Ridoh Adonis (South Africa), Bethuel Sibongiseni Ngcamu (South Africa)

# An empirical investigation into the information management systems at a South African financial institution

## Abstract

The study has been triggered by the increase in information breaches in financial organizations worldwide. Such organizations may have policies and procedures, strategies and systems in place in order to mitigate the risk of information breaches, but data breaches are still on the rise. The objectives of this study are to explore the shortfalls of information security on a South African financial institution and further investigate whether business processes are responsive to organization's needs. This study employed both quantitative and qualitative research methods. Questionnaires were sent to staff level employees, and semi-structured in-depth interviews were conducted with senior management at the organization. The study revealed that employees require training on information management and that there are major training deficiencies for training officers to conduct beneficial information management training at the organization. Information security program that include business risk analysis were not implemented, which results in inadequate information management planning and decisions. A standardized or uniform house rule policy was not consistently implemented across the organization, which resulted in certain areas not protecting information. The qualitative findings revealed that the external cleaning company could obtain access to customer information, if customer data are left lying around. Furthermore, there is major misalignment between policy setters and employees in this organization. The findings allow senior managers to construct projects and program with their teams to improve the state of information management in the organization which spans across the people aspect, technology systems and general information management processes. Furthermore, external companies should start signing Non-Disclosure Agreements - which is not being done currently as this opens the door for data fraud. The organization has information management and security policies in place, but the study concluded that employees do not understand these policies and should receive specialized training to ensure understanding and, ultimately, have employees following these information security policies.

**Keywords:** data breach, information management, business processes, information legislation.
**JEL Classification:** G2.

## Introduction

There has been a perception in financial institutions that employees breach data and fail to secure their organizational personal information. Duncan (2015) states that South Africa faces unique challenges in relation to hacking and the intentions of stealing personal information; it is, therefore, important for South African organizations to understand their vulnerabilities. According to PWC (2011), South Africa's Law Reform Commission looked at North America and various European countries when developing South Africa's data privacy legislation. On an international stage, a $3 million fine was handed down to a health insurance company in America as a result of data breaches (KPMG, 2013). Kieke (2014) states that the Advocate Health Group reported in 2013 that four of its computers were stolen; this was one of the largest Health Insurance Portability and Accountability Act of 1996 breaches ever reported. The study has been triggered by the increase in information breaches in organizations with few researchers who have researched this field of study. Organizations may have policies and procedures, strategies and systems in place in order to mitigate the risk of information

breaches; however, data breaches are still on the rise with less published data scholarly.

There have been high profile data breaches in the United Kingdom, which has resulted in guidance and recommendations to help organizations to implement and monitor policies on personal information standards (Young, 2010). Garrison and Ncube (2011) states that organizations could lose consumer confidence and market share as a result of data breaches, which could, therefore, be very costly to the organization. According to Fisher (2013), data breaches could result in fraudulent activities taking place. Based on all of these factors highlighted thus far, the primary objectives of this study are to: explore the short falls of information security on a South African financial institution, investigate if data remain separate and privacy is ensured, investigate responsiveness of business processes on information management; investigate the capability of systems on information management, investigate the strategies formulated for information management; investigate projects and program aimed at addressing information management; and investigate contingency plans on how to respond to the financial risk in respect to information management.

The next section critically reviews the existing literature on information management followed by the research methodology. The results of the study are, then, presented, analyzed and discussed with the literature reviewed. This paper further concludes and

provides recommendations for the study and for future researchers, as well as the limitations of the study.

# 1. Literature review

## 1.1. Information privacy in financial institutions.
For organizations, there are many risks related to information security which could result in a loss of creditability for the organization, as well as monetary damage, therefore, making sure that information is secure and safe has become one of management's top priorities (Bulgurcu, Cavusoglu and Benbasat, 2010). When customer information is breached by organizations, it has a long-term negative impact on the organization (Malhotra and Malhotra, 2011). Bulgurcu et al. (2010) note that in order to reduce these risks, organizations require technology-based solutions, but organizations also have to focus on individual and organizational perspectives and employee compliance with information security policies as employees can, many a time, be the weak link in information security. According to Kosciejew (2014), governments or regulators should impose auditing requirements on organizations who use personal information and that any application that looks at personal information should be inspected.

With the rising number in security risk incidents, information systems are becoming more exposed to risk and breaches (Al-Mukahal and Alshare, 2015). In order to gain a competitive advantage, organizations need to know how to analyze and manage information technology risks, as information technology has become the backbone of commerce (Nazimoglu and Ozsen, 2010). The use of information technology is considered as the common denominator for the competiveness of an organization (Moghavvemi and Salleh, 2014). With the need for technology on the rise and the need to secure these technologies from breaches, Al-Mukahal and Alshare (2015) mention that employees also breach data and that the reason for employees violating or not violating security policies when it comes to information management could vary from deterrence, neutralization, rational choice theories to habit, protection motivation and planned behavior of individuals.

D'Arcy and Green (2014) argue that it has been found that security related and general working environment factors could contribute to employees' security compliance, while an employee's position, the industry in which the organization operates and the amount of time that an employee has been employed at the organization also plays a role in employee security compliance. According to Thompson and Van Niekerk (2012), employees can often be the weakest link when it comes to safe guarding information security, which is likely due to a lack of concern of information security, as individual employees may not feel that it is their responsibility to protect this information. This study assesses employees' perceptions of data breaches, as well as the likelihood of respondents across the value chain of the organization breaching organizational personal information.

## 1.2. South African legislative framework on information management.
According to Malhotra and Malhotra's (2011) research, consumers are concerned about the information collected on them and how it is being used and protected by organizations. The Protection of Personal Information (POPI) Act 4 of 2014 was promulgated on 26 November 2013 by the South African government. POPI focuses on protecting the flow of information and advancing the right of access to information, if any organization processes personal data, then, it needs to be done in compliance with the POPI Act (South Africa, 2013). This Act can be regarded as one of the broadest privacy legislations in the world and that the requirements, therefore, make it difficult to fully understand the implications of the Act (Burmeister, 2014). The Promotion of Access to Information Act (PAIA) 2 of 2000 was assented by the South African presidency in February 2000. This Act was "to give effect to the constitutional right of access to any information held by the State and any information that is held by another person and that is required for the exercise or protection of any rights (South Africa, 2000). The PAIA gives effect to the constitutional right of access to information whereby all South Africans are given the right to access records held by government institutions and private bodies. The Consumer Protection Act (CPA) 68 of 2008 includes a section on the consumer's right to privacy whereby the CPA states that every person has the right to pre-emptively block any approach or communication if the communication is for the purpose of direct marketing (South Africa, 2008). According to the Department of Trade and Industry (2009), consumers have the right to protect their privacy in respect to unsolicited or unwanted marketing correspondence, as consumers can refuse to receive SMS's, telephone calls, letters or spam emails and should be given the right to opt out to any of this correspondence.

## 1.3. Research methodology.
This study followed both a qualitative and quantitative approach. According to Creswell (2003), an integrated approach of using qualitative and quantitative methods involves strategies of collecting data either simultaneously or sequentially in order to best understand the research problems. Data were collected by means of a questionnaire which was sent to non-senior management at the organization. There were 81 questionnaires returned, and there were 9 in-depth interviews conducted with senior management. A sampling procedure is followed to collect information from a population and, therefore, refers to a process used to select a portion of the population for study purposes (Nieuwenhuis,

2007). Neelankavil (2007) explicitly explains the sampling process to consist of defining the population, obtaining a list of the population, selecting a sample frame, determining the sample methods, developing a procedure for selecting the sample units, determining the population size and drawing the sample. There are various types of sampling techniques used in research, while some of these include stratified sampling and purposive sampling. For the quantitative research, portion of this study, a census was conducted. This is important, as all individuals who are not part of the strategic management group were deemed selectable to partake in the study. The researcher attempted to get responses from all of these individuals. According to the Australian bureau of statistics (2013), whether taking a census or selecting a sample, both of these methods give the researcher the ability to draw conclusions about the whole population.

It is further explained that a census studies every unit or everyone in a population and is known as a complete enumeration, while a sample is a subset of units in a population selected in order to represent all units in the interested population of the researcher and is known as partial enumeration. Non-probability sampling was used for the in-depth interviews, as certain individuals who hold a senior management position were identified. Trochim (2006) describes this in more detail by stating that non-probability sampling methods are mainly of a purposive nature, as there is a specific plan in mind to sample the problem and, furthermore, explains non-probability sampling as sampling that does not involve a random selection to identify the population. In this research, there was testing conducted on the reliability and validity of the data and findings in order to check its applicability, consistency and neutrality.

Morse, Barret, Mayan, Olson and Spiers (2002) note that there has been an increase in requiring 'rigour' during the course of research whereby strategies for evaluating trustworthiness need to be implemented in order for the research not to lose its utility "hence, a great deal of attention is applied to reliability and validity in all research methods'. Cronbach's alpha coefficient was applied to all statements consisting of Likert scale responses in the questionnaire. According to Chigamba and Fatoki (2011), the Cronbach's alpha coefficient is used to test the reliability of the scales used by the researcher, with the alpha coefficient ranging from 0 to 1 with the higher score indicating a higher degree of reliability of the scale. Cooper and Schindler (2003) state that a reliability coefficient of 0.700 or higher is considered as the acceptable reliability coefficient. The reliability scores for all sections exceeded the recommended

Cronbach's alpha value of 0.700. An overall Cronbach's alpha value of 0.847 was achieved in this study. This indicates a degree of acceptable, consistent scoring for the different sections of the research. No questions were, thus, omitted from the analysis. Collins and Hussey (1997) state that the reliability of open questions is low in comparison to the higher validity of using closed-ended questions, as generalizations can be construed and used as different settings with a lower reliability. The research questionnaire used for this study consisted of close-ended questions which provided reliable data, as respondents were required to select responses from pre-defined listings.

The interviews were recorded by the researcher with the consent of the participants. All interview participants were asked the same questions. Cooper and Schindler (2003) state that the demographic and enterprise data completed by the respondents are reviewed against the research delineation to ensure the respondents are aligned to the research delineation, while Fraenkel and Wallen (2001) add that an instrument is valid if it measures what it is intended to measure and accurately achieves the purpose for which it was designed.

Current staff members of the selected financial institution in South Africa were included for this research study. The population was approximately 1400 people. The population consists of staff members across the value chain and comprises staff members holding various positions in the organization. The positions include: executive management; senior management (non-executive); middle management; non-managerial specialists; lower level management; and agent level staff. For this study, the structured questionnaire was distributed by sending the questionnaire via email to all middle managers in the organization for them to distribute to their staff members and also printing out questionnaires as a follow up to the email and giving these to managers for them to distribute to their staff.

As not all managers would pass on the questionnaires to their staff and for those managers who did distribute the questionnaire to staff, some staff ignored the questionnaire, as it was not mandatory to respond or partake in the research; therefore, it is estimated that approximately 500 employees received the questionnaire. There were 81 questionnaires returned with a response rate of 16.2%, while semi-structured interviews were done with 9 senior management members at the organization. The structured questionnaire used to gather information from staff level members of the organization was measured by the Likert scale. The items were measured using a five-point Likert scale with a range from (1) strongly disagree, (2) disagree and (3) undecided to (4) agree and

(5) strongly agree, testing the perceptions of the leaders through leading statements. Both the questionnaire and interviews were divided into a biographical section and 5 other sections or dimensions. The biographical information used in the data collection instruments included: gender, age, level of education, staffing level and length of service in the respondent's current position. The dimensions used includes breaching of data in a financial institution, information management mitigation in a financial institution, information management preparedness in a financial institution, information management systems in a financial institution and information management risk response and recovery in a financial institution. A positivist paradigm philosophy was adopted with the research strategy and objectives of this study where it is believed that reality is stable and can be observed. According to Guba (1990), methods used in a positivist paradigm are empirical and quasi-experimental, while Carr and Kemmis (1986) add that a positivist paradigm enables a degree of technical control over natural objects.

Pilot studies are usually put forward as a test in order to test and refine aspects of the study (Yin, 2011). In this research, a pilot test was performed on the questionnaire where by three participants from different areas of the organization completed the questionnaire in order to determine how long the questionnaire took to complete and whether the questions posed any difficulty in completing. The three respondents completed the questionnaire within a time of 15 to 20 minutes and understood the flow of the questionnaire. A pilot test was performed on the interview questions whereby one senior management participant was interviewed in order to determine whether the questions posed any difficulty in understanding. Length of interview was not a factor, as different participants would provide longer or shorter answers to the interview questions. The results of the data analysis and the discussion of findings will be presented in the next section.

**1.4. Analysis of the findings.** A total of 81 employees responded to the questionnaire. There were more females than males that partook in the quantitative portion of the study with a percentage of 38% males to 62% females. Three-quarters of the respondents (78%) had been in employ for less than 3 years in the position. The senior managers interviewed include the senior manager of compliance and operational risk, head of information technology, head of data, senior manager of collections, head of human resources, senior manager for information technology operations, senior manager for decision technology, senior manager for information architecture and senior manager of value added products. There were more males than females who took part in the interviews, of the 9 interview respondents, 7 were males, while 2 were females. In addition, 3 respon-

dents were between the ages of 31 to 40, 2 respondents between the ages of 41 to 50, and 3 respondents between the ages of 51 to 60; 8 of the 9 respondents had a tertiary level education.

For the quantitative analysis, the majority of research participants were in agreement with the sub-dimensions on the breaching of data in a financial institution, with the exception of only two disagreements on the fact that data breaches have a positive impact and that customers are not concerned with information management. Furthermore, 61% of the research participants did not agree that data breaches do not affect its economic condition and that it occurs accidentally (69%). This is in disagreement with Zhang, Reithel and Li (2009) who state that data and security breaches negatively impact the economic condition of the organization. The Chi-square test that was done on breaching of data in a financial institution indicates that the scoring patterns are somewhat similar, proportionally. This is confirmed by the Chi-square p-values ($p < 0.05$) which confirm that the differences observed per option per statement were significant. The sig. values (p-values) or level of significance are less than 0.05, which implies that the distributions were not similar. Even though the majority of respondents agreed, gaps were also found which necessitates interventions or control measures to be implemented by decision makers of the institution. From the in-depth interviews on this dimension, research participants indicated that there were policies at the organization, but they were not standard across the organization, and there were external cleaning staff who may have access to customer information should it be left on desks after shifts.

Just under ½ of the respondents did not disagree to the statement in the questionnaire that in this financial institution, customers were not concerned about information management. In addition, 1/3 of respondents did not disagree to the statement in the questionnaire that data breaches have a positive impact. These are, therefore, in disagreement with Malhotra and Malhotra (2011) who note that when customer information is breached by organizations, it has a long-term negative impact on the organization, while this is also in disagreement with Bulgurcu, Cavusoglu and Benbasat (2010) who explain that the risk of information security breaches could result in a loss of creditability for the organization, as well as monetary damage. There are 26% of respondents who did not agree to the statement in the questionnaire that employees are trained on information security policies. This is, therefore, in disagreement with Abu-Musa (2012) who notes that training in the operation of security processes is key to information security, while Fourie (2011) states that information professionals need

to provide training and support as part of the promotion process of personal information management. Hagen and Albrechtsen (2009) add that training and educating employees is more effective than formal procedures and controls put in place by the organization, but many organizations do not provide adequate training to employees in relation to information security. Furthermore, under the dimension of breaching data in a financial institution, the in-depth interviews made reference to external cleaning staff coming in during the evening, and these cleaning staff would, therefore, have access to customer information if it is left on desks. This would, therefore, constitute as a data breach. This cause of a data breach is not mentioned in previous literature reviewed.

The majority of research participants were in agreement with eight sub-dimensions on information management mitigation in a financial institution with the exception of one, namely: *I have access to customer information that is not a necessity to perform my job*, while four statements did not have an outright majority selection by participants. Statements that did not have an outright majority selection are: *information is protected from the moment it is created until the end of its cycle* (agreed 38%, undecided 35%, disagreed 27%). This is in disagreement with Gable (2014) who notes that an Information Governance (IG) program should be adopted to protect private information which ensures that personal information is protected from the moment it is created till the time it undergoes final disposition; *I have attended information management training which is beneficial to me* (agreed 37%, undecided 14%, disagreed 49%); *employees' knowledge is regularly tested on information security policies and procedures* (agreed 37%, undecided 26%, disagreed 37%); and *there is low risk of information breaches* (agreed 31%, undecided 43%, disagreed 26%). Chi-square tests were on done information management mitigation in a financial institution. Most of the scoring patterns were somewhat similar, proportionally. This is confirmed by the Chi-square p-values ($p < 0.05$) which confirm that the differences observed per option per statement were significant. *Employees knowledge is regularly tested on information security policies and procedures* did not have significant differences in opinions. This is confirmed by the Chi-square p-values being 0.146. From the in-depth interviews on this dimension, it is noted that a Data Governance Council (DGC) has been formed to assist in controlling information management. The majority of research participants were in agreement with the sub-dimensions on information management preparedness in a financial institution with the exception of only one statement where the majority of participants were undecided on the fact that information security forms part of the annual organizations budgeting. The research findings

revealed the majority agreements to employees are the strongest link in information security (78%).

The majority of research participants were in agreement with the sub-dimensions on the information management systems in a financial institution with the exception of one disagreement on the fact that technology based solutions are all that are required to ensure information security, while three statements did not have a majority selection. Statements that did not have an outright majority selection are: *the standard of information security systems is assessed against international accepted rules and practices* (agreed 49%, undecided 48%, disagreed 3%); *all business stakeholders are involved when implementing IT systems* (agreed 36%, undecided 41%, disagreed 23%); and *information systems are becoming more exposed to risk and breaches* (agreed 43%, undecided 40%, disagreed 17%). Chi-square tests were done on information management systems in a financial institution. Most of the scoring patterns are somewhat similar, proportionally.

From the in-depth interviews on this dimension, it is noted that there are technological systems used to protect information such as email alerts, passwords on computers, firewall technology and virus management technology. There are 38% of respondents who agreed to the statement in the questionnaire that information security forms part of the annual organizations budgeting, while 53% were undecided and 9% disagreed. The majority of respondents were in disagreement with Stewart (2012) who highlights that certain organizations who take information security into account when doing their financial budgeting increase the effectiveness of the spending for the organization, stakeholders and customers.

The majority of research participants were in disagreement with the sub-dimensions on the risk response and recovery in a financial institution, while two statements did not have a majority selection. Statements that did not have an outright majority selection are: *I reactively respond to information risks* (agreed 37%, undecided 30%, disagreed 33%); and *there are instances when I do not get notifications on information risks* (agreed 39%, undecided 26%, disagree 35%). Chi-square tests were done on information management preparedness in a financial institution. Most of the scoring patterns are somewhat similar, proportionally. From the in-depth interviews on this dimension, it is noted that line managers and the operational risk area gets notifications on information risks.

## Conclusion

This study reached several conclusions based on the empirical findings. Firstly, the results of the analysis conclude that there are big deficiencies for training officers to conduct beneficial information management

training at the organization. This training covers a number of different aspects of information management. This implies that all areas of the organization were under-skilled on various characteristics or aspects of information management which could have detrimental consequences for potential data breaches. This study recommends that skills development and training officers must conduct skills audits in relation to employees' knowledge of information management in order to create a centralized hub for training and skilling for this topic of information management. Furthermore, this will enable all employees across the organization to understand the implications of data breaches and what their responsibilities are to stop data breaches. This training needs to include how data breaches affect the economic condition of the organization, and employees should be trained on information management policies and procedures, as opposed to just making the policies available. Secondly, an information security program that includes business risk analysis is not implemented in this financial institution. This implies that there are no proper investigations and pre-work done by the organization to base future information management strategies on. It is recommended that the Data Governance Council (DGC) at the organization conducts business impact analysis in relation to information security in order to quantify risk management. This will further aid to achieve a comprehensive information security program whereby all breaches of information are assessed. This study recommends that the human resources department appoints a fraud or data breach investigator to investigate internal data breaches. The data breaches should be split into two areas. The first being accidental data breaches. Such accidental data breaches should be sent to skills development and training officers who can incorporate action items into their training to educate and up-skill employees on data breaches. The second area is where employees purposefully violate information policies and guidelines with the purpose of harmful intentions. Thirdly, a standardized or uniform house rule policy is not consistently implemented across the organization. This implies that each department or team within departments can decide not to apply any house rules, which could lead to data breaches. It is recommended that policy makers at the organization standardize policies to ensure these are applicable to all areas in the organization. This is more applicable to house rules such as clean desk policies. All line managers across the organization should ensure that all papers are removed and disposed of before employees end their shift. The clean desk policy should be part of the employees' tasks and, therefore, part of the organizational guidelines for all departments. Fourthly, the external cleaning company is not signing a Non-Disclosure Agreement with the organization. This implies that if external cleaning staff should

find customer information while cleaning, then, the cleaning company could possibly not be held liable if the information is used for fraudulent purposes.

It is further recommended that all external cleaning staff at the organization or the cleaning company sign a Non-Disclosure Agreement that states that all information found whilst cleaning is that of the financial institution and cannot be used by anyone else. This does not prevent fraudulent activity, but will give the financial institution in the study more legal leverage should fraud occur from this source. Fifthly, a project to protect information throughout its lifecycle is not to be implemented. This implies that information could be breached at various points of its lifecycle. Sixthly, employees are not regularly tested on information security policies. This implies that employees may not actually understand policies on security and this, therefore, increases the potential of data breaches. Further conclusions reached are that information security are not comprehensively budgeted for by all areas of the organization, but are done in silos by certain areas only. Better security management on $3^{rd}$ party customer data transfer should be implemented, and the IT area should benchmark its security systems against international practises and guidelines. Overall, the results of this study shed light on the key factors to be considered by organization in relation to information-related aspects and, therefore, provide a solid foundation for the organization to work off to improve the state of information management. Therefore, this study has improved the understanding of information management at the organization, as well as other similar organizations. The findings also contribute to the growing body of literature on information management in South Africa.

## Implications of the study

This study is the only one to provide recommendations that speaks to the specific needs of information management at the organization. It provides a bespoke study that looks at the shortfalls specific to the organization and, therefore, the findings and recommendations can be taken as is by senior management to formulate strategies on information management. Some of these factors identified in the study could be adopted by other organizations, as it enables people working with information management to understand various pitfalls of information management and, furthermore, corroborates previous literature.

## Limitations and guidelines for future research

There are some limitations to this study. The first limitation of the study is that the study set was limited to an organization operating in South Africa. Caution, therefore, needs to be taken when generalizing the results of the study. The second limitation is that only a few employees or respondents were in the employ of the organization in their current position for more

than 3 years, which might limit the generalizability of the results. Furthermore, the organization is a larger established institution; therefore, employees at smaller organizations may regard their security responsibilities as an additional duty than that of an established office, as depicted in the results of this study. Future researchers investigating the study of information management could expand the research into other areas of the private sector where data sharing practices have been implemented.

Furthermore, future researchers may want to implement a modelled framework for any of the dimen

sions discussed in this research in order to provide a generic step by step model that organizations can implement on information security. In addition, future researchers should consider linking risk factors to both causes and consequences. It is believed that the results of the current study should provide future researchers with the rationale to continue to investigate the process, program and systems of information management in organizations. This study was performed prior to the operative sections of POPI coming into effect, and it is recommended that an analysis similar to the one undertaken here should be performed once POPI becomes effective.

## References

1. Abu-Musa, A. (2010). Information security governance in Saudi organizations: an empirical study, *Information Management and Security*, 18 (4), pp. 226-276.
2. Al-Mukahal, H.M. & Alshare, K. (2015). An examination of factors that influence the number of information security violations in Qatari organizations, *Information and Security*, 23 (1), pp. 102-118.
3. Australian bureau of statistics. (2013). *Census and sample*.
4. Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information security compliance: An empirical study of rationality based beliefs and information security awareness, *Journal of Information security compliance*.
5. Burmeister, B. (2014). Pay attention to the Protection of Personal Information Bill, *Finweek*, p. 7.
6. Caldwell, F. (2008). Risk intelligence: Applying KM to information risk management, *Vine*, 38 (2), pp. 163-166.
7. Carr, W. & Kemmis, S. (1986). *Becoming Critical: Education, Knowledge and Action Research*. London: Falmer Press.
8. Chen, J., Pedrycz, W., Ma, L. & Wang, C. (2014). A new information security risk analysis method based on membership degree, *Kybernetes*, 43 (5), pp. 686-698.
9. Chigamba, C. & Fatoki, O. (2011). Factors Influencing the Choice of Commercial Banks by University Students in South Africa, *International Journal of Business and Management*, 6 (6), pp. 66-76.
10. Collin, C. (2009). Observations on the UK transformational government strategy relative to citizen data sharing and privacy, *Transforming Government: People, Process and Policy*, 3 (4), pp. 394-405.
11. Collins, J. & Hussey, R. (2009). *Business Research: A practical guide for undergraduate and postgraduate students*. 3rd ed. Hampshire, U.K. Palgrave Macmillan.
12. Cooper, D.R. & Schindler, P.S. (2003). *Business Research methods*. 8th ed. Boston: McGraw-Hill.
13. Cullen, R. (2009). Culture, identity and information privacy in the age of digital government, *Online Information Review Journal*, 33 (3), pp. 405-421.
14. D'Arcy, J. & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance, *Information Management and Computer Security*, 22 (5), pp. 474-489.
15. Department of Trade and Industry. (2009). *The Consumer Protection Act: Your guide to consumer rights and how to protect them*.
16. Duncan, A. (2015). *Hackers steal 1 billion personal data points – IBM*.
17. Fenz, S., Heurix, J., Neubauer, T. & Pechstein, F. (2014). Current challenges in information security risk management, *Information Management and Computer Security*, 22 (5), pp. 410-430.
18. Fisher, J.A. (2013). Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach, *William and Mary Business Law Review*, 4 (1), pp. 215-239.
19. Fourie, I. (2011). Personal information and reference management: Librarians increasing productivity, *Library Hi Tech*, 29 (2), pp. 387-393.
20. Fraenkel, J.R. & Wallen, N.E. (2000). *How to design and evaluate research in education*. London. McGraw Hill.
21. Gable, J. (2014). Principles for protecting information privacy, *Information Management Journal*, 48 (5), pp. 38-42.
22. Garrison, C.P. & Ncube, M. (2011). A longitudinal analysis of data breaches, *Information Management and Computer Security*, 19 (4), pp. 216-230.
23. Guba, E.G. (1990). *The paradigm dialog*. California. Sage.
24. Hagen, J.M. & Albrechtsen, E. (2009). Effects on employees' information security abilities by e-learning, *Information Management and Computer Security*, 17 (5), pp. 388-407.
25. Haneef, S., Riaz, T., Ramzan, M., Rana, M.A., Ishaq, H.M. & Karim, Y. (2012). Impact of Risk Management on Non-Performing Loans and Profitability of Banking Sector of Pakistan, *International Journal of Business and Social Science*, 3 (7), pp. 307-315.
26. Herath. T. & Rao, H.R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness, *Journal of Decision Support Systems*, 47, pp. 154-165.
27. Jianping, C. & Zhongwei, Y. (2009). The characteristics and enlightenment of legislation on financial privacy protection in the USA, *International Journal of Law and Management*, 51 (4), pp. 226-233.

28. Kieke, R.L. (2014). Recent data breach stresses the importance of effective privacy efforts, *Journal of Health Care Compliance*, 16 (1), pp. 45-50.
29. Kosciejew, M. (2014). Proposing a Charter of Personal Data Rights, *Information Management Journal*, 48 (3), pp. 27-31.
30. KPMG. (2013). *A practical response to POPI.*
31. Lacey, D. (2010). Understanding and transforming organizational security culture, *Information Management and Computer Security*, 18 (1), pp. 4-13.
32. Malhotra, A. & Malhotra, C.K. (2011). Evaluating Customer Information Breaches as Service Failures: An Event Study Approach, *Journal of Service Research*, 14 (1), pp. 44-59.
33. Malmir A. & Malmir, M. (2015). Government's civil liability towards individuals' privacy in cyberspace, *International Journal of Law and Management*, 57 (2), pp. 98-106.
34. Moghavvemi, S. & Salleh, N.A.M. (2014). Effect of precipitating events on information system adoption and use behaviour, *Journal of Enterprise Information Management*, 27 (5), pp. 599-622.
35. Morse, J. M., Barret, M., Mayan, M., Olson, K. & Spiers, J. (2002). Verification Strategies for Establishing Reliability and Validity in Qualitative Research, *Journal of Qualitative Methods*, 1 (2), pp. 13-22.
36. Nazimoglu, O. & Ozsen, Y. (2010). Analysis of risks dynamics in information technology service delivery. *Journal of Enterprise Information Management*, 23 (3), pp. 350-364.
37. Neelankavil, J.P. (2007). *International business research*. New York: Library of Congress Cataloging-in-Publication Data.
38. Nieuwenhuis, J. (2007). Qualitative research designs and data gathering techniques. In Maree, K. (ed). *First Steps in Research*, pp. 70-97. Pretoria: Van Schaik.
39. Pope, J.A. & Lowen, A.M. (2009). Marketing implications of privacy concerns in the US and Canada, *Direct Marketing: an international Journal*, 3 (4), pp. 301-326.
40. PWC. (2011). *The protection of personal information bill: The journey to implementation.*
41. Rooney, J. & Cuganesan, S. (2015). Leadership, governance and the mitigation of risk: a case.
42. South Africa. (2000). Promotion of Access to Information Act, No.2 of 2000.
43. South Africa. (2008). Consumer Protection Act, No. 68 of 2008.
44. South Africa. (2013). Protection of Personal Information Act, No.4 of 2013.
45. Stewart, A. (2012). Can spending on information security be justified – Evaluating the security spending decision from the perspective of a rational actor, *Information Management and Computer Security*, 20 (4), pp. 312-326. Study, *Managerial Auditing Journal*, 30 (2), pp. 132-159.
46. Sumanjeet, Dr. (2010). The state of e-commerce laws in India: a review of Information Technology Act, *International Journal of Law and Management*, 52 (4), pp. 265-282.
47. Thomson, K. & van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organisational behavior, *Information Management and Computer Security*, 20 (1), pp. 39-46.
48. Trochim, W.M.K. (2006). *Nonprobability sampling.*
49. Tsohou, A., Kokolakis, S., Lambrinoudakis, C. & Gritzalis, S. (2010). A security standards framework to facilitate best practices awareness and conformity, *Information Management and Computer Security*, 18 (5), pp. 350-365.
50. Willenweber, K., Jahner, S. & Krcmar, H. (2008). *Relational risk mitigation: The relationship approach to mitigating risks in business process outsourcing.*
51. Yin, R.K. (2011). *Qualitative research from start to finish*. New York: Guilford Press.
52. Young, L. (2010). Date Protection – Specification for a Personal Information Management System, *Records Management Journal*, 20 (1).
53. Zaman, M. (n.d). *Predictive Analytics: The Future of Business Intelligence.*
54. Zhang, J., Reithel, B.J. & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management and Computer Security*, 17 (4), pp. 330-340.
55. Zhou, L., Vasconcelos, A. & Nunes, M. (2008). Supporting decision making in risk management through an evidence-based information systems project risk checklist, *Information Management and Computer Security*, 16 (2), pp. 166-186.