International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 6, September-October 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Cyber Security Awareness and Corporate Agility of Deposit Money Banks in Nigeria

Dr. Agbeche Aaron

Michael and Cecilia Ibru University, Ughelli, Nigeria

ABSTRACT

This article looks at corporate agility from indicators such as sensing agility, decision making agility, acting agility or practice. It went on to review what cyber security awareness entails by stating some of the most possible threat that people encountered on a daily bases. The article identify poor management of cyber security solutions provided by modern internet security experts in the form of difficulty of tracing the cyber-crime attackers, limited cybercrime laws, and limited IT security knowledge among internet users as the problems that the study addresses. Theory of protection motivation was used primarily to explain cyber security awareness, and how and when a user adopts adaptive behaviors. The article conclude that cyber security awareness is more important now than it has ever been before and that threats to personal and corporate information are increasing and identities are getting stolen every day. The article recommend that government, deposit money banks, users, mass media and manager should introduce and enforce cybercrime laws, train ,offers advices and create more awareness among their staff and clients of the organization on the need to be aware of internet threat and be careful in their dealings on a daily bases.

KEYWORDS: *Cyber Security, Training, Information Availability, Corporate Agility, Alertness, Adaptability*

How to cite this paper: Dr. Agbeche Aaron "Cyber Security Awareness and Corporate Agility of Deposit Money Banks in Nigeria" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-6, October 2021, pp.1339-1345, URL: www.ijtsrd.com/papers/ijtsrd47613.pdf

IJTSRD47613

Copyright © 2021 by author (s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0)

1. INTRODUCTION

Deposit money banks in Nigeria on a daily bases are working hard to identify with their counterparts globally; some in their desire to attain international recognitions has resolve to station their offices outside the shore of Nigeria. While others has resolves to the use of the internet facilities or technology as a basic medium for rendering their services to members of the public or getting proximate to their customers. The desire to get to its customers with ease came as result of the drastic increase in information technology in the past decades and with massive global rates of internet consumption by individuals and organizations ranging from academia and government to industrial sectors (Aloul, (2012; Jalali, Siegel &Madnick, 2019 ; Lee, Chong &Ramayah, 2017).

As such, it is important to note that over the time past and in this present era, information technology has actually made significant impacts on the operations of this deposit money banks and is still going to change the directions of doing things in the nearest future. While some banks now develop apps that can be downloaded on to mobile devices, others have come up with devices that allows for quick transaction delivery. All these the deposit money banks does to ensure that they remain relevant in the ever competitive financial industry (Zwilling, Klien, Lesjak, Wiechetek, Cetin &Basim, 2020); where digital applications have continue to transform daily life and facilitating diverse lifestyles in many other areas.

Furthermore, Zwilling*et al.,* (2020) emphases that the ease of technology usage as well as the increased demand for online connectivity (in education, retail, tourism, and even autonomous vehicles) has expanded opportunities for internet usage on a global scale. Indeed, some of these uses include sending money to people at different location with ease, payment for bills, ease of wire transfer for transactions, surfing the web to know what new ideas our competitors has been doing, utilizing search engines to find desired content, assisting recommender systems in the form of decision support tools and using social media to name only a few

(Zwillinget al., 2020). Notwithstanding the lots of benefits that are associated with the adoption of such device in banking transactions and other services rendered by the deposit money banks, many organizations, individuals and institutions of business has suffered greatly from all manner of internet threat that has come as a result of lack of awareness of the various antics of dubious elements in the society (Choi & Yi, 2009). In fact, they often fail to possess the minimum required knowledge to protect their computing devices. In worst case scenarios, deposit money banks, its customers and individuals suffer from total lack cyber hazard awareness. Hence, their readiness to utilize protective cyber security measures is non-existent.

Cyber hazards are the work of "bad hackers" (otherwise known as "black hats"), who act on their own or within an organized criminal group to commit cyber-crime. In both cases, their intention is to engage in cyber-crime in any of its various forms, ranging from violation of individual privacy to identity theft and credit card fraud(Zwillinget al., 2020). Cyber-criminals use malicious software and hacking tools to sabotage computers, mobile devices, and communication network infrastructure, including cyber security protection tool disruption (Abawajy, 2014). While protective tools are generally installed on computers and in infrastructure, studies show that they do not completely mitigate cyber security breaches (Funnel, Jusoh&Katsabas, 2006; Parsons, McCormac, Butavicius, Pattinson, &Jerram, 2014; Schultz, 2005). This is because the weakest link in the cyber security chain remains human error (Anwar, He, Ash, Yuan, Li &Xu, 2017; Vance, Siponen&Pahnila, 2012; Schneier, 2004). Organizations have come to recognize that behaviors deriving from the human factor are responsible for cyber security flaws and may pose a liability for information security (Sasse and Flechais, 2005).

In view of these threats and weaknesses in terms of human errors, deposit money banks have embraced and have continue to emphases the need for individuals within and outside the banks to develop resistance to the criminal intents of cyber-crime organizations and individuals; as these organizations and individuals makes use of their human weaknesses to perpetuate their crime on a daily bases. Also, Since human mind capabilities are limited in terms of grasping important changes that take place in the environment surrounding it, so has the current business environment for any organization in the world become complicated and highly dynamic for them to comprehend (Zain et al., 2005). Therefore, it has become necessary that organizations in dire need to secure it current and future goals of customer satisfaction, has stressed the need for individuals within and outside of the deposit money banks to develop a sensing agility, decision-making, and agility in carrying out work properly (Markos&Sridevi, 2010; Warr&Inceoglu, 2012); by being conscious of cyber-crime alert or any other devices that is being used to defraud them.

Apart from being able to resist these criminal elements tactics, the issue of agility or corporate agility should become the watch words of the modern organization. Corporate agility is one of the methods for responding to changes and revolutionary factors that affects the smooth running of business. Agility provides the organization with the possibility of quick response and compatibility with environment and allows the organization to improve its efficiency (Yeganegi&Azar, 2012). Corporate agility has great impacts in the life of the organization as it provides personnel with knowledge, high skills, restructuring and organizational processes, employing new technology (Sherehiy, 2008). Corporate agility refers to organizations' ability to thrive by sensing and responding to environmental changes which has become critically important nowadays when the business environment is getting highly competitive and turbulent. It is regarded as a key business factor and a potential enabler to organization's competitiveness (Mathiassen& Pries-Heje, 2006)

Regardless of the different scholarly works that has been done on the issue of firm agility; research on cyber security awareness and corporate agility in deposit money banks are few. Rather research on organizational agility is emerging more in the information systems field (Izzaet al., 2008) due to the extensive reliance of contemporary organizations on information in general and information system in particular. As such, the problem that this article addresses is the poor management of cyber security solutions provided by modern internet security experts which exhibits itself in the form of difficulty of tracing the attackers, limited cybercrime laws, and limited IT security knowledge among internet users. For example, in May 2017 the WannaCry ransom ware attack—a type ofmalware that blocks access to computer systems until a ransom is paid—affected companies worldwide, even though a patch for the exploited Windows vulnerabilities had been made available by Microsoft months earlier in March 2017 (Microsoft, 2017).

2. Literature Review

2.1. Corporate Agility

The concept of agility has been discussed by so many researchers differently. Agility was coined in a

manufacturing context-particularly in relation to flexible manufacturing systems (Christopher &Towill, 2001). Agility refers to the proactive responses to changes (Bessant*et a*l., 2001). Agility can also be referred to the use of changes as inherent opportunities in turbulent environment (Sharifi& Zhang, 2001). Furthermore, agility is the ability to survive and progress in the variable and unpredictable environment (Dove, 2001). Sherehiy, (2008) defined the process of agility in terms of the capabilities necessary to achieve light movement in the organization. Agility is the ability to respond to unpredictable changes with quick response and profitability (Erande&Verma, 2008). Agility is an organizational ability to react quickly and effectively to an environment which can change radically (Janssen, 2010). Agility refers to the ability of rapid and easy movement and rapid thinking with a thoughtful method. Agility can be defined as swiftness and quick response of a harmonious group to the changes made by the environment surrounding them in order to reach a goal (Yeganegi&Azar, 2012).

Corporate agility is the organization's ability to work comfortably in a quickly and consistently changing and fragmented global market environment, through producing high quality and effective performance (Tsourveloudis&Valavanis, 2002). Corporate agility enables the organization to carry out a series of specific tasks successfully, in addition to managing the opportunities and risks in the business activities effectively (Ardichvile*et al.,* 2003). Corporate agility is not only "flexible" to cater for predictable changes but also is able to respond and adapt to unpredictable changes quickly and efficiently (Oosterhout*et al.,* 2006). From the process-based perspective, corporate agility is a set of processes that allow an organization to sense changes and respond efficiently and effectively in timely and cost-effective manner in the internal and external environments. Sensing refers to an organization's ability to detect, capture and interpret organizational opportunities (Seo& Paz 2008). Responding represents an organizational ability to mobilize and transform resources to react to the opportunities that it senses (Gattiker*et al.,* 2005; Oosterhout*et al.,* 2006). These two capabilities must be aligned to optimally obtain corporate agility (Overby*et al.,* 2006). Corporate agility is a proactive management strategy that aims at maintaining the organization's resources and achieving the desires of customers in a timely manner (Hitt*et al.,* 2007). Corporate agility is the organizational capacity to sensor response successfully to the opportunities and threats in the market in a timely manner (Overby*et al.,* 2006). Corporate agility is a proactive management strategy that aims at maintaining the organization's resources and achieving the desires of customers in a timely manner (Hitt*et al*., 2007). The three indicators popularized by Park (2011) were adopted for this article. These indicators are sensing agility, decision making agility and acting agility/ practice.

Sensing Agility

Sensing agility is the organizational capacity to inspect and monitor events and changes in the surrounding environment (customer preferences changes, the movements of the new competitors, new technology) in a timely manner (Park, 2011). The task of sensing means the strategic monitoring of environmental events that could have an impact on organizational strategy, competitive work, and future performance, including several activities such as access to information related to the events which show environmental change, on the one hand, and getting rid of the trivial information, on the other hand, in light of predetermined foundations and rules.

Decision-Making Agility

Decision-making agility process is the ability to collect, accumulate, restructure and evaluate relevant information according to a variety of sources to explain the implications of the business without delay, and to identify opportunities and threats based on the interpretation of events, along with the development of action plans, which direct the reconfiguration of resources and the development of new competitive procedures. The decision-making task consists of several interrelated activities, which explain many events and identify opportunities and threats in the surrounding environment. The task of decision-making focuses on collecting information from multiple and diverse sources in order to understand the implications of their work. The task of decision-making seeks to capture the utmost opportunities and minimize the impact of threats on the life of the organization (Houghton et al., 2004).

Acting Agility/Practicing

The acting task consists of a set of activities for re-assembling organizational resources and modifying business processes on the basis of the principles of work resulting from the task of decision-making in order to address the change that occurs in the surrounding environment (Eisenhardt& Martin, 2000). Organizations can change the business processes by various procedures and resources, redesigning the organizational structure of the organization.

2.2. Cyber Security Awareness

The information security community has come to realize that the weakest link in a cyber-security chain is human (Sasse, 2005). To develop effective cyber-

security training programs for employees in the workplace, it is necessary to understand the security behavior of both men and women, and the similarities and differences of their security behaviors. As Hackers are continuously identifying new means of stealing information. Unfortunately, the presence of "uneducated" users in an organization makes them an easy target for hackers and vulnerable to privacy attacks (Khattak, Manan, and Sulaiman, 2011). User education and training is a must to combat IT security threats. Users should not only learn the material but they should also apply it in their daily life. This is not a simple task to achieve and not the sole responsibility of the user or the organization. Many groups have to be involved to produce an IT security-aware resident.

There are multiple different schemes that have been happening recently that are associated with Internet usage. Some of these scams involve hackers cracking passwords to get access to personal information and criminals using phishing techniques to gather information that they can use to steal individual's identities (Jansson& von Solms, 2013).The internet is not a secured space. It is an area where there currently are not many regulations. It is where anyone can put up, take down, or gather as much information as they want (Hall, 2012).

Cyber security is becoming an increasingly talked about topic. With more and more people making their personal information available online than ever before, it is becoming a hacker's paradise. However, most individuals do not know about all of these scams and are unaware when they are happening to them. Because of this, people do not know how to protect themselves and how to stop being a target. Cyber security needs to be more common knowledge and education needs to be more readily available. It is important for us to help educate individuals on what they can do to stop and prevent potential cyber security attacks. It is also especially important that our customers and staff to be able to recognize potential threats. Majority of people are not only unaware that cyber threats are real, but are also unaware of what to do about them. Most people just hope or assume that identity theft and phishing attacks are not going to happen to them. But, making society aware that even the smallest tasks can pose potential threats is crucial for their safety.

Awareness is the first step in reducing the number of identity thefts and personal information threats. Individuals believe that if they have a unique password then they are protecting themselves enough that they do not have to worry about cyber security threats (McCrohan, Engel, & Harvey, 2010). While this is a good first step, and it is strongly recommended to create unique passwords, it is not enough to keep information private. Most hackers have the technology and knowledge to know how to decrypt these passwords or bypass them completely. Each day that our technology is improving is another day that hackers are figuring out how to crack that technology.

Likewise, much of the population believes that installing virus protection or spy software onto their computers is enough. They think that this software is going to save them from ever being hacked or having their information stolen (McCrohan, Engel, & Harvey, 2010). This is also simply not true. We need to change this way of thinking by helping society recognize the signs of the potential threats and risks. We then need to hand them the information that they need to keep themselves safe and protected. Some of the signs that users need to be aware of that usually indicate a phishing attempt are: words being misspelled, a certain degree of urgency or "deadlines", fake names and web links, and a request for personal information (Lungu&Tăbuşcă, 2010).

3. Cyber Security Awareness and Corporate Agility

Hearth and Rao (2009) secure management of information systems is crucially important in information intensive organizations. Although most organizations have long been using security technologies, it is well known that technology tools alone are not sufficient. Thus, the area of end-user security behaviors in organizations has gained an increased attention. In information security observing end-user security behaviors is challenging. Moreover, recent studies have shown that the end users have divergent security views. The inability to monitor employee IT security behaviors and divergent views regarding security policies, in our view, provide a setting where the principal agent paradigm applies. In this paper, we develop and test a theoretical model of the incentive effects of penalties, pressures and perceived effectiveness of employee actions that enhances our understanding of employee compliance to information security policies. Based on 312 employee responses from 77 organizations, we empirically validate and test the model. Our findings suggest that security behaviors can be influenced by both intrinsic and extrinsic motivators. Pressures exerted by subjective norms and peer behaviors influence employee information security behaviors. Intrinsic motivation of employee perceived effectiveness of their actions was also found to play an important role in security policy compliance intentions. In analyzing the penalties, certainty of

detection was found to be significant while surprisingly, severity of punishment was found to have a negative effect on security behavior intentions. We discuss the implications of our findings for theory and practice.

According to Vance, Siponen and Pahnila (2012) employees' failure to comply with IS security procedures is a key concern for organizations today. A number of socio-cognitive theories have been used to explain this. However, prior studies have not examined the influence of past and automatic behavior on employee decisions to comply. This is an important omission because past behavior has been assumed to strongly affect decision-making. To address this gap, we integrated habit (a routinized form of past behavior) with Protection Motivation Theory (PMT), to explain compliance. An empirical test showed that habitual IS security compliance strongly reinforced the cognitive processes theorized by PMT, as well as employee intention for future compliance. We also found that nearly all components of PMT significantly impacted employee intention to comply with IS security policies. Together, these results highlighted the importance of addressing employees' past and automatic behavior in order to improve compliance.

Mohamed and Ahmad (2012) in their study on information privacy concern, antecedents and privacy use in social network sites: evidence from Malaysia, the research aims at gaining insights into information privacy concerns, its antecedents and privacy measure use in social networking sites. The Social Cognitive, Protection Motivation theories and gender factor were used as a basis to develop and confirm a research model. Using a cross-sectional survey design and cluster sampling technique, four-hundred thirteen questionnaires were distributed to undergraduates at a public Malaysian university; three-hundred forty were included in analyses. Data was analyzed using structural equation modeling technique. Results suggest that in order of importance only perceived severity, self-efficacy, perceived vulnerability, and gender are antecedents of information privacy concerns with social networking sites; response efficacy and rewards were not significant antecedents contrary to many past findings in the literature that used Social Cognitive and Protection Motivation Theory as a theoretical basis. Information privacy concerns explain privacy measure use in social networking sites. The implications of these results and study limitations are discussed.

Ng, Kankanhalli and Xu (2009) studying user's computer security, a health belief perspective. The damage due to computer security incidents is motivating organizations to adopt protective mechanisms. While technological controls are necessary, computer security also depends on individual's security behavior. It is thus important to investigate what influences a user to practice computer security. This study uses the Health Belief Model, adapted from the healthcare literature, to study users' computer security behavior. The model was validated using survey data from 134 employees. Results show that perceived susceptibility, perceived benefits, and self-efficacy are determinants of email related security behavior. Perceived severity moderates the effects of perceived benefits, general security orientation, cues to action, and self-efficacy on security behavior.

4. Conclusions and Recommendations

Cyber security awareness is more important now than it has ever been before. Threats to personal and corporate information are increasing and identities are getting stolen every day. Making individuals and corporation aware of this is the first step. The second step is giving individuals and the corporate entity the tools and knowledge that they need to protect themselves. Based on these conclusions, the article recommends that:

A. Governments should produce cybercrime laws and enforce them. They should also work closely with other governments since many attacks can be conducted from abroad.

B. Deposit money banks should have trained computer emergency response teams (CERT) that are dedicated to the detection, prevention, and response of cyber security incidents.

C. Media houses should continuously post IT security advices, report IT security incidents, and the penalty that the attackers got this will put fear in the mind of those thinking of such an act.

D. Users (staff and customers of these deposit money banks Apps and other software) should train themselves by constantly reading magazines, books and online articles on IT security threats and what to do to protect themselves from such threats.

E. Telecommunication companies (ISPs) should offer advices on how to use the internet safely or configure any internet device securely.

F. Managers of deposit money banks should offer security training to its employees and clients. This could be online or onsite training or a combination of both.

REFERENCE

[1] Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237-248.

[2] Aloul, F. A. (2012). The need for effective information security awareness. *Journal of advances in information technology*, *3*(3), 176-183.

[3] ance, A., Siponen, M., &Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198.

[4] Anwar, M., He, W., Ash, I., Yuan, X., Li, L., &Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437-443.

[5] Ardichvili, A., Cardozob, R., &Rayc, S. (2003). A theory of entrepreneurial opportunity identification and development. *Journal of Business Venturing*, 18(1), 105-117.

[6] Bessant, J., Knowles, D., Francis, D., & Meredith, S. (2001). *Developing the agile enterprise, agile manufacturing: The 21st century competitive strategy*. New York: Wiley

[7] Choi, C., & Yi, M. H. (2009). The effect of the internet on economic growth: Evidence from cross-country panel data. *Economics Letters*, *105*(1), 39-41.

[8] Christopher, M., &Towill, D. (2001). An integrated model for the design of agile supply chains. *International Journal of Physical Distribution & Logistics Management,* 31(4), 235-246.

[9] Dove, R. (2001). *Responsibility: The language, structure, and culture of the agile enterprise.* New York: Wiley

[10] Eisenhardt, M., & Martin, J. (2000). Dynamic capabilities: What are they? *Strategic Management Journal,* 21(1), 1105-1121.

[11] Erande, A., &Verma, A. (2008). Measuring agility of organizations: A comprehensive agility measurement Tool (CAMT). Old dominion university, proceedings of the 2008 IAJC-IJME International Conference.

[12] Funnel, S. M., Jusoh, A., &Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, *25*(1), 27-35.

[13] Gattiker, T., Chen, D., & Goodhue, D. (2005). Agility through standardization: A Crm/ Erp application. *In F. R. Jacobs & B. E. (Eds.), Strategic erp extension and use (pp. 87-96.). Stanford Business Books*.

[14] Hall, C. (2012). Security of the internet and the known unknowns. *Communications of the ACM*, 55(6), 35-37.

[15] Herath, T., &Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

[16] Hitt, M. A., Hoskisson, E. R., & Ireland, R. D. (2007). *Management of strategy: Concepts and cases*. New York: South-Western.

[17] Houghton, R., El Sawy, O. A., Gray, P., Donegan, C., & Joshi, A. (2004). Vigilant information systems for managing enterprises in dynamic supply chains: Real-time dashboards at western digital. *MIS Quarterly Executive,* 3(1), 19-35.

[18] Izza, S., Imache, R., Vincent, L., &Lounis, Y. (2008). An approach for the evaluation of the agility in the context of enterprise interoperability. *Enterprise Interoperability*, 3(1), 3-14.

[19] Jalali, M. S., Siegel, M., &Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems*, *28*(1), 66-82.

[20] Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology,* 32(6), 584-593.

[21] Khattak, Z., Manan, J and Sulaiman, . S (2011) Analysis of open environment sign-in schemes-privacy enhanced & trustworthy approach, *Journal of Advances in Information Technology*, 2(2), 109-121.

[22] Lee, K. G., Chong, C. W., &Ramayah, T. (2017). Website characteristics and web users' satisfaction in a higher learning institution. *International Journal of Management in Education*, *11*(3), 266-283.

[23] Lungu, I., &Tăbuşcă, A. (2010). Optimizing anti-phishing solutions based on user awareness, education and the use of the latest web security solutions. *Informatica Economica*, 14(2), 27-36.

[24] Markos, S., &Sridevi, M. (2010). Employee engagement: The key to improving performance. *International Journal of Business and Management,* 5(12), 1-15.

[25] Mathiassen, L., & Pries-Heje, J. (2006). Business agility and diffusion of information technology. *European Journal of Information Systems,* (15), 116-119.

[26] McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal Of Internet Commerce*, 9(1), 23-41.

[27] Microsoft, (2017). Microsoft security bulletin MS17-010: Critical, Microsoft, TechNet

[28] Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, *28*(6), 2366-2375.

[29] Ng, B. Y., Kankanhalli, A., &Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825.

[30] Oosterhout, M. V., Waarts, E., & Van Hillegersberg, J. (2006). Change factors requiring agility and implications for it. *European Journal of Information Systems*, 15(2), 132-145.

[31] Overby, E., Bharadwaj, A., &Sambamurthy, V. (2006). Enterprise agility and the enabling role of information technology. *European Journal of Information Systems,* 15(2), 120-131.

[32] Park, Y. (2011). The dynamics of opportunity and threat management in turbulent environments: The role information technologies. Doctor Dissertation.

[33] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., &Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security*, *42*, 165-176.

[34] Sasse, M. A., &Flechais, I. (2005). Usable security: Why do we need it? How do we get it? *In: Cranor, LF and Garfinkel, S, (eds.) Security and usability: Designing secure systems that people can use. (pp. 13 - 30).* O'Reilly: Sebastopol.

[35] Sasse, M. A., &Flechais, I. (2005). Usable security: Why do we need it? How do we get it?. O'Reilly.

[36] Schneier, B. (2004). Customers, passwords, and Web sites. *IEEE Security & Privacy*, *2*(4), 88-99.

[37] Schultz, E. (2005). From the Editor-in-Chief: the human factor in security. *Computers and security*, *24*(6), 425-426.

[38] Seo, D., & Paz, A. (2008). Exploring the dark side of is in achieving organizational agility. *Communication of the ACM,* 51(11), 136-139

[39] Sharifi, H., & Zhang, Z. (2001). Agile manufacturing in practice: Application of a methodology. *International Journal of Operations & Production Management*, 21(5), 772-794.

[40] Sherehiy, B. (2008). *Relatioships between agility strategy, work organization and workforce agility.* Doctor Dissertation, University of Louisville

[41] Tsourveloudis, N., &Valavanis, K. (2002). On the measurement of enterprise agility. *Journal of Intelligent & Robotic Systems*, 33(3), 329-342.

[42] Vance, A., Siponen, M., &Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198.

[43] Warr, P., &Inceoglu, I. (2012). Job engagement, job satisfaction, and contrasting associations with person–job fit. *Journal of Occupational Health Psychology*, 17(2), 129-138.

[44] Yeganegi, K., &Azar, M. (2012). *The effect of IT on organizational agility: Proceedings of the 2012 international conference on industrial engineering and operations management,* Istanbul, Turkey.

[45] Zain, M., Rose. R., Abdullah, I., &Masrom, M. (2005). The relationship between information technology acceptance and organizational agility in Malaysia. *Information & Management*, 42(1), 829-839

[46] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., &Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 1(1), 1-16.