International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Factors Affecting Adoption of Information Security Management Systems: A Theoretical Review

CPA. Philip K. Kiilu[1], Dr. David M. Nzuki[2]

[1, 2]Kenyatta University, Nairobi, Kenya

Abstract: ***In the last two decades, Information Technology has emerged in the world affecting our personal, social and public life and has made a significant impact on the quality of life. It handles data and information represented in digital, text, image, graphics or voice media and deals with communication, storage, processing, and printing or exhibition in the manner desired by users. It is an outcome of the advances in telecommunication and computer technology [1]. As a result all sectors of economy have not been left behind in Information Technology adoption since information systems offer significant cost benefits, time savings, productivity gains and process re-engineering opportunities associated with the use of data warehouse for information processing. The amount of sensitive data, customers, market demands and new technologies force the use of sophisticated IT solutions and constant development in this area. The growing infrastructure is becoming more and more complex. This usually invisible infrastructure is the very complex technology system that every function within every organization is built upon; from assessing loan applications to detecting money laundering, to making payments into accounts, provision of government services to manufacturing and Insurance. Simply put, when this technology does not work, the businesses do not work. Such problems are causing huge losses to the economy. For example, in 2012, millions of Royal Bank of Scotland customers were affected by problems with online banking and payments after a software upgrade went wrong. This happened for three hours on a Monday, one of the busiest online shopping days of the year in the US. As it was described, "that cost the bank 175 million pounds (286 million dollars) in compensation for customers and extra payments to staff after the bank opened branches for longer in response" [REUTERS, 2013].***

Keywords: Information System Security (ISS), Information Technology (IT),Information Security Management System (ISMS), Technology Acceptance Model(TAM),Critical Success Factors (CSF),Information Technology(IT)

1. Background of the Study

The development of information security policies, standards, procedures, and guidelines is only the beginning of an effective Information Security Program. A strong Information Security architecture will be rendered less effective if there is no process in place to make certain that the employees are made aware of their rights and responsibilities with regard to organization information assets.[2]

According to the Kenya Cyber Security Report [3]; Achieving Enterprise Cyber Resilience through Situational Awareness, 2015, in 2012, many organisations were focused only on what security tools they should buy. This traditional approach focused on technology and point solutions that were not effective. The top three methods used by Cyber criminals were Key loggers, stealing of passwords and ATM skimming. In comparison, 2015, the top three were Ransomware, Database Transaction manipulation and Social Engineering.

2. Statement of the Problem

With the ever increasing demand for technological innovation, and adoption of Information Systems, users continue to be vulnerable and exposed to Information System Security threats. With a growing population of internal and external users accessing an increasing number of applications, the need has grown exponentially for organizations to develop a new generation of security tools that can help them better comply with regulations, control access to confidential data and limit identity theft. At the same time, organizations are challenged to institute security measures that satisfy users who are demanding both stronger security and ease of use and control; often competing priorities.

This study intends to look into the factors affecting Information Security Systems adoption in organizations.

3. Objectives of the Study

1) To find out factors affecting adoption of Information System in organizations.
2) To find out the trend of Information System Security adoption in organisations.
3) To elucidate on the ever changing Information Security environment and enable organizations make informed Information Risk Management decisions.

4. Empirical Review

According to a Kenya Cyber Security Report survey in 2015 [3], 99% of the respondents believe Information security threats are here to stay but are solvable, 64% of the respondents have not implemented regular employee awareness and training while 35% do not utilise security testing tools and only 24% use vulnerability scanning and penetration testing tools.

According to Paula[4], Wycliffe Momanyi, Chief Information Security Officer, Kenya Commercial Bank Group, agrees that while vulnerabilities in software and network constitute the target of information security breaches, and defending these resources remain the focus of every organisation, the weakest link continues to be the user/people. This resonates with the 2007 Global Security

Survey by Delotte Touche Tohmatsu, 'The greatest root cause of external breaches continues to be human factor'. Organizations have made efforts towards educating their clients including providing information on their internet portals though in the face of targeted attack, these efforts are proving inadequate.

In fact, social media platforms such as Facebook, google plus, twitter, Instagram, WhatsApp, cafe mom, Gather among many others have created environment for attackers to mine more information from the end users. This information in turn is used to make a user believe that he/she is communicating with a legitimate source. There is a risky tendency of social media users sharing their information on the social media.

Insider fraud is another major contributor to information systems insecurity giving all information and security practionersa headache. Due to the nature of the systems environment, some employees are assigned privileged access to various systems making it easier to carry out cyber-crime since they are familiar with the systems, security devices and the procedures in place.

Vlasta Svatá and Martin Fleischmann in their publication Is/It risk management in banking industry [11]say the current financial crisis may be regarded as an opportunity to correct certain aspects of financial systems, namely those that had led to it.Thus all is not lost in Information Security systems management, organizations should understand the core problems of risk management and, at the same time, choose the most appropriate framework to resolve these problems.

Information Security Management System (ISMS)
According to ISO/IEC 27001:2013, ISMS is a systematic approach to manging sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. Organizations, their information systems and networks are exposed to security threats such as fraud, espionage, fire, floods and sabotage from a wide range of sources. There is need to look into information systems holistically and have the right information systems security management in place. (ISO/IEC 27001:2005)

5. A Review of Information Security Management System Theories

Theory of Critical Success Factors

Critical Success Factors are the limited number of areas in which satisfactory results will ensure successful competitive performance for the individual, department and organization [15] Critical Success Factors are the few key areas where things must be right for the business to flourish and for the managers' goals to be attained. The identification of Critical Success Factors (CSFs) can bridge the gap between literature and practice in the field of Information Security Management (ISM)[12].One of the key influential practical guideline is the Standard of Good Practice for Information Security that points out some Critical Success Factors of successful ISM (ISO 27001). ISO/IEC 27001:2013 (ISO 27001) is an international standard that describes best practice for an Information Security Management System (ISMS). The accreditationof ISO 27001certification demonstrates that an organisation is following international information security best practices.

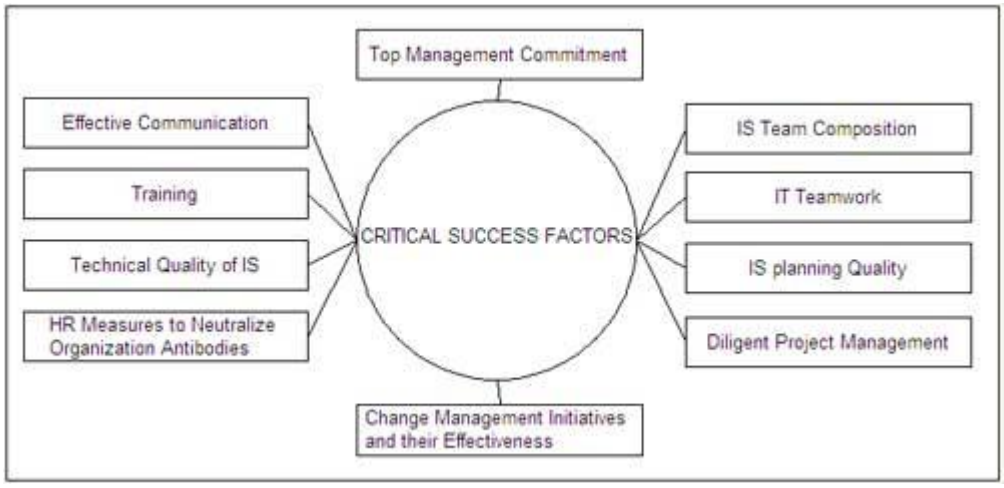

Figure1.2: Theory of Critical Success Factors

The Six Key Information Security Policy Components (Critical Success Factors) (ISO-27002, 2005, p. 5)

1) A definition of information security, its overall objectives, scope and the importance of Information security as an enabling mechanism for information sharing.
2) A statement of managements intent, supporting the goals and principles of Information Systems Security in line with the business strategy and objectives.
3) A framework for setting control objectives and controls, including the structure of risk assessment and risk management.
4) A brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including: compliance with legislative, regulatory, and contractual requirements security education.

5) A definition of general and specific responsibilities for information security management, which include reporting information security incidents.
6) References to documentation which may support the policy, e.g.The adoption of more detailed security policies and procedures for specific information systems or security rules with which users should comply.

Technology Acceptance Model (TAM)
A theory of innovation developed by Davis,Bagozzi & Warshaw (1989) in which the main elements are :
a) Perceived usefulness;
b) Perceived ease of use;
c) Attitude toward using technology and
d) Behavioural intention.

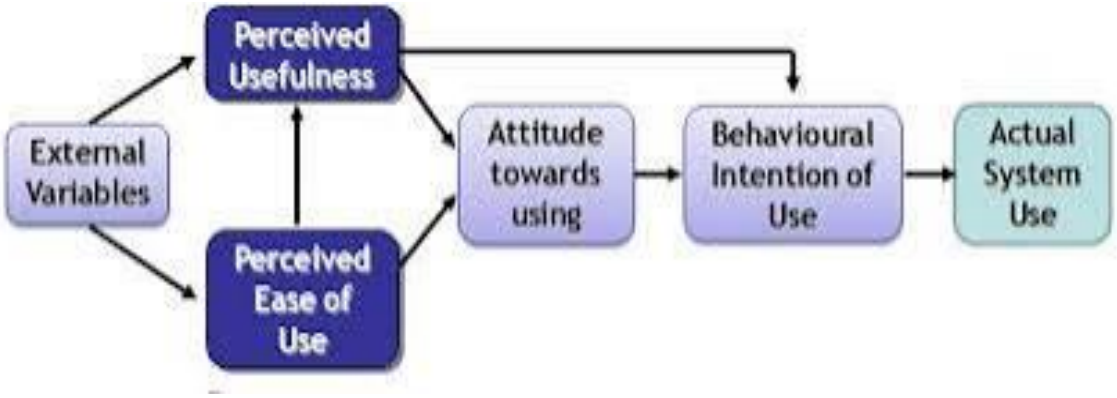

Figure 2.1: TAM Model: How users come to accept and use technology

6. Information Security Management adoption in Organizations

A Kenya Cyber Security Report survey in 2015[3] inspected network traffic inside a representation of Kenyan organizations. The organisation's goal was to find out whether there are malicious threats hiding inside the organisations information systems infrastructure that current information security solutions or practices do not detect or prevent. This study found out that in all organizations, malicious traffic reached the end-user computers and was able to bypass the current network solutions.68% of attacks were customized malware, at least 2 infrastructure devices (servers) were infected in all organizations, there was an average of 15 infected end-user computers sending loots of traffic to malicious hosts and all organizations were exposed to malicious software that had penetrated their perimeter security.

An effective Information Security Management System encompasses a layering of multiple solutions focusing on people, process, technology and risk. The key note here is the management of each layer should be based on its context among the diverse capabilities and limitations of others. When all the layers are combined, it creates a powerful tool that can offer organizations a much more successful way to manage their information security challenges than any single stand-alone solution.

Organizations still face a lot of challenges in implementing Information Security Systems though a considerable effort has been demonstrated. According to Taiwo Longe (Chief Information Security Officer, Central Bank of Nigeria)[13] on implementing ISS for the bank, "It was definitely a challenging process however, due to top management commitment and support, staff cooperation and participation, and of course the unrelenting effort of the ISMS Secretariat, the Bank stood as one entity and overcame this challenging task." ISO/IEC 27001 Information Security Management, BSI Case Study Central Bank of Nigeria, Nigeria. Also in the same project John Ayoh, Director Information Technology Department, CBN explains: "For this phase of the Information Security Program, we will definitely say that we have achieved our immediate objective of establishing the Information Security Management System. However, we do recognise that the onus is on us to ensure a continuous improvement process; the effort is still on-going to guarantee that the ISMS is adequately maintained and sustained." Implementing ISO 27001 helped CBN establish a leadership position as financial regulators not just at the national level but at the international level. It also gives CBN's stakeholders a level of assurance in knowing that controls have been implemented in ensuring the safety and security of their information assets.

7. Information Security Framework in Organizations

According to Governor Andrew M. Cuomo, in his publication *[16]*,nearly all institutions—almost 90%—reported having an information security framework in place that includes what are considered to be the key pillars of such programs: (1) a written information security policy, (2) security awareness education and employee training, (3) risk management of cyber-risk, inclusive of identification of key risks and trends, (4) information security audits, and (5) incident monitoring and reporting. However, information security frameworks at medium and large institutions tend to be particularly well developed, with 89% and 98%, respectively, having implemented all five pillars. Large institutions, however, are also more likely to have additional features integrated into their information security frameworks, such as a comprehensive communications plan to respond to inquiries in the event of a breach.

Approximately 84% of all institutions have a designated communications officer for responding to inquiries subsequent to a cyber-security breach. Large institutions, however, are more likely than small and medium institutions

to have a communication plan for addressing stakeholders that may be impacted by a cyber-security breach. Nearly 83% of large institutions have such a plan, as compared to two-thirds (65%) of small and medium institutions.

8. Emerging challenges in Information System Security Management

With the ever dynamic information systems environment, various challenges have emerged in therecent past.

1) **Insider Threats. (The enemy within)**
   According to the Kenya Cyber Report, 2015, 80% of system related fraud in 2015 was perpetrated by employees and other insiders. There are increasing cases of privileged user interrogating the system since they are familiar with it for various reasons such as disgruntlement, revenge and financial gain.
2) **Emerging technologies and Enterprise Resource Planning (ERP) adoption.**
   Emerging technologies and social media are providing ideal platform for Information Systems breach. More often than not, users are tempted to share private information on social networks not thinking of how such information can be used against them. Almost all organizations in spite of the industry in which they operate, are or have recently adopted ERP in order to achieve a competitive edge and serve their clients better. ERPs have numerous benefits but at the same time expose the organization jewels (data) since they are interfaced with other core systems.
3) **Inadequate Budgets and Lack of top management support**
   Most organizations to do dedicate adequate financial resources to Information Security Solutions.Infact, they wait until a breach is experienced, then funds are now allocated.
4) **Security Awareness Training**
   Most organisations spend their big Information Systems financial allocations strengthening the core systems. This not leaves the end users untrained, uninformed and unmonitored but also exposes the organizations to cyber-attacks.
5) **Data Exfiltration/Extrusion**
   The unauthorized copying, transfer or retrieval of data from computers or servers is another challenge. Common with privileged users or cyber criminals or use of BYOD (Bring Your Own Device).Large volumes of data may be leaked costing the organization a fortune.
6) **Poor Identity and Access Management**
   Identity and access processes are not well adopted in organisations exposing them to security breach leading unauthorised and inappropriate information access. Thus Logical Access Management is key in order to safeguard information.
7) **Government legislation and industry regulations**
   The enforcement of Information Security Policies and procedures relies on the government, political will of decision makers and industry legislations. It is of paramount importance to have both in place. Developing nations in particular have a challenge the government legislations where even the legislators are either not IT informed or IT experienced to the right legislations in place.

Key points to note on Information Security Management

1) Information security is a significant boardroom issue that executives need to understand to conduct business electronically.
2) Security incidents have grown from minor annoyances to significant issues with billion dollar impacts.
3) Electronic commerce has created new channels for conducting business that relies upon an effective information security program to gain the trust of customers.
4) Security incidents will continue to grow in speed, complexity, and business impact.
5) The information security market is immature, and complete solutions may not exist today.
6) Government and industry legislation will continue to evolve in an effort to protect consumers and enterprises that conduct more of their business electronical

9. Methodology

This theoretical review looks at the Factors affecting Adoption of Information Security Systems in general across different organisations in different sectors of the economy. The researcher reviewed past related studies in order to arrive at the conclusion.

10. Conclusion

Based on the discussions above, it is evident that adoption of Information Security Systems is looked at as a quite complex task within organisations. Nevertheless, itis key in protecting one of the organisation's valued and key resource, Information. It requires discipline, proper documentation, and adequate budget, enforcement of policies and procedures and deployment of the right personnel.

Organizations are encouraged to adopt Information Security standards which provide adequate guidelines on Information Systems Security including the framework which can adopted.

The Information risk space keeps on mutating therefore it's the full responsibility of organization managers to be on the lookout of emerging IS threats and have mitigation measures in place.

References

[1] James A O' Brien and George M. Marakas, 2006, 7th Edition, Management Information Systems.
[2] Thomas R. Peltier, CISSP, CISM,May/June 2005, Implementing an Information Security Awareness Program.
[3] Kenya Cyber Security Report; Achieving Enterprise Cyber Resilience through Situational Awareness, 2015.
[4] Paula Musuva Kigen et al, Kenya Cyber Security Report, 2015, p24

[5] Dr.Kodukula Subrahmanyam et al,Apr 2014, Information Security and Risk Management for Banking System, volume 10 number 3
[6] Catharine Lemieux, 2003 ,Network Vulnerabilities and Risks in the Retail Payment System Emerging Issues Series, Supervision and Regulation Department Federal Reserve Bank of Chicago August (S&R-2003-1F)
[7] KarolinaPilarczyk,2016, Importance of Management Information System in Banking Sector.
[8] Magutu, Peterson Obara, et al,2011 E-Commerce Products and Services in the Banking Industry.
[9] Ames M. Ashfield, SVP, and David Shroyer, SVP,2009, E-Commerce Products, Bank of America.
[10] Paula Musuva Kigen et al,2015, Kenya Cyber Security Report : Achieving Enterprise Cyber Resilience Through Situational Awareness.
[11] Vlasta Svatá and Martin Fleischmann,, 2011 IS/IT Risk Managementin Banking Industry.
[12] Tu et al,2014,Critical Success Factors Analysis on Effective Information Security Management: A Literature Review.
[13] Central Bank of Nigeria,ISO/IEC 27001, 2015, Information Security Management, BSI Case Study Central Bank of Nigeria, Nigeria.
[14] Price Waterhouse Coopers,May 2014,The cyber threat to banking, A global industry challenge.
[15] Christine V. Bullen & John F. Rockart, June, 1981,A Primer on Critical Success Factors.
[16] Governor Andrew M. Cuomo, 2014, Report on Cyber Security in the Banking Sector ,New York State.
[17] eenan, P. B. (2003) "Spatial Decision Support Systems," in M. Mora, G. Forgionne, and J. N. D. Gupta (Eds.)
[18] Decision Making Support Systems: Achievements and challenges for the New Decade
[19] Keenan, P. B. (2003) "Spatial Decision Support Systems," in M. Mora, G. Forgionne, and J. N. D. Gupta (Eds.)
[20] Decision Making Support Systems: Achievements and challenges for the New Decad