ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 12, Issue, 01, pp.9854-9859, January, 2020

DOI: https://doi.org/10.24941/ijcr.37470.01.2020

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

SECURITY GUARANTEE OF E -COMMERCE PAYMENT SYSTEM IN NIGERIA

[1,*]Chijioke, I. A., [2]Prof. H. C. Inyama, and [3]Dr. Onyesolu, M. O.

[1]Department of Computer Science, Federal Polytechnic, Oko
[2]Electronics and Computer Engineering Department, Nnamdi Azikiwe University Awka
[3]Department of Computer science, Nnamdi Azikiwe University Awka, Nigeria

ARTICLE INFO

Article History:
Received 04th October, 2019
Received in revised form
20th November, 2019
Accepted 19th December, 2019
Published online 30th January, 2020

Key Words:

E-Commerce System Security, E-Commerce Security Threats, Cyber-Attacks and Security, CIA Triad, E-Commerce Security Function, Vulnerabilities and Risks.

ABSTRACT

With the enormous rise in social media users globally, e-commerce payment systems are becoming ubiquitous, being applied rapidly in all facets of life. However, securing e-commerce payment systems have become more complex and have further made the CIA triad: confidentiality, integrity, and availability of enterprise's data insecure, and prone to breaches and fraudulent activities. Securing enterprise e-commerce payment system is of paramount importance. An important facet of implementing e-commerce payment system in an organization is the development of security related issues within the enterprise information systems for the organization processes. In this study, the Enterprise Information Systems (EIS) security conceptual framework was adopted that comprised: security policy, security awareness, access control, and top level management support. A narrative review of prior research that focused on vast works of literature that revealed significant information on our conceptual framework and existing systems on e-commerce payment systems security, analysis and synthesis was adopted. The authors also extracted peer-reviewed articles within the last five years from electronic databases, using some keywords such as "e-commerce system security", "e-commerce security threats", "cyber-attacks and security", etc. Findings of the study show that breaches and fraudulent activities exist that may be perpetrated against e-commerce payment systems such as Skimming attacks, phishing attack, hacking, and physical attack, etc. Also, systems strategies that guarantee e-commerce payment systems security exist within the implementation of procedures, policies, resources, and operations to mitigate certain e-commerce payment systems security threats, vulnerabilities, and risks. Result from this study may bring trust and enhance e-commerce payment system adoption rate, new innovation and influence that may advance and guarantee e-commerce payment systems security innovations in Nigeria.

Citation: ***Chijioke, I. A., Prof. H. C. Inyama, and Dr. Onyesolu, M. O.*** **2020.** "Security Guarantee of e -Commerce Payment System in Nigeria", *International Journal of Current Research*, 12, (01), 9854-9859.

INTRODUCTION

The need for secure e-commerce payment system technological innovations has become increasingly evident and significantly important in developing countries, especially in Nigeria, where internet services, computerized systems, and information infrastructure play critical roles in the society. E-commerce technological innovations have significant importance, especially in the financial and banking sectors (Nasir, Wu, Yago, & Li, 2015), and has positively affected financial institutions, especially in time-saving and service delivery. The emergence of e-commerce payment systems also has created a much global impact in terms of usage rate, with its global reach to tens of millions of users (Nasir, et al., 2015).

Corresponding author: **Chijioke, I. A.,**
Department of Computer Science, Federal Polytechnic, Oko.

Information Technology (IT) has brought with it e-commerce self-service products and services and other technology-driven products and services such as internet banking, telephone banking, mobile banking, and e-commerce payment systems (Adjei, 2015; Aguboshim, 2019). Also, the rapid IT impact on e-commerce payment systems was accompanied by a corresponding rise in network security breaches resulting in big losses to the enterprise information and data (Bamrara, Singh, & Bhatt, 2013). The numerous opportunities in the e-commerce payment systems also brought with it fierce security challenges (Nasir, et al., 2015). Technology, though complex and modern, has become enablers of enablers, making people rely extensively on technology. These technologies are enabled in a complex interconnectivity platform that seemingly opened up avenues for theft, fraud and other forms of security threats by offenders who might even come from within the organization (Bamrara, et al., 2013). E-commerce has been predicted to be one of the major drivers of economic growth for developing countries (Nasir, et al., 2015).

This is because e-commerce plays a significant role in its contribution to the national economy in terms of the wealth created and the number of people employed within its services. In the past, organizations have implemented information security systems for securing e-commerce payment systems in their business processes. These information security systems have now evolved into what is more commonly known as Enterprise Information Systems (EIS) (Chaudhry, Chaudhry, Reese, & Jones, 2012). As a result of these complex security risks, the need for EIS security to protect e-commerce payment systems and data becomes more relevant (Allassani, 2014). Enterprise information system security can provide technical solutions in the form of intrusion detection systems, anti-virus software, firewall systems, and cryptology (Allassani, 2014). In addition, the behavior and activities of their employees are influenced and managed through information security policies on the use of e-commerce payment systems. One important key to implementing an enterprise information system in an organization is the adoption of security-related issues within the e-commerce payment systems of the business processes. The authors, in this paper, reviewed relevant literature that is related to the conceptual framework and to the security policies that are associated with enterprise information systems within the e-commerce payment systems. Adequate implementation of security policies, awareness of same by employee and top management, and access control were identified as four major issues affecting e-commerce payment systems security. These issues were consistent with our conceptual framework when presented within the context of corporate governance for the security of the enterprise information systems.

By establishing some strategies for implementing a secured e-commerce payment system that may impact data trustworthiness, accountability and compliance especially with users, we identified some future directions for this research. We postulate a system of activities that can handle threats to organizations' data: confidentiality, integrity, and availability within the operations of the EIS security conceptual framework: security policy, security awareness, access control, and top-level management support. We also seek to implement secure e-commerce payment systems that will present a functional e-commerce payment systems operation that is clean, safe, concise, familiar, responsive, consistent, attractive, enjoyable, efficient, and reliable to handle every e-commerce service delivery to customers. It is anticipated that findings from this study may encourage social change as more e-commerce payment systems will be more secured to leverage customers' confidence, improve user morale, preference, attraction, and productivity, and also increase the use of secure e-commerce payment systems other financial bodies globally. A successful e-commerce payment system though will attract diverse security breaches is welcome, because offense informs defense. Therefore the knowledge of the flaws or intending flaws and the workaround can inform and constitute part of the intelligent countermeasures constructed to build significant mitigations or countermeasures against intending attacks. This will no doubt create new innovation and influence that will impact more researches on secure e-commerce payment systems and advance the use of secure e-commerce payment systems.

Problem Statement: Security breaches among e-commerce payment systems have been on the increase despite the advancement in technology (Fenz, Heurix, Neubauer, & Pechstein, 2014). Security threats on e-commerce payment systems threats are not effectively mitigated against the organizations' data: confidentiality, integrity, and availability (Fenz, et al., 2014; Silic & Back, 2014). E-commerce payment systems security functions should include policies, resources, activities, operations and implementation procedures defined to mitigate most security threats, vulnerabilities, and risks. The general IT problem is the implementation of enterprise information systems security: security policy, resources, security awareness, access control, and top level management support procedures, and operations to mitigate most security threats, vulnerabilities, and risks. The specific IT problem is that some IT managers of e-commerce payment systems security function lack strategies to mitigate most security threats, vulnerabilities, and risks of e-commerce payment systems.

Conceptual Framework: For this study, the Enterprise Information Systems (EIS) security was adopted as the conceptual framework that comprised: security policy, security awareness, access control, and top level management support. Information security policies are set of rules, standards, practices, and procedures set up by an organization to maintain a secure IT system. The credibility of the entire information security program of an organization depends upon a well-defined information security policy (ISP) to actualize work-related groups that influence customers' decision-making (Sommestad, 2018). E-commerce payment systems security threats, vulnerabilities, and risks differ from one organization to another. Therefore, the threat analysis tools for guaranteeing e-commerce payment systems security should be integrated within the organization's information security policy so as to ensure security controls at local settings. Tools for e-commerce payment systems security threat assessment must encompass information security policy for effective security management in the area of confidentiality, integrity and availability of organization data, based on organization's risk appetite and culture. Policy gaps are the foundation of most security failures (Aguboshim & Udobi, 2019). Researchers believe that developing a well-defined system interface development process and information security policy are the most practical ways to preserve and protect e-commerce payment systems (Aguboshim & Miles, 2018; Choi, 2019), and the first step toward preparing an organization against attacks from internal and external sources (Kajtazi, Cavusoglu, Benbasat, & Haftor, 2018). Ineffective implementation of security policy may lead to weaknesses in enterprise information systems security.

However, the focus should shift more toward organization-specific information security needs, because there is still lacking contributions that would show how contextual factors could be successfully integrated into ISP development (Paananen, Lapke, & Siponen, 2019). There are supportive organizational factors such as culture and end-user involvement that significantly influence employees' attitudes towards compliance with ISP which in turn affects guaranteed and secured e-commerce payment systems (Amankwa, Loock, & Kritzinger, 2018). Also, leadership appears to exhibit the weakest influence on attitudes towards compliance with ISP (Alshare, Lane, & Lane, 2018). Overall, organizations' attitudes and behavioural intentions towards ISP compliance together influenced the establishment of information security compliance in organizations. While security policies, procedures, and controls are the most implemented security

measures, Allassani (2014) claimed that they are not the most effective in information security

Literature Review: E-commerce payment systems are simply defined as organized and systematic adoption of the internet for ordering and purchasing of goods and services. On the other hand, e-commerce encompasses both the buying and selling of information, products and services using the internet (Norhayati, Kamariah, & Noraini, 2015). As the use of the internet becomes ubiquitous, more technological innovations are put in place to drive e-commerce platforms, bringing about numerous challenges especially security bridges. Over the years there have been enormous advances in securing guarantee e -commerce payment system that are likely to shape the cybersecurity environment in the next decade (Dupont, 2013), and their possibility to produce great effect in the EIS security (Hinduja & Kooi, 2013). In the last decades, the IEEE Security & Privacy has focused on a wide variety of important policies that has not only contributed to the understanding of security, but also to the innovative and effective solutions to information technical security problems (Pfleeger, Predd, Hunker, & Bulford, 2010). These trends come with their challenging needs and requirements for more mobile data transactions, more connections, more movement and flows of e-commerce payment systems. As a result this massive data storage and interconnectivity in the e-commerce industry, enterprise data and information are exposed to more opportunities for malicious exploitation and threats, less security, and less control.

Much prior research has also focused on e-commerce fraud types: identity theft, intellectual property fraud or insurance fraud. However Scholarly research in the area of fraud is difficult (Goode & Lacey, 2011). Studies of financial and e-commerce fraud are hampered because it is difficult, if not impossible, to access offenders. Firms may be reluctant to admit experiencing security or fraud problem within their operations, while managers may resist enquiry or analysis from outside groups, including academic researchers to study their firms for fear of exposing their reputation to the public. It is also difficult for external researchers to gain access to the organization's original, unsanitized data. This is one of the reasons why determining what contributes to e-commerce information insecurity has proven to be complex in nature (Fenz, et al., 2014), because such activities required to handle threats to the organizations' data confidentiality, integrity, and availability is also complex. Despite the implementation of advanced security technical controls, e-commerce information systems have remained vulnerable. This is because there are evidences that suggest that human vulnerabilities are increasingly exploiting information systems (Stewart & Lacey, 2012). Some researchers have noted a number of reasons for this, ranging from problems with the usability and adoption of e-commerce (Hartzog & Stutzman, 2013; Okesola & Grobler, 2014), compromised decisions by customers (Greavu-Serban & Serban, 2014) and limited ability to comply with security policy, security awareness, access control, and top level management support systems or instructions (de Albuquerque & dos Santos, 2015; Shehata, 2015). However, Dwivedi, et al., (2015) summarized and categorized these mistakes into four categories: process (management process and technical project management methodologies), people involved in a project, product (project size and urgency, including its goals, performance, robustness, and reliability), and technology (IS failures resulting from the use and misuse of modern technology). Nevertheless, Study by Ho, Hsu, and Yen (2015) has provided an improvement strategies to manage the EIS security by proposing four core control items of the Enterprise Information Systems (EIS) security namely: security policy, security awareness, access control, and top level management support Information or human resource security.

Information Security Technical Controls: Failures and Successes: Astakhova (2015) cited some eloquent figures from InfoWatch Analytical Center, in the first half of year two thousand and fourteen that recorded 654 cases of leakage of confidential information, which was 32% more than what it was in previous year, while 71% of those who leaked information were employees of companies. Employees are prone to fall victim to social engineering attacks because of greed, self-interest, guilt, likelihood to trust others, ignorance or neglect of organization program and policies (Greavu-Serban & Serban, 2014). The severity of these threats and the degree to which they are effectively mitigated are not efficient (Silic & Back, 2014). This is because top managers, middle managers, and employees alike, have continued to neglect information security policies and principles, which in turn, resulted in far more frequent security breaches than are necessary. Most IT audit reports have indicated that the root cause of most security breaches is failure to comply with technical, operational, and management policies. Most reports show that the physical security and environmental controls for the numerous IT rooms are often deficient with no provisions for redundant data telecommunications lines to provide service in case of failure of serving lines. In some cases there are no documentation of the IT assets or interconnections relating to the Security Technology Integrated Program (STIP). In summary, these deficiencies or neglects to information security principles or policies often place at risk the confidentiality, integrity, and availability of the data stored, transmitted, and processed. Measuring security technical control successes is hard, complex, multidimensional, emergent, irreducible, and resident in an abstraction, and context that affect environment (Pfleeger, et al., 2010). Understanding what causes failures and avoiding them can be a good way to understand how to measure successes in security. Information system success should be dependent on interrelated variables such as System Quality, User Satisfaction, Information Quality, Individual Impact, and Organizational Impact.

Developing More Effective e-commerce Information Security Technical Controls: Technology cannot solve our security problems until we understand technology and the problems (Stallings & Brown, 2012). Security problems, like IoT problems are more of social and organizational problem, rather than a technical problem, more about psychology, rather than technology (Cottrell, 2016). This is because the technical systems are managed and used by people. Despite the advancement in technology, security breaches have been on the increase involving both small and large organizations (Fenz, et al., 2014). In the past, attacks on company's sensitive data and information were fairly straightforward to identify and easy to capture the attention of virus attacks, network intrusion attempts, and block same just at the perimeter. With the rise of multi-functional malware, these easy mitigation approaches could no longer help. Recently, the increasing dependency on data and electronic services, and complex connectivity, originally intended to secure confidentiality, integrity, and availability of data, have now made devices with software-defined behavior or network connectivity to be

susceptible of being compromised by external party (Fenz, et al., 2014). These are dangerous trends in information security. However good practices exist such as computer and network installations, good system development, critical business applications that provide high-level techniques of information security. Other good practices included methodologies that impact assessment of crucial elements and applications that identifies and criticality examines the business processes in relation to confidentiality, availability and integrity of data. In a social network sites (SNS) for instance, some of the technical controls implemented are customization of access controls based on the users' groups and information type, setting privacy in a user-friendly way to make for flexibility, integrating with a user-friendly interface that is easily understood by any typical SNS user; and customized search implemented to further enhance the preservation of the user's privacy (Okesola & Grobler, 2014). Information security control is therefore a complex task which involves the implementation and monitoring of more than 130 security controls (Montesino & Fenz, 2011). Result from the analysis of three widely used information security standards and best practice guidelines by Montesino and Fenz (2011), showed that about 30% of the security controls included in ISO 27001 and NIST SP 800-53 can be automated by existing tools. It is therefore necessary to automate as many controls as possible in order to achieve greater efficiency of information security management (Shahpasand, Shajari, Hashemi-Golpaygani, & Ghavamipoor, 2015) to ensure the confidentiality, integrity and availability of organization data.

METHODOLOGY

A narrative review approach was adopted in this study to review significant information on the conceptual framework, existing systems that enhance e-commerce payment system security, analysis, and synthesis of prior research. According to Hill and Burrows (2017), a narrative review is adopted where summaries of different primary studies from which conclusions may be drawn into a holistic interpretation contributed by the reviewers' own experience, existing theories and models are needed. A narrative study approach is best suited to a study that can be described as descriptive or explanatory (Bell**,** 2017; Privizzini, 2017). Results from narrative studies are of a qualitative rather than a quantitative meaning (Scarnato, 2017). The strengths of narrative study are in its ability to comprehend the diverse and numerous understanding around scholarly research topics and the opportunity to speak with self-knowledge, reflective practice and acknowledgement of shared views and knowledge (Malcolm, 2017). Researchers with diverse understandings have co-opted the concept of narrative reviews as best suitable for comprehensive topics and have used narrative inquiry or narrative research to name their methodology (Bell**,** 2017; Privizzini, 2017; Rutherford, 2017). In this paper, we lay out more clearly the methodological commitments of narrative inquiry. Within narrative inquiry, we have made the search criteria and the criteria for inclusion explicit. Our review process included key words and term identification, article identification, quality assessment, data extraction, and data synthesis. Methodological triangulation is the use of multiple sources of data that pertains to a case or phenomenon, to gain multiple perspectives, maximize reliability and validation of data and build coherent justification of data interpretation (Durif-Bruckert, et al., 2014).

We adopted methodological triangulation to ensure the reliability and validity of data, and justification of interpretations from the reviews.

Data Collection: This review was based on a literature search of online information obtained from the following international library databases: the ProQuest databases, ScienceDirect, and collection of scholarly and peer-reviewed journals, and other related texts. A combination of phrases and terms were used as key search words in the databases for related literature on e-commerce payment system security. Such phrases and terms included: *e-commerce system security, e-commerce security threats, cyber-attacks and security, CIA triad, e-commerce security function, vulnerabilities and risks,* and many others. We conducted a thorough review of the literature and incorporated 41 references into our study. Thirty-nine (95%) of total references incorporated in the study are peer-reviewed, while Thirty-one (79%) are of peer-reviewed journals that are within the last 5 years.

Analysis and Synthesis of Prior Research: Some socio-technical trends that are likely to shape the e-commerce payment system security environment in the next decade have been identified (Dupont, 2013), and their possibility to produce a great effect in the information security technical controls observed (Hinduja & Kooi, 2013). Over the years there have been enormous advances in the field of technical information security controls with complex and matured technical controls such as anti-virus, client-based firewalls, and real-time patching (Stewart & Lacey, 2012). In the last decades, the IEEE Security & Privacy has focused on a wide variety of important policies that have not only contributed to the understanding of security, but also to the innovative and effective solutions to information technology security problems (Pfleeger, et al., 2010). In spite of vast adoption and implementation of advanced security technical controls, e-commerce payment information systems have remained vulnerable. Some researchers have noted a number of reasons for this, ranging from problems with the usability of information systems (Hartzog & Stutzman, 2013; Okesola & Grobler, 2014), compromised decisions by users (Greavu-Serban & Serban, 2014) and limited ability to comply with Knowledge Management Systems or instructions (de Albuquerque & dos Santos, 2015; Shehata, 2015). Dwivedi, et al. (2015) summarized and categorized these mistakes into four categories: process (management process and technical project management methodologies), people involved in a project, product (project size and urgency, including its goals, performance, robustness, and reliability), and technology (IS failures resulting from the use and misuse of modern technology). Nevertheless, security policy, access control, and human resource security are proven three core control items of the Information Security Management improvement strategies to manage the Information Security of the organization

Conclusion

It is believed that no single tool can exploit the full security control automation potential. A combination of different tools is required. Security technical control is a knowledgebase affair. The analysis and synthesis of prior research have revealed and identified the interdisciplinary nature of the problem of the assessment of the human factor, and ways of reducing the risk to the e-commerce information system security.

Security automation can decrease human intervention, costs and complexity of security activities. Security professional should begin to think differently by separating epistemic risk from aleatory risk. By contrast, epistemic risk reflects the incomplete state of our knowledge about a process, while aleatory risk represents the inherent randomness in a process. Therefore epistemic risk can be reduced by continuously collecting and compiling more and better evidences from various activities conducted during the system development life cycle. This will increase our knowledge and understanding of all facets of security platforms, to improve the process of building our systems, establishing assurance, and enhancing preventive measures, and more. The main objective of this study was to inform IT, managers of e-commerce payment system security function, the strategies to withstand most security threats, vulnerabilities, and risks of e-commerce payment systems. What contributes to information insecurity has proven to be complex, dynamic and more of psychological in nature. Security measures need to be complex in order to handle the complex security threats. Organizations' data confidentiality, integrity, and availability are becoming complex, dynamic and psychological. Perimeter defenses, control over devices, employee's adherence to policies, control over policy enforcement, and enterprise definitions are no longer reliable as all security platforms are complex, dynamic and psychological. Attackers are personalizing their attacks. Security defenses must be personalized as well, with a holistic approach that expands beyond the technical security to include all arms of enterprise information systems security that comprised: security policy, security awareness, access control, and top level management support, including the environment, the technology, and the people. IT managers of e-commerce payment security systems must put in place good policies coupled with good formulation and communication of same, information security policies intentions, principles, rules and guidelines which should be adhered that could avert all forms of security breaches.

REFERENCES

Adjei, J. K. 2015. Explaining the role of trust in cloud computing services. *Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media, 17*(1), 67-54. doi:10.1108/info-09-2014-0042

Aguboshim, F. C. 2019. *User Interface Challenges of Banking ATM Systems in Nigeria*. LAP LAMBERT Academic Publishing, Germany. ISBN-13: 978-613-9-45034-3. ISBN-10: 6139450349, EAN: 9786139450343. https://www.lap-publishing.com/

Aguboshim, F. C., & Miles, G. S. 2018. Well-defined interface development process: an important interface design strategy to create easy-to-use banking ATM system interfaces in Nigeria. *International Journal of Engineering Science and computing (IJESC),8(12)*, 1-25.

Aguboshim, F. C., & Udobi, J. I. 2019. Security issues with mobile IT: A Narrative Review of Bring -Your-Own-Device (BYOD). *Journal of Information Engineering and Application (JIEA),* 9(1), 56-66. doi:10.7176/jiea/8-1-070

Allassani, W. 2014. Determining factors of bank employee reading habits of information security policies. *Journal of Information Systems and Technology Management, 11*(3), 533-548. doi:10.4301/S1807-17752014000300002

Alshare, K. A., Lane, P. L., & Lane, M. R. 2018. Information security policy compliance: a higher education case study. *Information and Computer Security, 26*(1), 91-108 doi:10.1108/ics-09-2016-0073

Amankwa, E., Loock, M., & Kritzinger, E. 2018. Establishing information security policy compliance culture in organizations. *Information and Computer Security, 26*(4), 420-436. doi:10.1108/ics-09-2017-0063

Astakhova, L. V. 2015. Information security: Risks related to the cultural capital of personnel (Review). *Scientific and Technical Information Processing, 42*(2), 41-52. doi:10.3103/S0147688215020021

Bamrara, A., Singh, G., & Bhatt, M. 2013. Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector. *International Journal of Cyber Criminology, 7*(1), 49-61.

Bell, E. E. 2017. A Narrative Inquiry: A Black Male Looking to Teach. *The Qualitative Report, 22*(4), 1137-1150. Retrieved from http://nsuworks.nova.edu/tqr/vol22/iss4/12

Chaudhry, P. E., Chaudhry, S. S., Reese, R., & Jones, D. S. 2012. Enterprise Information Systems Security: A Conceptual Framework. *International Federation for Information Processing*, 118–128.

Choi, Y. 2019. Organizational Control Policy, Information Security Deviance, and Moderating Effect of Power Distance Orientation. *International Journal of Cyber Behavior, Psychology and, 9*(3), 48-60. doi:10.4018/ijcbpl.2019070104

Cottrell, L. 2016. IoT problems are about psychology, not technology. Retrieved from http://www.tripwire.com/state-of-security/security-data-protection/iot/iot-problems are-about-psychology-not-technology/

de Albuquerque, A. j., & dos Santos, E. 2015. Adoption of information security measures in public research institutes/adoç'o de medidas de segurança da informaç'o em institutos de pesquisa p'blicos. *Journal of Information Systems and Technology Management : JISTEM, 12*(2) 289-315. doi:10.4301/S1807-17752015000200006

Dupont, B. 2013. Cybersecurity Futures: How Can We Regulate Emergent Risks? *Technology Innovation Management Review, 3*(7), 6-11.

Durif-Bruckert, C., Roux, P., Morelle, M., Mignotte, H., Faure, C., & Moumjid-Ferdjaoui, N. 2014. Shared decision-making in medical encounters regarding breast cancer treatment: the contribution of methodological triangulation. *European Journal of Cancer Care, 24*(4), 461-472. doi:10.1111/ecc.12214

Dwivedi, Y., Wastell, D., Laumer, S., Henriksen, H. Z., Myers, M. D., Bunker, D., Srivastava, S. C. 2015. Research on information systems failures and successes: Status update and future directions. *Information Systems Frontiers, 17*(1), 143-157. doi:10.1007/s10796-014-9500-y

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. 2014. Current challenges in information security risk management. *Information Management & Computer Security, 22*(5), 430-410. doi:10.1108/IMCS-07-2013-0053

Goode, S., & Lacey, D. 2011. Detecting complex account fraud in the enterprise: The role of technical and non-technical controls. *Decision Support Systems, 50*(4), 702-714. ISSN 0167-9236.

Greavu-Serban, V., & Serban, O. 2014. Social Engineering a General Approach. *Informatica Economica, 18*(2), 5-14. doi:10.12948/issn14531305/18.2.2014.01

Hartzog, W., & Stutzman, F. (2013). Obscurity by design. *Washington Law Review, 88*(2), 385-418.

Hill, C., & Burrows, G. 2017. New voices: The usefulness of a narrative approach to social work research.

Qualitative Social Work: Research and Practice, 16(2), 273-288. doi:10.1177/1473325017689966

Hinduja, S., & Kooi, B. 2013. Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security Journal, suppl. Special Issue: Security in a digital world: Understanding, 26*(4), 383-402. doi:10.1057/sj.2013.25

Ho, L., Hsu, M., & Yen, T. 2015. Identifying core control items of information security management and improvement strategies by applying fuzzy DEMATEL. *Information and Computer Security, 23*(2), 161-177. doi:10.1108/ics-04-2014-0026

Kajtazi, M., Cavusoglu, H., Benbasat, I., & Haftor, D. 2018. Escalation of commitment as an antecedent to noncompliance with information security policy. *Information and Computer Security, 26*(2), 171-193 doi:10.1108/ics-09-2017-0066

Malcolm, P. M. 2017. Peer support in mental health: a narrative Review of its relevance to social work. *Egyptian Journal of Social Work, 4*(1). 19-40. doi:10.21608/ejsw.2017.8725

Montesino, R., & Fenz, S. 2011. Information Security Automation: How far can we go? Availability, Reliability and Security (ARES), 2011 Sixth International Conference on. doi:10.1109/ares.2011.48.

Nasir, M. A., Wu, J., Yago, M., & Li, H. 2015. Influence of Psychographics and Risk Perception on Internet Banking Adoption: Current State of Affairs in Britain. *International Journal of Economics and Financial Issues, 5*(2), 461-468.

Norhayati, M. A., Kamariah, N. M., & Noraini, M. A. 2015. The Conceptual Framework for E-Commerce Adoption Model. *American Journal of Economics, 5*(2), 148-154. Doi: 10.5923/c.economics.201501.16

Okesola, J. O., & Grobler, M. 2014. Developing a secured social networking site using information security awareness techniques. *South African Journal of Information Management, 16*(1), 1-6. doi:10.4102/sajim.v16i1.607.

Paananen, H., Lapke, M., & Siponen, M. 2019. State of the Art in Information Security Policy Development. *Computers & Security, 10*(1), 10-16. doi:.1016/j.cose.2019.101608

Pfleeger, S. L., Predd, J. B., Hunker, J., & Bulford, C. 2010. Insiders Behaving Badly: Addressing Bad Actors and Their Actions. *Information Forensics and Security, IEEE Transactions on, 5*(1), 169-179. doi:10.1109/TIFS.2009.2039591.

Privizzini, A. 2017. The Child Attachment Interview: A Narrative Review. *Frontiers in Psychology, 8*(1), doi:10.3389/fpsyg.2017.00384

Rutherford, J. S. 2017. Monitoring teamwork: a narrative review. *Anaesthesia, 72*(1), 84-94. doi:10.1111/anae.13744

Scarnato, J. M. 2017. The value of digital video data for qualitative social work research: A narrative review. Qualitative Social Work: Research and Practice, doi:10.1177/1473325017735885

Shahpasand, M., Shajari, M., Hashemi-Golpaygani, S. A., & Ghavamipoor, H. 2015. A comprehensive security control selection model for inter-dependent organizationalassets structure. *Information and Computer Security, 23*(2), 218-242. doi:10.1108/ICS-12-2013-0090

Shehata, G. M. 2015. Leveraging organizational performance via knowledge management systems platforms in emerging economies: Evidence from the Egyptian Information and Communication Technology (ICT) industry. *VINE, 45*(2), 278-239. doi:10.1108/vine-06-2014-0045

Silic, M., & Back, A. 2014. Information security. *Information Management & Computer Security, 22*(3), 279-308. doi:10.1108/IMCS-05-2013-0041

Sommestad, T. 2018. Work-related groups and information security policy compliance. *Information and Computer Security, 26*(5), 533-550. doi:10.1108/ics-08-2017-0054

Stallings, W., & Brown, L. 2012. Computer security: Principles and practice (2nd ed.). Upper Saddle River, NJ: Prentice Hall.

Stewart, G., & Lacey, D. 2012. "Death by a thousand facts", *Information Management & Computer Security, 20*(1), 29-38. doi:10.1108/09685221211219182.

****