Archives of Business Research – Vol.7, No.6
Publication Date: June. 25, 2019
DOI: 10.14738/abr.76.6589.
Kwadade-Cudjoe, F., Enoch, Y. H., & Bunmi, A. A. (2019). Effect of Cyber Security on Networks Operations (A case study of Vodafone Ghana). *Archives of Business Research,* 7*(6),* 16-32.

Effect of Cyber Security on Networks Operations (A case study of Vodafone Ghana)

Francis Kwadade-Cudjoe
FBCS, FIMIS, PhD, MBA, BSc (Hons)
Senior Lecturer, Knutsford University College and Adjunct Lecturer,
GIMPA Business School, Accra, Ghana

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

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

ABSTRACT

Several networks are being constructed every day, however, making sure the security of the network is not compromised, is very important. The study examined the effect of cyber security on networks operations using Vodafone Ghana as a case study. Using questionnaires, a convenience sampling technique was used to collect primary data, which was then subjected to series of processes and analyses. Vodafone Ghana has been checking the operational status of its implemented security measures, example, recording and maintaining access logs, and checking for unauthorized access to important information. However, it was revealed that the organization's firewall system to protect undesired access to its servers from the outside world was not fully secured. As people may themselves be an attack vector through social engineering, everyone within an organization ultimately shares responsibility in ensuring best-practice cyber security processes are carried out. This requires staff education with regular updates to materials on hand, as new threats arise.

Keywords: Cyber, security, network and operations

INTRODUCTION

Construction of computer network systems is rampant these days, but not all of them are effectively secured. The functioning of a network system hinges on the quality of security application on the network that does not compromise on the network competences (Geer, Soo Hoo & Jaquith, 2003). In essence, for constructing a secure network, organizations should recognize all the likely attacks as well as their mitigation methods, and should do risk analysis to find the risks involved in scheming the network. Besides, organizations should also recognize how to design security policies to apply to the network and instruct the employees to properly protect the organization's information. Lack of security system remains a big setback to organizations in an effort to minimize security vulnerabilities (Wael, 2010). More importantly, theft and destruction of organizations' assets through breakage into the premises are sometimes perpetrated by guards and other employees of the organization (Wael, 2010).

Hackers pose a security risk in that they could compromise vital company information. Information security management is concerned with countermeasures to protect the information assets from various threats, using principles, best practices, and technologies (Peltier, 2005). Once hackers access a computer system, they could steal or alter the

information stored on it or corrupt its operations and program it to attack other computer systems (Dhillon, 2007; Peltier, 2005; Reynolds, 2012; Stamp, 2011). Hackers may be motivated by a multitude of reasons, including profit, protest, challenge, or publicity (Sterling, 1993).

The threat of attacks on information assets in the business sector is a mounting and developing threat (Public Safety Canada, 2013a). Threats-attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the threats or attack determines the appropriate level of response and/or mitigation measures (Public Safety Canada, 2013a). Network attacks have been revealed to be as wide-ranging as the system that they try to infiltrate. Also, attacks are acknowledged to be, either deliberate or unintended and technically, knowledgeable intruders have been involved in targeting the protocols expended for protected communication amongst networking devices (Reed, 2003).

TECHNO-ETHICAL INQUIRY THEORY

Technological advances have a transforming revolutionary effect on society (Moor, 2005). According to Moor (2005), as the social impact of technological revolutions grows, ethical problems increase. Techno-ethics is broadly concerned with the responsible use of technology for advancing human interests in society. Techno-ethics has been defined in a variety of ways (Bao & Xiang, 2006; Galvan, 2001; Jonas, 1985). Techno-ethics as understood in this review of the study rests on a pragmatic worldview concerning the relation between technology and human welfare. Techno-ethics attempts to provide conceptual grounding to clarify the role of technology in relation to those affected by it and to help guide ethical problem-solving and decision making in areas of activity that rely on technology (Luppicini, 2009).

Techno-ethical inquiry theory can be used to examine whether a practice is effective (efficient and ethical), whether the end justifies the means, and whether the benefits outweigh the costs and side effects. Techno-ethical inquiry theory is a scientific method in that it stipulates specific rules and steps for conducting an ethical inquiry into the value and utility of technological practices using a pragmatic decision-making framework, weighing ends (output) of actions against the means (input) in terms of efficiency (perceived output benefits exceed perceived input costs) and fairness (including considerations of side effects) - (Luppicini, 2009). Techno-ethical inquiry theory is a value theory that provides the conceptual grounding for this assessment. The guiding principles of techno-ethical inquiry theory are as follows:

1. Techno-ethical inquiry theory treats technology as a self-producing social system on the basis of knowledge creation (facts and values);
2. The derivation of meaning about system operations involves multi-perspective and multi-aspect inquiry; and
3. The third principle places communication (achieving mutual understanding) as a core goal. A successful techno-ethical inquiry theory identifies all relevant knowledge (facts and values) and priorities (value ranking) applicable to the technological relations to which a techno-ethical inquiry is applied (Luppicini, 2009).

Techno-ethical inquiry theory is a social systems theory and methodology for guiding technological systems research in technology assessment and design. It is well suited for examining the effect of cyber security on networks operations because, first, it places ethical and technical elements at the core of organizational studies. Second, it can be used to frame a multi-perspective, multi-stakeholder view of how ethical hacking practices are meeting the needs of the organization and at what potential cost through the consideration of technical

knowledge (facts and values) relevant to the design context. Third, its pragmatic philosophical orientation aligns with organizational management practices and their emphasis on efficiency and improvement (Luppicini, 2009). Drawing on entrenched scholarship in techno-ethics from Bunge (1977), techno-ethical inquiry theory assumed a pragmatic orientation to moral norms grounded in human activity and existing knowledge. The five steps of Techno-Ethical Inquiry (TEI) theory (Luppicini, 2009) can help frame an understanding about perceived ethical dimensions (whether actions are ethical or unethical) as well as efficiency considerations involved in ethical hacking implementation. The five TEI steps (Luppicini, 2009) can be listed as follows:

Step 1: Evaluate the intended ends and possible side effects to discern overall value;
Step 2: Compare the means and intended ends in terms of technical and nontechnical aspects (moral, social);
Step 3: Reject any action where the output (overall value) does not balance the input in terms of efficiency and fairness;
Step 4: Explore relevant information connected to the perceived effectiveness and ethical dimensions of ethical hacking for key stakeholder groups; and
Step 5: Consider technological relations at a variety of levels.

What is Cyber?

Cyber is a prefix used in a growing number of terms to describe new things that are being made possible by the spread of computers. Anything related to the internet also falls under the cyber category (Dhillon, 2007). Some popular words that use the cyber prefix include the following:

Cyber crime, Cyber forensics, Cyber bully, Cyber buck, Cyber security and Cyber punk.

Cyber Attacks and Cyber Security

Cyber-attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber-attack determines the appropriate level of response and/or mitigation measures: that is, cyber security (Public Safety Canada, 2013b). Cyber-security is a defensive measure, adopted in response to cyber-attacks. It can be understood as a process of applying information security measures to protect the confidentiality, integrity, and availability (CIA) of information. Hackers pose a security risk in that they can compromise the confidentiality, integrity, and availability (CIA) of information. Information security management is concerned with countermeasures to protect the CIA of information assets from various threats, using principles, best practices, and technologies. Once hackers access a computer system, they can steal or alter the information stored on it, or corrupt its operations and program it to attack other computer systems (Dhillon, 2007; Peltier, 2005; Reynolds, 2012; Stamp, 2011).

Three Common Group of Hackers

Hackers can be divided into three groups: white hats, black hats, and grey hats. According to Graves (2007), ethical hackers usually fall into the white-hat category, but sometimes they are former grey hats who have become security professionals and who use their skills in an ethical manner. Graves offers the following description for the three groups of hackers:

- **White Hats** are the good guys, the ethical hackers who use their hacking skills for protective purposes. White-hat hackers are usually security professionals with knowledge of hacking using the hacker toolset, and who use this knowledge to locate weaknesses and implement countermeasures (Graves, 2007).

- **Black Hats** are considered the bad guys: the malicious hackers or crackers who use their skills for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote machines, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, deny legitimate users service, and basically cause problems for their targets (Graves, 2007).
- **Grey Hats** are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Both are powerful forces on the Internet, and they will remain permanent. Some individuals qualify for both categories. The existence of such individuals further clouds the division between these 2 groups of people (Graves, 2007).

Computer Network

According to Kumar, Park and Subramaniam (2008), a computer network is the collection of computers that work together in order to allow sharing of resources and information. In recent years, so many networks are being built and some of the organizations are able to provide security to their networks. The performance of a network depends on the amount of security implemented on the network without compromising the network capabilities (Geer, 2003). For building a secured network, administrators should know all the possible attacks and their mitigation techniques, and should perform risk analysis to find the risks involved in designing the network. They must also know how to design security policies for implementing the network and to educate the employees, to protect the organization's information (Mitnick & Simon, 2002).

For any organization, having a secure network is the primary thing to reach their business requirements. A network is said to be secured when it can sustain from attacks, which may damage the whole network. Over the last few decades, internetworking has grown tremendously and lot of importance is given to secure the network (Reed, 2003). To develop a secured network, network administrators must have a good understanding of all attacks that are caused by an intruder and their mitigation techniques. Choosing a particular mitigation technique for an attack has an impact on the overall performance of the network, because each attack has different ways for mitigation (Reed, 2003). By performing risk analysis, network administrators will identify the assets that need to be protected, threats and vulnerabilities that the network may pose. With the help of risk analysis, administrators will have sufficient information about all risks which helps to build a network with high security (Reed, 2003). After risk analysis, designing a set of security policies is very important to provide high level of security. Security policies provide information for network users for using and auditing the network (Reed, 2003).

Network Operations

According to Whitman and Mattord (2012), as the computers and networked systems increases in the world of today, the need for increase and strong computer and network security also becomes increasingly necessary and important. The increase in the computer network system has exposed many networks to various kinds of internet threats and with this exposure, one can see that the need for increased network security is vital and important in every organization. The security may include identification, authentication and authorization, and surveillance camera to protect integrity, availability, accountability, and authenticity of computer hardware or network equipment (Whitman & Mattord, 2012). There is no laid-down procedure for designing a secured network. Network security is sometimes more than what people always thought it to be, malware, virus, trojan, hackers, etc. Network security could be caused by unintentional human error and it could be compromised by human nature as well

(Whitman & Mattord, 2012). A common network security problem most organizations face sometimes has to do with the company's employees and the various errors they make.

Effect of Cyber Security on Network Operations

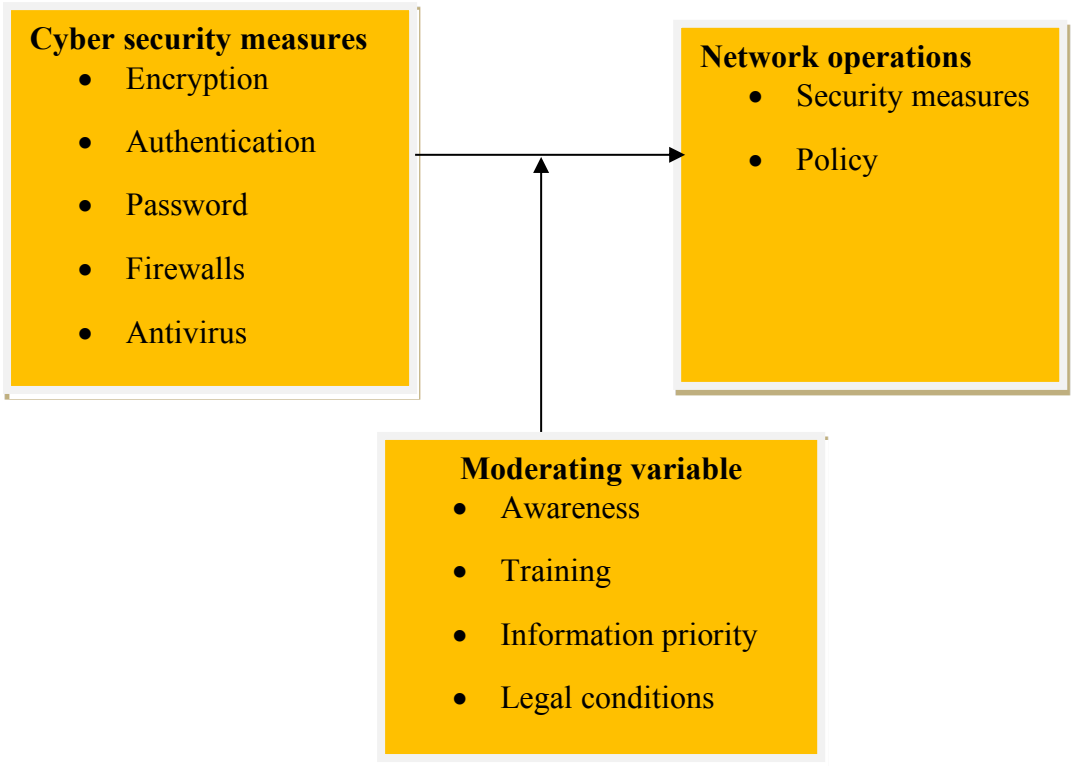

Figure 1: Cyber security measures and its moderating variables

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). Considering the complexity of securing data in a networked environment of Vodafone Ghana, the researchers proposed a newly designed data security-measure system, which was particularly designed to address the needs of Vodafone Ghana. By extracting the 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 (Figure 1). Normally, new threats to information systems occur from unexpected sources when organizations become more reliant on them (Nyanchama, 2005). Threat is an indication of impending danger or harm (Johnson, 2008). A security threat is a condition of vulnerability that may lead to an information security being compromised (Kumar, Park & Subramaniam, 2008).

Standard Services Offered to Combat the Attackers

Because of the onslaught of hacker attacks, companies offer ethical hacking services to combat the attackers. Coffin (2003), in his article 'IT takes a thief: Ethical hackers test your defenses', points out that what goes into ethical hacking depends on the range of services required, the size of the client and how much that client is willing to pay. Typical services offered to combat attackers include: External/Internal network Hacking, Application testing, Wireless Lan Assessment and War Dialing.

Attacks and Attacks Mitigation

Nowadays there are so many attacks which cause serious problems to an enterprise network. To protect the network from attacks, the network administrator must detect all the vulnerabilities present in the network and must know how to defend and mitigate all attacks. An attack occurs in several stages for successful execution against an enterprise network (Duane, 2006). Initially, an attacker may have limited information about the target network, so one of the primary objectives of an attacker is to gather intelligence or information about the target vulnerabilities. After gathering information about the target network, a range of attacks can be launched against the organization. For gathering information, attackers typically do not require in-depth knowledge about the target network. For example, they can just use WHOIS to find the domain name and IP address of the target network which is not a crime. This information can be used later to perform an attack. All the network attacks can be divided into 2 parts (Duane, 2006):

1. Attacks that require less intelligence about the target network, and
2. Attacks that require more intelligence about the target network.

According to Angela and Becky (2008), attacks that require less intelligence about the target network are divided into, example, Access, Denial of Service (DoS) and Distributed DoS attacks.

Attacks that require more intelligence about the target network are divided into:

1. Worms, Viruses and Trojan horses,
2. Application layer attacks, and
3. Threats to management protocols.

Access Attack

Access attack can be known as accessing network traffic in an illegal way. With the help of access attacks, intruders can retrieve data, gain access and can escalate their access privileges across the networks or systems. They are used to gain access to confidential databases, web accounts and other sensitive information. Access attack can occur in different ways (Cisco Systems, 2006; Richard, 2004). Access attack consist of, for example, password attack, trust exploitation and buffer overflow.

Password Attack

Passwords are used to authenticate users. Passwords are very sensitive data and are easily captured by hackers because they are human understandable. Password attacks are used to guess system passwords. It is done by a series of attempts to the system by an attacker. A dictionary attack is the common example for password attack. Dictionary attack will try all possible passwords until it finds the correct password. Password attack can be implemented by, brute-force attack, Trojan horse programs, IP spoofing and packet sniffers. Users must understand how important it is to secure their passwords (Cisco Systems, 2006; Richard, 2004). Some of the techniques for mitigating password attack are:

1. Do not share passwords with others,
2. Do not use same password on multiple systems; use different passwords for each system,
3. Change passwords every 6 to 12 months,
4. After a certain number of unsuccessful login attempts, disable the account,
5. Do not use plaintext passwords, and
6. Use strong passwords, using upper and lowercase letters, special characters, and numbers.

Trust Exploitation

Devices operating in a shared environment should trust the information coming from other devices. Hackers will try to exploit this trust by gaining access to one of the compromised device in the network. With trust exploitation, a hacker can listen or send or modify data as a trusted user. For example, if Demilitarized Zone (DMZ) host is compromised, then attacker can exploit the inside host connected to the inside firewall interface, because inside host trusts the DMZ host. Having tight constraints on trust levels within a network can mitigate trust exploitation. Systems inside the firewall should never completely trust systems on the outside firewall. Trust should be limited to specific protocols. In the above example, when the DMZ host is controlled by an attacker, his next goal is to compromise the inside systems connected to the trusted interface of the firewall. It can be done by finding the permitted protocols from the DMZ host to the inside interface and then searching the vulnerabilities on the inside host. This attack can be stopped if the firewall has minimum or no connectivity from the DMZ host to inside hosts (Cisco Systems, 2006).

Buffer overflow

Buffer overflow attack is the most common attack that can compromise the security of a computer system in a network environment. Buffer overflow is a process of overflowing or overloading the space in a buffer. This is done by writing a program which stores data beyond the allocated end of a buffer in memory. Buffer overflows usually occur as a consequence of a bug and the improper use of languages, such as C or C++, that are not memory-safe. Buffer overflow attack helps almost all existing malicious worms to propagate themselves from one machine to another machine. With buffer overflow attack, an attacker can insert his own code into a victim's machine so that he can control or compromise the services of the host (Cisco Systems, 2006). Having an up-to-date bug reports for the network and application server products will help to detect the buffer overflows and apply the latest patches to these products. The most common way to mitigate buffer overflow attacks is to check buffers at constant times (Fu-Hau Hsu, Fanglu & Tzi-Chiueh, 2008). If a buffer contains more data, it is clear that the buffer is overflowed and that buffer can be restricted.

Denial of Service (DoS) and Distributed DoS Attacks

A Denial of Service (DoS) attack damages or corrupts a computer system or denies all forms of access to the network, systems or services even within the hacker's community. DoS attack is regarded as less important and considered a bad form because it requires little effort to execute. Although DoS implementation is easy and can cause little potential significant damage, the attack deserves special attention from security administrators. DoS attack tries to prevent legitimate users from accessing the network by sending huge numbers of data packets to the network. Since the Internet has limited resources, it is hard to cope with heavy traffic, thereby, denying access to legitimate users (Stallings, 2003). Distributed Denial of Service (DDoS) attack refers to the next generation of DoS attacks on the Internet. Victims of DDoS attack experience packet flooding from various sources perhaps spoofed IP source addresses that bring their network connectivity to a grinding malfunction. In the past, an attempt to flood a target host with packets is the typical DoS attack. The hacker uses a terminal to scan for systems to hack. After handler systems are accessed, the hacker installs software on these systems. This software attempts to scan for, compromise, and infect agent systems. When the agent systems are accessed, the intruder then loads remote control attack software to accomplish the DDoS attack (Bidou, 2000).

Viruses, Worms and Trojan horse Attacks

Viruses, Worms and trojan are the programs which when injected, spread through emails and Internet packets and begin to replicate themselves and send copies to other nodes in the network (Stallings, 2003). Some threat is categorized according to minor or primary vulnerabilities for the end user, which could be handled by a layman by just explaining what s/he has to do. These attacks could be solved by the use of antivirus software or by restoring the affected machine to factory settings. For example, the SQL Slammer worm replicates once every eight seconds; within ten minutes, it had spread to almost all parts of the world. It creates chaos, hampered credit card transactions, interrupted airline reservations, and many other related activities of disruption (Stallings, 2003). An IDS detects intrusion and misuse by collecting and analyzing the information from different variety of network sources.

METHODOLOGY

The study employed a survey research design, and adopted the quantitative research approach, where the primary data was collected from the employees of Vodafone Ghana, Accra, Head Office branch. Interactions with the staff in the organization made it possible to understand the dynamic factors of the research by having a direct experience. The target population for the study was the staff of Vodafone Ghana, Head Office, Accra. The total number of staff at the organization is estimated to be two hundred and fifty-four (254), and the sample size of the study was fifty-five (55) respondents, using convenience and quota approach. The justification for this sample size was to ensure that there will be fair representation, and available employees were selected to participate in the research study under free will, without any form of compulsion. A questionnaire, one of the most widely used data collection methods, was used to carry out the study. This instrument helped in gathering the required information for the study. The questionnaire was developed, piloted and tested to verify that the questions are clear and not ambiguous, such that responses will also be consistent with the purpose of the study. Questions were reviewed during the pilot study, so as to improve the reliability and validity of the questionnaire. The researchers then administered questionnaire on one-on-one basis. With the aid of Microsoft Excel 2013, frequency distribution tables, pie charts and percentage tables were developed to critically analyze the data and evaluate the study. The primary data collected through questionnaires were labeled and coded for easy access and presentation. Participants were assured that their identity together with the name of the Department they work at, would remain confidential.

DISCUSSION OF RESULT

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), which amounts to a response rate of 91%. A response rate of 91% is considered 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% in this study.

For the age of the respondents, 24% of the respondents are over 40 years; 30% of the respondents are between 36-40 years, and 20% of the respondents are 31-35 years old. Again,

18% of respondents are between 26-30 years, with about 8% of the respondents below 26 years. It can 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.

The study sought to find out the highest level of education attained by the respondents. The analysis indicates that 14% of the respondents have professional education, 10% have certificate/diploma education, 16% are HND holders, 48% have first university degree and 12% are Master's degree holders. It was also seen that all the respondents are tertiary or professional qualification holders, making them matured enough to give well-informed, reliable and better responses to the questions within the Questionnaire.

The respondents were asked to indicate how long they have been working with the organization. Their responses showed that only 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.

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.

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. 26% 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 68% (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.

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, in Vodafone's conditions of employment contract, there are security roles and responsibilities aimed to protect sensitive data.

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.

In response to whether Vodafone, Ghana checks the operational status of the 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.

On the issue of whether the organization's cyber security risks 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.

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.

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 the most cyber security risks Vodafone Ghana faces has been DoS.

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.

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, 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.

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 include the following;

- **Insider threat:** A dissatisfied employee may provide a vector for insider security events, while the inadvertent injection of malware through removable media or web interconnections can make any employee the origination point for a network security violation;
- **Mobility:** Management and security of mobile networks, and smart mobile devices become even more challenging when employees want to use their own devices for business purposes. The bring-your-own-device trend exasperates this challenge, 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:** One of the greatest challenges to security professionals, was the perception that the internet is a secured critical infrastructure. The internet is an open connection of diverse networks. The challenge for Vodafone Ghana, was to start treating critical networks as if they are critical to their operations; and
- **Password Management:** It was revealed that 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.

RESULTS AND DISCUSSION

Vodafone Ghana's physical and logical network security and its firewall system to protect against undesired access to its servers, from outside the organization, was found to be not very secured. The research 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. The finding is consistent with other similar studies by Health Information Trust Alliance (2014), that organizations generally understand that, they should be measuring and monitoring their security controls through common channels. The channels include, among others, 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. The study deduced that upon termination of an employee's appointment, Vodafone made sure that there was retrieval process of sensitive information held by the employee in an appropriate manner. This is consistent with that of Public Safety Canada (2013), which demonstrated that cyber-attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information (Public Safety Canada, 2013).

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 anywhere in the world.

MITIGATING DENIAL-OF-SERVICE ATTACKS USING CAPTCHA

Typically, the Denial-of-service (DoS) attack is performed by automated software (also called bots). They send large number of fake requests to a network resource until it exceeds the server capacity (buffer overflow), consequently, resulting in the DoS attack. To prevent these attacks, researchers have proposed a client authentication mechanism known as CAPTCHA (which stands for **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.

In this project, a text-based CAPTCHA is used to authenticate users before allowing them access to the web services. A text-based CAPTCHA was adopted because it is mostly used, and in addition, cost less for enterprises. The aim is to distinguish between legitimate users and

bots, thereby adding an extra layer of security and also to ensure that the webpage is always accessible to legitimate users.

IMPLEMENTATION OF AN AUTHENTICATION MECHANISM (CAPTCHA)

To demonstrate the authentication mechanism using the CAPTCHA, a sample Vodafone webpage was developed, then the CAPTCHA was incorporated into the webpage in order 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:

1. On loading the webpage, (in this case a sample Vodafone website), 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.

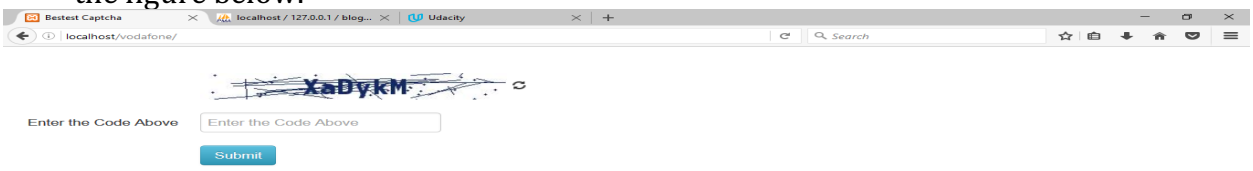

Figure 4.15: The CAPTCHA

2. 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 (that is protecting the target resources).
3. 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.

Figure 4.16: 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.

As a word of caution, Vodafone Ghana could expect to see a higher risk of business impacting threats, with the shift from computer-based attacks, generating large number of lower bandwidth events, to virtual server or cloud-based attacks, generating ultra-high bandwidth events. With these new vector attacks, it becomes even more beneficial to identify and mitigate large DDoS attacks while traffic is in the network cloud.

CONCLUSIONS

There is no doubt that given today's evolving threat of network landscape, it is understandable that organizations would like to take a proactive approach against threats, create an environment of continuous compliance, and have responsive IT operations and processes. Organizations want to reduce risk exposure and the attack surface, detect and respond to advanced threats, and drive down security operations costs.

In this study, DoS attack was identified as one of the major challenges faced by Vodafone Ghana. Consequently, CAPTCHA was developed and incorporated into the Vodafone website in order to mitigate the DoS attack. By using this approach, a layer of security authentication is added which subsequently allows humans to have access to important web pages thus, removing traffics from bots and mitigating DoS attacks.

RECOMMENDATIONS

Based on the findings of the study, the researchers put forward the following recommendations:

1. As people can themselves be an attack vector through social engineering, everyone within an organization ultimately shares responsibility in ensuring best-practice cyber security processes are carried out. This requires staff education with regular updates on new events, as new threats arise;
2. The management of organizations, including 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. Password policies should be implemented and enforced to ensure the selection of strong passwords; and
3. A text-based CAPTCHA could be used as a security measure to control intruders into network systems. However, the CAPTCHA should begin taking into account users with vision disability. Therefore, there is need to develop a more robust CAPTCHA mechanism that will take into account 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. CAPTCHAs could be made more interesting, for example, game based to reach these goals.

References

Angela, O., & Becky, P. (2008). Nmap in the enterprise: Your guide to network scanning. Burlington, MA: Syngress Publishing, Inc.

Bao, Z., & Xiang, K. (2006). Digitalization and global ethics. *Ethics and Information Technology*, *8,* 41-47.

Bidou, R. (2000). *Denial of service attacks.* Retrieved from: http://www.docstoc.com/docs/85149779/Denial-of-Service- Attacks [Accessed 25th May, 2018].

Bunge, M. (1977). *Towards a technoethics*, *Monist*, *60*(1), 96-107.

Cisco Systems (2006). Implementing Secure Converged Wide Area Networks (ISCW). Indianapolis: Cisco Press.

Coffin, B. (2003). *IT takes a thief: Ethical hackers test your defenses.* Retrieved from http://findarticles.com/p/articles/mi_qa5332/is_/ai_n29015644 [Accessed 25th May, 2018].

Dhillon, G. (2007). *Principles of information systems security: Text and cases*. New York: John Wiley & Sons.

Duane, De. C. (2006). Self-defending networks: The next generation of network security. New York: Cisco Systems, Inc.

Fu-Hau, H., Fanglu & Tzi-Chiueh (2008). Scalable Network-based Buffer Overflow Attack Detection. San Jose, CA: IEEE Xplore.

Galván, J. (2001). Technoethics: Acceptability and social integration of artificial creatures. Retrieved from http://www.eticaepolitica.net/tecnoetica/jmg_acceptability%5Bit%5D.htm [Accessed 25th May, 2018].

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

Graves, K. (2007). *CEH Official Certified Ethical Hacker Review Guide* (1st ed.). Indianapolis: Wiley Publishing, Inc.

Health Information Trust Alliance (2014). Management of Network Security Applications. In proceedings of the 21st NIS-NCSC National Information Systems Security Conference, Alington, Virginia.

Jonas, H. (1985). *On technology, medicine and ethics*. Chicago: Chicago University Press.

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

Luppicini, R. (2009). The emerging field of technoethics. In R. Luppicini & R. Adell (Eds.), Handbook of research on technoethics (pp. 1-19). Hershey, PA: Information Science Reference.

Mitnick, K., & Simon, W. (2002). The art of deception: Controlling the human element of security. New York: Wiley Publishing.

Moor, J. H. (2005). What is computer ethics? In T. W. Bynum (Ed.), *Computers and ethics*. Basil Blackwell, pp. 266-275.

Moradi, M. (2015). *CAPTCHA and its alternatives: Security and Common Networks/ Volume 8, Issue 12.* Retrieved from http://doi.org/10.1002/sec.1157 [Accessed 25th May, 2018].

Nyamchama, M. (2005). Enterprise Vulnerability management and its role in information security management. Journal of Management Information Systems, 13(2), 29-57.

Peltier, T. R. (2005). *Information Security Policies, Procedures, and Standards: Guidelines for effective information security management*. Boca Raton: Auerbach Publications.

Public Safety Canada. (2013a). *Canada's Cyber Security Strategy*. Retrieved from http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx [Accessed 25th November, 2018].

Public Safety Canada. (2013b). An open letter to Canadians on cyber security awareness. Retrieved from http://www.publicsafety.gc.ca/cnt/nws/nws-rlss/2013/20131003-eng.aspxx [Accessed 25th November, 2018].

Reed, D. (2003). *Network Model to Information Security.* Retrieved from http://www.sans.org/reading_room/whitepapers/protocols/applying-osilayer-network-model-information-security_1309 [Accessed 25th May, 2018].

Reynolds, G. W. (2012). *Ethics in information technology*. Boston, MA: Cengage Learning.

Richard, A. D. (2004). Cisco Router Firewall Security. New York: Cisco Press.

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

Sterling, B. (1993). *"Part 2(d)". The hacker crackdown*. McLean, Virginia: IndyPublish.com.

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. (2012). *Management of information security*, Course Technology, Boston.

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