Examination of the impact of cyber security on networks operations: A case of Vodafone Ghana

Francis Kwadade-Cudjoe
FBCS, FIMIS, PhD, MBA, BSc (Hons); Senior Lecturer, Knutsford University College and Adjunct Lecturer, Regional Maritime University, Accra, Ghana

Yusuf Hyelnasinyi Enoch
BSc Information Technology, Knutsford University College, Accra, Ghana

Adelore Abosede Bunmi,
BSc Information Technology, Knutsford University College, Accra, Ghana

doi: https://doi.org/10.37745/bjmas.2022.02018 Published June 16 2023

Citation: Kwadade-Cudjoe F., Enoch Y.H., and Bunmi A.A. (2023) Examination of the impact of cyber security on networks operations: A case of Vodafone Ghana, *British Journal of Multidisciplinary and Advanced Studies*: Engineering and Technology, 4(3),76-97

ABSTRACT: *Computer network operations of organizations are always prone to cyber-attacks from different people, including misguided employees within the organization, due to the errors they make which lead to exploitation by cyber criminals. These people normally have destructive tendencies better known to themselves, as they would go to every extent to make sure that their nefarious intentions are achieved. It therefore, behooves on network operation technologists to innovate concrete and tested security measures to secure organizations' network systems against hackers. The destruction could impact the activities of the organization to come to complete halt, as important information, a resource of the enterprise, may be damaged, stolen or lost. Some of these hackers may then turn around and demand huge sums of money from the organization before the stolen information may be released; likely the restored software may be tainted and therefore, different from the original state. Consequently, management of organizations should make adequate security preparations to forestall these destructive propensities of hackers. Vodafone Ghana therefore, should reinforce its security system to make sure the firewall and password systems, and access to its servers from the outside world are not compromised.*

KEYWORDS: network operations, cyber, security, crime and attack.

INTRODUCTION

Organizations are incessantly constructing computer networks to enable them reach out to their customers and consumers, but not all of them are security-sensitive to their networks. Geer, Hoo & Jaquith (2003) strongly advised that the good performance of a network system hinges on the quality of security measures applied on the network, which prevents the compromise of the network competencies to threats. In essence, to construct a secure network for managerial success, organizations should recognize all the likely attacks as well as their mitigation methods and do good risk analysis to unearth the underhand threats/risks involved with the network (Diesch & Krcmar, 2020).

Furthermore, organizations should conscientiously recognize how to design security policies to apply to the network and instruct the employees, as well as all stakeholders, to protect the organization's information from threats. Nonexistence of suitable security system remains a big impediment to organizations looking for minimization of security exposures (Wael, 2010). Moreover, theft and destruction of organizations' assets through breakage into the premises are generally performed by employees of the organization (Wael, 2010).

However, Jackson and Youssef (2023) queried if cyber security is being taught well at all to protect network operations? According to them the problem of where to start is perception, where one option is to teach the policy, e.g. ISO/IEC 27001 Standard, Cyber Essentials Plus and Cyber Security Body of Knowledge Frameworks (CyBok).

Hackers are scourges and dangerous as a security risk in that they could destroy vital company information when they manage to get access to the network. Information security management is concerned with procedures to protect the information from threats, using tools, processes, methodologies, principles and technologies (Peltier, 2005; Reynolds, 2012; Stamp, 2011). Hackers may be motivated by a multitude of reasons, including profit, aggressiveness, intimidation or publicity (Sterling, 1993).

The attacks on information, assets and finance of the organization through example unauthorized access, manipulation and interruption, are intensifying and therefore, developing nuisance; the severity of the threats/attack determines the appropriate level of response and/or mitigation measures (Public Safety Canada, 2013a).

Network attacks have been revealed to be global, encompassing and wide-ranging just as the number of systems that they try to infiltrate. Again, attacks are recognized to be deliberate and premeditated, and technically knowledgeable invaders have been involved in targeting the protocols used for protecting communication, amongst networking devices. Network security therefore, necessitates the usability, stability, honesty, and security of the network and data (Reed, 2003; Sandeep, Thirupathi, Kumar & Naresh, 2019).

There are six (6) different types of hackers; white, grey, green, blue, red and black. The white and grey hat hackers are security professionals who help the enterprise network system to identify vulnerabilities and correct them, but as the spectrum gets to green, blue, red and black things get muddled and swaggered (Froehlich & Bacon, 2021).

Engebretson (2011) indicated that if hackers have the intent to provide the organization a realistic attack simulation so that the company could improve its security through early discovery and mitigation of vulnerabilities, the attacker should be considered a white-hat. Froehlich and Bacon (2021) added that white-hat attackers are ethical, as they penetrate with the owner's consent to enable them identify vulnerabilities of the current system. A white-hat hacker therefore, is a hacker who is committed to full compliance with legal and regulatory statutes as well as published ethical frameworks that apply to the task at hand (Engebretson, 2011; Froehlich & Bacon, 2021).

According to Engebretson (2011) and sustained by Hanna and Teravainen (2021), a black-hat hacker then is a hacker who either ignores or intentionally defies legal or regulatory statutes with presumably little interest in ethical frameworks. Significantly, some illegal individuals outside the organization who do not have access to the organization's computer system or network could cause external threat. Such hackers typically break into organization's network through the internet or server and they could be skilled or inexpert.

Therefore, a good security system should effortlessly frustrate this kind of attack. More importantly, these kinds of hackers could not be undervalued since they could cause serious damage to network systems. This study, consequently, would examine the mitigating threats to network security infrastructure.

Background and Statement of the Problem

The enormous development of the world wide web (www), internet, mobile apps and browsers seem to have brought numerous good things like electronic commerce, email, social media and easy access to vast stores of reference material (Laudon & Traver, 2022). As with most technological advances and developments in general, there is also the other side where criminals clandestinely steal the organization's information and transmit it through the internet to other private destinations (Graves, 2010).

The state of security on the internet is not the best and getting worse (Landoll & Landoll, 2005). Furthermore, the outdated means of protecting computer networks, such as firewalls and software encryption are inadequate and unsuccessful. It can be noted that most of the wireless ad-hoc network systems seem vulnerable to physical attack or harm due to its feature of open medium dynamic altering topology; checking and management point not being centralized, clear line not well defended and co-operative algorithms not effective (Graves, 2010).

Since the techniques developed on fixed wired networks to detect intruders have been rendered inapplicable in this new environment, the requirement for ways and approaches to develop new architecture and mechanisms to protect mobile computing applications and wireless networks is important (Graves, 2010).

Presently, there are countless attacks which cause serious problems to enterprise networks. To protect the network from attacks, organization through their network administrator should detect all the susceptibilities existing in the network and know how to guard and mitigate all the attacks. Besides, an attack could happen in numerous phases of an enterprise implementing network. Initially an attacker could have restricted information about the target network, so one of the primary objectives of the attacker would be to gather intelligence or information about the target susceptibilities. After gathering information about the target network, a range of attacks can be launched against the organization (Landoll & Landoll, 2005).

As many organizations started to spread numerous business functions to the public network, safety measures became extremely desirable to make sure that the network is not interfered with or does not fall to wrong hands. If a network is accessed by a hacker or dissatisfied employee, it could create havoc for the organization's proprietary data, affect company productivity negatively, and retard the ability to compete with other businesses (Graves, 2010). More so, unauthorized network access could also harm an organization's connection with customers and business partners who could question the organization's capability to protect their confidential information. Furthermore, any part of a network can be susceptible to attacks or unauthorized activity as earlier discussed. Again, organization's competitors or even internal employees could violate all routers, switches and hosts (Graves, 2010). In order to determine the appropriate ways of protecting an organization's property against attackers, the organization should understand the attacks that could be instigated and the havoc they could cause to business infrastructures. It is, therefore in the wake of examining the impact of cyber security on networks operations that the researchers deemed it appropriate to undertake this study at Vodafone Ghana.

Objectives of the Study

The main objective of the study is to examine the impact of cyber security on networks operations, using Vodafone Ghana as a study. The specific objectives of the study are to;

i. determine the availability of physical and logical network security at Vodafone Ghana,
ii. examine information security standards employed to protect sensitive data, and
iii. identify the challenges of cyber security on networks operations.

Research Questions

The research questions that would help collect good data from respondents to achieve the objectives are:

i. what is the availability of physical and logical network security at Vodafone Ghana?
ii. what are the security standards implemented to protect sensitive data?
iii. what are the challenges of cyber security on the network operations?

Significance of the Study

The researchers are dedicated to giving out the result of this study to management at Vodafone Ghana, with the hope that the study would not just be an extraction of truth but would give information to better comprehend mitigating threats to network security infrastructure. In the light of this observation, it is envisaged that the results of this study will fill some gaps and at the same time make modest contributions to knowledge on network infrastructure systems. The findings and recommendations of this study will provide a framework for the implementation of sound network security infrastructure practices. The results of the study, conclusions and recommendations are hoped to spur further research to utilize technology and network systems to meet the challenges and threats of the emerging security issues globally. It will also be a heuristic tool for future research. The findings of the research would be of immense help to students in tertiary institutions and other researchers to investigate further into the area of study. It is hoped that the result of the research would facilitate optimal business decisions when the recommendations are complied with.

Scope of the Study

This research covered the impact of cyber security on networks operations, using Vodafone Ghana as a study. While there are numerous branches of Vodafone in Ghana, the study was conducted at the head office branch in the Greater Accra Metropolis, specifically Kwame Nkrumah Circle. Thus, the findings of this study were limited to the views expressed by respondents from head office branch and not entirely the views of all employees of Vodafone Ghana.

LITERATURE REVIEW

The review was considered on the network security system's areas important to prevent intrusion of hackers and criminals who manage to get access to network systems and leak information to the outside world.

Techno-ethical Inquiry Theory

This is the application of ethical behaviour of human beings within the bigger picture of technological environment. Luppicini, (2009) defined techno-ethics as an interdisciplinary field embracing all the ethical aspects of technology within the society controlled by technology; it is about human processes and practices linked to technology which is embedded within the socio-political and moral life of human beings.

Moor (2005) encapsulated the idea that technological revolution has 3 stages – introduction, permeation and power, and the information revolution is an example of this; so as the social impact of technological revolutions propagates, ethical problems increase and therefore, technological ethics is broadly concerned with the responsible use of technology and its growth for advancing human interests in society. This review has explored technological ethics as the study of global view concerning the relationship between technology and human behaviour. This has therefore, enquired the techno-ethics attempts made to provide conceptual grounding to clarify the role of technology in relation to those affected by it thereby helping to leverage ethical problem-solving and decision making in areas of activity underlying technological inquiry (Luppicini, 2009).

According to Luppicini, (2009), the contemporary society that we find ourselves places colossal emphasis on how the scientific world of technological innovation is leading to changes in the globe we live, at an extraordinary velocity that is difficult to keep up and moreover, explain. Luppicini (2009) therefore, associated this phenomenon as a conflict with traditional humanistic notions that put human beings at the centre of life and society. The technological society is not allowing the societal world to be manipulated by humans anymore, as it is the technological modernisms that are controlling the world; with the advent of prevailing science and technology, human reality is subsumed under traditional humanistic notions of individual life and society (Luppicini, 2009).

Luppicini (2009) supported his view with the fact that different dimensions of human life and society, including physical being, conscious experience, human values, societal norms, cultural meaning, law and interactions, are intertwined within the intermediated system of technology firmly grounded at the base of current life within the society. Furthermore, Luppicini (2009) lamented that the rise of the technological society is accompanied by a social and ethical crisis that society is powerless and therefore, struggling to deal with. He ascribed this to the tremendous power and impact of the technological interlock, social and ethical considerations which are now at the forefront of public concern and interest. There is plethora of social and ethical considerations connected to the internet use, including privacy issues, censorship, cybercrime and cybersecurity that are to be dealt with by the society (Luppicini, 2009).

Data Science

Apart from the mechanisms put in place within the network operations of an enterprise to prevent intruders into the system, the BCS (British Computer Society) has introduced Data Science as a new course in Information Technology; this course is for professional standard development across many different disciplines to help manage the network systems imposed by the technological advancement on human beings (Penketh, 2022). Penketh (2022) reiterated that Data Science is a foundation of Artificial Intelligence (AI) and Machine Learning (ML) which inspires confidence as technology is used to bring together professional standards to ensure ethical and well-governed data in safe hands of human beings.

It is a fact that most data handlers in establishment are not well trained and groomed to handle data properly and are mostly the biggest challenge of data leakage. Penketh (2022) intimated that good data is required by all, from citizens through to practitioners and it needs to be produced and safeguarded to the highest professional level. Finally, Data Science knowledge has the potential to raise both the quality of data-driven insights and provide confidence to the public over how their data is being used and managed (Penketh, 2022).

Cyber

According to merriam-webster.com (n.d.), cyber is related to information technology and involves computer networks, such as the internet, world wide web (www) or virtual reality. Cyber as a prefix is used in a lot of terms to describe events that are being made possible by the spread of computer systems. Anything related to the internet or wide world web also falls under the cyber category (merriam-webster.com, n.d.). Some popular words associated with cyber prefix include, among others:

i. Cyber security,
ii. Cyber attack,
iii. Cyber crime,
iv. Cyber gamification, and
v. Cyber forensics.

Cyber Security

Kaspersky.com (n.d.) describes cyber security as the method of protecting computer systems, servers, electronic and network systems, data and mobile devices from malevolent attacks.Clark (2022) wrote that a threat is always looming so far as we trust machines to defend against humans; he posited that there were inherent limitations when it comes to securing a network system with human security team, as they would take the salary increment alright as skilled people, but the terrain was adaptable to shifts. Clark (2022) mentioned that human beings must sleep, take holidays and sometimes fall sick; however, 24/7 monitoring of the network is the key to ensuring the system is protected against attackers who are never off the scene.

According to Clark (2022), AI and ML are known to be faster than human beings and already revolutionizing many industries, and moreover starting to become more prevalent in the cyber security industry. Furthermore, AI and ML are designed to easily adapt and do not need inherently trust to provide instant solution, as increasingly network system attacks are caused by insider threats, which are becoming common (Clark, 2022). Kaspersky (n.d.) declared that there are different contexts, including conglomerate, enterprise, business and mobile computing, and again diverse categories of situations where cyber security is applied, including:

Network Security – the approach of protecting/securing computer network from intruders who may be either targeted or opportunistic attackers and malware;

Application security – focuses on shielding software and devices from threats whereby a successful security is built into the system at the design stage, well before a program or device could be organized;

Information security – protects the veracity and privacy of data in both transit and storage;

Operational security – comprises the processes and decisions for handling and protecting data assets. The authorizations that enable users to access a network and measures that determine how and where data is stored/shared are contained within this security;

Disaster recovery and business continuity – how an enterprise respond to a cyber-security incident or other events that cause the loss of data. Disaster recovery policies dictate how the organization restores its operations and information loss to return to the same operating capacity as before. Business continuity is the blueprint the organization falls on while trying to operate when deprived of certain resources; and

End-user education – addresses the most unpredictable cyber-security component, normally people. Any user can accidentally introduce virus to an otherwise secure system by failing to follow good security practices. Users, therefore, need to be taught to delete suspicious email attachments, not plug in unidentified USD drives and other various important lessons vital to the security of the enterprise (Kaspersky.com, n.d.).

Cyber Attacks
These include the unauthorized access, use, manipulation, interruption or destruction of electronic information and physical infrastructure used to process, communicate and/or store that information. They are normally carried out by criminals with the intention to destroy either the data or the network system or both.

According to Pratt (2022), a cyber-attack is an attempt to gain unauthorized access to a computer system or computer network with the intention to destroy the system or network; this can happen when an infiltrator intends to disable, disrupt or destroy the computer system or alter, delete, manipulate or steal the data held within the network. Anyone who carries out cyber-attacks are regarded as cybercriminals, bad/threat actors or hackers and they belong to criminal syndicate working with others to find weaknesses/vulnerabilities to exploit for criminal gain (Pratt, 2022). The severity of the cyber-attack determines the appropriate level of response and/or mitigation measures to restore the system.

Pratt (2022) mentioned some of the most common types of cyber-attacks, including:
i. Malware,
ii. Phishing,
iii. Smishing,
iv. Man-in-the-middle,
v. DoS and DDoS,
vi. SQL injection,
vii. Domain name system (DNS) Tunnelling, and
viii. Brute-force attack.

Malware – this is a malicious software that is created by cyber criminals for attacking information systems. This is used by hackers to steal/secretly copy sensitive data, block access to files, disrupt system operations or make systems inoperable (Pratt, 2022). Examples are:

Ransomware – designed to block access to a computer system until a sum of money is paid. It was formerly aimed at individuals but currently spread to businesses; a report from cybersecurity & compliance company revealed that about 78% of organizations experienced an email-based ransomware attack in 2021 (Pratt, 2022).

Spyware – premeditated to obtain covert information about another's computer activities by transmitting data covertly from their hard drive (Pratt, 2022).

Trojans – download onto a computer system and disguise as a legitimate program in order to hide malicious code within genuine software to gain users' system access (within their software) – (Pratt, 2022).

Phishing – hackers publicly create email messages to entice recipients to expose/uncover them. The messages sent out by the predators' trick recipients into downloading the malware within the email by either opening an attached file or embedded link. A report from cybersecurity &

compliance company revealed that about 83% of organizations experienced a phishing attack in 2021, with an increase of 46% from 2020 (Pratt, 2022).

SMiShing (SMS Phishing/Smishing) – an evolution of phishing attack methodology via test (technically, Short Message Service). Hackers send socially created texts that download malware when recipients click on them. Proofpoint mentioned that about 74% of organizations experienced attacks in 2021, up from 61% in 2020 (Pratt, 2022).

Man-in-the-middle (MitM) – attackers secretly insert themselves between 2 parties, such as individual computer users and their financial institutions so that s/he can intercept and alter data travelling between them. Depending on the attack, it may be classified as man-in-the-browser, monster-in-the-middle, machine-in-the-middle or eavesdropping attack (Pratt, 2022).

DoS and DDoS – DoS (Denial of Service) attack involves hackers sending large requests to prevent users from accessing online services and DDoS (Distributed Denial-of-Service) attack happens when hackers bombard an organization's servers with large and flooding messages from sources perhaps spoofed IP source addresses that bring organizations network connectivity to a grinding malfunction. In both cases, hackers send volumes of simultaneous data requests to prevent users from accessing connected and legitimate online services / requests (Pratt, 2022).

SQL Injection – is a common attack vector that occurs when hackers insert malicious code into servers using SQL (Structured Query Language) programming language for backend database manipulation to access and reveal sensitive information that was not intended to be displayed (Pratt, 2022).

Domain name system (DNS) tunnelling – this is a sophisticated attack where the DNS protocol instead of being used for requests and replies to perform legitimate IP address lookups is exploited and the malware uses the DNS to implement a command-and-control channel with its handler for data exfiltration, i.e. unauthorized transfer of information from an information system (Pratt, 2022).

Brute-force attack – employing trial-and-error method to crack login credentials, such as usernames, passwords and encryption keys and hoping that the multiple attempts pay off with the right guess (Pratt, 2022).

Cyber Crime

Known also as computer crime is the use of the computer system to promote illegal ends, such as fraud, child pornography, intellectual property, stealing identities or violating privacy (Dennis, 2023). Dennis (2023) hinted that this is normally carried through the internet and has grown significantly due to the computer system becoming central to activities, such as, commerce, entertainment, governance or banking (Dennis, 2023).

Cyber crime is an attack on information about individuals, organizations, etc. and do not take place on a physical body, but on the personal or corporate body, which is the set of informational attributes that define people and enterprises on the internet (Dennis, 2023). According to Dennis (2023), in the digital age, our virtual identities are essential elements of everyday life, as we are in a bunch of numbers and identifiers in multiple computer databases owned by businesses and governments. Cyber crime therefore, highlights the centrality of network computer systems in our lives, as well as the delicateness of such apparently solid facts by way of individual identity (Dennis, 2023).

Furthermore, Dennis (2023) mentioned that there is a strong belief that new technologies are likely to create criminal opportunities, but few new types of crimes, as there are already many types; criminals do not need a computer system to commit crimes, such as fraud, trafficking in child pornography and intellectual property, steal an identity or violate someone's privacy. All these activities existed before the 'cyber' prefix became accepted and globalized, as cyber crime involving the internet epitomizes an extension of existing criminal conduct alongside some different unlawful activities (Dennis, 2023).

Cyber Gamification

According to Carson (2022), cyber gamification is a strategy that encourages people to solve security-related challenges through competitions and gaining rewards, thereby improving their hands-on technical expertise and teamwork skills. Furthermore, gamification may be purposely for hacking, where games theory and mechanics are used for fun, understanding and improving cybersecurity decision-making (Carson, 2022). Moreover, Carson (2022) mentioned that gamification is not new in business, as many organizations use gamification for performance management and customer loyalty programs to earn appreciation from management.

Ratnayake (2022) added that businesses are adapting their processes and services to create spatial and embodied experiences, where users can explore websites, create avatars / embodiments and replicate real-world experiences through the internet to enable them understand their network system better and protect it from intruders.

Cyber Forensics

Lutkevich (2021) described cyber forensics as the application of investigation and analysis techniques to gather and preserve evidence from a particular device (example, a computer system), suitable for presentation in a court of law. The goal is to perform a structured investigation and maintain evidence to discover exactly what happened on a computer device and who was responsible (Lutkevich, 2021).

According to Moore (2022), digital forensic encompasses the recovery, investigation, examination and analysis of data that has been found on digital devices; the primary objective is to identify, scientifically secure and preserve potentially relevant digital devices, including computer system, mobile phone, smartwatch on a person's wrist and internet WiFi router.
Furthermore, Moore (2022) mentioned that forensic methodologies may differ, based on the environment one operates; the United Kingdom has five (5) steps – identification, preservation,

collection, analysis and reporting. However, the reporting is the most unspectacular part of the 5 steps, as the presentation of data for legal teams/court can be puzzling – the wording must be consistently comprehensible to a technical amateur and with few, but acceptable words (Moore, 2022).

Network Operations Centre

Kumar, Park and Subramaniam (2008) explained computer network operation as the collection of computer systems working together to allow the sharing of both hardware and software resources, including information. Awati (2021) defined network operations centre (NOC) as a centralized point where enterprise IT administrators (internal or third party) supervise, monitor and maintain a telecommunication network.

Large enterprises with extensive networks and commercial service providers typically have a room equipped with devices that provide visualizations of the network on a workstation at which the detailed status of the network with the software can be viewed and managed. For such large enterprises, the NOC acts as the nervous system to operationalize, manage and optimize business-critical tasks, including network troubleshooting, software distribution and updating, router and domain name management, performance monitoring and co-ordination with affiliated networks (Awati, 2021).

According to ibm.com (n.d.), NOC is a centralized location where computer systems, telecommunication or satellite network systems are monitored and supervised 24/7; NOCs oversee large organizations' complex networking environment, including servers, databases, firewalls, devices and related external services. Furthermore, NOCs deal with issues that could disrupt network performance, including identifying malware, managing volume of users and website traffic, maintenance and optimizing the network performing rate through updates (ibm.com, n.d.).

According to Whitman and Mattord (2012), the more computer and networked systems increase, the more the need network security becomes increasingly necessary and important. Computer network systems are always exposed to various kinds of internet threats and therefore, the need for increased network security, which is vital and important in every organization. Network security problems most organizations face sometimes has to do with the employees within the organization, as the errors they make lead to exploitation by cyber criminals.

Effect of Cyber Security on Network Operations

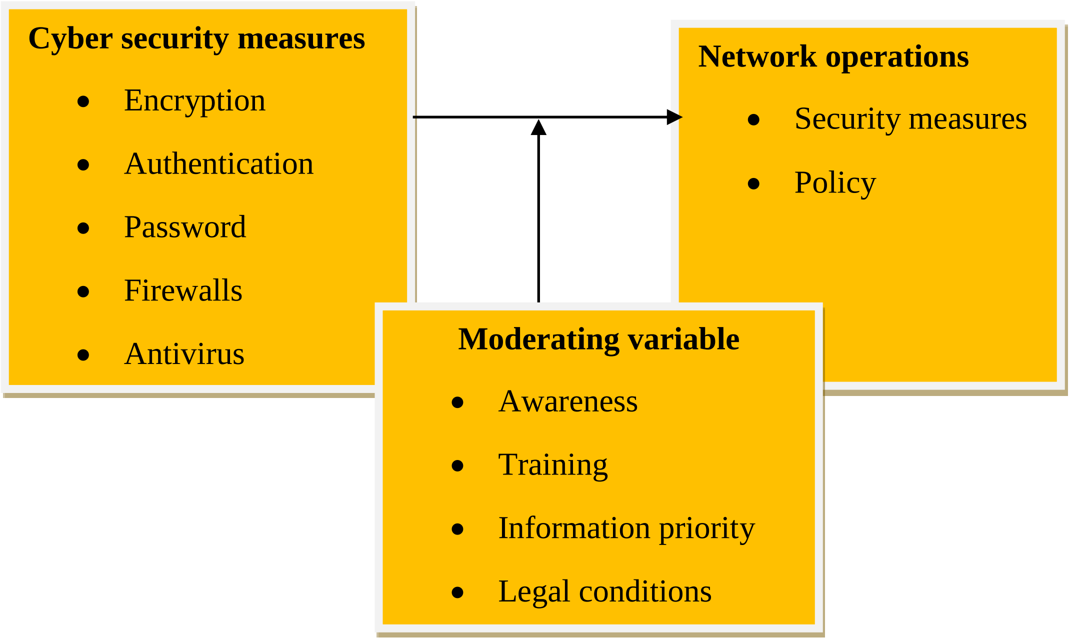


Figure 1: Cyber security measures and its moderating variables

In the above network environment, existing cyber security measures are available. The data source has been developed independently and divided into three parts (Figure 1). By extracting data from the original data sources, the researchers improved and simplified the cyber security measures' structure, addressed awareness, training, information priority and legal conditions which were important for data encryption, authentication, password, firewalls antivirus and guard within Vodafone Ghana.

The exposure of classified information during security breach incidents can result in huge losses to both consumers and enterprises (Ou, Zhang, Angelopoulos, Davison & Janse, 2022). Normally, new threats to information systems occur from unexpected sources and the impact on organizations are substantial, ranging from loss of productivity to damaging reputation (Nyanchama, 2005). Building software for a network operation is time consuming, challenging and expensive, so incorporating vulnerability prediction models with ML techniques to identify vulnerable software components is important to protect and secure the system from cyber criminals (Abunadi & Alenezi, 2016).

Standard Services Offered to Combat Attackers

According to Coffin (2003), companies offer ethical hacking services to combat attackers and the typical services offered to combat the attackers include:

External network hacking - This includes scanning the target's web server, firewall and routers for vulnerabilities from an external source. This is the most provided ethical hacking service (Coffn, 2003).

Internal network hacking - This involves deploying a team to the target site, where they conduct penetration testing on the company's servers and routers, using its own equipment. This is a good test for defending against disgruntled employees, industrial saboteurs or anyone else who might try to intrude upon a company's network from within (Coffin, 2003).

Application testing - This growing arena for the ethical hacking industry is aimed specifically at clients who have developed their own software, such as custom web-based voting and polling programs or online stores and payment programs. Any software not delivered shrink-wrapped falls under the custom application category. Comparatively, scanning web servers for vulnerabilities are easy since they are all relatively uniform. When scanning custom applications, the ethical hacker must reverse-engineer the program and analyze the lines of coding (Coffin, 2003).

Wireless LAN Assessment - This is an increasingly common service, as many firms employ wireless networks within their facilities. Such networks enable laptop users to move their computers from office-to-office while remaining connected to the local network. The problem with these systems is that outsiders around the facility can use that same wireless technology to log in to the company's network without the company knowing it. The most common way to perform a wireless LAN assessment is to conduct 'war driving' – physically traveling around the target facility in search of wireless access points (Coffin), 2003).

War Dialing - An old hacking technique where a hacker breaks into a network by calling phone numbers in the hopes of hitting an unsecured modem that the target has accidentally left active or forgotten. Automated programs enable hackers to dial thousands of numbers in a matter of moments. The technique always works and is one of the tests ethical hackers run that usually turns up an intrusion alert (Coffin, 2003).

Social Engineering - Just as war dialing, social engineering is a simple but effective technique. An intruder calls someone within the target company and convinces him/her to give up sensitive IT information over the phone. Ethical hackers test against this vulnerability by performing social engineering of their own to highlight what ploys the client's personnel will fall for and how to educate itself against such ploys (Coffin, 2003).

Thrashing - Another old hacker trick in which an intruder comb through the garbage of a target company in search of documents that contain important IT data, such as access numbers and passwords, is using subcontractors; these subcontractors coordinate activities well so that they are not suspected of any sinister moves (Coffin, 2003). However, many firms choose to stick exclusively with technology testing. Some companies, including financial institutions, employ armed guards, trashing carries with the possibility of a tragic misunderstanding between the ethical hacker and his/her client's security personnel (Coffin, 2003).

METHODOLOGY

Survey research design was employed where data was collected from the employees of Vodafone Ghana, head office branch. The study adopted the qualitative research approach as the best since it gave the researchers the ability to collect primary data which was converted into variable frequencies, averages and ranges from the organization (Bryman & Bell, 2007) and tested it against what pertains in life.

The target population for the study was the staff of Vodafone Ghana, head office, Accra, which was estimated to be over two hundred and fifty (250), out of which fifty-five (55) was estimated for the sample size. A stratified random sampling of convenience and quota was used for the research, which gave information quicker to take cognizance of certain characteristics of the population to enrich the sample (Salkind, 2006).

Questionnaire was used for the data collection method, which provided an effective way of collecting responses from the respondents. This instrument was developed, piloted and tested to verify that the questions were clear and not ambiguous, such that responses would also be consistent with the purpose of the study. Questions were reviewed where necessary, based on response from the respondents, during the pilot study. This was done to improve the reliability and validity of the questionnaire.

Secondary data collected from network operation materials were merged with the primary data collected through questionnaire, where possible (Bishop, 2006). This was coded for easy access, qualitatively analyzed and presented. Findings were arranged in logical and sequential format so that conclusions could be drawn from the analyses. Respondents were advised that their participation was confidential and voluntary, and assured of a copy of the results from the study, based on request.

ANALYSES AND DISCUSSIONS OF RESULTS

A total of fifty-five (55) questionnaires were distributed to Vodafone Ghana, Head Office staff, of which fifty (50) were duly filled and returned; three (3) copies were filled wrongly, while two (2) were not returned. This brings the total questionnaire for the analysis to fifty (50), giving a response rate of 91% which was very good, as it fairly represented the views of the entire research population.

The demographic characteristics of the sample, include the gender, age, academic qualification and how long staff have been working with the organization. These characteristics have been found to be indicators of employees' attitude towards work in general.

On the gender distribution of respondents, males and females were represented by 62% and 38% respectively. This implies that most of the respondents for this study were males, making males outnumber females by 24% (Table 1).

For the age of the respondents, 24% of the respondents were over 40 years; 30% of the respondents between 36-40 years, and 20% were 31-35 years old. Again, 18% of respondents were between 26-30 years, with about 8% below 26 years. It could therefore, be deduced from the data collected that, most of the respondents were between the ages of 36-40 years. The study comprised respondents that were at diverse age brackets and, consequently, reinforce and reflect the thoughts and views from diverse groups of respondents from the organization (Table 2).

The study sought to find out the highest level of education attained by the respondents. The analysis indicated that 14% of the respondents have professional education, 10% have certificate/diploma education, 16% were HND holders, 48% have first university degree and 12% were Master's degree holders. All the respondents were tertiary or professional qualification holders, making them matured enough to give well-informed, reliable and better responses to the questions within the Questionnaire (Table 3).

The respondents were asked to indicate how long they have been working with the organization. Their responses showed that 14% have been working for less than a year, 12% and 38% of the respondents have been working for between 1 to 3 and 3 to 5 years respectively, 20% have been working between 5 to 7 years while 16% have more than seven (7) years. It could be observed that, about 74% (3-5 years, 5-7 years and over 7 years) of the respondents have worked in the organization for more than 3 years. This is good for the study, as majority of respondents have been with the organization for long time, and are familiar with the operations of Vodafone, Ghana (Table 4).

On the question of how secured the organization firewall system was to protect against undesired access to the organization's servers from outside the organization, 6% of the respondents said it was Very Secured, 46% said it was Secured, 36% were Not Sure, 4% said it was Poorly Secured, whiles 8% said it was Not Secured. It can therefore be deduced from the 52% (Very Secured and Secured) respondents that the organization's firewall system to protect against undesired access to organization servers from outside the organization was secured (Table 5).

The respondents were asked whether the organization has wireless internet connection, and how strict was the access rules that only its employees can use the wireless network. 36% of them said it was Very Strict, 42% said it was Strict, 10% of them said they were Not Sure, whereas 6% said it was Poor Restriction and 6% responded that it was Not Strict. It can be concluded from the 78% (Very Strict and Strict) respondents that the organization has wireless internet connection, which was strict in terms of the access rules, and to the extent that only its employees can use it (Table 6).
It was asked whether in Vodafone's conditions of employment contract, there was any security roles and responsibilities aimed to protect sensitive data. 72% of the respondents Agreed, 14% Disagreed, whiles 14% were Not Sure. It can be deduced from the 72% of agreed

respondents that the conditions of employment contract in Vodafone have security roles and responsibilities aimed to protect sensitive data (Table 7).

When asked whether upon termination of a person's employment, there was any retrieval process of sensitive information access from an outgoing employee in an appropriate manner. 66% of the respondents Agreed, 16% Disagreed, whiles 18% of them were Not Sure. The 66% of Agreed respondents indicates that upon termination of a person's employment, Vodafone Ghana makes sure that there is retrieval of sensitive information from an employee in an appropriate manner (Table 8).

In response to whether Vodafone, **Ghana checks the operational status of implemented security measures** such as, by recording and maintaining access logs and checking for unauthorized operations to important information, 68% of the respondents Agreed, 14% Disagreed, whereas 18% of the respondents were Not Sure. Since 68% of respondents agreed that Vodafone Ghana checks the operational status of the implemented security measures, such as by recording and maintaining access logs, it implies that the organization checks for unauthorized access to operational and important information (Table 9).

On the issue of whether the organization's cyber security (network operations) have been down due to computer viruses, 12% of the respondents Agreed, 72% Disagreed, whereas 16% were not sure. The 72% disagreement indicates that the organization has not been affected much by cyber security risks, example, where the computer network system has been attacked by viruses (Table 10).

In response to whether the organization's website has been subjected to hacker attack, 32% Agreed, 50% Disagreed, whiles 18% were Not Sure. The results show that, Vodafone Ghana's website has not been affected much by hacker attacks (Table 11).

On the issue of which other cyber security risks the organization has ever been exposed to, 42% said Denial of Service (DoS), 14% said Theft of customer/citizen data, 8% said Stolen Computers/Laptop, 6% stood for Internal employee vandalism, 4% mentioned Website vandalism, whiles 12% said No Risks, and 14% were Not Sure. The results imply that Vodafone Ghana has been facing cyber security risks and the most is DoS (Table 12).

The respondents were asked whether cyber security risks were mostly characterized as borderless, where attackers and cyber victims seem to be located anywhere in the world. 66% of the respondents Agreed, 24% Disagreed with the statement, and 16% were Neutral. The results indicate that cyber security risks have mostly been characterized as borderless, where attackers and cyber victims seem to be located anywhere in the world (Table 13).

Regarding whether cyber security risks were usually considered as having multiple effects i.e. automation enables a criminal to plant an attack and leave it to multiply itself at a very fast rate and with minimal human intervention. 66% of the respondents Agreed, 22% Disagreed with the statement and 12% were Neutral. The results implies that cyber security risks were usually considered as having multiple effects in Vodafone Ghana, where automation enables a criminal to plant an attack and leave it to multiply itself at a very fast rate and with minimal human intervention (Table 14).

Respondents were further asked to identify any challenges of cyber security, not mentioned above, on network operations. Some of the responses outlined by the respondents included the following;

- **Mobility:** Bring-your-own-device has challenges for management, when the organization looks at protecting the critical information needed to manage the organization and the network, without sacrificing the privacy of employee's personal information and activities;
- **Internet:** The perception that the internet is a secured critical infrastructure, is a big challenge for security professionals, as it is an open connection of diverse networks. The challenge for Vodafone Ghana, was to start treating such critical networks as critical to their operations; and
- **Password Management:** One of Vodafone Ghana’s challenge was to put in place and enforce stronger user-controlled passwords that were less likely to be broken. This educational and administrative challenge requires creative solutions and enforced policies.

DISCUSSION OF FINDINGS

Vodafone Ghana has been checking the operational status of the implemented security measures within the organization, by recording and maintaining access logs, checking for unauthorized operations to important information and that the organization’s cyber security (network operations) have not been down from computer viruses.

However, the physical and logical network security, including firewall system to protect against undesired access to its servers from outside the organization, was found not to be very secured at the time of the research. It was revealed that the organization has wireless internet connection, which was strict in terms of the access rules, that only its employees could use the wireless network. This is consistent with similar surveys by Health Information Trust Alliance (2023), that organizations recognize they should be measuring and monitoring their security controls through common channels; channels include penetration testing, vulnerability assessment, risk assessment, audit, patching reports, incident statistics, anti-virus software updates and coverage with internal audit, and information/cyber risk assessment.

Furthermore, the information security standards used to protect sensitive data at the organization was found to be working alright, as the study deduced that upon termination of an employee’s appointment, there was retrieval process of sensitive information held by the employee in an appropriate manner. This is consistent with that of Public Safety Canada (2013b), which demonstrated that cyber-attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information.

In addition, it was revealed that Vodafone Ghana’s cyber security risks have been controlled, as computer viruses have not affected its website; it has never been subjected to hacker attack. It was gathered that most cyber security risks Vodafone Ghana has ever been exposed to, was denial of service (DoS) attack. The study revealed that cyber security risks were mostly characterized as borderless, where attackers and cyber victims seem to be located globally.

Mitigating Denial-of-Service attacks using CAPTCHA

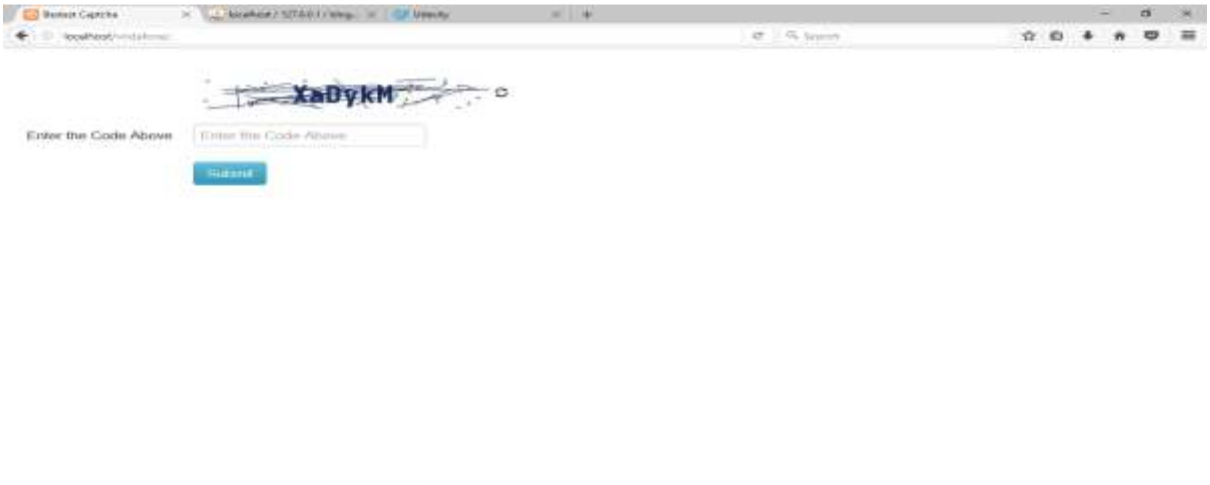
The Denial-of-service (DoS) attack normally sends out large number of fake requests to a network resource until it exceeds the server capacity (buffer overflow); consequently, resulting in the DoS attack. These attacks are prevented with a client authentication mechanism known as CAPTCHA (**C**ompletely **A**utomated **P**ublic **T**uring Test To Tell **C**omputers and **H**umans **A**part) to distinguish between traffic from human users and bots. CAPTCHAs are used on web sites to prevent automated form submissions, email-creations and online forum posts.

A text-based CAPTCHA is used to authenticate users before allowing them access to the web services, which is not costly for enterprises. The aim is to distinguish between legitimate users and bots, thereby adding an extra layer of security and to also ensure that the webpage is always accessible to legitimate users.

Implementation of an authentication mechanism (CAPTCHA)

To demonstrate the authentication mechanism using CAPTCHA, a sample Vodafone webpage was developed, then the CAPTCHA was incorporated into the webpage to filter the various requests sent to the webpage. PHP, Java script and html were used for the implementations. In addition, XAMPP / WAMP were used to provide local web services for testing purposes. The authentication procedure via the developed CAPTCHA is explained below:

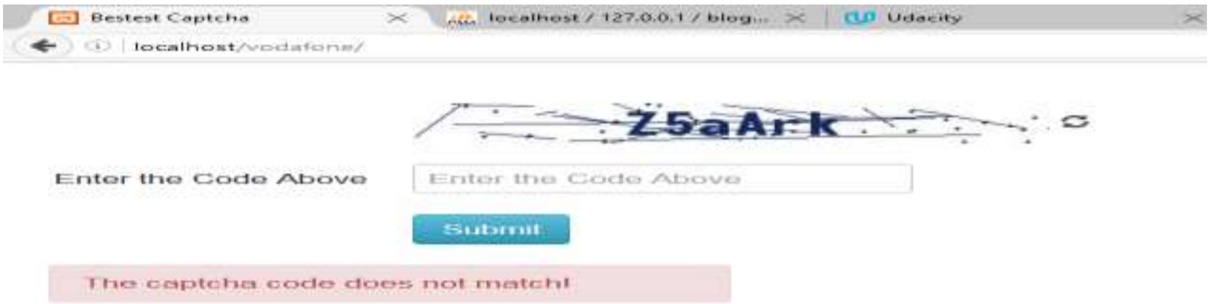
i. On loading the webpage, the user will be presented with image on which some text is displayed. The image is randomly selected from set of images available (i.e., from the CAPTCHA engine). An example is shown in the figure below.



Enter the Code Above: Enter the Code Above

Figure 2: The CAPTCHA

ii. It is compulsory for the user to enter the same letters in text as presented in the image, into a provided text field that is displayed on the authentication page.
iii. On submitting the entered text, the server checks if the text entered by the user matches the text generated in the image. If it does, the user is allowed to gain access to the website. Otherwise, an error message is displayed and the user has to enter a new text.



The captcha code does not match!

Figure 3: The Error Message

The image above shows the error message displayed when the user enters a wrong text into the text field, therefore access to the webpage is denied.On entering the correct text on the CAPTCHA authentication page, the user is granted access to the webpage, and thus, the website's resources.It is advisable Vodafone Ghana should expect a higher risk of business impacting threats, with the shift from computer-based attacks, which would generate large number of lower bandwidth events to virtual server/cloud-based attacks and generating ultra-high bandwidth events. The anticipation of these new vector attacks would help Vodafone Ghana to identify and mitigate large DDoS attacks while traffic is in the network cloud.

CONCLUSIONS

There is no doubt that the contemporary global evolving hazards on the network environment, would energize Vodafone Ghana to maintain the proactive approach against threats, create an environment of continuous compliance, and have responsive IT operations, processes and management to subdue all cyber threats. The organization should continue to strive hard to reduce risk exposure and the attack from cyber aggressors, detect and respond to advanced threats, and drive down security and operations costs.

Recommendations

The following recommendations would inure greatly to the benefits of Vodafone Ghana and other network systems:
i. As people may be an attack vector through social engineering, the staff of Vodafone Ghana should ultimately share responsibility in ensuring best-practice cyber security processes are carried out. This requires staff education with regular updates on new cyber threats;
ii. The management of Vodafone Ghana, should use risk analysis as the basis for formulation of network security policy as well as selecting information security controls. Network policy should be implemented and enforced to keep information secured. It is essential that the

organization's data is kept secured and therefore, should be removed from the lunchroom to a secured space. Password policies should be implemented and enforced to ensure the selection of strong passwords; and

iii. A text-based CAPTCHA could be used as a first security measure to control intruders into the network system. However, the CAPTCHA should consider users with vision disability. There is the need, therefore, to develop a more robust CAPTCHA mechanism that will consider all types of users. According to Moradi (2015), improvements that could be made to current and future CAPTCHA include, improving user-friendliness and design structure, and the introduction of gamification to make it interesting for staff to be fully involved in network operation security.

TABLES

Table 1: Gender of respondents

		Frequency	Valid Percent	Cumulative Percent
Valid	Male	31	62.0	62.0
	Female	19	38.0	100.0

Table 2: Age of respondents

		Frequency	Valid Percent	Cumulative Percent
Valid	Below 26yrs	4	8.0	8.0
	26-30yrs	9	18.0	26.0
	31-35yrs	10	20.0	46.0
	36-40yrs	15	30.0	76.0
	41years and above	12	24.0	100.0

Table 3: Qualification of respondents

		Frequency	Valid Percent	Cumulative Percent
Valid	Diploma	5	10.0	10.0
	HND	8	16.0	26.0
	First Degree	24	48.0	74.0
	Professional Certificate	7	14.0	88.0
	Master's Degree	6	12.0	100.0

Table 4: Tenure of respondents

		Frequency	Valid Percent	Cumulative Percent
Valid	Less than 1 year	7	14.0	14.0
	1-3 Years	6	12.0	26.0
	3-5 Years	19	38.0	64.0
	5-7 Years	10	20.0	84.0
	7 Years and above	8	16.0	100.0

Table 5: Organization firewall system

		Frequency	Valid Percent	Cumulative Percent
Valid	Very Secured	3	6.0	6.0
	Secured	23	46.0	52.0
	Not Sure	18	36.0	88.0
	Poorly Secured	2	4.0	92.0
	Not Secured	4	8.0	100.0

Table 6: Wireless internet connection

		Frequency	Valid Percent	Cumulative Percent
Valid	Very Strict	18	36.0	36.0
	Strict	21	42.0	78.0
	Neutral	5	10.0	88.0
	Poor Restriction	3	6.0	94.0
	Not Strict	3	6.0	100.0

Table 7: Conditions of employment contract

		Frequency	Valid Percent	Cumulative Percent
Valid	Yes	36	72.0	72.0
	No	7	14.0	86.0
	Not Sure	7	14.0	100.0

Table 8: Retrieval process of sensitive information

		Frequency	Valid Percent	Cumulative Percent
Valid	Yes	33	66.0	66.0
	No	8	16.0	82.0
	Not Sure	9	18.0	100.0

Table 9: Operational status of the implemented security measures

		Frequency	Valid Percent	Cumulative Percent
Valid	Yes	34	68.0	68.0
	No	7	14.0	82.0
	Not Sure	9	18.0	100.0

Table 10: Cyber security risks

		Frequency	Valid Percent	Cumulative Percent
Valid	Yes	6	12.0	12.0
	No	36	72.0	84.0
	Not Sure	8	16.0	100.0

Table 11: Subjected to hacker attack

		Frequency	Valid Percent	Cumulative Percent
Valid	Yes	16	32.0	32.0
	No	25	50.0	82.0
	Not Sure	9	18.0	100.0

Table 12: Cyber security risks (the organization has ever been exposed to)

		Frequency	Valid Percent	Cumulative Percent
Valid	Denial of service	21	42.0	42.0
	Internal employee vandalism	3	6.0	48.0
	Theft of customer/citizen data	7	14.0	62.0
	Stolen computers/laptop	4	8.0	70.0
	Website vandalism	2	4.0	74.0
	No Risks	6	12.0	86.0
	Not Sure	7	14.0	100.0

Table 13: Cyber security risks are mostly characterized as borderless

		Frequency	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	5	10.0	10.0
	Disagree	7	14.0	24.0
	Undecided	5	10.0	34.0
	Agree	25	50.0	84.0
	Strongly agree	8	16.0	100.0

Table 14: Cyber security risks are usually considered as having multiple effects

		Frequency	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	6	12.0	12.0
	Disagree	5	10.0	22.0
	Undecided	6	12.0	34.0
	Agree	29	58.0	92.0
	Strongly agree	4	8.0	100.0

REFERENCES

Abunadi, I., & Alenezi, M. (2016). An empirical investigation of security vulnerabilities within web applications. *Journal of universal computer science*. July 2016.

Awati, R. (2021). What is a network operations centre (NOC)? Retrieved from: https://www.techtarget.com/searchnetworking/...

Bishop, L. (2006). A proposal for achieving context for secondary analysis. *Methodological innovation online.* 1(2), 10-20.

Bryman, B., & Bell, E. (2007). *Business research methods* (2nd ed.). NY: Oxford University Press.

Clark, T. (2022). Trusting machines to defend against humans. *The Magazine for the IT Professional, ITNOW.* Autumn 2022.

Carson, J. (2022). Cybersecurity gamification: Cyber challenges to prepare you for a real attack. Retrieved from: https://www.delinea.com/blog/cybersecurity-gamification.

Coffin, B. (2003). It takes a thief: ethical hackers test your defenses. Retrieved from: https://www.thefreelibrary.com/It+takes+a+thief...

Dennis, M. A. (2023). Cyber crime. Retrieved from: https://www.britannica.com/topic/cybercrime.

Diesch, R., & Krcmar, R. (2020). Linking information security metrics to management success factors. DOI: 10.1145/3407023.3407059.

Engebretson, P. (2013). *The basics of hacking and penetration testing: Ethical hacking and penetration testing made easy (2nd ed.).* Retrieved from: https://www.sciencedirect.com/book/9781597496551.

Froehlich, A., & Bacon, M. (2021). White-hat hacker. Retrieved from: https://www.techtarget.com/searchsecurity/definition/white-hat.

Graves, K. (2010). *CEH Official certified ethical hacker review guide*. California: Sybex.

Geer, D., Soo Hoo, K., J., Jaquith, A. (2003*). Information Security*: *Why the Future Belongs to Quants*. New York: IEEE Security and Privacy.

Hanna, K. T., & Teravainen, T. (2021). What is a black hat hacker? Retrieved from: https://www.techtarget,com/searchsecurity/definition/black-hat.

Health Information Trust Alliance (2023). Health Information Trust Alliance Common Security Framework. Retrieved from: https://learn.microsoft.com/en-us/compliance/regulatory/offering-hitrust.

Ibm.com (n.d.). What is a network operations centre? Retrieved from: https://www.ibm.com/topics/network-operations-centre.

Jackson, V., & Youssef (2023). Is cyber security being taught correctly? *The Magazine for the IT Professional, ITNOW.* Spring 2023.

Kaspersky.com (n.d.). What is Cyber Security? Retrieved from
https://www.kaspersky.com/resource-centre/definitions/what-is-cyber-security.

Kumar, J., Park, Y., & Subramaniam (2008). Understanding the value of countermeasures portfolios in information Systems Security. *Computers and Security, 6, 22-35.*

Landoll, D. J., & Landoll, D. (2005). *The security risk assessment handbook: A complete guide for performing security risk assessments*. Boca Raton: CRC Press.

Laudon, K. C., & Trevel, C. G. (2022). *E-commerce 2021–2022 Business. Technology*. Education. ISBN 13: 978-1-292-40931-3.

Luppicini, R. (2009). Technoethical inquiry: From technological systems to society. *Global Media Journal.* 2(1). Retrieved from: https://www.semanticscholar.org/paper/Technological.

Lutkevich, B. (2021). What is cyber forensics? Retrieved from: https://www.techtarget.com/.../comp.

Merriam-webster.com (n.d.). What is Cyber? Retrieved from:
https://www.merriam-webster.com/dicionary/cyber.

Moradi, M., & Keyvanpour, M. R. (2015). CAPTCHA and its alternatives: A review. *Security and Communication network*. 8(12). p.2135-2156.

Moor, J. H. (2005). Why we need better ethics for emerging technologies. *Ethics and Information Technology*. 7(3), 111-119. DOI:10.1007/s10676-006-0008-0.

Moore, A. (2022). Digital forensics and crime scene investigation. *The Magazine for the IT Professional, ITNOW.* Autumn 2022.

Nyamchama, M. (2005). Enterprise vulnerability management and its role in information security management. *Journal of Management Information Systems*. 14(3), 29-56.

Ou, X., Zhang, X., Angelopoulos, S., Davison, R. M., & Janse, N. (2022). Security breaches and organization response strategy: Exploring consumers' threat and coping appraisals. *International Journal of Information Management*. 65. 102498.

Pratt, M. K. (2022). What is a cyber attack? Retrieved from: https://www.techtarget.com/searchsecurity/definition/cyber-attack.

Peltier, T. R. (2004). *Information Security Policies, Procedures, and Standards: Guidelines for effective information security management* (2nd ed.). Boca Raton: Auerbach Publications.

Penketh, C. (2022). UK takes leadership on Data Science standards. *The Magazine for the IT Professional, ITNOW.* Autumn 2022.

Public Safety Canada. (2013a). *Action Plan 2010-2015 for Canada's Cyber Security Strategy*. Retrieved from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt.

Public Safety Canada. (2013b). *An open letter to Canadians on cyber security awareness (Archived).* Retrieved from: https://www.publicsafety.gc.ca/cnt/nws/nws-rlss/2013/20131003-en.aspx.

Ratnayake, D. (20, p22). Cyber gamification. *The Magazine for the IT Professional, ITNOW.* Autumn 2022.

Reed D. (2003). Applying the seven OSI Layer *Network Model to Information Security.* Retrieved from: https://www.sans.org/white-papers/1309.

Reynolds, G. W. (2014). *Ethics in information technology* (5th ed.). Boston, MA: Cengage Learning.

Salkind, N. J. (2006). *Exploring research* (6th ed.). USA: Prentice Hall.

Sandeep, V., Thirupathi, P., Kumar. P., & Naresh, S. (2019). Goals and model of network security. *International Journal of Advanced Science & Technology*. 28(20), p. 593-59.

Stamp, M. (2011). *Introduction in information security: Principles and practice* (2nd ed.). Hoboken, NJ: John Wiley & Sons.

Sterling, B. (2008). *The hacker crackdown: Law and disorder on the electronic (eBook).* Retrieved from: https://www.gutenberg.com>files.

Wael, R. (2010). Database security Concepts-, approaches, and challenges. *IEEE Transactions on Dependable and Secure Computing.* 2(1), 2-18.

Whitman, M. E., & Mattord, H. J. (2018). *Management of information security*. Boston: Cengage Learning.