A Security Management Framework for Telecommunications in Africa

Ezekiel Uzor Okike, Ernest Boikobo Seboko
University of Botswana Gaborone, Botswana

Abstract

In this paper we identify the security challenges associated with Internet based services especially in the telecommunications domain. The reasons for specific vulnerabilities are highlighted with a view to proffering appropriate security mitigation plans based on the IT-GS, NIST, ISO/IEC 27001, ISO/IEC 27002 and IASME cyber security frameworks. With a focus on the African telecommunications environment and the associated technological challenges, an analysis of the Strength, Weaknesses, Opportunities and Threats (SWOT) is presented with a viewing to identifying a clear direction plan for the implementation of appropriate security mitigation plan for telecoms security in the African context. Based on the SWOT analysis, an IT security management framework for Africa is presented. The framework includes appropriate recommendations for secured telecommunication operations and services in Africa.

Keywords – Telecommunications, cyber security, vulnerabilities and threats, cyber security frameworks, security mitigation plans

1. Introduction

Developing countries trail behind in many things especially in the technology space such as telecommunications. In the context of Africa, this concern has taken precedence on how telecommunications infrastructure is rolled out, what to use, how to use it and security provisions for services and operations. With the dynamic nature of ICT the major modifications and technological advancements are always meant to better systems, uptime, scalability and security.

Digital planet [1] traced the origin of telecommunications since 1812 and explain the concept as "the technology of long-distance communication". In addition, "the invention of the telephone by Alexander Bell in 1844 extended the capability of telecommunications to the spoken word". In today's telecommunications, networked computers connected with other information and communication technologies help humans and machines to send and receive data, images, and software across desired locations within seconds.

To date, developments in the field of telecommunications have witnessed new technologies in basic network anatomy infrastructure in both local area network (LAN) and wide area network (WAN) technologies. A typical LAN includes a collection of computers and peripherals where each computer and networked peripheral is a node on the network. Nodes are connected to hubs or switches which allow any node on the network to communicate. In a WAN, each individual network site is a node on the wide area network. The largest and best-known WAN is the Internet. Hence, by connecting to a network that is part of the Internet, a computer can connect to millions of other Internet connected devices. The possibility of large WANs is due to a web of telephone lines, microwave relay towers and satellites that span the globe. In most cases, WANs are private operations designed to link geographically dispersed corporate or government offices and individual homes.

Statement of the Problem

The greatest challenge in Internet enabled communications today is security (Cyber security). Although organizations are investing so much to enforce appropriate security measures in Internet enabled communications, there are still breaches and intrusions (security threats) ranging from property theft to identity theft, software sabotage, hacking and electronic trespassing [1]. Therefore, the infrastructural development of a telecommunication setting should be cognizant of security response readiness, and risk mitigation strategies in vulnerability situations.

Study Objectives

The objectives of this paper are to identify contemporary security challenges in modern telecommunications networks and services, to identify the security measures in place and their effectiveness, and to propose a security mitigation plan for service providers and customers to address security threats, and to make appropriate recommendations for safer transactions over the Internet via telecommunications service. The study applied the IT-GS 2017, NIST, ISO/IEC 27001, ISO/IEC 27002, and IASME cyber security

 | DOI: 10.20533/jitst.2046.3723.2022.0093

frameworks in recommending security mitigation plans for telecommunications security in Africa.

2. Literature Review

Current security and privacy issues [2] identified wide ranging security and privacy issues in telecommunications but did not proffer comprehensive security mitigation plans based on existing security frameworks. Some of the identified security challenges in telecommunications are as follows:

i. Insecure telecommunications component channels such as web browsers, https protocols, Operating systems, hardware, and databases of which each individual components have their vulnerabilities. In addition, issues with major web browsers including Mozilla Firefox, Google chrome, and Internet explorer have also been fully analyzed and discussed in [3], [6], [7], [8], [9], [10], [11].

ii. Challenges with digital certificates and https as an illusion of safety. This in essence implies that a configuration of digital certificates can provide encrypted communication, but does not guarantee server-side identity, thus, making the system vulnerable to cyber-attacks. Moreover, servers in https protocols may still be weak and compromised even though users have the illusion that they are protected from cyber security risks [12], [13], [14], [15], 16].

iii. Security challenges with Internet of Things (IOT) especially with private users. Some of these include direct cyber-attacks through the Internet routers [17], weak device private keys [16], surreptitious eaves dropping, message modification and possible node impersonation [4, 18].

iv. Ransomware attacks [19].

v. Security challenges with the use of Google services. Some of this include collection and storing of personal information from massive users, and getting geolocation information from users, and saving information through goodly browser.

Similarly, document analysis of efficient group key management[3] identified major security challenges with Device-to-Device (D2D) communications by documenting and analyzing a wide range of literature on the subject of D2D communication and Group Key Management (GKM). The study made recommendations as per D2D communications security requirements, GKM security requirements, and the role of cryptography solutions in establishing a shared secret. Furthermore, in [4] an analysis of Information Systems security challenges in online services and the effectiveness of security measures in place to tackle the identified challenges was presented. Subsequently, security critical issues in telecommunications[5] appraised business and security critical issues in telecommunications industry from an African perspective. The study also made some recommendations on overcoming security challenges in telecommunication and highlighted the need to apply available security frameworks in security solutions for telecommunications. The later recommendation has not been visibly adopted in most available security solutions in telecommunications for instance in as documented in [20], [21], [22] to mention a few.

3. Telecommunications Network and Cyber Security

The main focus of this paper is about telecommunications network and cyber security. This section presents contemporary security challenges and vulnerabilities in Internet enabled communications, especially telecommunications.

3.1. Contemporary Security Challenges and Vulnerabilities

The Figure 1 shows a typical architecture of a web-based application which includes a web client (user), communication lines, corporate servers, corporate systems, and databases [23]. Potential vulnerabilities associated with each component are also identified. For instance, floods, fires, power failures, and other electrical problems can cause disruption at any point in the network. Equally, when large amount of data are stored in electronic form, they become more vulnerable to cyber-attacks than when they exist in manual formats. Other factors such as unauthorized access, abuse or fraud, poor management decisions, thefts, cyber-attacks through malicious software, viruses, denial -of-service, system malfunctioning etc. account for systems vulnerabilities as summarized in Figure 1.

The Internet presents more vulnerability due its virtual openness. Vulnerabilities has also increased from the widespread use of emails, instant messaging, social media chatting, sharing of files over peer-to-peer (P2P) networks, and use of wireless networks at public places such as hotels, libraries, and airports.

3.2. Survey of Security Threats Over the Internet

Security threats over the Internet are essentially cyber threats or cybercrime - any crime accomplished through the knowledge or use of computer or network technology.

 | DOI: 10.20533/jitst.2046.3723.2022.0093

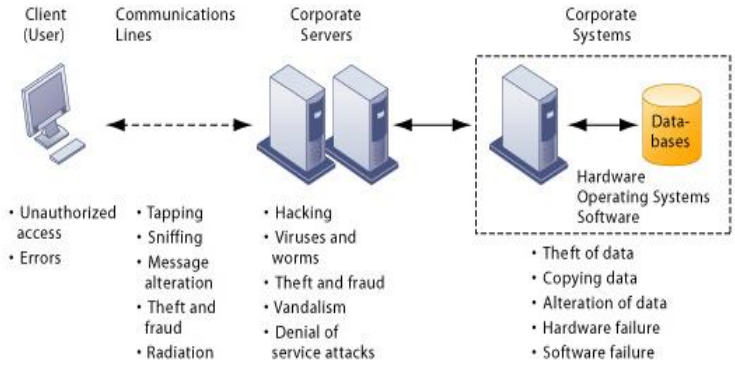

Figure 1. Contemporary Security Challenges and Vulnerabilities [23]

Some examples of cyber-criminal activities are cyber stalking (harassment through the internet), stealing information from computers, databases, software piracy, identity theft, spoofing, phishing, virus attacks, malware, spyware, hacking, and electronic trespassing of communication devices [1]. Various issues in telecommunications network security have also been discussed in [4] and the measures in place to combat the threats.

3.3. Telecommunications Service Provision

Impact of telecoms on economic growth [24] studied the impact of telecoms on economic growth in developing countries and suggested the following benefits:

i. Generating a growth dividend because of the spread of telecommunications reduces costs of integration, expands market boundaries, and expands information flows.

ii. Just-in-time in management production rely on efficient communication networks. In addition, we suggest in this paper that a very significant issue is the contribution of telecommunications in 4IR.

iii. The Fourth industrial revolution (4IR) is completely reliant on telecommunications, and this is probably the most significant benefit of telecommunications.

3.4. Classification and Assessment of Telecommunications Security Vulnerability and Safety Measures

The telecommunications industry has the best technologies that are meant to improve the space and make life easy. Consequently, companies deploy state-of-the-art equipment which come with huge expenditure. These assets easily become target of theft and vandalism in developing countries due to poverty and corruption. For instance, towers for mobile telecommunications (2G, 3G, 4G and now 5G) deployed in isolation and unattended sites become victims sooner or later. To mitigate against this, closed circuit television (CCTV) and access control systems need to be deployed in all sites to counter any form of theft. Also, cables for PABX and fibre are always stolen in mine holes which disrupt and cause network outages. Deploying security companies to physically look after this equipment is good practice against infrastructure theft or vandalism.

The cyber-attacks in form of malwares and viruses or any form of attack meant to disrupt the operations of network infrastructures. The mitigation approach is through the use of firewalls, strong anti-virus programs and acceptable ethical behaviors of staff in organizations. It is also possible to have necessary security technologies in place and still encounter attacks if company personnel are not security privy or do not have requisite skills to use deployed technologies for security.

Other forms of cyber-attacks and security challenges on telecommunications infrastructure are:

Phishing and social engineering

Phishing is deemed a form of social engineering where an email with malicious content is sent to an unsuspecting individual. When the email is opened, the malware replicate itself to steal files or documents. Acquiring and installing appropriate software to detect and block phishing is a proper approach to this challenge.

Unethical behavior of in-house staff

The case in point is relative to employees voluntarily giving information to outside parties who could use such access privileges against the organization. There are cases of disgruntled employees seeking revenge in organizations who engage in unethical behaviors. Some may unknowingly give information to unsuspecting

 | DOI: 10.20533/jitst.2046.3723.2022.0093

individuals pretending good intentions, yet they have ulterior motives. This calls for security awareness training and well-grounded employee relations in organizations.

Distributed Denial of Service (DDoS)

The DDoS network attack which renders a certain element unavailable while it is still available. This could be a form of sabotage aimed at deteriorating trust of service users to certain service provider. According to the 2016 Data Breach Investigations Report, the telecommunications sector was hit around twice as hard as the second placed sector (financial exchanges), with a median DDoS packet count of 4.61 million packets per second. Hardware and software infrastructure to detect DDoS attacks or protect the system from such attacks exist in the form of firewalls and powerful Network security tools.

Network security

Vulnerability also lie with network devices. The configuration done on devices may dictate how secure the environment is. It should be noted that use of USB devices in the network may pose a network attack through a malware

3.5. Other Security Challenges in Telecommunications

Other security challenges in telecommunications have been created by the following recent work ethics:

Remote working

COVID-19 has birthed the common practice of working from home. This means employees connecting remotely through VPN's. VPN's by nature pose security threats and some are even red flags. These may result in identity theft which may allow one to use someone's credentials without being detected because the assumption is that it is the actual owner of credentials since there is no physical verification. However, with more technological advancement of recent times, multi factor authentication (MFA) and advanced firewall technologies have made it difficult for intruders to have it easy. MFA deploys a third layer authentication that dictates that having only username and password cannot grant you access. A third level verification which could be in the form of one-time-pin (OTP) sent as a text message (SMS) to one's phone or an authentication application such as google authenticator and Microsoft authenticator licensed to produce OTP's. Fingerprint and facial recognition technologies for authentication are also becoming prominent.

Rapid technological changes

The rapid advancement of technology is always a challenge to companies in developing countries since keeping up with the upgrades and changes is problematic. Today we are talking of 5G when some parts of the globe are starting to actualize 4G. Hence, to keep up with upgrades may require appraising and training staff to bridge the skill divide gap. For instance, VPN and firewalls technologies advance rapidly meaning that personnel need to be trained to stay abreast with the advancements.

3.6. Fighting Cyber Security in Telecommunications

Cybercrime in the telecommunications sector is both compound and varied. Therefore, it requires a befitting defensive mechanism. For telecommunications companies to effectively counter cybercrime, they need to increase acknowledgement and cognizance, educate their employees and invest in suitable technology solutions. But the first step must be investing in the right people, that is hiring people with requisite skills that are relevant to security environment who can appreciate security concerns in telecoms and use their skills to manage the infrastructure against potential threats.

3.7. The Impact of Security Breaches

Security breaches often result in losses in the ICT equipment and pertinent data which comes with a huge economic cost, in terms of loss of revenue in replacing expensive equipment, or business losses through disrupted services while awaiting compensation in form of insurance covers from insurance companies. This may in a way ruin the brand resulting in loss of customers. In regulated environment with a regulatory body, a security breach may mean instigating a compliance review which may mean license revocation if after due diligence checks it is established that certain standards and compliance regulations are not satisfactory. In some cases, fines may be imposed to that effect.

3.8. Security mitigation Plans

One practice in overcoming telecommunications security breaches is to mitigate against its effect. The goal of a mitigation plan is to see the risk being managed and also to do proper SWOT analysis. The plan dictates the identification and following business objectives that are in line with the organizational policy and strategy. There is also the

 | DOI: 10.20533/jitst.2046.3723.2022.0093

need for the identification of business assets supporting business objectives and ensuring service availability and uptime. This is achieved by drafting a comprehensive risk assessment plan meant to deliver mitigation. Figure 1 shows a security risk mitigation life cycle. The figure starts by identifying business objectives, identifying business assets supporting the objectives, performing a risk assessment plan, performing risk mitigation by mapping risks to control, performing risk treatment, and reevaluating risk.

4. Proposal of an IT Security Framework for Telecommunication services in Africa

Analyzing SWOT (Strength, Weaknesses, Opportunities and Threats) is a good approach in mitigating against telecommunications breaches. The Table 1 is an example of a SWOT analysis plan anchored on existing security management frameworks such as IT-GS 2017, NIST800-53, ISO/IEC27001, ISO/IEC27002, IASME.

4.1. Security Mitigation Development Life Cycle

The Figure 2 present a security mitigation development plan which is anchored on existing security frameworks as explained below.

4.2. A Security Management Framework for Telecommunications in Africa

A careful look at telecommunications in the African context reveals that service providers have deployed data centers in most environment as part of efforts to actualize the digital drive. However, in some environments the enterprise architecture is still the traditional network which does not support the full potential for cloud computing. Therefore, the following are recommended for better telecoms service in African countries:

i. Deployment of modern technologies in telecoms

ii. Deployment of Software defined Network (SDN).

iii. Deployment of Close circuit Television in appropriate locations for monitoring equipment.

iv. Constant penetration checks to detect any vulnerabilities.

v. Manpower training to develop staff skill in appropriate needs areas.

vi. Appropriate investment in Cyber Security.

vii. Adherence to IT- Grundschutz 2017 (IT-GS 2017) standard protection guidelines[25]:

- Structured Analysis.
- Determine the need for protection and indicating protection requirements (Normal, High, Very high).
- Modelling and selection of security requirements in line with a and b above.
- IT-GS check review as in c above to determine met requirements.
- Continuous risk analysis and taking necessary measures.
- Timely implementation of appropriate measures.

Adherence to NIST [26] standard protection guidelines: The framework aims to secure critical infrastructures, and organizations implement it to strengthen their cyber defenses. The four functions of the framework are identify, detect, respond, and recover:

- Organization must identify function guides in detecting security risks to asset management, business environment, and IT governance through comprehensive risk assessment and management process.
- Detect function defines security controls for protecting data and information systems (access controls, training and awareness, data security, information protection procedures, and maintaining protective technologies. Detect also gives guidelines for detecting anomalies in security, monitoring systems, and networks to uncover security incidences.
- Response function includes recommendations for planning responses to security events, mitigation procedures, communication processes during a response, and activities for improving security resiliency.
- Recovery function provides guidelines that an organization can use to recover from attacks.

viii. Adherence to IASME [27] security governance standard. IASME governance are cybers security standards designed to enable small and medium sized enterprises to realize adequate information assurance. It outlines the criteria for considering a business to have satisfactorily implemented cyber security measures, thus, enabling companies to show their customers their readiness to protect business and personal data. governance.

 | DOI: 10.20533/jitst.2046.3723.2022.0093

ix. Adherence to ISO IEC 27001/ISO 27002 [28]. This cyber security framework provides requirements for managing information security systems. It observes a risk-based process that requires businesses to put in place measures for detecting security threats that impact their information systems. ISO 27001 recommends various controls including security policies, while ISO 27002 provide enhanced security controls and policies to manage IT assets and inventory, user access, and operational security.

Table 1. SWOT Analysis Matrix and Appraisal for Developing Countries

Strength	**Weaknesses**
• What do we do well? • What unique about your products / services? • What do others see as your strength? • Data center infrastructure brings closer to the world with cloud platform. • More technological advancements bring improved security. • Broader coverage even to most remote areas.	• What could I improve? • How Competitive are your products? • What do others see as your weakness? • In some developing countries telecommunications providers have not yet tapped in the new enterprise network advancements of Software Defined Networks (SDN) which are more secure than the traditional network pane. • Poor organizational culture may render security awareness drills unsuccessful in an environment where employees do not take internal briefs seriously. Some do not read internal mail which are used to communicate internally.
Opportunities	**Threats**
• What is the new market segment? • What trends can one utilize? • How can I turn strength into opportunities? • COVID era brought about working from home which made people need internet at their homes, this has brought even more security concerns. • Also, COVID propelled for e-learning, e-commerce, e-governance. With enhanced technology advancements, a better perspective on security is modelled.	• What can harm you? • What are your competitors doing? • What threats do your weakness expose to you? • One is forced to upgrade to implement new security improvements. • Open market that may not close for new entrants. • More ICT graduates are unemployed which may fuel cybercrimes and hacking since they are technologically advanced.

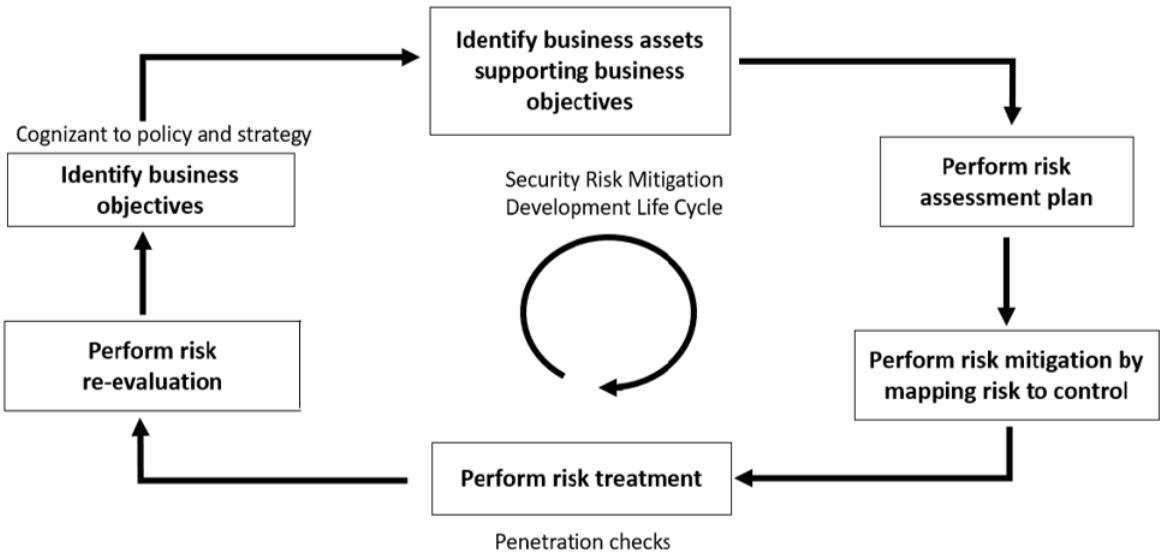

Figure 2. Security Risk Mitigation Development Life Cycle

 | DOI: 10.20533/jitst.2046.3723.2022.0093

5. Conclusion

The need to clearly identify the security challenges associated with internet-based services cannot be overemphasized. In the telecommunications domain two types of users are professional users and private users. For professional users (military, police, security services) confidentiality, authenticity, and availability are crucial factors. For private users (individuals and business organizations) privacy, anonymity and availability are equally crucial. Professional systems delegate security functions to educated and trained actors, while private users cannot delegate security if they want to protect their privacy [2]. Therefore, as telecommu- nications services penetrate the African continent, the need to evolve appropriate security management plans for all categories of users, and especially for the vastly non-technical IT users becomes very imperative. Additionally, telecoms providers need to ensure that they are security certified on appropriate security standard to make their clients have confidence in security of their services.

6. References

[1] Beekman, G. and Beekman, B. (2012). Digital Planet: Tomorrow's Technology and You Complete, Prentice Hall, Boston.

[2] Jevremovic, A., Veinovic, M. and Shimic, G. (2017). An Overview of Current Security and Privacy Issues in Modern Telecommunications. Serbia Nis, October 18-20, Telsiks, Serbia. Pp. 119-123.

[3] Okike, E. U. and Ratlhako, B. (2020). Document Analysis of Efficient Group Key Management Using D2D Communication. J. Engr Design Anal. 3(2). Pp. 72-77.

[4] Okike, E. U. and Mogapi, G. (2021). A Pedagogic Analysis of Information Systems Security Measures in Online Services", in Proceedings of ICITST, WorldCIS, WCST, WCICSS, Infonomics Society: London. Pp. 71-76.

[5] Okike, E. U. and Seboko, B. E. (2021). Appraisal of Business and Security Issues in the Telecommunications Industry in Developing Countries: An African Perspective. In Proceedings of the 16th International Conference for Internet Technology and secured Transactions (ICITST-2021), Infonomics Society, London.

[6] Bott, E. (2020). Do You Save Passwords in Chrome? Maybe You Should Reconsider Security. https://www.zdnet.com/article/do-you-save-passwords-in-chrome-maybe-you-should-reconsider/. (Access date: 2 October 2020).

[7] R. Zhao, and C. Yue, "All Your Browser-Saved Passwords Could Belong to Us: Security Analysis and a Cloud-Based New Design", in Proceedings of the 3rd ACM Conference on Data and Applications Security and Privacy, San Antonio, 2013, pp. 333-340.

[8] Gasti P. and Rassmussen, K. B. (2012). On the Security of Password Manager Database Formats", in Proceedings of the 17th European Symposium on Research in Computer Security, Pisa. Pp. 770-787.

[9] Silver. D., Jana. S., Bonch. D., Chen, E. and. Jackson, C (2014). Password Managers Attack and Defenses. In Proceedings of the 23rd USENIX Security Symposium. Pp. 449-464.

[10] Google Chrome. (2020). https://www.google.com /chrome/browser/privacy/whitepaper.html#autofill. (Access Date: 3 October 2020).

[11] Kamonu, O. K. Frank, I. and Yemi, A. (2014). Computer Security Measures, Tools, and Best Practices. British Journal of Science and Technology. 4 (31), Pp. 4380.

[12] NVD. (2014). NVD-CVE-2014-0160-NIST. https: //nvd.nist.gov/vuln/detail/CVE-2014-0160**.** (Access Date: 12 January 2022).

[13] NSA (2014). Hearbleed. https://www.wired.com/ 2014/04/nsa-explained-heartbleed-two-years/. (Access Date: 11 January 2022).

[14] Marlinspike, M. (2009). New Tricks For Defeating SSL in Practice, Black Hat DC. 2/2009, Arlington. https://www.blackha**t**.com/presentations/bh-dc09/. (Access Date: 14 January 2022).

[15] Adrain, D. et al, (2015). Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. In Proceedings of the 22nd ACM SIGSAC Conference on Communications Security (CCS '15)", ACM: New York, NY, USA. Pp. 5-17.

[16] Reed, A. and Kranch, M. (2017). Identifying HTTPS-Protected Netflix Videos in Real Time. In Proceedings of the 7th ACM Conference on Data and Applications Security and Privacy (CODASPY '17), ACM, New York, NY, USA. Pp. 361-368.

[17] Bloomberg (2016). Potential hacking after router issues. ttps://www. bloomberg.com/news/articles/2016-11-28/deutsche-telekom-probes-potential-hacking-after-router-issues. (Access Date: 12 January 2022).

[18] Samsung. (2017). Smart TV Hack Security. http://www.forbes.com/sites/thomasbrewster/2017/03/cia-wikileaks-samsung-smart-tv-hack-security. (Access Date: 12 January 2022).

[19] The Hacker News. (2017). http://thehackernews .com/ 2017/04/nsa-hacking-tools.html. (Access Date: 12 January 2022).

[20] Anikin, I. V. (2016). Information Security Risks Assessment in Telecommunication Network of the University. In IEEE Conference Proceedings, Dynamics of Systems, Mechanics and Machines. pp. 1-4.

[21] Nugent, J. H., Raisinghani, M. S. (2022). The Information Technology and Telecommunications Security Imperative: Important Issues and Drivers. Journal of Electronic commerce research. 3(1), pp. 1-13.

 | DOI: 10.20533/jitst.2046.3723.2022.0093

[22] Jonekheere, E. and Lohsoonthorn, P. (2004). Geometry of Network Security. In Proceedings of the 2004 American Control Conference, Boston, MA. pp.976-981.

[23] Laodon, K. C., Laodon, J. P. (2013). Essentials of Management Information Systems, 10th ed. Pearson, Boston.

[24] Waverman, L., Meschi M., Fuss, M. (2021). The Impact of Telecoms on Economic Growth in Developing Countries. http://semanticscholar.org/paper /the-impact-of-telecoms-on-economic-growth-in-develo ping-countr ies-in-fuss/aadce. (Access Date: 2 January 2021).

[25] IT-GS (2019). Compendium. Http://www.bsi.bun dde/sharedDocs/downloads/EN/BSI/Grundschutz/Internati onal/bsi-it-gs-comp-2019.pdf?_blob=publicationfile& v=1. (Access Date: 2 April 2021).

[26] NIST. (2021). Security Framework. Https://www. nist.gov/cyberframework. (Access Date: 12 December 2021).

[27] IASME security governance. http://www.iasme.co .uk/audited-iasme-governance. (Access Date: 14 January 2022).

[28] ISO/IEC 27001-27002. http://www.it-cisq.org. (Access Date: 14 January 2022).

 | DOI: 10.20533/jitst.2046.3723.2022.0093