ISSN No:-2456-2165

Level of Awareness of Cybersecurity for Business Protection in Nigeria

Nwokorie Euphemia Chioma
Department of Computer Science
School of Information and Communication Technology
Federal University of Technology
Owerri, Imo State-Nigeria

Njoku Donatus Onyedikachi
Department of Computer Science
School of Information and Communication Technology
Federal University of Technology
Owerri, Imo State-Nigeria

Okolie Stanley Adiele
Department of Computer Science
School of Information and Communication Technology
Federal University of Technology
Owerri, Imo State-Nigeria

Odii Juliet Nnenna
Department of Computer Science
School of Information and Communication Technology
Federal University of Technology
Owerri, Imo State-Nigeria

AMAEFULE Ikechukwu Augustine
Department of Computer Science, Faculty of Science
Imo State University, Owerri, Imo State-Nigeria

Agbakwuru Aphonsus Onyekachi
Department of Computer Science, Faculty of Science
Imo State University, Owerri, Imo State-Nigeria

Abstract:- Nigeria is among the countries with growing incidents of cybercrime activities. The Nation is also seen as a source of significant cyber threats targeting other nations of the world. This has made businesses in Nigeria to suffer reputational loss and the economy losing huge investment opportunities. However, certain measures have been put in place to address this ugly situation occasioned by cyber-threats, and the government has made effort to improve cybersecurity awareness in the country. Unfortunately, many organizations in Nigeria have not taken the issue of cybersecurity awareness properly, especially in the context of business environments and functions. This paper looks at the influence of the knowledge of cyber security, measures taken by various organisation, and approaches to keep businesses safe.

Keywords:- *Business, Cybercrime, Cybersecurity, Cyber-threat, Nigeria.*

I. INTRODUCTION

The presence of Information Technology (IT) in business is becoming increasingly more important as more business communities integrate their business processes with IT. Business can use IT system to help it in different aspects including a platform for businesses such as storing and retrieving information, work synchronization, forming business strategy and communication [13]. Cybersecurity is important for all businesses. This is mostly in form of data security. For instance, it is expected of an organization to ensure that information like those of customer and client, payment, personal file, bank account, details are properly secured. This is because it is often impossible to replace such information if lost. Also, having such information in the hands of criminals is dangerous. Similarly, data can be lost as a result of a flood or fire outbreak, this can be devastating but of less consequences than when data is lost to hackers or infected by malware. Managing and protecting organizational or personal data is primary and fundamental to the security of business and the privacy requirement of clients, workers and associates.

A business may have the following kinds of data that are of customer's interest and privacy: account and financial information, transaction accountability, contact and address information etc. Likewise a business data can be information of employee such as payroll bank account information, social security codes, home address and phone number, nature of work and personal email addresses. This data can as well include trademarked and sensitive business information for example, business accounts or financial records, advertising or marketing strategies, product designs and tax information.

There is need to protect and handle business data or generally business environment. Business data are most likely to be at risk when they are being moved that is transferred from one point to another. The state of data risk is however less when all business related data are stored on a single computer that is not connected to the internet. But most of the businesses today, require data to be transferred or moved and used throughout the organization or business environment. Significant data must be accessed and used by organizational workers and/or staff. These data are analyzed and studied for the purpose of marketing, for contacting customers and clients, and even shared with main partners. The movement of data exposes them to danger and at the same time devastates business growth.

Many businesses have been paralyzed by cyber threat or attack. It is possible to have a network of devices in a company to have been infected with malicious software such as a virus. Such network of devices (or computers) infected by virus is known as botnet. Cybercriminals or attackers can regulate a botnet as a group without the knowledge of the owner with the aim of increasing the magnitude of attack. Business owners or those wishing to

ISSN No:-2456-2165

start up new ones should have a forthright plan and policy which include a set of rules. These set of rules can state something's like the way each type of business data should be managed, validated and protected with respect to its destination.

In this paper, a conceptual review of cyber threats with approaches to a secured business environment in Nigeria. In order to do this, the paper has been divided into five sections namely: introduction, previous studies, measures to cybersecurity, and approaches to business data security and conclusion.

A. Previous Studies

The world has become an information-based society. This has impacted on both national and global aspects of economic and social development. Conversely, despite the promising features of the process of developing an information-based society and the perception that everyone is becoming dependent on various systems and thus exposed to the threats of cybercrimes which have the potential of causing injurious impact on private business and national economy.

Cyber-attack is observed as an electronic attack on systems of various companies or organizations, which particularly results in stealing their available assets stored in form of accessible digital information [1]. In Maintaining these attacks is simply "an attack on IT infrastructure targeted on inflicting damage and gaining sensitive and strategic data [2]. It is used in the context of politically or militarily motivated attacks." These days, the most common targets of cyber-attack are industries in such sectors likes energy, transportation, banking, infrastructure, financing, health service, sewage and drinking water supply systems or digital infrastructure (online-shops, clouds, etc). According to [3], it is expected that the development of cyber threats is going to progress incredibly fast. It is projected that the future cyber threats are going to be mainly targeted on back-up storage servers of large corporate companies possibly with the competition-driven purpose of frustrating their plans and causing damage. "Current threats include especially the fact that users tend to click on malicious links in their e-mail boxes." One such click can cause the passwords to be deciphered and expedite a system attack. Every single attack or threat emanates from some geographical area. Businesses are hit on daily basis by cyber-attacks. A former Cisco Chief Executive Officer (CEO), John Chambers, is reported to have said that there exist two types of companies: the ones that have been hacked and those are not yet aware that they have been hacked [4].

The report by [14] which is presented in [13] stated "The UK is under relentless cyber-attack and hacking is a rising risk to businesses. The number of security breaches large organizations are experiencing has rocketed and as a result, the cost to UK plc of security breaches is running into billions every year. Since most businesses now share data with their business partners across the supply chain, these numbers are startling and make uncomfortable reading for business leaders. Large organizations are more visible to attackers, which increases the likelihood of an attack on their IT systems. They also have more staff and more staff-related breaches which may explain why small businesses report fewer breaches than larger ones. However, it is also true that small businesses tend to have less mature controls, and so may not detect the more sophisticated attacks." African economies, specifically Nigerian businesses are becoming increasingly attacked by cyber criminals. [7] stated that a Mobile Malware Evolution 2018 report by Kaspersky Lab placed Nigeria among the top 10 nations worldwide that users of mobile devices are victimized by malware attack. The report from Kaspersky it was stated, maintained that Nigeria moved two places to become the third economy out of 10 attacked by mobile malware with record of 37.72% of the attacks. A Kenya-based IT and business advisory firm Serian reported that in 2017 the cost of cybercrimes in African economies was $3.5 billion. The annual losses to cybercrimes that year were estimated for Nigeria at $649 million [8]. Also, Cisco Cyber security Report Series, it is stated that "cybercrime has increased every year as people try to benefit from vulnerable business systems."

Cyber-threat has the capacity of rendering the business environment of a nation worthless. Over the years, the bad image of Nigeria occasioned by cybercrime activities has made other countries to brand the Nigerian business environment to be fraudulent. Similarly, [9] stated that "Long term commission of these crimes has left Nigerians and foreigners alike overly cautious to the extent where legitimate interactions of all forms originating in, or concerned with Nigeria and across cyberspace are now characterized with increasing disbelief." The impact of this on the businesses in Nigeria is loss of credibility among global businesses. The cybercrime notoriety associated with business environment in Nigeria makes foreign investors to be scared of investing their capital into Nigerian economy [5]. The 2017 report of the World Bank's Ease of Doing Business Ranking presented in Table 1 shows that Nigeria fared rather miserably [11]

Country	Ranking
Mauritius	25
Rwanda	41
Kenya	80
Botswana	81
South Africa	82
Nigeria*	145

Table 1:- Nigeria's* Ease of Doing Business Profile (2017) in Comparative Terms
*Source: World Bank, Ease of Doing Business, 2017

In an organization, every level must get educated and remain focused on the relationship between business and security. The fact that perfect security is not achieveable, there is no limit to the amount of money put into securing business environment. Luckily, with good risk management that focuses on smart security such that when properly implemented, is capable of driving business environment [6].

B. Common Types of Cyberthreats

➢ *Malware*

Malware refers to malicious software, which comprises spyware, ransomware, viruses, and worms. A network can be breached by malware through vulnerability. This usually occurs when a dangerous link or email attachment is clicked by a user and then leading to installing dangerous software. As soon as malware is inside a system, the following can occur:

- Access to vital components of a network is blocked – ransomware action.
- Installation of malicious software.
- Information can be secretly obtained from the hard drive (spyware).
- Certain components of the system can be disrupted and thereby making it inoperable or malfunction

➢ *Phishing*

The practice of phishing involves sending fraudulent messages that seem to come from a reliable source, usually through email. Phishing practice is aimed at stealing sensitive data such as credit card and login information of the victim. The practice can as well be to install malicious software on the computer or network of the victim. "Phishing is an increasingly common cyber-threat" (Cisco cyber security report series)

➢ *Man-in-the-Middle attack*

According Cisco cyber security report series, Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, take place when attackers insert themselves into a two-party transaction. Data can be filtered and stolen once attackers interrupt the traffic. Two common points of entry for MitM attacks:

- Attackers can insert themselves between a user and a public wireless network that is unsecured. Unconsciously, the user passes all information through the attacker.
- Once a computer system or network has been breached by a malicious software (or malware), the information of a legitimate user can be processed by an attacker by installing software.

➢ *Denial-of-Service Attack*

Denial-of-service attack is a cyber-threat in which systems, servers, or networks are flooded with traffic to deplete resources and bandwidth. The effect of this cyber-threat is that the system will not be able to accomplish request. Another way to implement this attack is by the means of distributed-denial-of-service (DDoS). DDoS is used to carry out denial-of-service attack by attackers using multiple compromised devices.

➢ *Structured Query Language Injection*

A Structured Query Language (SQL) injection is a type of cyber-threat which occurs when malicious code is inserted by attacker into a server that uses SQL and compels the server to make known its secret information. This can be carried by attacker by submitting malicious code into search box of a vulnerable website.

➢ *Zero-Day-Exploit*

According to Cisco cyber security report series, "A zero-day exploit hits after network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time. Zero day vulnerability requires constant awareness."

II. MEASURES OF CYBER SERCURITY

The cyber space presently is secured basically through private regulatory activity, defensive strategies and products, national laws and enforcement, and some limited forms of international cooperation and regulation [10].

A. Private Measures

This defines Non-governmental organizations render major roles in addressing the issues of cyber security. For instance, Internet Engineering Task Force (IETF) developed and privately controls the technical standards for the internet, including current and next-generation versions of the Internet Protocol ([10]. Similarly, technical standards for the Web is defined by the Web Consortium, housed at the Massachusetts Institute of Technology (MIT). Some other privately controlled institutions that provide substantial operational functions or roles on the area of cyber security are such major telecommunications carriers, Internet Service Providers (ISPs), and several other organizations, like [10]:

➢ "The Forum of Incident Response and Security Teams (FIRST), which attempts to coordinate the activities of both government and private Computer Emergency Response Teams (CERTs) and is also working on cyber security standards;
➢ The Institute of Electrical and Electronics Engineers (IEEE), which develops technical standards through its Standards Association and in conjunction with the U.S. National Institute of Standards and Technology (NIST);
➢ The Internet Corporation for Assigned Names and Numbers (ICANN‖), which operates pursuant to a contract with the U.S. Department of Commerce (September 2009) transferring to ICAAN the technical management of the Domain Name System" (Clarke and Knave).

B. Natinal Measures

Several initiatives have been put forward and carried out at various levels of national economies of the world to improve the cyber security arena. The U.S. for example, has implemented laws criminalizing various forms of conducts such as improper intrusion and deliberate damage of computer systems. These laws according to [10] have little or no power over persons, groups, or governments on whom the U.S. lack or cannot secure regulatory or criminal jurisdiction. The Bank of Ghana, in October 2018, issued a cyber-security directive for the nation's financial institutions, and directed that all banks are required to have a Cyber and Information Security Officer (CISO) that will

play an advisory role to senior management and the board on cyber security issues. The CISO are also to formulate adequate measures so as to be able to handle cyber and information security risks. In Nigeria, the Economic and Financial Crimes Commission (EFCC) declared in October 2009 that has shut down about 800 websites linked with cybercrimes and apprehended 18 cybercrime syndicates with the help of "smart technology" provided by Microsoft [8]. A report on the African Union Commission (AUC) and cyber security firm Symantec has it that 11 countries in Africa had explicit laws and provisions in place to solve the issue of cybercrime and electronic evidence: Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia [8]. In May 2015, the Cybercrimes ACT 2015, which is the first legislation in Nigeria that explicitly deals with cyber security, was passed [11].

C. International Measures

In improving and securing cyber space and reduce the risk of cyber threat, the National governments within continent and outside continent have collaborative in various ways to improve and secure cyber space and reduce the risk of cyber-threats by providing adequate cybersecurity and information measures. The most essential of these approaches is to provide better regulatory policy. The cooperation among national governments though usually informal, involves exchanging, information, investigating attacks or crimes, preventing or stopping malicious conduct, providing evidence, and perhaps arranging for individuals' rendition to a requesting nation [10]. Presently, only one cyber-related international treaty exists –the Budapest Convention on Cybercrime and NATO Cyber Defense Policy [12]. The first international treaty to address internet and computer crime is the Budapest Convention on Cybercrime. It is the only legal instrument designed to aid international cooperation against cybercrime. In September 2014, NATO allies endorsed an enhanced cyber defense policy and equivalent action plan [12]. The policy ratifies that international law applies in cyberspace, and identifies cyber defense as part of NATO's core task of collective defense. In Table 1: From the report by World Bank, Ease of Doing Business, 2017, the report can be represented in figure 1

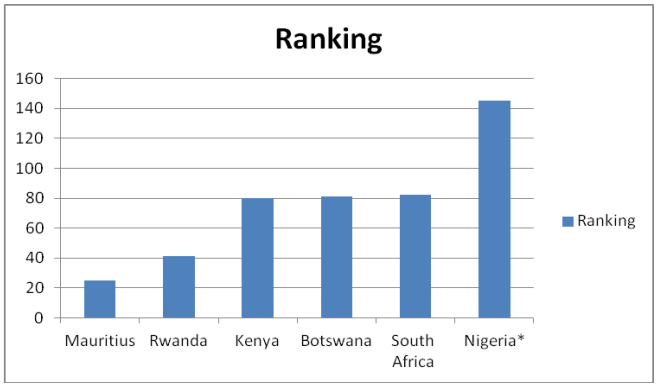

Fig 1:- Ranking of Countries with fear of Cybercrime in Africa
Source: World Bank, Ease of Doing Business, 2017

In fig.1 above, it was observed that Nigeria has the highest rank of fear in doing business with ease in the cyberspace with Mauritus has the least. In representing this report with aggregating percentage

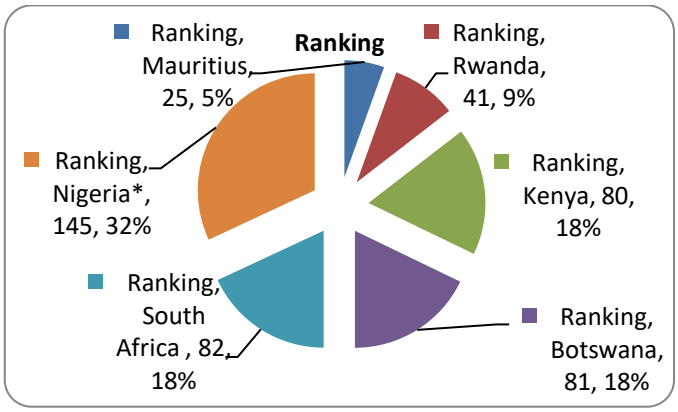

Fig 2:- Percentage Ranking of Cybercrime in Africa
Source: World Bank, Ease of Doing Business, 2017

It is showned that Ngeria has 32% of fears in doing business via cyberspace, with South Africa, Kenya and Botswana 18% respectively, Rwanda 9% and Maruirtus 5%.

III. APPROACHES TO BUSINESS SECURITY

These sections, certain steps that businesses can take to have their environment effectively protected and secured against cyber space malicious attack are outlined below.

A. Back up Data

Sustaining business integrity requires business data safety. When business' data are backed up, it helps organizations to recover whatever that might have been lost to cyberattacks. It is important that businesses regularly back up vital data and information pertaining to their financial records and business plans. Also important and crucial to business policy is the safety of customer records and personal information, and this should be backed up as well.

Using multiple means of keeping or storing business files is a good idea that can help guarantee data security. An effective multiple data storage (or back up) system typically involves incremental back-ups on daily basis to portable external device and/or cloud storage service, server back-ups on weekly basis, quarterly basis, or yearly basis.

B. Secure Business Devices

Another way to secure business environment is to be aware of malicious software known as malware or viruses that can destroy data and information contained in personal or organizational business file that is stored on computers, laptops and mobile devices. It is important that security software be installed on business computer and devices so as to prevent them from being infected. Such security software should include anti-virus, anti-spy ware and anti-spam filters, and ensure that it is automatically updated. The essence of automatic update is that vital security upgrades

based on current viruses and malicious threat may be contained in updates.

Also, in protecting internal networks, it is important to set up firewall security. Firewall installation on portable business devices, updating and patching them, will prevent malicious attack entering business network.

C. Monitor Computer Equipment and Software

The record of all computer equipment and software used by businesses should be maintained. Business items and equipment should be monitored to prevent illegal access. Employees or workers should be aware of where and how they use their devices. An unknown malicious threat can inadvertently transfer from portable computer equipment into business system. Also, always get rid of any software or equipment that are no longer needed in business and make sure that no sensitive data or information is on them when discarding.

D. Protect Important Information

It is important to protect important information. Organizations should ensure that business data are encrypted when stored or being sent electronically (online) so that it can be accessed only by legitimate users. With business data encrypted, they are converted into a secret code before sending over the internet. The risk of data theft, destruction or damaging is reduced by this practice. Always ensure that network encryption is turned on.

E. Password/PIN Management

Creating strong password is important in protecting business information and brings about improved data security. It is essential to use passwords or personal identification number (PIN) on all computers and devices that store or hold business information. The use of simple password or PIN will leave a business vulnerable to potential attack or hack.

One way of managing business data and/or information is by changing passwords every frequently. Using the same password for everything makes business vulnerable. It is worthwhile using password manager that creates and stores passwords in a well secured manner.

In the administrative management passwords, it is necessary to change default passwords and endeavour to entirely disable administrative access so as to prevent cybercriminals from gaining access into a business or organization computer or network. Management of administrative passwords is very important and plays pivotal role in the continuous existence and success of a business. Each password should be changed at any time to something new to avoid easy manipulation or guess by intruders. This is because cybercriminals have the ability to gain full access to the entire system of a business from an administrator level account.

F. Use Spam Filters

Spam messages are usually sent from a person or an organization that is unknown to the receiver. They often contain enticing contents. It is important to know that such messages do not have to be replied, unsubscribed, or call the number in the message. The best option is to delete them.

However, to reduce the amount of spam and phishing emails that are received by a business, spam filters can be used. The use of spam filter will reduce the possibility of employer or workers opening a fraudulent email accidentally.

G. Educate Staff about Onlin Safety

The need to be security conscious on cyber space is essential in business environments. It is important for a company to train it's staff on cyber threats they can encounter online and why they should adhere to the instructions so as to keep the business safe. The training should let them know their computer rights and responsibilities. The staff are also to know their network access usage, and specific types of online activities that are acceptable when using business computers, devices and emails.

In order to ensure good cyber security practices for business safety and success, employees should be trained on good passwords maintenance, fraudulent email awareness, local and international cyber security law awareness and reporting suspicious online practices will be worthwhile.

H. Put Business Security Measures in Place

Every organization should put in place policies and process for staff that defines the frameworks of acceptable standard when accessing: data, emails and the internet. These policies should be reviewed regularly by employees to keep them aware.

The type of business information staff can share online and where should be set by strong social media policy. This policy is necessary because a convincing scam can be developed by cybercriminals which is tailored to employee by exploiting the personal information they post online to build a profile.

I. Protect Customers and Clients

The level of trust the customers and clients have on a business determines the length they are willing to go with the business. It is important to keep safe the customer information database regardless of the size. The reputation of a business can be dealt a heavy blow when customers' personal information is lost. There may also be legal actions from customers and clients.

It is essential to make customers know that information about them are not shared or revealed without their consent. Organizations should provide a secure online business platform for transactions and make sure that any personal information that may be stored is secure. Also, adherence to privacy laws that determine what business can be done with

the customers' personal information is important. An up to date awareness of privacy policy is important too.

J. Insure Business Environment

It is important to protect businesses against impacts as a result of a cyber-attack by way of cyber insurance. Dealing with a cyber-attack can cost more than repairing of databases, strengthening of security measures or replacing of stolen or lost computers. Though cyber insurance cannot protect a business from cybercrime, it can protect the business against the costs arising from the attack.

K. Keep Update on Latest Cyber Security Risk

Businesses trading online should concern themselves with online transaction issues and payment fraud. Business owners should keep themselves updated and stay informed with latest cyber threats –scams and security risks. It is wise to subscribe to services that provide online alert service on up to date information on cyber security issues and solution.

IV. CONCLUSION

In this paper, cyber security knowledge to help business Nigeria has been presented. With the growing use of computer equipment and other IT devices in doing business, many cyber space criminals has also entered arena to exploit and make merchant of genuine businesses. The advancement and changes of online business techniques have had positive and negative impacts. Looking at the global market today, it can be seen that businesses in developing countries like Nigeria are easy target of cybercriminals. Now, with most businesses becoming increasingly dependent on computer equipment, the risk of cyber-attack cannot be avoided. It is therefore important to reduce the exposures to cyber-attack by developing data and information security strategy. Knowing that cyber threat risk can come from employees and customers, businesses should therefore develop security frameworks or approaches that consider people, policy and the technology so as to achieve their objectives. .

ACKNOWLEDGMENT

We sincerely appreciate everyone who contributed to the development of this paper, most especially the Vice Chancellor of Federal University of Technology Owerri for encouraging further research through the establishment of Cybersecurity department and the School of Information and Communication Technology (SICT)

REFERENCES

[1]. Susanto H., and Almunawar N. M. (2012). Information Security Awareness Within Business Environment: An IT review. PhD Colloquium, June 2012, 1-18.
[2]. J. A. Green (2015). Cyber Warfare a Multidisciplinary Analysis. Rontledge Studies in Conflict, Technology and Security, 182. iSBN 978-1-138-79307-1.
[3]. Mura, L., Buleca, J., Hadduová, Z., Adrejkovič, M. (2015). Quantitative Financial Analysis of Small and Medium Food Enterprises in a Developing Country, In: Transformation in Business and Economics, Vol. 14, No. 1(34), pp. 212-224.
[4]. K orauš, A., Veselovká, S., and Kelemen, P. (2018). Cyber Security as Part of the Business Environment. International Relations, 2017: Current Issues of World Economy and Political Conference Proceedings 18th International Scientific Conference Smolenice Castle , 30th Nov.-1st Dec., at Smolenice Castle, Slovakia.
[5]. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html
[6]. Okoli A. l. C., and Idom A. M. (2018). The Internet and National Security in Nigeria: A Threat-Import Discourse. Covenant University Journal of Politics & Internationall Affairs. 6(1), 20-29.
[7]. Chabinsky S. (2015). Why Your Business Environment Should Drive Cybersecurity. Cyber Security NewsCyber Tactics
[8]. Ogunfuwa, I. (2019). Nigerian businesses at risk as cyberattacks rise. Punch news, Source on 11/oct/2019, time: 11:03am.
[9]. Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, 22(2), 77-81.
[10]. Osho, O. & Onoja, A.D. (2015). National Cyber Security Policy and Strategy of Nigeria: A qualitative analysis. International Journal of Cyber Criminology (IJCC), 9 (1), 120 143.001:10.5281/ZENODO.223 90.
[11]. Tonge, M. A., Kasture, S. S., and Chaudhari, R. S. (2013). Cyber security: challenges for society-literature review. IOSR Journal of Computer Engineering, 12(2). 67-75.
[12]. Okoh, J. and Chukwueke D. E. (2016). The Nigerian Cybercrime Act 2015 and its implications for financial institutions and service providers. financierworldwide.com
[13]. Holdorf, M. P. (2015). Prospects for an International Cybersecurity Regime. INSS Strategic Paper, 1-12.
[14]. Sofaer,D. A., Clark, D., and Diffie, W. (2018) Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy http://www.nap.edu/catalog/12997.htmlCyber Security and International Agreements, Internet Corporation for Assigned Names, 185-205.
[15]. Potter, C., and Waterfall, G. (2012). Information Security Breaches Survey 2010. Price Water House Coopers. Earl's Court, London.