information classification

Many authors explain the reasons for information sensitivity classification (The Open Group, 2009; Bradley, 2007). Organisations classify their information so that they can control exactly who may access their sensitive information or confidential information, protect their sensitive information or confidential information and make it easy for those so authorised to find their sensitive information (The Open Group, 2009). Data classification has been regarded by Tumulak (2010) as an important process of achieving data privacy in organisations.

The need for research on sensitive information classification has been stressed by Thompson and Kaarst-Brown (2005). More research should be done to establish how sensitive information should be conceptualised and also to understand the difference between sensitive information and other organisational information. They argue that because these research gaps hinge directly on the information, research to accommodate them should be done at the same time as research efforts that are linked to IS security architecture, such as systems that have multiple layers of security. Recent developments in the IT field have created the need to understand sensitivity cues (Thompson & Kaarst-Brown, 2005).

Information classification is important during the information protection process, and there are many different classification schemes available. The Open group (2009) came up with a four-level classification scheme called the "G8 Traffic Light Proposal" and these levels are the following:

- Red: Highly sensitive
- Amber: Sensitive
- Green: Normal Business
- White: Public

The ISO 27002 Classification scheme has five levels, namely:

- Top secret
- Highly confidential
- Proprietary
- Internal use only
- Public documents

Nawafleh, Hasan and Nawafleh (2013) propose a three-level classification scheme, namely:

- Sensitive data classification
- Private Classification
- Public classification

The researcher's view is that organisations should use the ISO 27002 classification scheme to classify their sensitive information, since it is an international standard that has been tested and widely approved.

The United States federal government has elaborated on the importance of research on how sensitive information should be classified and understood (Thompson & Kaarst-Brown, 2005). The US government also stresses the importance of conducting research on the classification of sensitive information, because the US classification of national security information is out-dated. This view is also supported by McCullagh (2007), who adds that the current classification of sensitive data is ineffective for determining the conditions of data processing.

A report compiled by the US General Accounting Office (GAO, 2000) has highlighted the need for categorising data used by all federal agencies. The terrorist attack on the World Trade Center in New York and the Pentagon in Washington DC on September 11, 2001, moved the intelligence committees of both houses of the US Congress to propose the review of the statuses, policies and procedures governing the classification of national security information (US Congress, 2003). The Open Group (2009) states that the recent information classification systems are used by specialists and only a small portion of the information is labelled.

Organisations should be able to classify information based on its sensitivity, taxonomy and probability, and use the classification to protect sensitive information in their organisations (The Open Group, 2009). This will enable them to understand which information should be the most protected and which the least protected.

Some authors (The Open Group, 2009; Bataller, 2012; Richardson & Michalski, 2007; Fowler, 2003) have also stressed the need to have a classification system for information to realise the goal of performing a sensitivity assessment. Farrell's view (2002) is that organisations must perform a sensitivity assessment even if they understand the different protection needs for information contained in both their manual and electronic systems.

5. Cyber security awareness

Cyberspace is the new challenge facing organisations nowadays, and cyber security is a top imperative for both enterprises and governments (Stevens, 2013). Cyberspace is regarded as the information space that consists of the total sum of all computer networks (Schmidt, 2014). Cyber security is the protection of organisational business information and valuable intellectual property in digital format against theft and misuse (Kaplan, Sharma & Weinberg, 2011). Reddy and Reddy (2014) define cybercrime as using a computer primarily to engage in any illegal activity of commission and theft, and these include, but are not limited to, network intrusions, dissemination of computer viruses, identity theft, stalking, bullying and terrorism. Cyberattacks ought to be prevented by organisations using approaches to cyber security. This is because employees have increased their presence on the internet, and more organisations are encouraging their clients and customers to join their networks. Moreover, professional cybercrime organisations and hackers are more technologically advanced than the corporate security teams (Kaplan et al, 2011). Adler's view (2013) is that cyber security has two dimensions: technical – involving technologies, tools and skills to detect cyberattacks, and management – defining data governance structures and culture. This is line with Kaplan et al (2011) who state that, to combat cybercrimes, cyber security should be addressed at the most senior level of an organisation, and it should be a key part of business strategy rather than merely technological governance. Organisations should protect their data rather than protecting their perimeter, for example, by limiting access to their live data by employees such as application developers, infrastructure architects and engineers. Big data capabilities are being used as a central part of the solution to combat cybercrimes in organisations (Stevens, 2013). Organisations have to be aware of cyber security and develop strategies to combat cybercrime. Kortjan and Von Solms (2014) also state that cyber security awareness is of fundamental importance in all organisations.

6. Towards a security strategy model to protect organisational data assets

In this section, a security strategy model to protect organisational data assets is proposed in the security strategies of Tumulak (2010), RSA (2010) and ITNobb (2010). Tumulak (2010) suggests a security strategy for improving business processes and reducing data losses, which is illustrated in Figure 1.

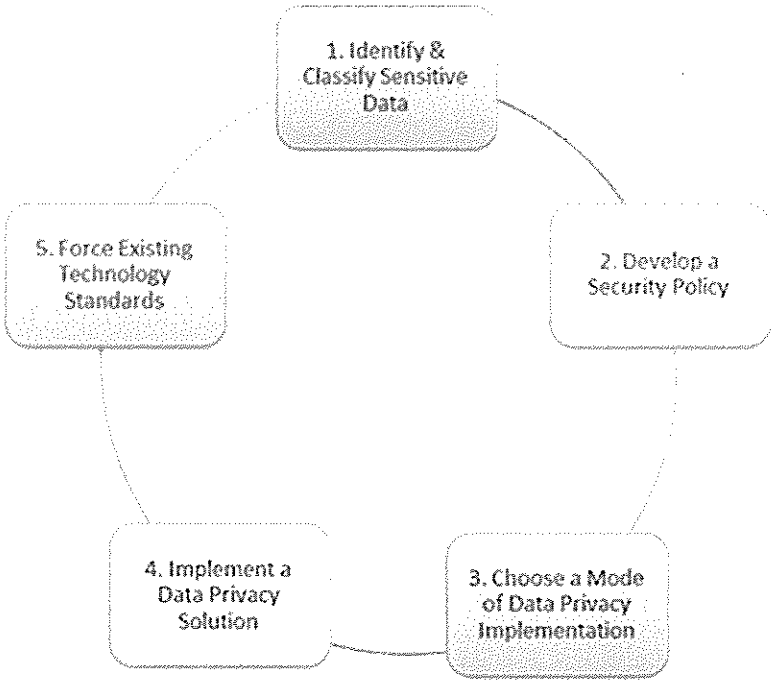

Figure 1: Security strategy for business processes improvement (Source: Tumulak, 2010)

Organisations need to identify sensitive data and consider data classification first in their security strategy (Tumulak, 2010). This also involves the determination of organisational data confidentiality levels, the location of the organisational sensitive data and defining data access models. Organisations need to develop a security policy that includes (a) determination of an acceptable level of threat, (b) identification of the legislative measures applicable to the organisation and (c) the development of an authentication and authorisation policy (Tumulak, 2010). The next step is to choose a mode of data privacy implementation followed by data privacy solution implementation. The data privacy solution comprises (a) network-level encryption (b) application-level encryption, (c) database-level encryption, (d) storage-level encryption, (e) secure key management, (f) cryptographic operations, (g) authentication and authorisation, (h) logging, auditing and management, (i) backup and recovery, and (j) hardware. According to Tumulak (2010), the last step of the strategy is to force existing technology standards, which include (a) controlling secure transport standards, (b) controlling authentication, authorisation and auditing technologies, (c) using standard and proven cryptographic algorithms such as Advanced Encryption Standard (AES) and Rivest-Shamir-Adelman (RSA) Encryption Standard, and (d) using standard software interfaces.

According to RSA (2010), there are six best practices for preventing enterprise data loss. These are (a) understanding the most sensitive data in the organisation, (b) identifying the location of the most sensitive data in the organisation, (c) knowledge of the origin and nature of the organisational risks, (d) selecting the appropriate controls based on policy, risk and the location of the sensitive data, (e) managing security centrally and (f) performing audit security. There are some similarities between the security strategies proposed by Tumulak (2010) and RSA (2010). These include the identification, location and classification of sensitive data, as well as developing the appropriate security policies. ITNobb (2010) also proposes five security technologies that can be used to protect organisational data. These are (a) disk and file-level encryption, (b) network intrusion detection, (c) authentication, (d) secured coded application and (e) backups. Using these three security strategies, a security strategy model to protect organisational data assets is proposed as shown in Figure 2.

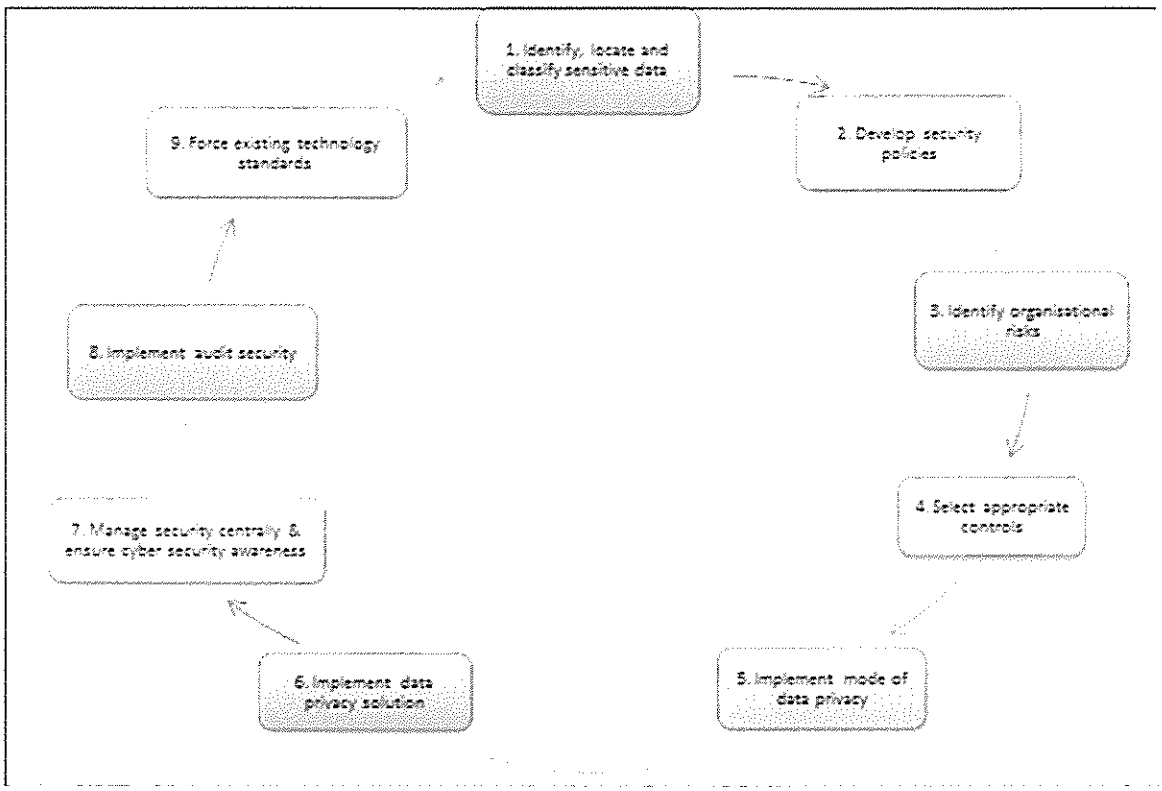

Figure 2: A security strategy model for the protection of organisational data assets

The first process in the security strategy is identifying, locating and classifying sensitive data. The identification and location of sensitive information is explained in section 2 of this paper, while the classification of information is explained in section 4. The second step is the development of security policies. Organisations should have a data security policy, which lists data security methods and sensitive data management. These procedures and the policy should be regularly communicated to all staff and subsequently enforced. There should be a continual update of the data security policy, and data integrity should be the hallmark of any organisation. It is also the view of Ross (2008) and Kavanagh (2006) that not only should organisations have a policy in place, but that policy as well as the standards should be enforced by the relevant level of management. Security models should be developed to support organisational strategy, and such models should ensure confidentiality, integrity and reliability of data to protect sensitive information. Security is related to change management, and the change management should be properly communicated to end users to ensure that they receive it well in their organisation (Ashenden, 2008). Management should have sufficient communication on information security with end users.

The third step of the security strategy is the identification of organisational risks. To safeguard sensitive information, organisations need to develop and implement policies and procedures to protect sensitive information, assess organisational data with a dedicated data security team, enforce hardware and software standards to eliminate unknown factors that access sensitive information without being authorised to do so, educate employees, validate the people and systems, and update the program with changes as needed, and, finally, mitigate risk by adopting insurance coverage (Augustinos, 2009).

The fourth step of the security strategy is the enforcement of security controls. Technical controls must be used to prevent unauthorised data access, and they should not be used in an isolated manner (Jones & Colwill, 2008). A data privacy solution should be implemented as part of the security strategy. Sensitive information should be encrypted using data protection tools and privacy-enhanced technologies. Security should be managed centrally, and organisations should ensure that their employees are aware of cyber security. Cyber security should be a key part of business strategy rather than simply part of technological governance, that is, cyber security should be given a "business back-up" approach. A security audit as well as enforcing existing technology standards should be implemented as part of the security strategy. Organisations should enforce hardware and software standards to eliminate unknown factors that might allow access to their sensitive information. These

standards would give the best practice baseline for IT governance, since they are the basis of information security.

7. Conclusions

In this paper, the notions of protection and management of sensitive information were investigated. Sensitive information needs to be identified, handled and protected in any organisation to ensure its safety and provide for data governance. The ISO 27002 classification scheme, which comprises five classification levels: top secret, highly confidential, proprietary, internal use only, and public documents, is proposed for organisations to classify their information. Organisations need to be aware of cyber security and prevent cybercrime by using technology, tools and skills to detect cyberattacks and to define data governance structures as well as culture. A security strategy model was created for the protection of organisational data assets using the security strategies from Tumulak (2010), RSA (2010) and ITNobb (2010). This model is based on the nine-phase process presented in Figure 2. It is anticipated that this model will be useful for providing enterprise data protection in all organisations as part of the contributions toward community engagement.

8. Future work

Future work in this area would include further investigation of cyber security awareness in organisations, which could lead to the development of a framework and its validation for such purposes. Secondly, the proposed model could be enhanced further and validated by implementing it in industries that are already working towards protecting their sensitive data using modern techniques, as well as those that have not yet commenced such processes.

References

Abraham, S. (2011) "Information security behavior: factors and research directions", *Proceedings of the 17th Americas Conference on Information Systems (AMCIS)*, Detroit, Michigan.

Acquisto, A., Friedman, A. and Telang, R. (2006) "Is there a cost to privacy breaches? An event study", *27th International Conference on Information Systems*, Milwaukee.

Adler, R. M. (2013) "A Dynamic Capability Maturity Model for Improving Cyber Security", *IEEE*, pp 230 – 235.

Ahmad, A., Bosua, R. and Scheepers, R. (2014) "Protecting organizational competitive advantage: A knowledge leakage perspective", *Computers & Security*, Vol. 42, pp 27 – 39.

Ajigini, O. A., Van der Poll, J. A. and Kroeze, J. H. (2012) "Towards a Management Framework to protect sensitive information during migrations", *The 2nd International Conference on Design and Modeling in Science, Education and Technology (DeMSet)*, Orlando, Florida, USA, pp 6 – 13.

ALRC (2000) "ALRC report 108", [online], www.alrc.gov.au.

Arai, M. and Tanaka, H. (2009) "A proposal for an effective information flow control model for sharing and protecting sensitive information", *Australasian Information Security Conference (AISC)*, Wellington, New Zealand. Conferences in research and practice in Information Technology *(CRPIT)*, Ljiljana Brankovic and Willy Susilo, Eds.

Ashenden, D. (2008) "Information security management: A human challenge?", *Information Security Technical Report*, pp 195 – 201.

Augustinos, T. (2009) "Preventing and reacting to a data breach", *Risk Management*, Vol 56, No. 10, pp 45.

Bataller, E. (2012) "Data classification tips and technologies", *InformationWeek Report*, [online], www.networkcomputing.com/unified-communication/data-classification-tips-and-technologies/d/d- id/1233510?

Bayuk, J. (2009) "Data-centric security", *Computer Fraud & Security*, pp 7 – 11.

Bradley T. (2007) "Securing sensitive information: Protecting your network against information leakage", *CISSP-ISSAP*, Microsoft MVP - Windows Security.

Bruce, L. S. (2003) "Information Security – Key issues and developments", [online], www.pwcglobal.com/jm/images/pdf/information%20Security%20Risk.pdf.

Casey, E. (2006) "Investigating sophisticated security breaches", *Communications of the ACM*, Vol 49, No. 2.

Day, G. (2010) "Strategic Information Management through Data Classification", [online], wwww.boozallen.com/media/file/strategic-information-management-through-data-classification-vp.pdf.

Deshmukh, P. S. and Pande, P. (2014) "A study of electronic document security", *International Journal of Computer Science and Mobile Computing (IJCSMC)*, Vol 3, No. 1, pp 111 – 117.

Diffie, W. (2008) "Information security: 50 years behind, 50 years ahead", *Communications of the ACM*, Vol 51 No. 1.

Duri, S., Elliott, J., Gruteser, M., Liu, X., Moskowitz, P., Perez, R., Singh, M. and Tang, J. (2004) "Dataprotection and data sharing in Telematics", *Mobile Networks and Applications*, Kluwer Academic Publishers, Netherlands, Vol 9, pp 693 – 701.

Farrell, G. (2002) "Former Anderson executive to testify", *USA Today*, pp B1, April 10.

FATF/OECD (2009) "Anti-money laundering and combating the financing of terrorism in South Africa, Mutual Evaluation Report", [online], www.fic.gov.za/DownloadContent/NEWS/General/2008/FATF_ME_2009_FINAL

Fowler, S. (2003), "Information Classification – Who, Why and How?", SANS Institute, [online], www.sans.org/reading-room/whitepapers/auditing/information-classification-who-846.

Fung, P. and Jordan, E. (2002), "Implementation of information security: A knowledge-based approach".

GAO (US Government Accounting Office) (2000) "Federal information security: Actions needed to address widespread weaknesses", [online], http://www.gao.gov.

Gennotte, G. and Trueman, B. (1996) "The strategic timing of corporate disclosures", *Review of Financial Studies*, Vol 9, No. 2, pp 665 – 690.

Graham, B. (2005) "Hackers attack via Chinese web sites: US agencies networks are among targets", *Washington Post*, Thursday, August 25.

Gupta, M. (2010) "A new strategy for the protection of intellectual property", *Computer Fraud & Security*, pp 8 – 10.

Huth, C. L., Chadwick, D. W., Claycomb, W. R. and You, I. (2013) "Guest editorial: A brief overview of data leakage and insider threats", *Information Systems Front*, Vol 15, pp 1 – 4.

ISO 27002 News – Issue 9 (2007) "Establishing information classification criteria", The ISO 27002 Newsletter – News & views on the ISO/IEC security standard.

ITNoob (2010) "What is enterprise data protection?", [online], http://itquestions.com/1826/what-is-enterprise-data-protection.html.

Jones, A. and Colwill, C. (2008) "Dealing with the malicious insider", In: *9th Australian information and Warfare security Conference.*

Kaplan, J., Sharma, S. and Weinberg, A. (2011) "Meeting the Cyber security Challenge", [online], http://sas-origin.onstreammedia.com/origin/isaca/LatinCACS/cacs-lat/forSystemUse/papers/243.pdf.

Kavanagh, J. (2006) "Security special report: the internal threat", *Computer Weekly*, [online],www.computerweekly.com/Articles/2006/04/25/215621/security-special-report-the-internal-threat.htm

Knapp, K. J., Marshall, T. E., Rainer, R. K. and & Ford, N. (2007) "Information security: management's effect on culture and policy", *Information Management & Computer Security*, Vol 14, No. 1, pp 24 – 36.

Kolkowska, E. (2011) "Security subcultures in an organisation - exploring value conflicts", ECIS conference, Helsinki, Finland 9-11, *The 19th European Conference on Information Systems ITC and Sustainable Services Development.*

Kortjan, N. and von Solms, R. (2014) "A conceptual framework for cyber security awareness and education in SA", *SACJ*, No. 52, pp 29 – 41.

Ma, Q. and Pearson, J. M. (2005a) "ISO 17799: Best practices in information security management", *Communications of the Association for Information Systems*, Vol 15, pp 577 – 591.

Ma, Q. and Pearson, J. M. (2005b) "The inter-relationship between objectives and practices in information security management", *Proceedings of the 11th Americas Conference on Information Systems*, Omaha, NE, USA, August 11 – 14.

McCormick, M. (2008) "Data theft: a prototypical insider threat", In: S. Stolfo, S. Bellovin, S. Hershkop, A. Keromytis, S. Sinclair and S. Smith (eds.), *Inside attack and cyber security: beyond the hacker*, New York: Springer, pp 52 – 67.

McCullagh, K. (2007) "Data sensitivity: resolving the conundrum", British & Irish Law, *Education and Technology Association Annual Conference*, Hertfordshire, 16 - 17 April.

Nawafleh, S. A., Hasan, M. Y. F. and Nawafleh, Y. (2013) "Protection and defense against sensitive data leakage problem within organisations", *European Journal of Business and Management*, Vol 5, No. 23.

NIH (2008) "Guide for identifying sensitive information", [online], http://irm.cit.nih.gov/security/NIH_sensitive_info_Guide.doc.

NIST (2008) "An Introduction to Computer Security, The NIST Handbook", [online], http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter1-printable.html.

Olivier, M. S. (2002) "Database privacy – Balancing confidentiality, integrity and availability", *SIGKDD Explorations*, Vol 4, No. 2, pp 20.

PWC (2008) "Security breaches survey, enterprise and regulatory reform (BERR)", PricewaterhouseCoopers on behalf of the UK Department of Business, [online], www.pwc.co.uk.

Rakers, J. (2010) "Managing professional and personal sensitive information", *SIGUCCS*, October 24 – 27, Norfolk, Virginia, USA.

Rasmussen, G. T. (2008) "Safeguarding sensitive information – An ounce of prevention", [online], www.gideonrasmussen.com/article-09.html.

Reddy, G. N. and Reddy, G. J. U. (2014) "A Study of Cyber Security Challenges and its emerging trends on latest technologies", International Journal of Engineering and Technology, Vol 4, No. 1, [online],http://arxiv.org/labs/1402.1842.

Richardson, B. T. and Michalski, J. (2007) "Security framework for control, system data classification and protection", SANDIA report, [online], http://energy.sandia.gov/wp/wp content/gallery/uploads/Richardson-2007-3888P.pdf.

Rohm, A. J. and Milne, G. R. (2004) "Just what the doctor ordered – The role of information sensitivity and trust in reducing medical information privacy concern", *Journal of Business Research*, Vol 57, pp 1000 – 1011.

Ross, S. J. (2008) "Enforcing information security: architecture and Responsibilities", *Network Security*, pp 7 – 10.

RSA (2010) "Best Practices for Preventing Enterprise Data Loss", [online], www.nascio.org/committees/security/secuirtyvideo/whitepapers/emc.pdf

Sarrab, M. and Bourdoucen, H. (2013) "Runtime monitoring using policy based approach to control information flow for mobile Apps", *International Journal of Electrical, Electronic, Electrical Science and Engineering*, Vol 7, No. 11, pp 526 – 533.

Schmidt, N. (2014) "Critical Comments on Current Research Agenda in Cyber Security", *Defense and Strategy*, Issue: 1, pp 29 – 38, [online], www.ceeol.com.

Scholz, C. (1990) "The symbolic value of computerized information systems", In P. Gagliardi (ed.) *Secrecy*, New York: Human Sciences, pp 161 – 177.

Stevens, M, (2013) "Facing the Challenges of Cyber Security", [online], www.ibmbigdatahub.com/blog/author/michael-stevens.

Swartz, J. (2005) "2005 worst year for breaches of computer security", In: *USA Today*.

Taylor, R. G. (2006) "Management perception of unintentional information security risks", *27th International Conference on Information Systems*, Milwaukee.

The Open Group (2009) "COA paper – Information classification", [online], www.opengroup.org/jericho/COA_informationClassification_v1.0.pdf.

Thompson, E. D. and Kaarst-Brown, M. L. (2005) "Sensitive information: A review and research agenda", *Journal of the American Society for Information Science and Technology*, Vol 56, No. 3, pp 245 – 257.

Thomson, K. L. R., von Solms, R. and Louw, L. (2006) "Cultivating an organizational information security culture", *Computer Fraud & Security*, Vol 10, pp 7 – 11.

TJNAF (2007) "Security Plan for protection of sensitive information", Thomas Jefferson National Accelerator Facility.

Tumulak, D. (2010) "Enterprise Data Protection: A security strategy for improving business processes and reducing data losses", [online], www.212.45.99.23/whitepaper_library/safenet_enterprise_data_protection.pdf

US Congress (2003) "Joint enquiry into intelligence community activities before and after the terrorist attacks on September 11, 2001", [online], http://www.gpoaccess.gov/serialset/creports/911.html.

Whitman, M. E. and Mattord, H. (2008) *Principles of information security*, Course Technology, Boston, MA, 2nd edition.