An Investigation Of Existing Strategies Used To Counter Prevailing Cyber Threats And Vulnerabilities In Banks

Article · June 2020

CITATIONS
0

READS
72

3 authors, including:

Cpa Leonard
Jaramogi Oginga Odinga University of Science and Technology
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Solomon Ogara
Jaramogi Oginga Odinga University of Science and Technology
28 PUBLICATIONS **147** CITATIONS
SEE PROFILE

International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 7 Issue 6, June 2020

ISSN: 2394-4404

An Investigation Of Existing Strategies Used To Counter Prevailing Cyber Threats And Vulnerabilities In Banks

CPA Leonard Wafula Wakoli

Dr. Solomon Ogara

Dr. Samual Liyala

Jaramogi Oginga Odinga University of Science & Technology

Abstract: ***Financial institutions and banks world-wide re grappling with a myriad of challenges in relation to regulations, disruptive models and technologies, new competitors, a restrictive customer base that has unlimited number of expectations. To attempt to stay ahead of others, each financial institution and bank has kept pace with the growing technologies. For instance, the banks that embraced the use of ATM services when they first came attracted customers instantly. Banks have embraced mobile banking service to the letter. However, besides enjoying the services of these new technologies, banks are grappling with how to address the rising tide of cyber-threats to their service delivery. This paper seeks to understand the existing strategies that are used by banks operating in Kenya to counter the growing cyber-threats and vulnerabilities.***

Keywords of the abstract: cybercrime, cyber security, mobile banking, strategies, cyber threats, cyber vulnerabilities

I. INTRODUCTION

Financial services institutions and banks world-over have embrace information and communications technologies (ICTs) to the extent that any disruption of these technologies can bring operations down. With these technologies in place, customers can get service from their banks from anywhere on a 24/7 basis. Examples of ICT intervention for efficiency include: (1) Automated Teller Machines (ATMs).

Typically, an ATM can be used to offer the following services: Cash Withdrawals, checking account balances, order for bank statements or print mini statements, order for Cheque books.

The benefits of an ATM include: Banks keep their operating costs down since customers are encouraged to avoid banking halls, Customers have 24-hour access to their accounts seven days a week, There's no need to carry large amounts of cash around since a customer can access an of ATM any time he/she needs cash. (2) Electronic Funds Transfer (EFT). SWITCH and DELTA are the two main types of debit card used in the Kenya.

They can be used to pay for goods and services instead of cash or Cheques.

This type of payment system is what is referred to as electronic funds transfer (EFT). The main advantages of this mode of transferring cash include the updating of bank accounts on the fly and there is no need to use cash or wait for Cheques to clear. (3) Smart cards – these are like credit or debit cards except that smart cards have inbuilt microchips. The benefits of a microchip include Being used just like cash without the need to wait for authorization unlike EFT systems and that Smart card technology is more reliable than magnetic stripes which are easily damaged. However, the skyrocketing cyber-incidents on financial services institutions and banks call for urgent and focused strategies to counter the menace.

In as much as cyber threats and vulnerabilities are reaching alarming rates, existing initiatives have not adequately addressed the problem. Hence, the Government of Kenya, just like any other government, has no choice but to take the driver's seat as far as the fight against cyber-crime is concerned. To this end, the Government of Kenya passed the Computer Misuse and Cyber-crimes Act 2018. The Central

Bank of Kenya (CBK) has also continued to be on top of the issue through the issuance of Cyber-security Guidelines to all banks operating in Kenya.

The objective of this paper is to investigate and understand the strategies that have been put in place by organizations elsewhere and banks operating in Kenya to mitigate against the cyber-threats and vulnerabilities resulting in cyber-crime. To achieve this objective, this paper examines the existing cyber-security mitigating strategies/approaches world-wide, regionally and locally.

II. LITERATURE REVIEW

A. BACKGROUND INFORMATION

There are numerous challenges to cyber security and target both the public and private sectors in equal measure as so long as vulnerabilities exist. Due to the magnitude and impact of these challenges, researchers, academic and industry practitioners are jointly and separately putting a lot of efforts in seeking ways and means to address the challenges. This section gives a background of the cyberspace and its benefits, existing challenges, increasing cyber-threats, and the existing strategies used to counter the identified cyber-threats. The strategies are looked at from the global, regional, national, and organizational point of views.

The starting point is a synopsis of the cyberspace and its benefits and challenges, increasing cyber threats, then a review of the traditional strategies then a look at the modern ones.

B. THE CYBERSPACE AND ITS BENEFITS

According to the September 2015 Cyber-security Strategy of Japan, Cyberspace is a virtual domain where governments, organizations and individuals change ideas beyond geographical borders. The cyberspace has proved to be a true essential foundation of every country's social-economic activities. The evolution of Information and communication technologies (ICTs) is witnessing major disruptions in the way things are done. For instance, with the Internet technology, it is possible for someone to communicate instantly with others based anywhere around the world through email or social media platforms like WhatsApp, Facebook, Twitter, e.t.c. Hence, with these technologies, innovative services can be easily created for the benefit of all. To fully benefit from the power of ICTs, every effort must be made to counter any cyber-threats that may interfere with these benefits. In a nutshell, a free and fair cyberspace is mandatory for anyone to maximize the benefits from the cyberspace.

C. INCREASING THREATS IN THE CYBERSPACE

Cyber–threats/attacks against financial institutions and banks are on the rise world-wide based various research works and news in the recent times. This could be attributed to the over-reliance on the Internet and other technologies that are vulnerable to cyber-attacks. Globally, according to A.K.M, Bahalul Haque (February, 2019), Bangladesh continues to encounter serious cyber security challenges in the recent times. According to A.K.M. Bahalul Haque (February, 2019), most common malware categories found in organizations in Bangladesh in 2015 include viruses, Trojans and Worms.

The cyber threats vary in style and intent and they include Distributed denial of service (DoS) and payment system attacks that are reportedly very common. In 2017, it is reported that fifty UK financial institutions experienced cyber-attacks. The previous four year had only witnessed as reported by the UK's financial Conduct Authority. Based on the recent reports about cyber-attacks in banks and other organizations worldwide, the increasing pressures from regulators and other parties to confront cybercrime, the war is still far from being won.

Cyber-security has to be looked at holistically, i.e. it should not just be a preserve of the Information technology department but should be a concern for all and look at in the following perspectives: technology, processes and people. According to the study carried out by More et al. (2015), Cyber-crimes in India are growing at a rate of 107% per year with well over 12,000 cases per month.

This alarming statistic, according to the Business Insider India 2015 Report could be attributed to the increasing use of mobile smart phones for Internet banking which have increased vulnerabilities to a large extent.

Regionally, Rwanda, Tanzania, Mauritius Uganda have registered passive cyber-attacks in the past. As for Cyber-attacks, Morocco, Egypt, Nigeria, South Africa & Tunisia have been significantly affected in the past. A research on Internet banking and Commerce e-banking and cyber-security by French (2012) shows that organizations are investing heavily in external security at the expense of internal security. The end result is that cyber-crime continues to hit organizations in alarming proportions.

Locally, the Serianu 2018 Kenya Cyber security Report posits that malware attacks increased and included Emotet (Payment.xls), Trickbot and Zeus Panda. The Crypto mining malware also was experienced in Kenya. Kenyans, particularly those living in Nairobi – the capital city, have ventured into various Crypto currencies such as Bitcoin, Neo and Etheurium. This is fodder for hackers who place crypto mining malware on networks, we sites, devices e.t.c. to launch cyber-attacks. These attacks cause various impacts such as financial losses, for example through inflated electric bills; degradation in performance by slowing down machines, and machine maintenance problems, e.t.c. The survey indicates that crypto malware target financial institutions, educational institutions and manufacturing companies.

The Serianu 2018 Kenya Cyber security Report gives third-party exposure and SIM swap attack as being rampant in banks operating in Kenya. Third parties usually come in handy when an organization wants to focus on its core business. However, third parties bring about vulnerabilities such as compromising victims' accounts through key loggers and Collusion of vendor staff and malicious hackers. SIM swap attack or SIM intercept attack, according to whatis.techtarget.com, is a form of identity theft whereby an attacker tricks a cellphone carrier to switch a victim's phone number to a new device so as to gain access to a bank account, credit card number and other sensitive information.

The symptoms that can be used to identify a SIM swap attack include the discontinuation of sending or receiving text messages and calls to a device. After the attacker has successfully redirected a phone number, the victim's device will practically be incapable of making any communication.

C. EXISTING STRATEGIES USED TO COUNTER CYBER-THREATS

The cyberspace has brought monumental benefits to mankind. However, these benefits are being watered down by cyber-criminals who are working around the clock to negate these gains by perpetrating malicious activities to antagonize the benefits. These malicious activities are on the rise; hence, some action(s) must be taken very quickly.

Unfortunately, the cyberspace, which can be utilized by anyone with no regard to geographic and time constraints is fodder for the malicious attackers but not defenders.

To worsen the situation, the existence of interconnected information society, any malicious activity on the Internet will easily cause great damage within a short spell of time.

To prevent this, both public and private sectors are striving to make a secure cyberspace using various strategies. Two categories of strategies exist: traditional and modern. A cyber security strategy is a representation of a commitment from various stakeholders to collaborate in addressing cybercrime issues. Such a strategy should focus on the steps taken by stakeholders to respond to cybercrime. Bearing in mind the disastrous nature of cybercrime, ever country/nation is striving to put in place strategies to counter the menace.

Globally, according to the September 2015 Japan Cyber-security strategy, the following are the five basic principles in policy planning and implementation to attain a cyber-security strategy to counteract a cyber-threat:

(1) Assurance of the free flow of information – this is essential for the advancement of the cyberspace as a hub of innovations and inspirations.

(2) The rule of law – This should be applied in the interconnected and converged information society the same way it is in the physical world for a secure and reliable cyberspace with equal access for everyone. (3) Openness and interoperability – the cyberspace should be open to all those who want to utilize it. Nobody should be denied access to the cyberspace. (4) Autonomy – For full utilization of the Internet, autonomy is necessary, i.e. government should leave the Internet to regulate itself. (5) Collaboration among multi-stake holders: the cyberspace has various stakeholders who should share a common Vision of cyber security.

In Africa, Mauritius is one of the countries that have put strategies in place to address cyber security issues.

For example, Strategy 2017–2019 for the Republic of Mauritius has the following four key principles:

(1) Understanding the cyber threats – having a good understanding of the cyber threats targeting an organization makes it easier for the organization to counter them.

Understanding of cyber threats involves knowing their sources, their targets and impact. (2) Public & Private Partnership – for cybercrime to be tackled effectively, experience has shown that there should be collaboration between the industry and Government. This implies that the parties involved should forge mutually beneficial collaborations in sharing vital information and experiences to combat cybercrime. For example, banks should share information with Government and other partners such as Internet Service Providers (ISPs), academia, industrial practitioners, among others. (3) Striving for prevention instead of treatment – organizations that have had serious cyber incidents will reckon that it is far better to prevent than to respond to it after it has taken place. From experience, preventive measures are less costly than curative measures. (4) Effective legal framework – to deter cybercriminals from committing cybercrime with impunity, there should be effective legal frameworks in place. The fact that technology continues to evolve at a rapid pace implies that cyber criminals also evolve very fast. Hence, if there is no strong legal framework, the cyber criminals will act with impunity.

The Mauritius' cybercrime strategy, 2017-2019, proposes the following cybercrime awareness initiatives: (i) a comprehensive national awareness programme on cybercrime, (ii) Setting up of cyber security education and training programmes in schools, middle-level colleges and Universities. (iii) Consistent broadcasting of cyber security programmes on both national and private television channels to create cyber security awareness to the citizenry.

Locally, Kenya is yet to become strong in cyber security training. Considering effective legal framework, the Government of Kenya has taken steps to promote the improvement of cyber security through various Acts, including the Kenya Information & Communications Act CAP 411A as amended by the Kenya Information and Communication (Amendment) Act 2014, the formation of the National Kenya Computer Incident Response Team Coordination Certification (KE-CIRT/CC) Authority Framework. This framework provides a foundation for public key infrastructure implementation and Partnership with regional and international cyber security bodies and fora. Among the bodies that Kenya is in Partnership with are the International Telecommunications Union (ITU) and the East Africa Communications Organizations (EACO). The National KE-CIRT/CC is mandated by the Kenya Information & Communication Act (KICA), Part VIA section 83C to perform the following: (a) Facilitate e-commerce while eliminating its barriers. (b) Facilitate efficient management of critical Internet resources. (c) Promote confidence and trust in the use of e-transactions. (d) Design and promote a framework for facilitating the investigation and prosecution of cybercrime offenses. (e) Inform development of regulations. Other legal measures in Kenya include the passing of the Computer Misuse and Cybercrimes Act, 2018. Part II of the Act shows the establishment and composition of the National Computer and Cybercrimes co-ordination Committee.

The functions of the committee include: (1) Advising the Government of Kenya on the security related aspects touching on matters relating to block chain technology, critical infrastructures, mobile money and trust accounts;

(2) Coordinating National security organs in matters relating to computer and cybercrimes; (3) Receiving and acting on reports relating to computer and cyber-crimes; (4) Develop a framework to facilitate the availability, integrity and confidentiality of critical national information

infrastructure including telecommunications and information systems of Kenya; (5) Coordinating the collection and analysis of cyber-threats, and response to cyber incidents that threaten the cyberspace belonging to Kenya, whether such threats or incidents of computer and cybercrime occur within or outside Kenya; (6) Co-operating with computer incident response teams and other relevant bodies, locally and internationally on response to threats or computer and cybercrime and incidents; (7) Establishing codes of cyber security practice and standards of performance for implementation by owners of critical national information infrastructure; (8) Developing and management a national public key infrastructure framework; (9) Developing a framework for training on prevention, detection and mitigation of computer and cybercrimes and matters connected thereto and (10) Performing any other function conferred on it by the Act or any other written law. The Act outlines the offences, investigation process and penalties, punishment and international co-operation. For the legal framework to be robust and resilient to cybercrime, there is need for it to be continuously reviewed so as to be in tandem with the dynamism of technology.

Due to the high dynamic nature of technology, there are huge disparities between the law functionality and the cybercriminals. Hence the development of laws will always lag behind the advancement of technology. Hence, cybercrime offenders end up evading prosecution because of the weaknesses in substantive criminal laws that hardly address technology ways of offenders. It is hence critical that a robust legal framework for the enforcement of cybercrime issues be put in place for effective cybercrime measures. For capacity building, Universities in Kenya (both Public & Private) are not coming out forcefully to offer the computer forensics and cyber security training safe for a few like Jaramogi Oginga Odinga University of Science & Technology (JOOUST), Meru University of Science & Technology (MUST), Kabaraka University, Mount Kenya University and Strathmore University. Private entities like Modcom Institute of Technology and Cyber-Roam (both based in Nairobi) are also trying to fill the Cyber security training gap.

In this respect, the Government of Kenya should support Higher Education Institutions to set up cyber security training programmes by (i) Expanding Primary and Secondary education for cyber security, (ii) Discovering, fostering and acquiring the best brains as global players.

This can be reflected in the Presidential Digital Talent Internship Programme that nurtures top performs at Undergraduate programmes; particularly in ICT – related disciplines.

The interns are nurtured for one calendar year and the nurturing includes exposing the interns to various ICT technical skills. (iii) Building long-term career paths for cyber security experts. In Kenya, this has been left purely in the hands of the private sector entities like CISCO, Microsoft and IBM.

Universities are purely offering academic programmes; skill-based programmes are minimal or completely lacking. (iv) Strategizing human resources development for enhanced organizational capabilities – This is made possible through the enhancement of Public-Private collaboration frameworks for the sake of collective mitigation in the event of serious cyber-attacks.

The traditional cyber security strategies are concerned with countering direct attacks such as phishing, distributed denial of service (DDoS), and ransomware. However, cyber-criminals operate in an environment that is unregulated (dark web), hence, the barriers are remarkably less as compared to the open web. This implies that the good strategies to counter cyber-attacks require organizations to operate in the external threat environment (dark web). This would mean seeking out threats before they manifest into attacks; hence, intelligence gathering must be top-notch to be effective because cyber-attackers (threat actors) are continuously looking for weaknesses and ways to circumvent defense systems of organizations.

Modern strategies that can be used to counter cyber security threats include: (1) Information sharing – this is very critical because cyber criminals are normally highly motivated to exploit new technologies to take any advantage of vulnerabilities before defense mechanisms are put in place. Hence, organizations must strive to be up-to-date with the new technologies.

This is boosted by sharing accurate and timely information between organizations, intelligence agencies, law enforcement and industry experts to better understand any cyber threats and vulnerabilities in the new technologies for fast and effective responses. (2) Cybercrime intelligence – cybercrime intelligence and cyber defense; the fast changing phase of cyber threats and continued increase in complexity and sophistication of cyber-attack methods continue to render the efforts of collecting crucial intelligence information for fast and effective proactive and preventive mechanisms by organizations.

This however, can be improved by quick information sharing by stakeholders. Cyber-defense involves taking defensive actions against activities of cyber criminals that focus on harming the information systems.

A good cyber-defense environment consists of defensive technologies that have capabilities for real-life protection and incident response. Hence, for effective cyber-defense, intelligence gathering on the cyber-threat is critical.

(3) Public and Private Partnerships – in this paper, Public sector involves government institutions and agencies.

Private sector include non-governmental institutions/organizations like banks, commercial companies, Manufacturing and Transport companies. Since cybercrime has no borders; it is perpetrated by Internet connectivity and other ICTs, any organization – whether Public or Private that relies on the Internet is a potential victim of cybercrime. Hence collaborations between Public and Private sectors enables the sectors to identify cyber-threats in good time, cost effectively and with less effort as compared to when there is no collaboration. (4) International collaboration on Cybercrime – it is worth noting that cybercrime has no borders; it has a global dimension, hence requires a well-coordinated and cooperative international response. Individual countries have their own internal laws which may not be in tandem with laws of other countries. Some countries are yet to put in place cyber laws while on the end of the

spectrum, there are those countries that have put in place very comprehensive cyber laws.

Such discrepancies are an advantage to cybercrime perpetrators; they will target countries that have no or weak cyber laws. This is because governments can only regulate laws within their borders, not beyond. This means, if a cyber-criminal commits a cybercrime in a country that has cyber laws, he/she will flee to a country with weak cyber laws and if there is no collaboration between the two countries, the criminal will go scot-free. This calls for strong international collaboration to ensure that countries have the capacity to fight cybercrime.

Through collaborations, international standards and cyber laws can be formulated to operationalize the effective fight against cybercrime. Effective collaboration calls for harmonization of legal frameworks. This is because differences in national laws and the domestic agencies' capacity to implement the laws can create barriers towards effective international cooperation on cybercrime issues.

In line with this, Kenya acceded to regional and international cyber security bodies like the East Africa Communications Organization (EACO) and the International Telecommunications Union (ITU) respectively. (5) Cyber security awareness – experience has shown that cybercrimes are easily perpetrated by cyber criminals if victims have no cybercrime awareness on how to defend themselves.

In this study, we carried out a quick survey of on cybercrime awareness in banks and established that many computer users – particularly non-ICT professionals have very limited knowledge on cyber-threats. Hence, defense mechanisms by such users are very weak and cyber-criminals will always have a field day whenever they come across such naïve computer users.

It is against this background that cybercrime awareness education becomes significant and inevitable for the general public. Typically for banks, it may be necessary for banks to come up with initiatives that can promote cybercrime awareness amongst customers.

Bearing in mind the complexity and ferocity of the threat actors, financial services institutions should expand their view of the threat landscape so that they, apart from protecting themselves against direct attacks, they should also protect their customers so as to prevent successful attacks. Financial Services institutions and banks hold huge amounts of money and information, hence, attract a lot of cyber-attacks. The strategies to counter such attacks, according to H. Resenberg (2019), include the following: (1) Infusing external intelligence into the organization's cyber security operations. This enables the organizations to monitor hacker activity to identify key attack indications early enough for successful mitigation. (2) Going beyond compliance with Government mandates – this is vital because there are cyber security threats that cannot be countered by compliance with standards such as ISO Certifications or compliance with procedures and processes. Hence, it is important to focus on risk besides being compliant since focusing on risk will help an organization to become more prepared and actively engage threats before they manifest into attacks. (3) Monitoring and mitigation should be operationalized to respond more quickly – effective response can be enhanced through automation of procedures so as to enable organizations to mitigate threats in good time. (4) Focusing on threats that relate specifically to the organization – this is because there are hundreds of thousands of cyber threats out there; hence focusing on the specific ones will safe on costs, effort and time. (5) Cyber security training – this will make the employees to beware of common hacker tricks and hence be in a better position to defend the cyberspace within their jurisdiction.

Specific strategies include the following: Insider threats– according to www.csrc.nist.gov/organizations and www.cis.aueb.gr/publications, the following are some of the common general behavioral characteristics of insiders at risk of becoming a threat: Introversion, greed/financial need, vulnerability to blackmail. Compulsive and destructive behaviours, rebellious, ethical flexibility, reduced loyalty, entitlement, predisposition towards law enforcement, e.t.c. These characteristics can be used in detecting malicious insiders. Unintentional insider threat can be reduced through the following: (i) Training of employees to be able to deal with phishing and other social media threat vectors. (ii) Training the employees continuously to maintain acceptable levels of knowledge skills and abilities. (iii) Conducting meaningful training from time-to-time to improve awareness of risk perception and cognitive biases that hinder decision-making. (iv) Improving the usability of security tools. (v) Improving the usability of software to reduce system-induced human error. (vi) Enhancing awareness of the unintentional insider threat. (vii) Providing effective security practices - for example, a two-factor authentication for access. (viii) Maintaining staff values and attitudes that align with organizational mission and ethics.

More et al., (2015) considers preventive measures that can be used to curb cyber-crime in the banking sector to include the following: (1) Ensuring that the web site being used in Credit card transactions is secure. Photocopies of Credit cards should not be given to third parties sine they can land in wrong hands. (2) Lotteries – Responding to lottery messages or call can expose the user to cyber-criminals. (3) Unknown links – Avoid clicking on unknown links since they could be phishing e-mails from cyber-criminals. (4) Spam – Spam e-mails should be deleted immediately to avoid clicking on them inadvertently. (5) Safety of the bank/credit card – Bank account/credit cards should be securely kept and lost ones should be reported immediately. (6) Secure networks –the security of the network is very important otherwise transacting online can be very dangerous. Bahalul Haque A.K.A, (Feb 2019), in his study, recommends the following strategies that can help address the cyber security issues in Bangladesh in general and banks in particular: (1) Establishment of cyber infrastructure to oversee and manage security protocols. (2) Acquisition of effective equipment to improve the capacity of cyber security intelligence. (3) Deploy block chain technology. At the national level, A. K. A. Bahalul Haque (Feb 2019) posits that priorities of the Bangladesh National Security Strategy should constitute the following: Legal measures, Technical & Procedural measures and lastly, Organizational structures.

Considering third-party exposure, industry practitioners have recommended the following strategies: (1) Monitoring vendor access within the network on a 24/7 basis, (2) Ensuring

ISSN: 2394-4404

that business premises are under the full control of the business owner so as to guarantee physical, internal and operational security controls are in place. As for SIM swap attacks, the strategies include the following: (1) Utilization of the offer from a major cellphone provider to set up an account PIN or passcode separate from the phone number. (2) Keeping personal information utilized for protecting accounts very private and secure, (3) Avoiding to reply on SMS for primary communication since the data is not encrypted. (4) Enabling a two-factor authentication (2FA) for social media, credit card and bank accounts, (5) Removal of cell phone numbers from accounts that do not require them, (6) Downloading of Authenticator Applications such as Google Authenticator and Authy to link the physical cellular device and (7) Verification of the types of alerts set up for each account so as to identify false logon attempts.

Other strategies to combat SIM Swap attacks, according to the Serianu 2018 Kenya Cyber security Report include: the introduction of additional checks for SIM reissuing such as voice recognition and security queries.

III. CONCLUSIONS

This paper has examined the strategies used by Nations and organizations world-wide to counter cyber threats and vulnerabilities. The examination was narrowed down to the banks operating in Kenya. The examples of cyber-crime cases presented here give a global view, country view, and finally an organizational view of the state of affairs as far as cyber-crime is concerned. The Kenya cyberspace continues to expand, just like elsewhere; particularly since new technologies continue to be developed and the Internet bandwidth continue to expand to accommodate the increasing number of users; organizations are now over depending on information and communication technologies (ICTs).

REFERENCES

[1] A.K.M. Bahalul Haque (2019). Need for Critical Cyber Defence, Security Strategy and Privacy Policy in Bangladesh - Hype or Reality? International Journal of Managing Information Technology (IJMIT) Vol.11, No.1,. DOI: 10.5121/ijmit.2019.11103 37

[2] H. Rosenberg. The April 2019 Banking & Financial Services Threat Landscape Report. Intights Defend Forward. https//www.intsights.com (Accessed on May 24, 2020)

[3] More.(219). International Journal of Advanced Research in Computer Science and Software Engineering 5(12).

[4] September 2015 Cyber security Strategy of Japan. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Japan_2015_cs-strategy-en.pdf [Accessed on June 11, 2020]

[5] Serianu 2018 Kenya Cyber security Report. Available at:https://www.serianu.com/downloads/KenyaCyberSecurityReport2018.pdf [Accessed on June 13, 2020]

[6] Strategy 2017 – 2019 for the Republic of Mauritius. Available at: http://cert-mu.govmu.org/English/Documents/Cybercrime%20Strategy/National%20Cybercrime%20Strategy-%20August%202017.pdf [Accessed on June 13, 2020]

[7] World Economic Forum 2015, Global Cyber security Index and Cyberwellness Profiles [Online]. Available at: http://www.itu.int/dms pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf. [Accessed on May 28, 2020]