Analysis of Information Security Breaches in Kumasi Metropolitan Assembly Ghana.

George Atta Frimpong

2019 Laurea

Laurea University of Applied Sciences

Analysis of Information Security Breaches in Kumasi Metropolitan Assembly Ghana

George Atta Frimpong
Degree Programme in Business Information Technology
Bachelor's Thesis
May, 2019

Laurea University of Applied Sciences
Information Technology
Bachelor's Thesis

Abstract

George Atta Frimpong

Analysis of Information Security breaches in Kumasi Metropolitan Assembly Ghana

Year 2019 Pages 34

The significance of Information Technology in the business world of today cannot be underestimated. It has great influence on daily business transactions; however, information security remains a huge concern for both users and businesses. The threat landscape of information security keeps growing, making it more complex than ever. Over-reliance on technological solutions alone cannot guarantee a secured information environment; the human aspects of information security should be given a thought. Many of the operations required to secure information assets are to some extent dependant on the human factor. This study analysed the cause of information security breaches within Kumasi Metropolitan Assembly, Ghana.

The case company has had a series of security breaches, which have affected its business operations. Hence the need to look in to the cause and address the challenge.

Professional literature and articles were reviewed to build the theoretical bases for the study. The theoretical bases cantered on securing information assets with policies and frameworks. Moreover, securing information systems requires user awareness of security measures, as well as the understanding of security breaches. The main themes used in the knowledge base included Securing Information Assets in an Organisation, Information Security Policy Basics, Guidelines and Procedures, Standards, Baselines, Frameworks, Information Security Awareness and Training

The research deployed mixed data collections methods, including both qualitative and quantitative data collection methods; the study analysed various security breaches as well as interviews carried out with the IT manager at the organisation. The results of the data analysis revealed that the organisation does not have a clear security monitoring and acceptable use policy on the use of external devices by employees. Again, staff lack the requisite skills and training to understand how information security works.

The results are of use to the organisation and other similar institutions who intend to understand the cause of information security breaches at the work place. The study will also help the practitioner in drafting security policies and designing training for employees.

Key words: Business Impact Analysis, Bring Your own Device, ISO/IEC 27001, Kumasi Metropolitan Assembly , Information Security Management Systems, Data security, Security breaches.

List of Abbreviations

BIA	Business Impact Analysis
BYOD	Bring Your own Device
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ISMS	Information Security Management Systems
IOT	Internet of Things
IT	Information Technology
KMA	Kumasi Metropolitan Assembly

Table of Contents

1. Introduction

The business society today thrives virtually on the internet for communication and operations in order to stay relevant. To compete and survive in this turbulent operating environment organisations both public and private continue to spend heavily in information systems. (Ifinedo 2007.) The data assets that are held in these systems are of importance to the survival of every business entity, hence they have become a major managerial priority for practitioners (Lee 2009). Information assets such as data, have brought a lot of significance to organisation and customers at large. To protect data assets held in information systems, organisation often deploy several mechanisms which includes security technologies such as intrusion detection systems for protection against data theft and other attacks. Firewalls for instance provides comprehensive monitoring and defence against data leaks. Other web-based technologies such as anti-phishing, anti-spyware, antivirus, anti-malware have all been deployed to protect businesses against internal and external attacks, but they are not an assurance of a secured environment for information (Safa 2015.)

Information security is a matter of concern in most organisation. It is an issue that can be described as complex in nature. The main aim of information security is to protect the confidentiality, integrity and availability of information. These are the fundamentals for securing information. Achieving this milestone has been a major challenge in recent times. Just installing security hardware devices is not enough to secure the network environment. In a Global security survey conducted in 2007 by Deloitte, the focus has shifted to the human factor of information security. The study stipulates that there is a growing concern about employee security weakness and they also cite the human factor as the root cause for information security failures. (Deloitte 2007.)

Threats from within are viewed as more dangerous than external threats (Willison and Siponen 2009). An insider's failure to comply with security policies could be very detrimental to the operations of the organisation. Schultz (2002) defines an Insider as any individual who works in an organisation and uses the authority granted him for illegitimate gain. In an attempt to gain access to a network, hackers usually target people rather than computers to gain access. Users or employee's inappropriate information security behaviours such as using personal information as passwords and user names, writing their passwords on sticky papers, sharing credentials with colleagues, opening unknown links and attachments are some of the unacceptable information security behaviours noted by Furnell and Clarke (2012). Accepted Information security behaviour should be merged with technological aspects to mitigate the risk of information security breaches. The idea of using multiple security approaches is very necessary in curbing risk (Safa et al. 2015).

Whenever there is an information security breach companies suffer loses and their reputation is significantly affected (Safa 2013). Studies have revealed that employee's information security awareness plays a pivotal role in mitigating risk connected to their behaviour in organisations (Arachchilage and Love 2014). In another study Kritzinger and Von Solms (2010) asserted that, information security policy awareness is key to policy adherence on the part of employees. The delivery methods and enforcement elements are vital in this regard. Information security awareness can be derived from employee's experience, which is the main drive to managing incidents. The ability to develop familiarity and skills stems from information security awareness. (Safa et al. 2015.) In this vein, concentrating on technical aspects of information security alone is not enough as it very unlikely that users may not follow all the stipulated technical aspects of information security. This situation could lead to a security breach. When users fail to adhere to information security standards and measures, its relevance is of no use (Siponen 2001, 26).

Similarly, effective information security measures demand that users become aware of and practice the policy instructions spelt out in the information security document designed by their organisation. Consequently, it becomes essential to develop, deploy and maintain an effective information security culture of awareness. Recent studies have proved that the establishment of an information security culture in an organisation is necessary for information security to be effective. (Elloff and Von Solms 2000.) Employees through a proper implementation of a culture of awareness can be become a security asset instead of risk. Information security knowledge sharing and experiences not only shape employee's involvement with information security issues but increases their level of knowledge and awareness on information security. This study seeks to analyse the cause of information security breaches within Kumasi Metropolitan Assembly which have been recorded over a period.

1.1 Background Information of KMA

Kumasi Metropolitan Assembly is located in the Kumasi metropolis, the second capital and business district in Ghana. The unique position of the city makes it accessible from all corners of the country. Being the second largest city with growth rate of about 5.4% annually, the city is ideal for business and KMA is tasked with the management of the activities in the city. The Assembly aims to provide Socio-economic services by mobilizing and utilizing human and financial resources to improve the lives of residents in the metropolis. (KMA archives 2018.)
The institution has 14 separate departments which is tasked with different core mandates. They are; Information Technology and Information Service, Waste Management, Environmental Health Unit, Planning, Urban Roads, Engineering Dept, Treasury, Budget, Public Relations Unit, Internal Audit, Estate Department, Town and Country Planning, Birth and Death Registry and Statistical Dept. (KMA archives 2018.)

All these departments together form the Kumasi Metropolitan Assembly (KMA). The Assembly is committed to improving the quality of life of the people in the metropolis through the provision of essential services and creation of an enabling environment to ensure a sustainable development of the city.
The assembly's duties and core mandate are backed by the local Government act of 1993, Act 462, section 10 of Ghana's constitution. The law states that "The Assembly shall be responsible for the overall development of the district and shall formulate and execute plans, programmes, and strategies for the effective mobilization of the resources necessary for the overall development of the district". To be able to achieve this goal KMA must manage the city through good governance, local economic development, tourism promotion, improved sanitation and social services.

Data Security plays a very important role in the daily activities of KMA. The company handles a lot of data including contracts, marriage records, birth and death data within the Kumasi metropolis. Since the company works with multiple parties their data has to be secured. IT managers within KMA have a major role to play to ensure information security policies are adhered to. Unfortunately, this has not been the case. Several security breaches have been recorded and it is posing risk to data security. It is on record that about 40 security breaches have been recorded which have significantly affected the business operations of Kumasi Metropolitan Assembly (KMA).

1.2 Research objective and scope

Organisations use various technological means to guard their information assets against security threats, but the successful mitigation or avoidance of threats and risks cannot be achieved without employee's involvement. Employees play key part in safeguarding information and technology assets, given this scenario the study aims at analysing the cause of information security violations recorded over a period within the organization. In addition, ISO/IEC 27001 standard document will be deployed in analysing security breaches. The secondary objective is to help practitioners in drafting and designing information security policies and trainings for employees.

2 Literature Review

2.1 Securing Information Assets in an Organisation

The secure flow of data across networks is very crucial to modern day business organisations, hence organisations information security management must address issues related to security and privacy with urgency. The main aim of information systems is to make access to an organisations network readily available when the need be, but this cannot be achieved without understanding the fundamentals of information security. Information security in this regard is explained as the process of securing network systems and information also referred to as data from possible attacks, threats and vulnerabilities. (Ioannisdis, Pym and Williams 2012.) Attacks and threats on information security systems can be deemed as deliberate or unintentional attempts to compromise the integrity, confidentiality and availability of data. (Savola 2014.) The security of Information systems needs a routine assessment for everyday business; therefore, information security professionals have the responsibility of designing security frameworks which serves as a guide in implementing security policies within an organisation. Again, frameworks offer deeper understanding of best security model practices (Susanto 2011).

Fuchs (2011) also identifies information systems security as securing data, networks and IT systems from unauthorized access. Organisations have a huge responsibility to protect data collected and stored on their systems from attacks, however, data credibility and confidentiality must be maintained throughout the process. (Ankita 2012.) Ankita et al. (2012) further explained that information security begins and ends with data accessibility, validity and secrecy. Meanwhile the dependence on technological innovations by businesses and organisations is on the increase but data security is a difficult task (Ankita et al. 2012). Data security

is a fundamental tool of modern-day business strategies. Businesses around the globe interconnect on a common market place via the internet. These business transactions have resulted in large sums of data being transmitted via a secured network to ensure data validity, availability and confidentiality. The introduction of advanced technological innovations such as Internet of things (IoT devices), have made business activities more simplified and introduced more opportunities and challenges. (Susanto et al. 2011.) However, Almunawar and Tuan (2011) points to the fact that business leaders have a big role to play in providing security measures that seeks to address security challenges introduced by advanced technology.

Network security was the main defence mechanism for computer systems against attacks and malicious activities (Dawson, Burrel, Rahim and Brewster 2010). According to Dawson et al. (2010) network security on its own has proven not to be enough to avoid threats and vulnerabilities. Dawson et al. (2010) further explained that information systems alone do not provide the needed security to secure data. Businesses become more vulnerable to threats and attacks if the right security measures are not properly applied. This calls for security professionals to understand how information systems work and responds to them accordingly.

Dawson et al. (2010) again, stressed on the importance of integrating information security vectors in to policies. The main aim of securing information systems is to provide security for data transmitted. The cost associated with data security compromise as well as the extent of vulnerabilities could be reduced through secured systems. (Dawson et al. 2010.) Offsetting data security against accessibility has continued to be a daunting task. The challenges of balancing the two continue to pose difficulties for businesses (Liao and Chueh 2012). Zissis et al. (2011) noted that today's businesses thrive in a technology driven environment where information have become vulnerable to attacks. The above-mentioned phenomenon is as a result of inefficient management (Liao et al. 2012). Liao and Chueh maintained that effective management of information security is a panacea to keeping security vulnerabilities at bay from within and outside the organisation. The main challenge of modern-day organisations is maintaining data availability to users and also ensuring the integrity and confidentiality of information.

2.2 Information Security Policy Basics

Information security policy is a universal term which refers to any document that entails elements of a security program which ensures organisational security goals and objectives are met. (Landoll 2016.) Information security policies are issued and approved by senior management of an organisation to streamline the overall security program, user behaviour and system controls. This is a mandatory policy and all actors at play such as users and all information systems must adhere to the policy statement. Information security policy document within the organisational are directed at different levels, spanning from the organisational level to users then programs and systems. (Barry et al. 2010.)

Fig 1: is an illustration of the different levels of information security policy document, namely, security program, user, system and organisational levels.

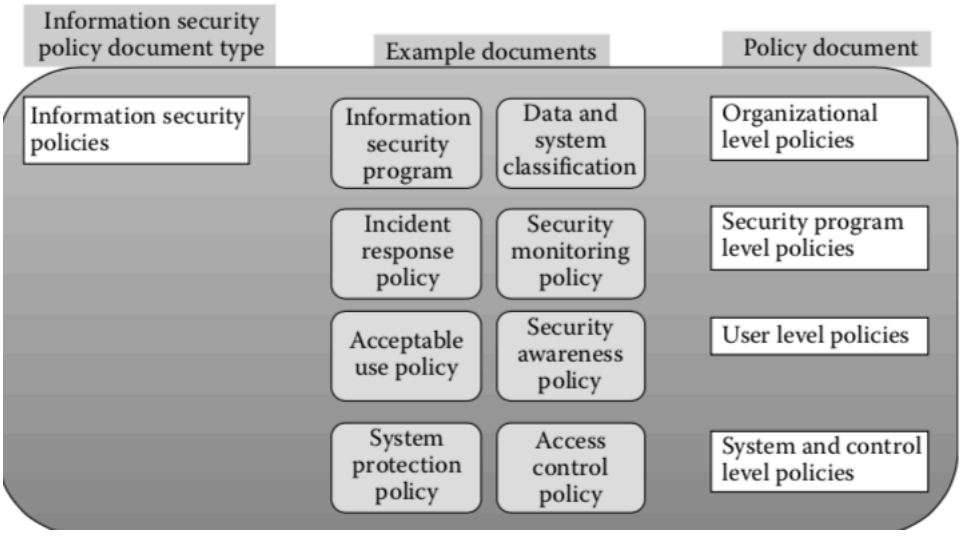

Fig 1: Information security policy levels (Barry 2010)

At the organisational level of information security, policy level elements such as overall information security program and data sensitivity are addressed. Senior management at the information security program policy stipulates the requirements of the information security program and assigns responsibilities and oversight controls. The classification of data and systems policy is defined by senior management into different levels. Depending on the sensitivity of data and criticality of the system, a classification is defined for both data and information systems. Within this level management establishes minimum controls for data sensitive. Minimum controls for sensitive data could be handling, labelling, transporting and destruction as well as the mode or medium by which information systems will be secured and managed.

2.3 Information Security Standards

Information security standards are a clarification of security requirements in information security policies that are geared towards improvements in selected, techniques and devices. (Thomas 2002.) The specified requirements spelt out in these standards makes them mandatory in information security policies (Douglas et al. 2016). The issuance of standards is the work of senior management as well as its approval. Sometimes these powers could be delegated to the information security officer or information security managers (Thomas et al. 2002).

Information security standards provides greater or much detailed explanation for information security policy level statements, the reason being that information security standards should have a direct relation with the information security policy statement. An information security standard may read as "For all password -based authentication, the organisation shall maintain all information systems enforce the following minimum parameter settings: 8 characters with both numeric and alphabetic characters, (b) password lifetime 90 days maximum, 1 day minimum". (Thomas et al. 2002.) These policy statements defined in the standards, sets out the mandatory requirements needed to maintain security within the organisation.

2.4 Information Security Guidelines and Procedures

Information security guidelines are clarifications of security requirements that are identified in information security policies. These identified requirements are selected techniques, devices and methods. Guidelines are not mandatory requirements as in the case of standards. Information security guidelines, when written should have a direct bearing to information security policy standards. An information security policy document such as system protection policy should have a corresponding policy guideline as system protection Guideline. Senior management or their delegates such an information security manager can issue and approve information security guidelines. (Barry et al 2010.)

2.5 Information Security Baselines

Information security baselines are mandatory benchmarks which specifies minimum security controls for a particular device or application. Security baselines ensures the effectiveness of a security control. A baseline could be a configuration baseline for operating systems and security settings. Baselines are normally large security settings and parameters as a result of known vulnerabilities within an application. As new vulnerabilities become known baselines are updated to meet new security requirements that seeks to mitigate security risks within an application or system. It is important for every organisation to create security baselines that specifies minimum security controls and settings for applications, devices and other areas within the organisation. (Barry et al 2010.)

2.6 Information Security Frameworks

Information security framework is a series of internationally recognised document which entails agreed and understood policies, procedures and processes that define how information is managed in a business. The policy framework can also be referred to as a template which is deployed while an organisation is in the process of developing an information security policy document. The security frameworks are for universal purposes and not company specific. It is used in conjunction with management practices to curb risk, vulnerability and increase confidence in an ever-connected world. (ISO/IEC 27002 2013.)

2.7 ISO 27000

ISO (International Organisation for Standardization) consist of standards that serves organisations with a standardized framework for information security policies and standard. ISO 27000 is a family of standards which are beneficial to organisations that seeks to protect information assets. The ISO 27000:2013 is a family of four series. They are ISO 27001:2013: Which entails the requirements for managing information security management system. ISO 27002:2013 being the second in the series consist of security code of practices. Third in the series is ISO 27003:2010, this is a guidance document for security management system during the implementation stages. The last in the series is ISO 27004:2009 it entails information security system measurements for analysis. (Karjalainen 2014.)

ISO 27001:2013 offers guidance principles in the management and establishment of information security management system. This standard adopts gradual approach to improving and maintaining information security at the management level. In applying this standard major consideration is looked at regarding the size and type of organisation. The document is generic in nature and offers wide and strategic adaptation during the implementation stage. The adaptation of this standard must be informed by an organisations business goals and needs. Indebt audit of an organisations information security risk is crucial in the selection of the most suitable standard and can be complimented with other policies with different options often referred to as extended control sets. The present state of security should inform the decision taken by the board and executive management on the policy selected, though the standard presents a variety of options. (ISO/IEC 2013.)

ISO 27002:2013 practically stipulates the code of practice and all other types of information security systems. (ISO/IEC 27002 2013.) This type standard is most appropriate to organisation that have had a complete assessment of their information security systems risks. Since the standard provides detailed guiding principles and recommendations it is best to first have a first-hand analysis of the security risk that exit before opting for this option. Organisations are not obliged to adopt the code of practice as a standard since it is only a guiding principle or guideline rather choose the most relevant that meets their needs. This standard is very crucial to every organisation that has information at its core of operations. (ISO/IEC 27002 2013.)

ISO 27003 is an implementation guide which aids organisation that chooses to implement the ISO 27000 standard. At the implementation stages of Information Security Management Systems development (ISMS) ISO 27003 is adopted to serve as a guideline during specification and design phases. ISO 27004 basically aids an organisation in the assessment of the initial phase of ISMS. Any organisation that implements ISMS has to evaluate the security standards and requirements to ascertain all security checks have been met. ISO 27003 helps in determining measurements and metrics with the aim of improving the effectiveness of ISMS. (ISO/IEC 2013.)

ISO 27000 is a family of standards which entails a comprehensive framework for the initiation and adaptation of security policies, controls and management of information systems. It is not obligatory for an organisation to adopt all the policies within the standards rather adopt them based their needs and business objectives. The standard embraces the different aspects or components that are suitable to an organisation’s information security. These controls are further applied in the development and implementation stage. ISO 27000 allows for continuous improvement in information security and offers deeper understanding by management in addressing the needs and objectives of the organisation.

2.8 Information Security Awareness and Training

Information Security management goes beyond hardware and software components, it is an end to end process which requires solution-oriented systems, policies and professionals. (Saxena 2010.) Data assets are crucial to modern day businesses and requires top notched security solutions to deal with every day threats (Btoush 2011). According to Btoush et al. (2011) threats to data assets are both technical and non-technical varying from social engineering attacks to sniffing of data. The lack of awareness on non-technical aspects of security accounts for a number of system and data breaches (Mittal 2010). Mital et al. 2010 explains human factor or human behaviour as a major pivot in security breaches within organisations. Information security breaches have a correlation with the man factor (human behaviour). Lacey (2010) further aligned organisational culture with human behaviour as a main pivot in information security implementation strategies. According to Lacey et al, information systems security breaches emanates from vulnerabilities in design flaws and lack of awareness on the part of employees. Awareness programs and information security initiatives tend to fail due to bad practices by employees and poor organisational structure and culture. The challenges posed by the above-mentioned factors can be reduced through reviews of problem areas and also through varying intervention strategies which seeks to develop, educate and promote change initiatives regarding information security breaches. Human factor cannot be ruled out when implementing security policies since it has the tendency to render security measures null and void. (Knapp and Ferrante 2012.)

Security policies which factors in employee behaviour and understanding level are very ideal in mitigating or reducing security breaches which has adverse effects on the organisation and computer systems. (Knapp et al. 2012.) Knapp and Ferrante further explained that information security policies should form the basis that seeks to direct and address expected employee behaviours. In the event of an unexpected behaviour, the policy must have recommended remedies spelt out in the document to address the challenge. Adopting security awareness program into the policy document is one sure way of curbing employees' attitudes and behaviours towards information security do's and don'ts. Security awareness programs must be designed to be more focused on communication and enforcement, then in this sense the human factor which is often neglected in information security consultations becomes part and parcel of information security policy. (Knapp and Ferrante et al. 2012.)

The advancement in IT solutions means more data is being transmitted every now and then but the security of these information assets is always in doubt. Sun (2011) noted that the security of information assets depends on the users or handlers of these assets. Sun cited the behaviour of users as the main obstacle to security. In this vain Kruger, Drevin, & Steyn (2010) views the human behaviour as critical to the overall success of information security implementation. The ability to handle and mitigate security risks is of great importance to the

safety of information assets. Hanersk and Lindström in 2011 studied security behaviours using the concept of discipline and agility. A security behaviour topology was used to identify behaviour patterns with regards to information security practices. It was revealed that discipline and agility shape the behavioural patterns of employees within an organisation. Indebt understanding of employee's behaviour and organisational culture helps policy makers to establish the mode with which behaviours affect security processes. It must be understood that organisational culture and employee behaviour are intertwined. They both need thorough understanding before a compromise could reached in making decisions on security policies.

One difficulty organisation face is reporting security breaches, Posey, Bennet and Roberts noted in 2011 that, organisation fear their reputation being damaged. Sometimes the consequences are so damning to an extent which is irreparable, but data security breaches occur on daily basis with some being intentional and others with malicious intent. The best way in dealing with this situation according Posey, Bennet and Roberts is continuous monitoring and vigilance by experts. They further indicated that best practices such as regular evaluation of internal activities is best at curbing security threats.

In another study, Hu, Dinev, Hart and Cooke in 2012 also stressed on employees within an organisation as the weakest link to corporate defences and information security. Organisations secure digital assets by implementing and developing security policies however, without widespread acceptance within the organisation, all the efforts will be a waste. These measures need to be accepted and put to use by employees. Failure on the part of employees to comply and adhere to information security could results in serious security breaches to information security assets. (Puhakainen & Siponen 2010.)

Employees have a role to play to ensure the success of information security strategies. Puhakainen and Siponen stressed on management putting measures in place to ensure employees understand security threats and the impact it has on the reputation of the organisation. When employees become aware of security measures, they tend to be more compliant hence the need for employee compliance is very critical.

Ensuring employee compliance with security policies is a big challenge; however, constant monitoring and auditing could help in addressing compliance issues and curb internal threats. (D'Arcy &Greene 2014.) Willison and Foster (2011) in their study indicated an omission which most policy makers ignore most of the time. Often internal threats or preferably insider threats are ignored, and more attention given to external ones. Insider threats are a serious concern and demand attention from professionals. Wolf, Haworth, and Pietron (2011) opined that end user awareness program is vital in mitigating security threats. An analysis of security awareness measures within the U.S federal law enforcement agencies shows a link between

security and end user behaviour (Wolf et al. 2011). The success of security awareness programs is largely dependent on employee willingness to learn and obey security policies (Wolf et al. 2011).

Given the increasing threats to information assets and advancement in intrusion technologies various security measures and initiatives such as user awareness programs have to be initiated to address emerging trends in security. Kruger et al (2010) expressed the need to focus on managerial information security awareness and corporate leadership in information security in the sense that effective awareness by managers improves on efficiency with regards to business and technology performance. Kruger further noted that equipping managers with security awareness skills helps in reducing security breaches amongst employees.

2.9 Information Security Breaches

The prevalence of new technologies has introduced new security challenges for organizations. Among these are Bring Your Own Device (BYOD) policies, social media and mobile devices. BYOD policies permit the use of employee's own devices to execute work which in the long run poses security challenges. In the event that these devices get hacked, stolen or misused, the company's information is put at risk. (Snell 2016.) BYOD policies is one main challenge to maintaining data security. The loss of a personal device containing a company's information could result in breached data (Prevoty 2015).

According to Denning and Denning (2016) failure to upgrade software often results in systems being compromised. Software's are susceptible to security breach hence the need to constantly upgrade them. Snell et al. 2016, noted that due to inadequate skills, some IT practitioners fail to educate their staff on software upgrades and security patches. This is practically human error which hackers usually exploit. Hershberger (2014) identified human errors as human vulnerabilities which attackers exploit. Adams and Makramalla (2015) identified human vulnerabilities to include but not limited to negligence, malicious employees and limited information security skills.

Human attitudes that makes information security more challenging involves opening spam emails, the utilization of weak passwords, opening malicious attachments and clicking unsecured links (Denning et al. 2016). Wikina (2014) asserts that, employees often lack the requisite skills to understand information security breaches. Wikina et al. (2014) further explained that employee carelessness or negligence is as a result of inadequate training. Often negli-

gence on the part of employees can lead to attacks such as malware, which are usually targeted at organizations. These attacks are very deceptive in nature. Victims are lured into opening fake messages that have trojans attached to it. It is unfortunate that employees lack the skills on what to do in such situations. Sherstobitoff (2008) is of the view that malware attacks are on the increase and targeted at organisations.

The up surge in information security breaches limits institutions capability of providing satisfactory services to consumers. Most security breaches happen as a result of stolen data and inadequate secured systems. Organisational leaders have to bring to the table impact-oriented security solutions that seeks to limit the damages organisations face as a results of security breaches. (Figg and Kam 2011.) Whenever there is a data breach, there is a shift in market valuation since potential investors react differently. The impact of data security breaches heavily rely on how the organisation handles the situation. Large organisations have difficulty addressing security breaches since they mostly deal with large volumes of data. IT leaders need to find a balance between data security breaches and investments (Fleming and Faye 2013).

The mitigation of security risks, threats and vulnerabilities requires investment in security solutions and expertise. The complex nature of information security needs essential tools to make institutions gain competitive edge. Proper and effective mitigating security strategies helps in reducing the overall cost of security. (Susanto et al. 2011.)

The Increasing number of security threats and the continuous reliance on technology requires organisations to put in place strategies that addresses and prevents attacks. In order to develop an effective security response, professionals have to detect and analyse data breaches and provide effective security response to curb incidents. Security solutions should be able to contain, eradicate and recover every compromised information (Hamm 2010).

Protecting user and corporate data has gained more prominence amid rigorous regulation being introduced. Gatzlaff and McCullough (2012) stated that corporate announcements on data breaches, government control and security standards have made safeguarding data assets a top concern among stake holders. Companies are not only required to make pronouncements on system security breaches but also pay damages. According to the General Data Protection Regulation, data compromises require organisations to pay a percentage of their annual turnover as fines. Compromised data must be brought to the publics notice since data breaches can result in financial losses, loss of sensitive data and trillions of private records. Data breaches does not only affect organisations but people whose personal information may have been stolen. (Ernst and Young 2001).

3 Research Methodology

This chapter discuss the methods and approaches used in conducting the research.

Data Collection Method

The study aimed at analysing the cause of information security breaches within Kumasi Metropolitan Assembly which have been recorded over a period. In the process, interviews have been conducted. Yin (2006) explained that case studies are used to determine how and why problems or situations occur. Case study methods presents a broad and meaningful understanding of situational events. The research methodology used are both quantitative and qualitative research methods. Data was collected via interviews and existing information security breach records. The method of data collection was chosen because it allows for an interpretive approach to collect and analyse data. Qualitative data collection approach provides an explanatory method to why certain phenomenon exists through interviews. Deploying mixed methods for data collection allows participants experiences and empirical data to be combined for reliable analysis and comparison.

Sampling Technique

The study exclusively focused on participants with insight on the subject under study. The sampling technique utilized is what Ma. Dolores (2007) describes as purposive sampling. Purposive sampling allows the researcher to select participants depending on their unique characteristics with respect to the subject under study. Purposive sampling is a non-probability sampling technique, the selection of participants solely lies on the researcher's case study and methodology. The technique is suitable for case study researches. It is important to note that the technique allows the researcher to identify participants who are most suitable to provide data which answers the research question. (C. Teddlie, F Yu 2007.) This technique is most suitable for this case study in the sense that participants needs to have more knowledge in the field been studied. Interviews were reduced to one participant being the head of Information Technology within the organisation. This was deemed appropriate because of his role and responsibilities within the company.

Data Analysis method

Data has been analysed using excel sheets, excel sheets allows for data mining and statistical analysis. Tools deployed for data analyses can be explained as gathering and summarizing the results obtained from the study. All data collected have been summed up and arranged in a manner that responds to the research objective; The cause of information security violations in the organisation. The main aim of the process is to arrive at an in-depth assessment of the themes and patterns that unfolds during interviews as well as analysing existing security breaches recorded by the company.

Reliability and Validity of Results

In case study researches, researchers collect multiple types of data to build up a concrete case for reliability and validity. The study sought for views of the IT manager regarding security breaches in the organization. This choice was made because the researcher was positive about the interviewee competence in answering the questions. Again, interview questions were made available days before the interview in order to give the manager time to understand the context of the interview. Based on this it can be said that the interview results and other data supplied by the company is valid and reliable.

The use of primary and secondary sources of data in the study reinforces validity and reliability. In order to arrive at credible conclusions and recommendations, all data collected were analysed. This approach gives room to eliminate any possible bias and minimize errors. In general, all findings, analysis, and conclusions are deemed valid and reliable.

4 Research Results

In this chapter the results emanating from the study have been presented and analysed.

4.1 Business Impact Analysis

The interview conducted sought to find answers on how the business operates its activities. It is important to understand how information is stored and processed within the organisation. The findings explore the business activities that could be exposed to security risks in the organisation. The IT manager at the firm indicated that the business relies heavily on some form of digital communication or service. He indicated that the company uses email addresses and the website for communication, whiles about half of customers details are stored electronically.

Figure 2 below illustrates the organisations reliance on information technology for business purposes.

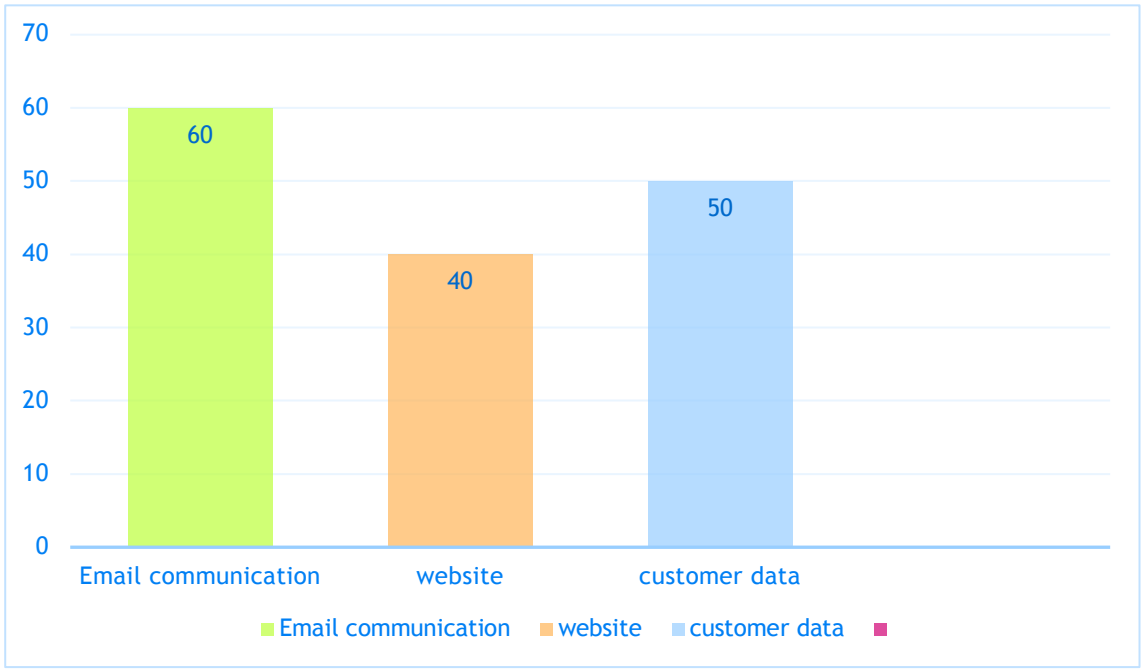

Figure 2: Medium of Communication and data at risk

The company uses emails and the website to communicate to a section of its customers and employees, but this practice is not widely used. About 60% of the company's communication is done via emails for communicating to partners and employees as well as customers. The company uses mainly postal mails to communicate to its customers in some situations. However, information posted on the company's website is very limited to just about 30% of their business operations. The website only highlights what the company is about and their operations. All transactions are done at the premises of the company. Again, storing of personal data on customers electronically forms only 50% of the data collected on customers. The remaining 50% is done manually. The safety of the data collected heavily lies on the mechanisms put in place and the employees handling them. It is worth noting that data stored electronically is exposed to risk and this is especially true with regards to the number of security breaches recorded within the organisation.

The interview again focused on how the organisation views information technology as a major core of their operations. The respondent indicates that the company has incorporated information technology into its core operations. Denoting the relationship between information technology and business in today's context, the organisation strives to meet its business demands. However, in meeting the day to day business challenges, the organisation allows the use of personal devices commonly termed as Bring Your Own Device (BYOD). BYOD is considered to be a major source of risk for businesses. This is as results of employees bringing in their own devices to execute business. Since there is no clear policy restricting the use of personal devices, the fundamental values of confidentiality, integrity and authenticity could be compromised with the use of BYOD. Confidentiality becomes compromised when unauthorized persons gain entry to access sensitive data which under normal circumstances is under restricted control. The use of personal devices which are insufficiently secured puts to risk the integrity of company data. Whenever personal devices are being used it is assumed that users are negligent, and their actions will harm business activities

Managing BYOD is more challenging because there are less technical measures that could be imposed on personal devices, besides the organisation doesn't have any policy covering use of personally owned devices for business. Maintaining high security standards should be the concern of every business which has information technology at its core of operations.

4.2 Information Security Awareness and Training

The study further identified how information security has been prioritized in KMA by senior management. The IT manager responded that Senior management view Information security as a priority but not a high priority, this is due to the cost involved. They see the cost involved as a barrier to improving on their information security. On average the company spends less than €8000 annually on information security investments and they are mainly invested in protecting customer data, assets, fraud,theft, staff and systems. The study also revealed that senior management is updated on the state of information security on annual bases.

The study sought further views on whether staff are trained to take up various roles regarding information security. The IT manager in a response stated the company lacked enough staff to handle various roles and responsibilities besides the few available do not have the requisite skills to handle various responsibilities. The respondent again stated that staff training has not been done for two years now citing budget constraints. In the past only IT staff and employees whose role involves information technology have been trained.

Fig 3 below is an illustration of the percentage of staff who undergo training

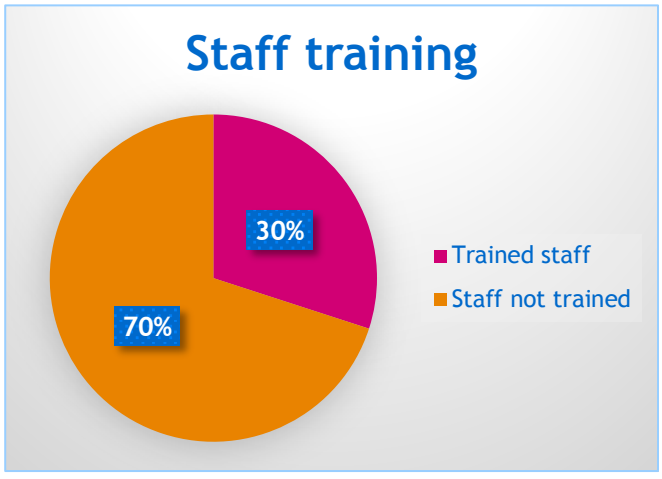

Figure 3: Staff training

The lack of training from the study can be linked to table 1 on page 24. A series of security breaches have been identified and a critical look at the table points to the of lack of understanding and knowledge of information security on the part of employees. Cases such as the

use of weak credentials reveals a lack of understanding with regards to secured passwords. It is required that strong credentials must be used at all times. Using weak credentials to login into systems is an information security risk. Four different cases of employees found to have been using weak credentials have been recorded. This among many other cases such as virus infections, spam emails and the use of unlicensed software could be attributed to the lack of education or training given to staff.

The company at the time of the study had an information security policy document but there are no clear specifications with regards to staff training. The document covers areas such as data classification, what can be stored on storage devices and what staff are permitted to do. With no clear sight on training initiatives within the document the study sought to find out why. Further probes revealed that barriers to staff training have become possible because there is the notion among management that induction training, irregular training and other forms of training deemed as mandatory can be ignored. Cost was another factor; management feels the cost involved in training personnel is too huge hence their unwillingness to train personnel on periodic bases.

4.3 **Incidents impacts and response**.

The study sought to analyse incidents recorded over a period and how they impact business activities within the organization. Only security breaches that have been accounted for are analysed in this study. Consistently the organization has experienced several security breaches over a period. At the time of interview, the company had recorded 41 incidents of security breaches spanning from 2014 to 2018. All recorded security breaches appear to run in cycle as to how they happen. They are attributed to employee negligence and lack of understanding in regard to information security handling.

Table 1 below shows the different types of security breaches recorded. The most commonly identified breach is virus infection followed by unauthorized access. The remaining other breaches were not quite often but their impact cannot be undermined. The IT manager at the firm identified virus infection and unauthorized access as the most disruptive breaches that affects the organization. Most of the virus infection were as a result of employees using unauthorized devices at the work premises. Devices includes usb drives, laptops, external hardrives etc. Employees sometimes also install unlicensed software's that comes with viruses that infects systems at the work place.

Table 1: Security breaches from 2014 - 2018

Type of incident	Number of Occurrence
Unauthorized access	12
Employees using weak credentials	4
Virus infections	15
Misaddressed email	4
Spam emails	3
Unlicensed software	2
Proprietary theft	1

(KMA archives, 2019)

Most of the incidents recorded were reported within a two-day period. In some cases, employees had complained about a corrupt file or virus infection and these disruptions have been identified within that period. In majority of the cases the IT personnel within the organization have identified the cases recorded. The findings show the lack of awareness on the part of personnel in the sense that most of the staff are particularly unaware or lack indebt

knowledge and understanding of information security threats and vulnerabilities. Incidents have not been reported right away and it took a while before it came to be noticed.

The most disruptive breaches being unauthorized access and virus infection were all recorded a day or two later. Having a dedicated person whose role is to handle security breaches will help in identifying security risks much faster. It has been very difficult pinpointing the exact cause of the top security incidents recorded due to the absence of a dedicated personnel to handle all these cases. The most suspected source has been attributed to the use of external devices and installation of third party or unlicensed software.

In responding to security breaches, the company at the time of interview did not have a clear contingency plan in place to handle cases. Cases were dealt with as they happen. Preventive actions have been updating antivirus software's and cautioning staff to desist from using staff computers for personal use. Formal training of staff has not been carried out for a period of time now, citing financial constraints.

Considering the extent of damage to business activities information gathered revealed that not all breaches have financial consequences or data loss. It varies depending on type of incident. Temporary loss of access to files is the most common effect and these are mainly due to virus infections. Even breaches that do not come with financial cost or data loss can still have an impact on business operations. The IT manager further revealed that irrespective of the security breach they have an impact, citing loss of revenue, complaints from customers, recovery cost, reputational damage and inconvenience at the work place as one of the negative impacts the company face. At the time of interview, the full cost of breaches could not be attained. In many cases some cost is not easily measurable, but it is estimated to cost hundreds of millions of dollars globally.

In contrast to ISO/IEC 27001 standards the organization failed to do the necessary risk analysis to ascertain the magnitude of security breaches alongside its financial cost. The standard requires organisations to establish a criterion for performing information security risk assessments and ensure that the risk assessment produces consistent, valid and comparable results. Again, the potential consequences after risk analysis must be identified and its magnitude properly assessed. Moreover, the identified risk should be analysed and prioritized for risk treatment. In all these aspects the company failed to follow the required guidelines and procedures hence their inability to do a proper risks assessment to find out the financial value of security breaches.

5 Summary recommendations

It is evident from the study that KMA as an organisation is not devoid of future security breaches. The recent security breaches and a lack of a clear policy guidelines on information security attest to this fact. However, it will be of great benefit for everyone at the organisation to assume that no system is secure. This would help in achieving the goal of risk minimization. As the study shows information security breaches is an on ongoing issue and the organisation must constantly enforce due diligence to monitor the situation.

While analysing the findings, some recommendations have been made to address the situation at hand:

BYOD Policy

The study showed that the use of BYOD or personal device have been a contributing factor to increasing virus attacks and unauthorized access to confidential information. There must be a clear Acceptable use and Security monitoring policy on the use of personal devices. This can range from monitoring as well as when and where it is appropriate to use the device. The policy should clearly specify what sort of devices are appropriate for instance jail broken devices or certain apps that compromise security should be made clear in the policy.

Password Guidelines

Use of strong passwords and keeping them confidential is highly recommended. Password is an important aspect of computer security. A weak password may result in a compromise of data security. A strong password should contain a mixture of both upper- and lower-case characters and at least eight alphanumeric characters long. Passwords should not be written on sticky notes or shared with any one.

Training

Constant training is key to building staff capacity on information security. Staff must be engaged in awareness training programs. Raising the awareness of staff on information security will help in spotting security breaches quickly without any delay. The study revealed that security incident normally takes a day or two for it to be reported. This affects business operations and causes delay. Regular trainings should be given a priority by management. Increased

support from senior management is very essential if the organization needs to improve on information security. Discussions on information security should be on the table at meetings and budget should be allocated to support training of staff.

Risk Handling

The principles of actions to address risks which have been outline in ISO/IEC 27001 standard have not been put to use by the organization. Management must follow the guidelines stipulated in ISO/IEC 27001 standard. A critical view of the risk approach deployed by the management does not fall in line with standards defined in ISO/IEC 27001 to address risk.

The standards state that in the planning of information security management system, the organization shall consider issues defined in the standards to determine risk and opportunities that's needs to be addressed. In the assessment of risk there must be a risk assessment criterion for assessing risk and also ensure the assessment produces valid and comparable results.

Again, risk owners must be identified and the realistic likelihood of occurrence of the risk outlined as well as its magnitude. While assessing the risk, a comparative analysis should be made, and the analysed risk prioritized. Taking into account the risk assessment results, the management team will select the appropriate treatment. In the meantime, it is clear the management of the organization did not take into account any of these measures, rather they handled risk as it occurs. No proper analysis has been made and the owners of risk were missing from their data. The way forward to handling risk is glare and proper actions or remediation must be adopted to prevent such happenings in the future.

6 Conclusions

The issue of information security has become a concern for the business. This fallout results from security breaches that significantly affects the business as well as customers. This study analysed the cause of ongoing information security breaches within the organisation. Analyses of security breaches from 2014 through to 2018 showed a variety of security breaches emerging from lack of understanding of information security among employees. There is the likelihood that the organisation will continue to experience security breaches studying the trend of the ongoing situation. It then becomes imperative for the organisation to equip employees with an understanding of basic information security principles. This will help protect customer data and that of the business. On the other hand, Management support for best Information security practices that seeks to reduce data security breaches seems to be on the low. Information security awareness must lead the fore front in curbing security breaches within the organization, much effort and resources should be channelled in providing training and supportive programs to sensitize information security awareness among employees. The study shows less support for training employees on information security awareness.

References

Printed sources

Adams, M., & Makramalla, M., 2015. Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review, 5*(1), 5-14.

Agarwal, A., 2012. Security enhancement scheme for image steganography using S-DES technique. *International journal of advanced research in computer science and software engineering*.

Arachchilage, N.A.G. and Love, S., 2014. Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, pp.304-312.

Btoush, M., Alarabeyat, A., ZBOON, M., RYATI, O., HASSAN, M. and AHMAD, S., 2011. INCREASING INFORMATION SECURITY INSIDE ORGANIZATIONS THROUGH AWARENESS LEARNING FOR EMPLOYEES. *Journal of Theoretical & Applied Information Technology*, *24*(2).

Caldwell, C., Zeltmann, S. and Griffin, K., 2012, July. BYOD (bring your own device). In *Competition forum* (Vol. 10, No. 2, p. 117). American Society for Competitiveness.

Cavusoglu, H., Mishra, B. and Raghunathan, S., 2009. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), pp.70-104.

D'Arcy, J. and Greene, G., 2014. Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, *22*(5), pp.474-489.

Dawson, M., Burrell, D.N., Rahim, E. and Brewster, S., 2010. EXAMINING THE ROLE OF THE CHIEF INFORMATION SECURITY OFFICER (CISO) & SECURITY PLAN. *Journal of Information Systems Technology & Planning*, *3*(6).

Denning, P. J., & Denning, D. E., 2016. Cybersecurity is harder than building bridges. *American Scientist*, *104*(3), 154-157. doi: 10.1511/2016.120.1

Deloitte. (2007). 2007 global security survey: The shifting security paradigm. 1-46.

Eloff, M.M. and von Solms, S.H., 2000. Information security management: a hierarchical framework for various approaches. *Computers & Security*, *19*(3), pp.243-256.
Figg, W.C. and Kam, H.J., 2011. Medical information security. *International Journal of Security (IJS)*, *5*(1), p.22.

Fleming, R.S. and Zhu, F.X., 2013. Meeting Service Level Challenges through Proactive Strategies. *Business Renaissance Quarterly*, *8*.

Foster, G. and Willison, D.J., 2011. Views on health information sharing and privacy from primary care practices using electronic medical records. *International journal of medical informatics*, *80*(2), pp.94-101.

Fuchs, L., Pernul, G. and Sandhu, R., 2011. Roles in information security–a survey and classification of the research area. *computers & security*, *30*(8), pp.748-769.

Furnell, S. and Clarke, N., 2012. Power to the people? The evolving recognition of human aspects of security. *computers & security*, *31*(8), pp.983-988.

Hamm, S.J., 2010. The role of the business press as an information intermediary. *Journal of Accounting Research*, *48*(1), pp.1-19.

Harnesk, D. and Lindström, J., 2011. Shaping security behaviour through discipline and agility: Implications for information security management. *Information Management & Computer Security*, *19*(4), pp.262-276.

Hershberger, P., 2014. Security skills assessment and training: The "make or break" critical security control. *SANS Institute InfoSec Reading Room*. Retrieved from https://www.sans.org/reading-room/whitepapers/leadership/security-skills-assessment-training-critical-security-control-break-o-35637

Hu, Q., Dinev, T., Hart, P. and Cooke, D., 2012. Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), pp.615-660.

Ifinedo, P., 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), pp.83-95.
International Organization for Standardization, 2013. *ISO/IEC 27001: 2013: Information Technology--Security Techniques--Information Security Management Systems--Requirements*. International Organization for Standardization.

Ioannidis, C., Pym, D. and Williams, J., 2012. Information security trade-offs and optimal patching policies. *European Journal of Operational Research*, *216*(2), pp.434-444.

Karjalainen, M., 2014. Developing an Information Security Management System.

Knapp, K.J. and Ferrante, C.J., 2012. Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations. *Journal of Management Policy and Practice*, *13*(5), pp.66-80.

Kritzinger, E. and von Solms, S.H., 2010. Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, *29*(8), pp.840-847.

Kruger, H., Drevin, L. and Steyn, T., 2010. A vocabulary test to assess information security awareness. *Information Management & Computer Security*, *18*(5), pp.316-327.

Kuo, R.Z. and Lee, G.G., 2009. KMS adoption: the effects of information quality. *Management Decision*, *47*(10), pp.1633-1651.

Lacey, D., 2010. Understanding and transforming organizational security culture. *Information Management & Computer Security*, *18*(1), pp.4-13.

Landoll, D., 2016. *Information Security Policies, Procedures, and Standards: A Practitioner's Reference*. Auerbach Publications.

Liao, K.H. and Chueh, H.E., 2012. Medical Organization Information Security Management Based on ISO27001 Information Security Standard. *JSW*, *7*(4), pp.792-797.

Mattord, H.J. and Whitman, M.E., 2006. Readings and cases in the management of information security.

Mittal, V., 2010. Customer engagement behaviour: theoretical foundations and research directions. *Journal of service research*, *13*(3), pp.253-266.
mployees to follow corporate security guidelines. *ICIS 2007 proceedings*, p.103.

Posey, C., Bennett, B., Roberts, T. and Lowry, P.B., 2011. When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security*, *7*(1), pp.24-47.

Puhakainen, P. and Siponen, M., 2010. Improving employees' compliance through information systems security training: an action research study. *MIS quarterly*, pp.757-778.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. and Herawan, T., 2015. Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, pp.65-78.

Savola, R.M. and Kylänpää, M., 2014, August. Security objectives, controls and metrics development for an Android smartphone application. In *2014 Information Security for South Africa* (pp. 1-8). IEEE.

Saxena, N., 2010, December. A comparative usability evaluation of traditional password managers. In *International Conference on Information Security and Cryptology* (pp. 233-251). Springer, Berlin, Heidelberg.

Schultz, M., 2002. The dynamics of organizational identity. *Human relations*, *55*(8), pp.989-1018.

Sherstobitoff, R., 2008. Anatomy of a data breach. *Information Security Journal: A Global Perspective*, *17*, 247-252. doi: 10.1080/19393550802529734

Siponen, M. and Willison, R., 2009. Information security management standards: Problems and solutions. *Information & Management*, *46*(5), pp.267-270.

Siponen, M.T., 2001. Five dimensions of information security awareness. *SIGCAS Computers and Society*, *31*(2), pp.24-29.
Sun, J., Ahluwalia, P. and Koong, K.S., 2011. The more secure the better? A study of information security readiness. *Industrial Management & Data Systems*, *111*(4), pp.570-588.

Snell, E. (2016, May). HR and IT joining forces against cyberattacks. *Benefits Magazine, 53*(5), 20-25.

Susanto12, H., Almunawar, M.N. and Tuan, Y.C., 2011. Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS*, *11*(5), pp.23-29.

Tallon, P.P., 2007. A process-oriented perspective on the alignment of information technology and business strategy. *Journal of Management Information Systems*, *24*(3), pp.227-268.

Teddlie, C. and Yu, F., 2007. Mixed methods sampling: A typology with examples. *Journal of mixed methods research*, *1*(1), pp.77-100.

Thomas, P.R., 2016. *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. Auerbach Publications.

Tongco, Ma Dolores C., 2007. "Purposive sampling as a tool for informant selection." *Ethnobotany Research and applications* 5: 147-158.

Wikina, S. B., 2014. What caused the breach? An examination of use of information technology and health data breaches. *Perspectives in Health Information Management*, 1-16.

Williams, B.L., 2013. *Information Security Policy Development for Compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2. 0, and AUP V5. 0*. Auerbach Publications.

Wolf, M.J., Haworth, D. and Pietron, L., 2011. *Measuring an information security awareness program*. University of Nebraska at Omaha.

Yin, R.K., 2006. Case study methods. *Handbook of complementary methods in education research*, *3*, pp.111-122.

Zissis, D. and Lekkas, D., 2012. Is cloud computing finally beginning to mature? *International Journal of Cloud Computing and Services Science*, *1*(4), p.172.

Electronic sources

(https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101

kma.gov.gh retrieved 2018.11.20

https://www.isaca.org/Pages/default.aspx?cid=1210053&Appeal=SEM&gclid=EAIaIQob-ChMIyOmwxoPZ4AIVw6SaCh0NJASuEAAYASAAEgLazvD_BwE&gclsrc=aw.ds Retrieved 2019.2.6

https://cours.etsmtl.ca/gti619/documents/divers/CSIsurvey2010.pdf

Retrieved 2018.10.13

Prevoty, Inc. (2015). The impact of security on application development: 2015 survey report. Retrieved from http://info.prevoty.com/impact-of-security-on-agile-development-report. Retrieved 2019. 20.3

Unpublished sources

KMA archives, 2018.

Figures

Tables