Int Journal of Social Sciences Management and Entrepreneurship 8(1): 970-983 2024

ISSN 2411-7323

www.sagepublishers.com

© SAGE GLOBAL PUBLISHERS

INTERNET OF THINGS AND CYBER ATTACKS AMONG FINTECH COMPANIES IN KENYA

[1] Karanja Maryanne Wanjiru, [2] Dr. Gatobu Purity

[1] MsC Student ICT Management, Jomo Kenyatta University of Agriculture and Technology

[2] Lecturer, Jomo Kenyatta University of Agriculture and Technology

ABSTRACT

In the advent of technological growth, information and communication growth, the internet security has become an issue of significant importance attracting the attention of cyber security experts, governments, organizations and individuals. Cyber security has become an issue of great concern to policymakers, organizations, governments, and people yet it has received little attention in empirical literature. Cyber insecurity has resulted to data loss, financial loss, cyber bulling, drive in crime among other problems. The general objective is to establish the effect of internet of things and cyber security on Fintech companies in Kenya. The specific objectives were to analyze the effect of security configuration on cyber security among Fintech companies in Kenya and to establish the effect of system configuration on cyber security among Fintech companies in Kenya. The study employed mixed method research design by incorporating both quantitative and qualitative research. The study population were 66 Fintech companies in Kenya. The study adopted a census approach covering all the 66 information technology managers in the 66 Fintech companies in Kenya. This study employed a semi structured questionnaire and secondary data collection template. The data collected were analyzed using descriptive statistics including mean, modes and measures of dispersion. Further, based on the Common Vulnerability Scoring System ranking, the data was analyzed to provide a combined risk rating and score. Regression model was employed to determine the effect of internet of things on cyber security of Fintech companies in Kenya. Upon data analysis the study concluded that security configuration and security configuration in the Fintech companies are significant determinants of the prevalence of cyber-attacks among the Fintech companies in Kenya. The study recommended that the companies should also ensure that their IoT devices are kept as current as possible and are adequately protected from threats. The Communication Authority of Kenya ought to enact policies that would ensure that genuine IoT devices are allowed to be introduced in Kenya. Furthermore, the Fintech firms ought to ensure that they put in place policies that would ensure that their software are sourced from genuine sources.

Key Words: Internet of Things, Cyber Security, Fintech companies, Security Configuration, System Configuration

Background of the study

In the advent of technological growth, information and communication growth, the internet security has become an issue of significant importance attracting the attention of cyber security experts, governments, organizations and individuals. Cyber security has become an issue of great concern to policymakers, organizations, governments, and people yet it has received little attention in empirical literature. Cyber insecurity has resulted to data loss, financial loss, cyber bulling, drive in crime among other problems (Dhatrak, *et al.*, 2020) yet little attention has been paid to it by scholars. Cyber security refers to techniques aim at protecting internet users, data, information and devices from internet attack (Bartczak, 2021). Cyber security has become a matter global concern with nations now laying strategies on dealing with it (Klimburg, 2012). Cyber security breaches pose a serious threat to all types of businesses and charities.

The concept of internet of things (IoT) refers to the transformation of the reality of ordinary physical objects to a new level where they can be used as services available on the Internet to provide information in order to improve business management systems and the quality of life Ruiz-de-Garibay et al, (2011). Over the years, the IoT has been growing over time. Over 20 years ago, only one million people were using IoT as a technology. In 2003, the numbers grew to half a billion people and in 2012, the numbers of IoT users rose to 8.7 billion. The number of users have been growing exponentially over the years reaching 28.4 billion in 2017. The Internet of Things is the wireless network of large number of devices, which are interconnected and can have a communication link between each other without any external interference caused by humans (Razzak, 2012).

Internet of Things combines all the peripherals like wireless sensors, networks, data acquisition, data analytics, cloud computing to provide solutions such that the peripheral objects are embedded in a network to provide object-to-object communication and user control over a same network (Dhatrak, et al., 2020). Internet of Things is characterized by a constantly growing network of connected devices, actuators and sensors that can interact with or collect data on their internal states or the external environment, using a variety of different protocols and standards (Europol, 2016).

Examples of IoT gadgets according to Ruiz-de-Garibay et al, (2011) include Philips DirectLife- a personalized fitness program that records your daily movements and easily transfers the information to a webpage that keeps track of your progress against your longer-term goals, Life Pod- which compiles activities that users execute through a 3G mobile phone which includes an RFID reader. The user touches an RFID tag on the mobile phone to obtain information from it or to send reports to the system, Bodytrace - which automatically transfer your weight to the Internet, so users can be assisted in monitoring and weight control diets and music player used through the popular music streaming application Spotify.

Statement of the problem

Most companies in Kenya today have embraced technology as part of them. Most of the work of these companies is technologically aided. Though information communication technology has increased efficiency and effectiveness of these companies, it has led to increased cyber-attacks (Wambalaba et al, 2021). The risks associated with cyber-attacks that is economic impact risks including financial losses, company market value risks and customer trust risks have been on the rise. Another risk is the social impact risks, which include cyber bulling, friendships and sexual solicitation. IoT affect businesses and economies worldwide and hence the urgent need of concern. According to Serianu (2018), Kenya’s economy lost more than KES 29.5 billion from cyber-attacks in 2018. In 2020, Cybercrimes in Kenya increased in nearly 140 million in 2020 (Julia, 2021). This represented an increase of approximately 40 percent from 84 million cybercrimes in

2020 (Statista, 2020). Kenya lost USD 232.6 million due to cyber-attacks in 2020. In 2021, about 39 million cyber threats were detected in Kenya and about 27000 cyber advisories issued between the months of April and June (Communications Authority of Kenya, 2021).

In addition to the Cyber-attack, the technological devices employed face various threats including both unstructured threats and structured threats (Jain et al. 2020). The devices also face attacks that include denial-of-service (DoS) physical attacks and system attacks (Obaid & Abeed, 2020). Vulnerabilities in the devices also expose the Fintech firms to cyber-attacks. The vulnerabilities could be hardware or software vulnerabilities (Jain et al. 2020). Despite the cyber security problems being witness because of the advent of IoT, there are limited studies focusing at the impact of IoT on cyber security particularly in the Fintech space.

Internet of Things is faced with a number of security threats. Because, IoT wearable banking equipment is manufactured by different manufacturers and needs different maintenance approaches, this lack of a popular standard that can lead to a flaw in the functionality of IoT. Furthermore, IoT may produce large quantities of data, generating additional costs associated with the storing and securing of all those data. In addition, IoT has increases the unemployment rate. Other threats include security threats to chatbots. These chatbot threats include spoofing or impersonating someone else, data manipulation, and data theft. IoT has led to the emergence of data breaches. Hackers can now attack IoT devices like smartwatches, smart meters, and smart home devices to gain additional user and organizational data (Nordin et al, (2020).

Several studies have been conducted on internet n things and cyber security (Ahmad & Habib, 2010; Moschovitis, 2018; Pal et al, 2020; Anand et al, 2020). In a study on network infrastructure and cyber security, Reuben and Ouma. (2021) and Moschovitis, (2018) and explicitly indicate how network setup and management relate to cyber-attacks. The proposed study seeks to fill the gap by determining how network setup and management may influence cyber-attacks. Studies carried out by Pal et al, (2020) and Anand et al, (2020) on device connection architecture gave an explanation of the concept but failed to relate the concept with cyber security. The proposed study seeks to fill the gap by finding out the effect of arrangement of devices and device communication path on cyber-attacks among the Fintech firms in Kenya.

Ahmad and Habib, (2010) and Waithaka, (2016) provided an explanation on security configuration and its components. Howerver the studies did not explain the effect of individual component on cyber security. This study therefore provides the influence of antivirus installation, user knowledge and level of information access on cyber-attacks among the Fintech firms in Kenya. In a research study conducted by Kilani, (2020) and Lenaeus et al, (2015) on system configuration, the authors did not pinpoint the critically of installation procedures, maintenance and availability of security access modules in enhancing cyber security. Therefore, the proposed study seeks to access the effect of installation procedures, maintenance and availability of security access modules on cyber security among the Fintech firms in Kenya. This study therefore aims at establishing the impact of internet of things and cyber-attacks among Fintech firms in Kenya.

Specific Objectives of the study

The specific objectives were;

i. To analyze the effect of security configuration on cyber attacks among Fintech companies in Kenya.
ii. To establish the effect of system configuration on cyber attacks among Fintech companies in Kenya.

LITERATURE REVIEW

Theoretical Literature

Decomposed Theory of Planned Behaviour.

The decomposed theory of planned behaviour is an improvement of the theory of planned behaviour by Ajzen, (1985). The theory of planned behaviour was decomposed by Taylor and Todd (1995). Taylor and Todd (1995) decomposed attitude towards behavior, subjective norm, and perceived behavioral control into multi-dimensional belief constructs within technology adoption contexts. The decomposed theory of planned behavior was improved by including three factors from the Innovation diffusion theory viewpoint, which are relative advantage, compatibility, and complexity. The relative advantage and compatibility were joined together in order to make some effect on perceived behavioral control (Taylor and Todd, 1995).

A study by Tsuen-Ho et al, (2006) on the application of the decomposed theory of planned behavior to analyze consumer behavioral intention towards mobile text message revealed that the decisive or crucial factors influencing the behaviour and intention of consumers in using m-coupons are attitude and perceived behavioural control, while subjective norms are not evident. The perceived usefulness under ‘behavioural attitude’ has a big effect on behavioural attitude; the influence of the primary group under ‘subjective norms’ was also evident, while self-efficacy under ‘perceived behavioural control’ is the most significant influential factor. Another research by Hsu & Chiu, (2004) on predicting electronic service continuance with a decomposed theory of planned behaviour suggested that users' continuance intention is determined by Internet self-efficacy and satisfaction. Satisfaction, in turn, is jointly determined by interpersonal influence, perceived usefulness, and perceived playfulness.

Cyber threats include unstructured threats that are caused by individuals with experience using tools cheaply available for hacking the system and structured threats that are caused by individuals with knowledge on the existing vulnerabilities within a specific system. Since these threats are controlled by humans, these individuals access the system to check on its complexibility and also compatibility with their systems and also look for the points of weaknesses for launching attacks. This theory helps explain the behaviour of these individuals on cyber-attacks.

Conceptual Framework

This section presents a conceptual framework. From this conceptual framework, the independent variables are security configuration and system configuration and cyber attacks as the dependent variable. The conceptual framework is presented in figure 2.1.

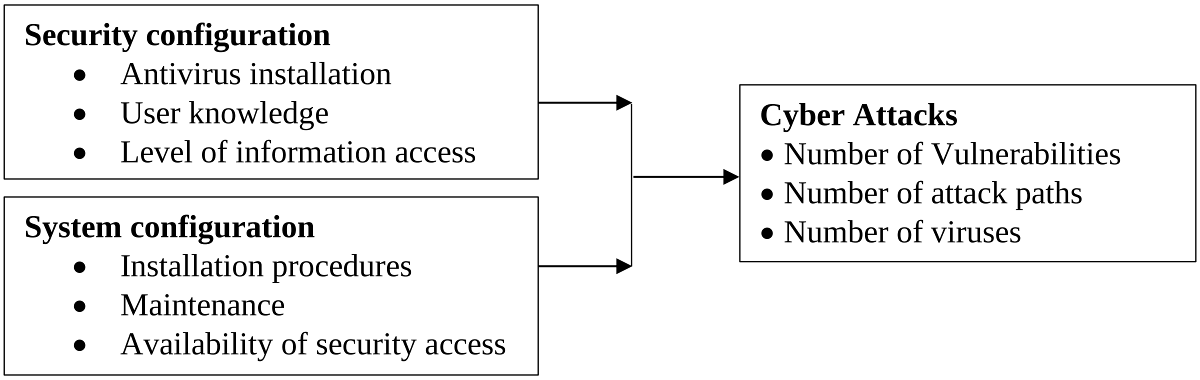

Figure 2.1: Conceptual Framework

Security Configuration

The antivirus installation is important as it would protect the devices from viruses, spyware, malware, Trojans, phishing attacks, rootkits and spam attacks, as well as any other cyber threats. The procedure of installing the antivirus is as follows; download the trend micro, maximum security, double-click the downloaded file to run the installer, click yes if the user account window appears, follow the instructions thereafter to complete installation and fill out the account information to activate protection.

The device use knowledge entails knowledge sharing drives innovation and the opportunity to develop a sustainable competitive advantage. However, in the extant knowledge management and information security literature, leakage from sharing activities is neglected. The risk of knowledge leakage is exacerbated with the pervasive use of mobile devices and the adoption of BYOD (Bring Your Own Device). We use the Decomposed Theory of Planned Behaviour (DTPB) to explain the causes behind this phenomenon and how it negatively affects organization’s competitive advantage (Agudelo et al, 2016).

Technology has transformed the way information is accessed and transferred. For personal communications there are blogs, wikis, and instant messaging. New software– like Blackboard or Angel, and podcasting–impacts the way instructors interact with classes. It is useful to consider to what extent these new venues of communication change professional assessments of the value and quality of educational information. Instructors have always endeavored to lead students to high quality information, often by recommending specific journals or researchers (Corby, 2008).

System Configuration

Before carrying out any system installation, effective planning simplifies your installation, which eliminates the need to stop and restart the process because you do not know the information requested by the installer and reduces post-installation problems. The following are tasks you should complete or information you should know before starting the installation; planning and gathering information that is the use of deployment guide and installation organizer and synchronizing cocks.

The most important resource of computer information system is the information, the quality of which resolves the implementation of tasks to achieve the final result. The quality of information means the combined implementation of its following properties, namely, completeness, reliability, timeliness, safety and storage reliability. Achieving the goals requires the functioning of computer information system, when the requirements of maximum reliability are provided, since the system errors turn into losses of various kinds. In this case, it is necessary to ensure the reliability of individual properties such as reliability, maintainability, storage ability, durability, which are realized through the maintenance and repair (Mehdiyev, 2017).

According to Lenaeus et al, (2015) assets including information assets, such as data and information systems, need to be protected from security threats. To protect their information assets, the fintech firms should be able to design their security programs. The programs should be implemented and the firms should maintain a security program information within the firm. This is to protect the firms from attacks.

Empirical Review

Security Configuration and Cyber Attacks

A research study was done by Waithaka, (2016) on factors affecting cyber security in national government ministries in Kenya. This study used primary data and employed a descriptive research design. The findings of the research conclude that factors affecting cyber security in the National Government Ministries in Kenya are principally divided in to external motivations for cyber-attacks and internal organizational system vulnerabilities. The internal organizational factors affecting cyber security that were identified include adherence of cyber security strategy and standards and employees' systems exploitation for personal gains.

Amrin, (2014) did a research on the impact of cyber security on SMEs. The findings of the study suggested that the Anti-virus/malware/spam are the most widely known type of IT security technologies. The use of encrypted login sessions and keeping media backups are also indications of good IT practices. Nevertheless, the use of legal software was low. One of the good practices of IT security technology is using open source operating systems and software. However, open source software is not common among non-IT related businesses, as the user without technical background might find it hard to use. Compared to Australian SMEs, European SMEs fall behind in adopting IT security technologies. The number of large enterprises is higher than SMEs, in case of using specific security technology.

A study conducted by Ahmad and Habib, (2010) on analysis of network security threats and vulnerabilities by development and implementation of a security network monitoring. The results of the study suggested that properly configured firewalls, strong passwords that changed on regular basis, antivirus update on regular basis among other security precautions are all elements used collectively to good security practices. Deficiencies in bad products can defeat with good practice, whereas bad process can be diluted otherwise excellent products. It is better to have no security devices instead of incorrectly configured security devices.

Lenaeus et al, (2015) did a study on how to implement security controls for an information security program at CBRN facilities and concluded that Configuration management is used to establish, implement, and actively manage the security configuration of systems. A rigorous configuration management and change control process reduces security risks for information systems. To support security within the life cycle of information systems, the versions of hardware and software that are in use should be kept as current as feasible. Hardware and software configurations should be reviewed and approved by the information or cyber security team within the facility. Reviews are often conducted annually, if not more frequently, to ensure configurations are adequate to meet identified threats.

Using systematic literature review, de Melo, Miani and Rosa (2022) investigated a security architecture for anomaly detection in home networks. Despite the benefits of this interaction, these devices are also prone to security threats and vulnerabilities. Ensuring the security of smart homes is challenging due to the heterogeneity of applications and protocols involved in this environment. The study proposed a Family Guard architecture to add a new layer of security and simplify management of the home environment by detecting network traffic anomalies.

Security is the major point in terms of IoT devices. Rabbi, Jubayer and Hossain (2019) conducted a study on vulnerabilities to internet of things and current state of the art of security architecture. The study employed the Kitchenham structure to conduct a systematic literature review. Because of its complex architecture and some definite feature like heterogeneity, limitations it differs from device to device. IoT device has led to increased cyber security.

Ye and Qian (2017) conducted a study on security architecture for networked internet of things devices. The study developed an IoT security architecture that can protect NoTs in different IoT scenarios. The security architecture consists of an auditing module and two network-level security controllers. The auditing module is designed to have a stand-alone intrusion detection system for threat detection in a NoT network cluster. The two network-level security controllers are designed to provide security services from either network resource management or cryptographic schemes regardless of the NoT security capability. The developed IoT security architecture consisted a network based one-hop confidentiality scheme and a cryptography-based secure link mechanism.

System Configuration and Cyber Attacks

A research by Kilani, (2020) on Cyber-security effect on organizational internal process using a quantitative approach and use of a questionnaire. The findings of this study show that cyber-security motivators that is the data growth, the technology expansion, the access to required resources, the operational control, and the technical control indirectly affect solid internal processes that are attributed to the consistency of technological infrastructure in an organization. Operational and the technical control affect the organizations cyber security and the cyber-attacks that may affect the organization.

A study by Lenaeus et al, (2015) on how to implement security controls for an information security program at CBRN facilities suggested that security controls need to be implemented that cover management, operational, and technical actions that are designed to deter, delay, detect, deny, or mitigate malicious attacks and other threats to information systems. The protection of information involves the application of a comprehensive set of security controls that addresses cyber security, physical security, and personnel security. It also involves protecting infrastructure resources upon which information security systems rely like electrical power, telecommunications, and environmental controls. The application of security controls is at the heart of an information security management system. The selection and application of specific security controls is guided by a facility’s information security plans and associated policies.

Moschovitis, (2018) in his study on cybersecurity program development for business found out that effective protection against viruses, Trojans and other malicious software requires a layered approach. Deployment of a combination of many techniques to keep the environment safe is necessary. Use of thumb drives and other removable media should also be applied with care because these media could have malicious software pre-installed that can infect your computer, the source of the removable media devices should be trusted before being used. Combining the use of web filtering, antivirus signature protection, proactive malware protection, firewalls, strong security policies and employee training significantly lowers the risk of infection. Keeping protection software up to date along with your operating system and applications increases the safety of your systems.

RESEARCH METHODOLOGY

The study used a descriptive survey design. The study population were 66 Fintech companies in Kenya. The units of observation were the 66 information technology managers in the Fintech firms under study. The IT managers have been selected because they have knowledge on issues related to internet of things and cyber attacks. Since the population under study is small, the study adopted a census approach covering all the 66 information technology managers of all the Fintech companies under study. Census approach is used when the study population is small. This study employed a semi structured questionnaire and secondary data collection template. The semi-structured questionnaires was developed as per the objectives of the study. The data collected were analyzed using descriptive statistics including mean, modes and measures of dispersion and Inferential statistics.

RESULTS AND DISCUSSION

The target population for the study was 66 respondents. The study adopted a census study. 6 respondents participated in the pilot study. A total of 60 respondents participated in the main study. However, out of the 60 questionnaires administered in the study, 51 questionnaires were dully filled and received back representing a response rate of 85 percent

Security Configuration

Primary data was adopted and was collected using a structured questionnaire. The responses were measured using a Likert Scale ranging from the values 1 to 5 with the value 1 representing that the response was in strong disagreement and the value 5 implying that the response was strongly in agreement. The study further computed the means with a mean of 1 indicating that the average response was in strong disagreement, mean of 2 implying disagreement, mean of 3 implying moderately in agreement, mean of 4 implying an agreement on average and finally a mean of 5 implying a strong agreement on average. A summary of the responses on the questions on security configuration are tabulated in Table 1.

Table 1: Descriptive Results for Security Configuration

	SD	D	N	A	SA		
	f %	f %	f %	f %	f %	M	S Dev
There are limitations in place to accessing files and sites within the company.	1 2%	2 3.9%	12 23.5%	17 33.3%	19 37.3%	4.0	1.0
The company system is set in way that automatically backs up company files already stored.	2 3.9%	4 7.8%	14 27.5%	16 31.4%	15 29.4%	3.7	1.1
The company has a unique server password accessible to limited company personnel.	5 9.8%	1 2%	13 25.5%	13 25.5%	19 37.3%	3.8	1.3
The company uses a secured Wi-Fi	2 3.9%	1 2%	9 17.6%	19 37.3%	20 39.2%	4.1	1.0
The company uses firewall protection in its system.	4 7.8%	5 9.8%	9 17.6%	23 45.1%	10 19.6%	3.6	1.2

It is clear from the results tabulated that the statement, there are limitations in place to accessing files and sites within the company received the following responses. 19(37.3%) of the responses concurred strongly, 17(33.3%) of them were in tandem whereas 12(23.5%) did not take any side. The line mean of the statement was 4.0 whereas its corresponding standard deviation was 1.0 indicating that the responses were in tandem that there are limitations in place to accessing files and sites within the company.

The company system is set in way that automatically backs up company files already stored attracted responses as follows. 14(27.5%) of the responses had a moderate perception, 16(31.4%) of those contacted concurred and 15(29.4%) had a strong agreement. The mean and standard deviation of the statement were 3.7 and 1.1 respectively. This implies that the respondents were in agreement that the company system is set in way that automatically backs up company files already stored.

Additionally, concerning the statement, the company has a unique server password accessible to limited company personnel, 19(37.3%) of the respondents recorded a strong concurrence, 13(25.5%) of them in concurrence and 13(25.5%) of them were neutral. The line mean and standard deviation of the statement were 3.8 and 1.3 in that order implying an agreement among the responses that the company has a unique server password accessible to limited company personnel.

On whether the company uses a secured Wi-Fi, the responses received were as follows. 9(17.6%) had moderate opinions, 19(37.3%) of those contacted agreed and 20(39.2%) had a strong agreement. The mean and standard deviation of the statement were 4.1 and 1.0 respectively. This implies that the respondents agreed that the company uses a secured Wi-Fi.

Finally, regarding the question, the company uses firewall protection in its system, 10 (19.6%) of the responses recorded a strong opinion, 23(45.1%) agreed whereas 9(17.6%) held a neutral stand. The mean and the line standard deviation were 3.6 and 1.2 indicating that the company uses firewall protection in its system.

System Configuration

The study utilized primary data collected using a structured questionnaire. The responses were measured using a Likert Scale ranging from the values 1 to 5 with the value 1 representing that the response was in strong disagreement and the value 5 implying that the response was strongly in agreement. The study further computed the means with a mean of 1 indicating that the average response was in strong disagreement, mean of 2 implying disagreement, mean of 3 implying moderately in agreement, mean of 4 implying an agreement on average and finally a mean of 5 implying a strong agreement on average. A summary of the responses on the questions on system configuration are tabulated in Table 2.

Table 2: Descriptive Results for System Configuration

	SD	D	N	A	SA		
	f %	f %	f %	f %	f %	M	S Dev
There is an initial trial period with limited access for new employees	1 2%	5 9.8%	10 19.6%	16 31.4%	19 37.3%	3.9	1.1
Employee system transactions are monitored regularly	0 0%	2 3.9%	10 19.6%	24 47.1%	15 29.4%	4.0	0.8
The company conducts regular trainings on the careful use of passwords and also technological devices	0 0%	4 7.8%	10 19.6%	23 45.1%	14 27.5%	3.9	0.9
The company system is configured in such a way that it prohibits sharing files from unknown sources	2 3.9%	3 5.9%	13 25.5%	20 39.2%	13 25.5%	3.8	1.0
Access to the wireless networks, equipment and other sensitive data is guarded using unique individual user names and passwords	3 5.9%	4 7.8%	12 23.5%	14 27.5%	18 35.3%	3.8	1.2
All the company systems are installed with up to date anti-virus software	2 3.9%	3 5.9%	5 9.8%	21 41.2%	20 39.2%	4.1	1.0

It can be noted from the tabulated results that the question, there is an initial trial period with limited access for new employees recorded responses as follows. 19(37.3%) of the responses recorded a strong concurrence, 16(31.4%) of them were in agreement whereas 10(19.6%) did not take any side. The line mean of the statement was 3.9 whereas its corresponding standard deviation was 1.1 indicating on average, the respondents agreed that there was an initial trial period with limited access for new employees.

Employee system transactions are monitored regularly recorded responses as follows. 10(19.6%) of the study participants did not take any position regarding the statement, 24(47.1%) of those were in tandem and 15(29.4%) had a strong agreement. The mean and standard deviation of the statement were 4.0 and 0.8 respectively. This implies that the respondents were in agreement that employee system transactions are monitored regularly.

It is clear from the results that the statement, the company conducts regular trainings on the careful use of passwords and also technological devices recorded the following responses. 14(27.5%) of the responses recorded a strong agreement, 23(45.1%) of them were in agreement whereas 10(19.6%) were moderate in their opinion. The line mean of the statement was 3.9 whereas its corresponding standard deviation was 0.9 indicating that the responses were in agreement that the company conducts regular trainings on the careful use of passwords and also technological devices.

The company system is configured in such a way that it prohibits sharing files from unknown sources attracted responses as follows. 13(25.5%) of the participants in the study did not take any position regarding the statement, 20(39.2%) of those contacted were in tandem and 13(25.5%) had a strong agreement. The mean and standard deviation of the statement were 3.8 and 1.0 in that order. This implies that the respondents were in agreement that the company system is configured in such a way that it prohibits sharing files from unknown sources.

Furthermore, concerning the question, access to the wireless networks, equipment and other sensitive data is guarded using unique individual user names and passwords, 18(35.3%) of the respondents recorded a strong agreement with regards the statement, 14(27.5%) of them were in agreement and 12(23.5%) of them were neutral. The line mean and standard deviation of the statement were 3.8 and 1.2 in that order implying that the respondents were in agreement that access to the wireless networks, equipment and other sensitive data is guarded using unique individual user names and passwords.

Finally, all the company systems are installed with up to date anti-virus software, the responses indicated that 21(41.2%) of the respondents were in tandem, 5(9.8%) recorded a neutral position whereas 20(39.2%) indicated a strong concurrence with the statement. The mean and the standard deviation of the statement were 4.1 and 1.0 in that order meaning that the responses were in agreement that all the company systems are installed with up to date anti-virus software.

Cyber Attacks

Primary data used in the study was collected using a structured questionnaire. The responses were measured using a Likert Scale ranging from the values 1 to 5 with the value 1 representing that the response was in strong disagreement and the value 5 implying that the response was strongly in agreement. The study further computed the means with a mean of 1 indicating that the average response was in strong disagreement, mean of 2 implying disagreement, mean of 3 implying moderately in agreement, mean of 4 implying an agreement on average and finally a mean of 5 implying a strong agreement on average. A summary of the responses on the questions on cyber attacks are tabulated in Table 3.

Table 3: Descriptive Results for Cyber Attacks

	SD	**D**	**N**	**A**	**SA**		
	f %	**f %**	**f %**	**f %**	**f %**	**M**	**S Dev**
The company has experienced malware attacks	2 3.9%	5 9.8%	2 3.9%	39 76.5%	3 5.9%	3.7	0.9
Phishing attacks are regularly experienced in the company	0 0%	6 11.8%	1 2%	39 76.5%	5 9.8%	3.8	0.8
The company often faces man-in-the-middle attacks	3 5.9%	3 5.9%	5 9.8%	39 76.5%	1 2%	3.6	0.9
Denial-of-service attacks are usually experienced in the company	5 9.8%	5 9.8%	5 9.8%	32 62.7%	4 7.8%	3.5	1.1

SQL injection attacks are faced by the company more often	1 2%	2 3.9%	5 9.8%	41 80.4%	2 3.9%	3.8	0.7

The company has experienced malware attacks attracted the following responses. 2(3.9%) of the participants in the study did not take any position, 39(76.5%) of those contacted were in concurrence and 3(5.9%) had a strong agreement. The mean and the corresponding standard deviation of the statement were 3.7 and 0.9. This implies that the respondents were in agreement that the company had experienced malware attacks.

Furthermore, regarding the statement, phishing attacks are regularly experienced in the company, 5(9.8%) of the responses were strongly in tandem, 39(76.5%) of them were in agreement whereas 1(2%) did not take any side. The line mean of the statement was 3.8 whereas its corresponding standard deviation was 0.8 indicating that the responses were in agreement that phishing attacks were regularly experienced in the company.

Additionally, with regards to the question, the company often faces man-in-the-middle attacks, 1(2%) of the respondents recorded a strong opinion with regards the statement, 39(76.5%) of them were in agreement and 5(9.8%) of them were neutral. The line mean and standard deviation of the statement were 3.6 and 0.9 in that order implying that the respondents were in agreement that the company often faces man-in-the-middle attacks.

It can be observed from the results tabulated that the statement, denial-of-service attacks are usually experienced in the company received the following responses. 4(7.8%) of the responses strongly agreed, 32(62.7%) of them were in agreement whereas 5(9.8%) did not take any side. The line mean of the statement was 3.5 whereas its corresponding standard deviation was 1.1 an implication of an average agreement among the responses that denial-of-service attacks were usually experienced in the company.

Finally, with regards the statement, SQL injection attacks are faced by the company more often, 2(3.9%) of the responses recorded a strong agreement, 41(80.4%) of them were in agreement whereas 5(9.8%) did not take any side. The line mean of the statement was 3.8 whereas its corresponding standard deviation was 0.7 indicating that the responses were in agreement that SQL injection attacks were faced by the company more often.

Correlation Statistics

Correlation analysis serves to determine the strength and direction of relationship between internet of things and cyber-attacks among Fintech companies in Kenya. The correlation results are outlined in Table 4.

Table 4: Correlation Results

		Cyber Attacks	**Security Configuration**	**System Configuration**
Cyber Attacks	Pearson Correlation	1		
	Sig. (2-tailed)			
	N	51		
Security Configuration	Pearson Correlation	.547**	1	
	Sig. (2-tailed)	0.000		
	N	51	51	
System Configuration	Pearson Correlation	.502**	.350*	1
	Sig. (2-tailed)	0.000	0.012	
	N	51	51	51

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

The correlation between security configuration and cyber-attacks from the analysis of the results of the study portrayed a positive and statistically significant relationship (r=0.547, p=0.000<0.05). This has the implication that security configuration positively affects cyber-attacks among the Fintech companies in Kenya. Finally, the correlation between system configuration and cyber-attacks from the analysis of the results of the study portrayed a positive and statistically significant relationship (r=0.502, p=0.000<0.05). This has the implication that system configuration positively affects cyber-attacks among the Fintech companies in Kenya.

Regression Results

Regression analysis serves to determine the linear relationship between the dependent and the independent variables in the study. The dependent variable was cyber-attacks while the independent variables were security configuration and system configuration.

Table 5: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.745a	0.554	0.516	0.38635

a Predictors: (Constant), System Configuration, Security Configuration,

It is clear from the results in Table 5 that the estimated model explains to a tune of 55.4% of the total variations in cyber-attacks among the Fintech companies in Kenya. This is supported by the R Squared value of 0.554 in the estimated model. This implies that the independent variables under study are significant in explaining the prevalence of cyber-attacks among the Fintech companies in Kenya.

Table 6: ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	8.546	4	2.136	14.313	.000b
	Residual	6.866	46	0.149		
	Total	15.412	50			

a Dependent Variable: Cyber Attacks
b Predictors: (Constant), System Configuration, Security Configuration,

The outcomes outlined in Table 6 points out the statistical significance of the estimated model. This is supported by the estimated P value in the model (0.000<0.05) as well as the estimated F value (14.313) less than the F critical 2.04099 in the F tables. The estimated results can therefore be used to give reliable inference.

Regression Coefficients

The dependent variable was cyber-attacks while the independent variables were network infrastructure, device connection architecture, security configuration and system configuration. The regression coefficient estimates for the variables are provided in Table 7. The estimated regression coefficients are used to estimate a regression model.

Table 7: Regression Coefficient Results

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-0.15	0.456		-0.328	0.745
	Security Configuration	0.256	0.099	0.287	2.587	0.013
	System Configuration	0.274	0.106	0.276	2.579	0.013

a Dependent Variable: Cyber Attacks

The estimated regression model was;

Y= -.15 + ..256X*1* + .274X*2*

Where

Y is cyber attacks among Fintech companies in Kenya

X_1 is security configuration and,

X_2 is system configuration.

The coefficient of the variable security configuration was positive (0.256) and statistically significant ($p=0.013<0.05$). This implies that a unit improvement in the security configuration by the Fintech companies in Kenya would yield a significant 0.256 unit improvement in the prevalence of cyber-attacks among the Fintech companies under review. Thus, the study concludes that security configuration in the Fintech companies is a significant determinant of the prevalence of cyber-attacks among the Fintech companies in Kenya.

Finally, the coefficient of the variable system configuration was positive (0.274) and statistically significant ($p=0.013<0.05$). This implies that a unit improvement in the system configuration by the Fintech companies in Kenya would yield a significant 0.274 unit improvement in the prevalence of cyber-attacks among the Fintech companies under review. Thus, the study concludes that system configuration in the Fintech companies is a significant determinant of the prevalence of cyber-attacks among the Fintech companies in Kenya.

Conclusions

The study concludes that security configuration in the Fintech companies is a significant determinant of the prevalence of cyber-attacks among the Fintech companies in Kenya. A rigorous configuration management and change control process reduces security risks for information systems. To support security within the life cycle of information systems, the versions of hardware and software that are in use should be kept as current as feasible. Hardware and software configurations should be reviewed and approved by the information or cyber security team within the facility. Properly configured firewalls, strong passwords that changed on regular basis, antivirus update on regular basis among other security precautions are all elements used collectively to good security practices. Deficiencies in bad products can defeat with good practice, whereas bad process can be diluted otherwise excellent products. The use of encrypted login sessions and keeping media backups are also indications of good IT practices.

The study concludes that system configuration in the Fintech companies is a significant determinant of the prevalence of cyber-attacks among the Fintech companies in Kenya. Assets including information assets, such as data and information systems, need to be protected from security threats. The Fintech firms should be able to design their security programs to protect the firms from attacks. Cyber-security motivators that is the data growth, the technology expansion, the access to required resources, the operational control, and the technical control indirectly affect solid internal processes attributed to the consistency of technological infrastructure in an organization. Operational and the technical control affect the organizations cyber security and the cyber-attacks that may affect the organization. Thumb drives and other removable media should also be applied with care as these media could have malicious software pre-installed that can infect your computer. Combining the use of web filtering, antivirus signature protection, proactive malware protection, firewalls, strong security policies and employee training significantly lowers the risk of infection. Keeping protection software up to date along with your operating system and applications increases the safety of your systems.

Recommendations to Practice

The study recommends that the Fintech companies in Kenya ought to be mindful of the network configurations within their companies. This is because, weak network infrastructure topology is a catalyzer of cyber security attack and that the modelling mode of the network influences the likelihood of cyber-attacks. In addition, the Fintech companies should regulate the number of devices connected to their systems, which could be effected by introducing various connection layers. This is because, as the number of IoT devices connected increases, so is the likelihood for cyber-attacks. The companies should also ensure that their IoT devices are kept as current as possible and are adequately protected from threats.

The study recommends that the Communication Authority of Kenya ought to enact policies that would ensure that genuine IoT devices are allowed to be introduced in Kenya. Furthermore, the Fintech firms ought to ensure that they put in place policies that would ensure that their software are sourced from genuine sources.

Recommendations for Further Research

The study recommends that further studies be conducted on banking and cyber security in Kenya.

REFERENCES

Agudelo, C. A., Bosua, R., Ahmad, A., & Maynard, S. B. (2016). Understanding knowledge leakage & BYOD (Bring Your Own Device): A mobile worker perspective. *arXiv preprint arXiv:1606.01450*.

Ahmad, N., & Habib, M. K. (2010). *Analysis of network security threats and vulnerabilities by development & implementation of a security network monitoring solution*.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211.

Ali, F., Yigang, H., & Yi, R. (2019). A novel security architecture of internet of things. *International Journal of Computer Theory and Engineering*, *11*(5), 89-96.

Amrin, N. (2014). *The impact of cyber security on SMEs* (Master's thesis, University of Twente).

Anand, P., Singh, Y., Selwal, A., Singh, P. K., Felseghi, R. A., & Raboaca, M. S. (2020). IoVT: internet of vulnerable things? Threat architecture, attack surfaces, and vulnerabilities in Internet of Things And Its Applications Towards Smart Grids. *Energies*, *13*(18), 4813.

Bartczak, K. (2021). Cybersecurity as the Main Challenge to the Effective Use of Digital Technology Platforms in E-Commerce. *European Research Studies*, *24*(2B), 240-256.

Corby, K. (2008). Technology and quality in educational scholarly communication. *Behavioral & Social Sciences Librarian*, *26*(3), 7-19.

de Melo, P. H., Miani, R. S., & Rosa, P. F. (2022). FamilyGuard: A Security Architecture for Anomaly Detection in Home Networks. *Sensors*, *22*(8), 2895.

Dhatrak, A., Sarkar, A., Gore, A., Paygude, M., Waghmare, M., & Sahane, H. (2020). Cyber Security Threats and Vulnerabilities in IoT. *International Research Journal of Engineering and Technology*, *7*(03).

Europol (2016). Cybersecurity and the Internet of Things – a Law Enforcement Perspective. Europol Unclassified – Basic Protection Level. Releasable to EU Member States and EU Institutions**.** The Hague, 24 April 2016.

Hsu, M. H., & Chiu, C. M. (2004). Predicting electronic service continuance with a decomposed theory of planned behaviour. *Behaviour & Information Technology*, *23*(5), 359-373.

Jain,N.K, Mittal, P. and Saini, R.K., (2020). Security Vulnerabilities in the IoT. In Privacy Vulnerabilities and Data Security Challenges in the IoT (pp. 93-114). CRC Press. (2022).

Kilani, Y. (2020). Cyber-security effect on organizational internal process: Mediating role of technological infrastructure. *Problems and Perspectives in Management*, *18*(1), 449.

Klimburg A, (2012). National cyber security framework manual.

Lenaeus, J. D., O'Neil, L. R., Leitch, R. M., Glantz, C. S., Landine, G. P., Bryant, J. L., ... & Johnson, C. (2015). *How to implement security controls for an information security program at CBRN facilities* (No. PNNL-25112). Pacific Northwest National Lab.(PNNL), Richland, WA (United States).

Mehdiyev, S. (2017). Computer System's Maintenance In A Corporate Environment. *Problems of information technology*, *8*(1), 84-90.

Moschovitis, C. (2018). *Cybersecurity Program Development for Business: The Essential Planning Guide*. John Wiley & Sons.

Obaid, H.S. and Abeed, E.H., 2020. Dos and DDoS attacks at OSI layers.International Journal Multidisciplinary Research and Publication, 2(8),

Pal, S., Hitchens, M., Rabehaja, T., & Mukhopadhyay, S. (2020). Security requirements for the internet of things: A systematic approach. *Sensors*, *20*(20), 5897.

Rabbi, F., Jubayer, A. & Hossain, S., M. (2019). Vulnerabilities to Internet of Things and Current State of the Art of Security Architecture. *International Journal of Recent Technology and Engineering*, 8(4), 1758-1763.

Razzak, F. (2012). Spamming the Internet of Things: A Possibility and its probable Solution. *Procedia computer science*, *10*, 658-665.

Reuben, James & Ouma, Johnmark. (2021). Intrusion Detection and Prevention of Cyber-threats using Open-Source Software for Fintech Startup Firms in Kenya.

Serianu (2018): Africa Cyber Security Report-Kenya.

Solutions, A. S. (2018). *Educational*. *Retrieved March*, *5*th 2024 from https://www.un.org/sustainabledevelopment/education/.

Statista, (2020): Cyber Crime & Security.

Tsuen-Ho, H., Yi-Sheng, W., & Su-Chan, W. (2006). Using the decomposed theory of planned behavior to analyse consumer behavioral intention towards mobile text message coupons. *Journal of Targeting, Measurement & Analysis for Marketing*, *14*(4), 309-324.

Waithaka, S. W. (2016). *Factors affecting cyber security in national government ministries in Kenya* (Doctoral dissertation, University of Nairobi).

Wambalaba, F., Musuva, P., Ouma, M. J., & Nicos, K. (2021). Cybersecurity Risks and National Policy Implications-East African Experiences.

Ye, F., & Qian, Y. (2017, December). A security architecture for networked internet of things devices. In *GLOBECOM 2017-2017 IEEE Global Communications Conference* (pp. 1-6). IEEE.