International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 08 | Aug 2018 www.irjet.net p-ISSN: 2395-0072

ECONOMIC IMPORTANCE OF INTERNET SECURITY IN SOUTH WEST, NIGERIA

OGUNLOLA O. Okunola[1], ABIODUN Opeyemi Anuoluwa[2]

Computer Science Department, The Federal Polytechnic, Ado Ekiti,Ekiti State, Nigeria

---

ABSTRACT: This work studied the economic importance of internet security. The use of internet for business and its corresponding security issues were reviewed; data on Internet security investment and cost of internet security breaches were collected on some small scale businesses using well-structured questionnaires and analyzed to find out if cyber security investment outweighs its benefits. The results of the analysis have shown that 78% of respondents were involved in online business, while 63% of them suffer regular attacks on their businesses. Dues to these attacks, losses were recorded. While 74% acknowledged loss of data and information on their businesses, 57 % showed that they lost customers in the process of such attacks. Hence, it is a good thing to prevent these attacks by budgeting significantly on investment on cyber security. For any business to succeed online such must invest on cyber security otherwise the business may not continue due to attacks.

Keywords: Cyber Security, Investment, Attacks, Internet, Economic.

1.1 INTRODUCTION

The Internet has undergone astounding growth, by nearly any measure, in recent years. The number of Internet users increased from roughly 360 million in 2000 to nearly two billion at the end of 2010. The number of hosts connected to the Internet increased from fewer than 30 million at the beginning of 1998 to nearly 770 million in mid-2010. According to industry estimates, this global network helps facilitate $10 trillion in online transactions every single year (DoCIPTF, 2011).

Today, the Internet is again at a crossroads. Protecting security of consumers, businesses and the Internet infrastructure has never been more difficult. Cyber-attacks on Internet commerce, vital business sectors and government agencies have grown exponentially. Some estimates suggest that, in the first quarter of this year, security experts were seeing almost 67,000 new malware threats on the Internet every day. This means more than 45 new viruses, worms, spyware and other threats were being created every minute (Daya, 2013). As these threats grow, security policy, technology and procedures need to evolve even faster to stay ahead of the threats (Alese, 2004).

When internet is accessed, computer sends a message over the Web that uniquely identifies computer and where it is located. This allows the information one has requested to be returned. Often, this requested information carries with it unwanted hidden software created by hackers and online criminals. This software installs itself on computer and can either be just a nuisance or pose a more serious threat, identity and sensitive financial information. Usually the nuisances are visible and easy to identify, while the more dangerous threats are typically invisible, silent, and difficult to detect until it's too late. The key to a safe, enjoyable Internet experience is to understand the difference between what a threat is and what is not.

Cookies, pop-ups, and adware are tools that track someone's online behavior, and are used to promote various products. Many cookies are harmless online information gathering and tracking tools. The majority of adware consists of pop-up ads that are merely unsolicited nuisances. The problem is that hackers and online criminals are increasingly using cookies and adware to quietly sneak onto someone's computer and to access someone's personal information without someone's knowledge. This "spyware" watches and records everything someone does online, leaving someone's passwords, private account information, and other personal and sensitive information vulnerable (Alese, 2004; Daya, 2013).

Once captured, this information can be sent back to online criminals for use in accessing someone's private information, stealing someone's identity, and money. It can also be used to highjack someone's computer for illegal purposes. Spyware finds its way to someone's computer through:

i. Web sites browse on the Internet.
ii. Adware and pop-ups that load onto someone's computer.
iii. Results of Internet searches.
iv. Unusual E-Commerce sites visit.
v. Software someone download onto computer from the Internet.
vi. Weaknesses in the operating system.

Over the past two decades, the Internet has become increasingly important to the nation's economic competitiveness, to promoting innovation, and to our collective well-being. As the Internet continues to grow in all aspects of our lives, there is emerging a parallel, ongoing increase and evolution in, and emergence of, cyber-security risks (Daya, 2013).

Today's cybersecurity threats include indiscriminate and broad-based attacks designed to exploit the interconnectedness of the Internet. Increasingly, they also involve targeted attacks, the purpose of which is to steal, manipulate, destroy or deny access to sensitive data, or to disrupt computing systems. These threats are exacerbated by the interconnected and interdependent architecture of today's computing environment. Theoretically, security deficiencies in one area may provide opportunities for exploitations elsewhere.

A typical business will have all kinds of data, some of it more valuable and sensitive than others, but all data has value to someone. Business data may include customer data such as account records, transaction accountability and financial information, contact and address information, purchasing history, buying habits and preferences, as well as employee information such as payroll files, direct payroll account bank information, Social Security numbers, home addresses and phone numbers, work and personal email addresses. It can also include proprietary and sensitive business information such as financial records, marketing plans, product designs, and state, local and federal tax information (Bagchi, & Udo, 2003).

Security experts are fond of saying that data is most at risk when it's on the move. If all business-related data resided on a single computer or server that is not connected to the Internet, and never left that computer, it would probably be very easy to protect. However, most businesses need data to be moved and used throughout the company. To be meaningful, data must be accessed and used by employees, analyzed and researched for marketing purposes, used to contact customers, and even shared with key partners. Every time data moves, it can be exposed to different dangers.

It is of utmost importance that business owners, have a straightforward plan and policy (a set of guidelines), about how each type of data should be handled, validated and protected based on where it is traveling and who will be using it.

1.1.1 Access Control

Not every employee needs access to all of information. Marketing staff shouldn't need or be allowed to view employee payroll data and administrative staff may not need access to all customer information.

When an inventory of data is made and one knows exactly what data one have and where it's kept, it is important to then assign access rights to that data. Doing so simply means creating a list of the specific employees, partners or contractors who have access to specific data, under what circumstances, and how those access privileges will be managed and tracked.

Business could have a variety of data, of varying value, including:

i. Customer sales records
ii. Customer credit card transactions
iii. Customer mailing and email lists
iv. Customer support information
v. Customer warranty information
vi. Patient health or medical records
vii. Employee payroll records
viii. Employee email lists
ix. Employee health and medical records
x. Business and personal financial records

xi. Marketing plans
xii. Business leads and enquiries
xiii. Product design and development plans
xiv. Legal, tax and financial correspondence

Privacy is important for business and customers. Continued trust in business practices, products and secure handling of clients' unique information impacts profitability. privacy Policy is a pledge to customers that one will use and protect their information in ways that they expect and that adhere to legal obligations. Policy starts with a simple and clear statement describing the information one collects about customers (physical addresses, email addresses, browsing history, etc), and what one does with it. Customers, employees and even the business owners increasingly expect to make their privacy a priority. There are also a growing number of regulations protecting customer and employee privacy and often costly penalties for privacy breaches. One will be held accountable for what he/she claim and offer in policy.

1.2 Aim and Objectives

The aim of this study is to analyze the economic importance of internet security. While specific objectives include assessing the use of internet for business and its corresponding security issues within the area covered by this work, collect data on Internet security investment and cost of internet security breaches with some small enterprises and analyze the data collected.

1.3 Motivation

As many businesses adopt internet for their operations, there is also increase in crimes on the cyberspace. For these businesses to strive and continue to stay on in the business, there must be investment on Internet security. This investment will surely increase the cost of running such businesses. One of the targets of any business is to reduce cost of running business while they increase their throughput. There is need to justify or otherwise additional investment on Internet security by these organizations.

This work therefore is specifically aimed at carrying out an analysis of the economic importance of internet security. More directly, this work intends to find out if cyber security investment outweighs its benefits

1.4 Overview of Methodology

In order to achieve the specific objectives of this work, literatures were reviewed to assess the use of internet for business and its corresponding security issues. Well-structured questionnaires were developed and administered to carefully selected respondents in order to collect relevant data. Percentage analysis, bar chart and chi-square were the statistical analysis methods used.

PRESENTATION AND DATA ANALYSIS

The data analyzed was obtained through a structured questionnaire distributed to small scale businesses in Akure and Ado Ekiti.

4.2 ANALYSIS OF RESPONDENTS

4.2.1 Usage of Internet Service for Business

Among the 100 respondents, 22 % indicated that they were not using Internet for their businesses and service delivery while 78% were using Internet for their businesses (Table 4.1 and Figure 4.1). This shows a good number of small scale business owners are now using Internet to drive their business.

Table 4.1: Percentage of Usage Of Internet Service for Business

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	22	22.0	22.0	22.0
	1	78	78.0	78.0	100.0
	Total	100	100.0	100.0	

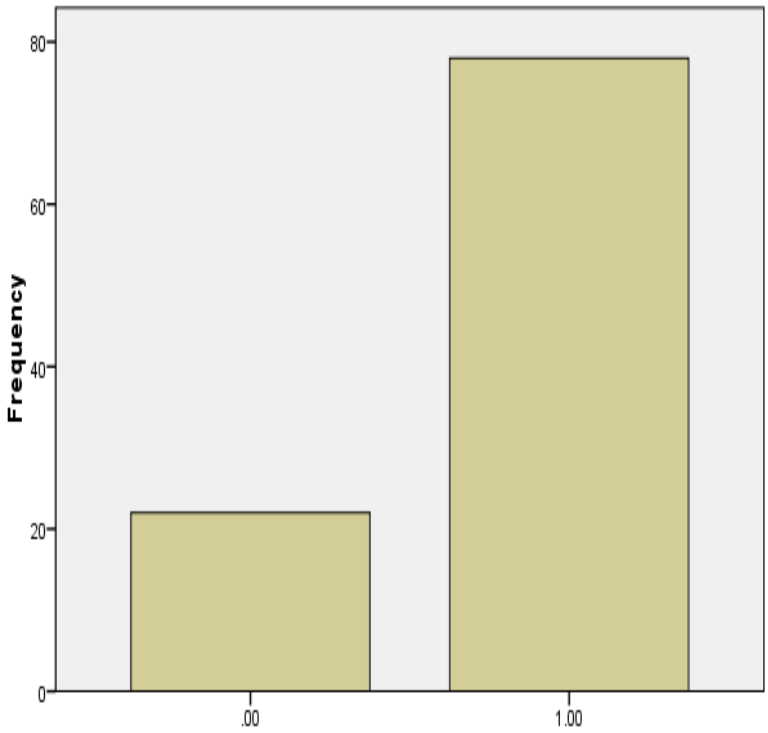

Figure 4.1: Percentage Analysis of Respondents that do businesses online

4.2.2 Experience of Online Attack on SME

Online attacks have been a major concern for business owners and other Internet users. Online attacks often lead to downtimes which invariably affect the business as well. Table 4.2 and Figure 4.2 show 63% of respondents acknowledging previous attacks on Internet while 37% of respondents denied such on their online business. This indicates that greater percentage of online businesses suffers attacks. Effort must be put in place to prevent these attacks less it leads to business disruptions through incessant downtime.

Table 4.2: Percentage Table of Attacks on Online Businesses

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	37	37.0	37.0	37.0
	1	63	63.0	63.0	100.0
	Total	100	100.0	100.0	

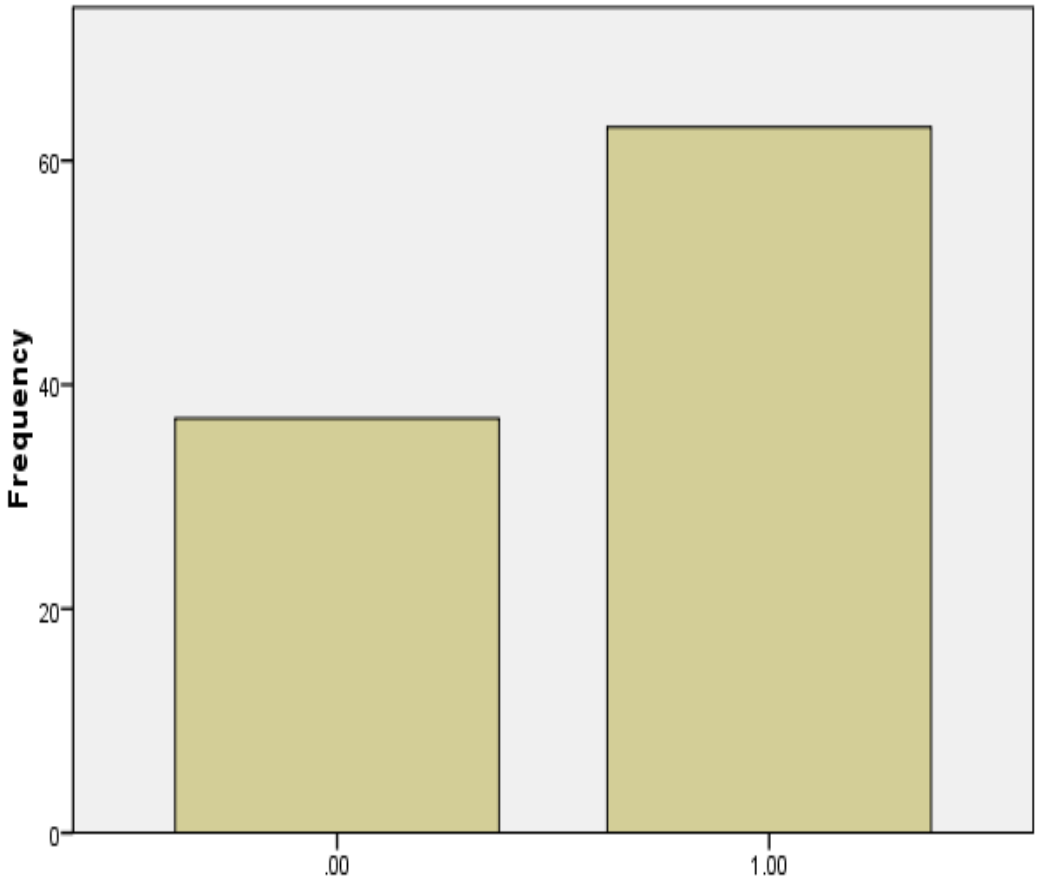

Figure 4.2: Percentage Analysis of the Respondents that Suffers Internet Attacks

4.2.3 Loss of Customer Due to Online Attacks on Online SME

As expected, attacks are aimed at disrupting online businesses which may lead to losses. Table 4.3 and Figure 4.3 clearly indicated that 57% loss customers due to online attacks which is not too good for businesses to succeed.

Table 4.3: Loss of Customers Due to Online Attacks

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	47	47.0	47.0	47.0
	1	53	53.0	53.0	100.0
	Total	100	100.0	100.0	

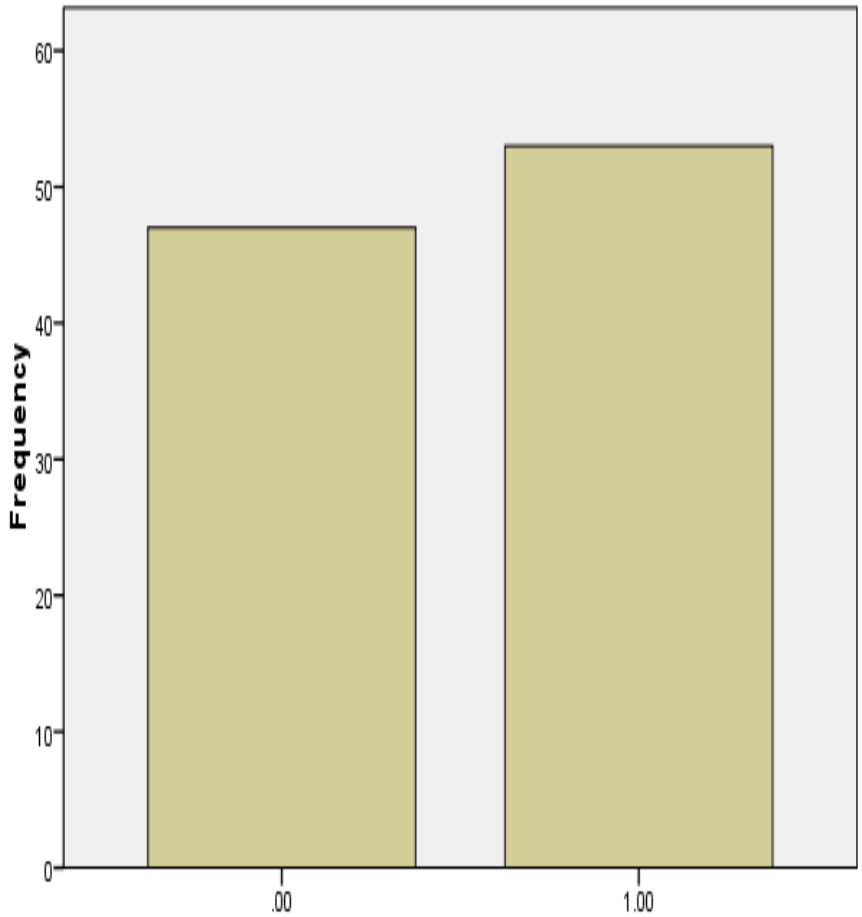

Figure 4.3: Percentage Analysis of the Respondents that Loss Customer Due To Attack

4.2.4 Loss of Data and Information

It is obvious that for any business to survive data are very important. Loss of data during attacks is very high as shown in Table 4.4 and Figure 4.4 (74% of the respondents). This is not too good to continue; hence investment on its prevention is not out of place.

Table 4.4: Loss of Data/Information

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	42	42.0	42.0	42.0
	1	58	58.0	58.0	100.0
	Total	100	100.0	100.0	

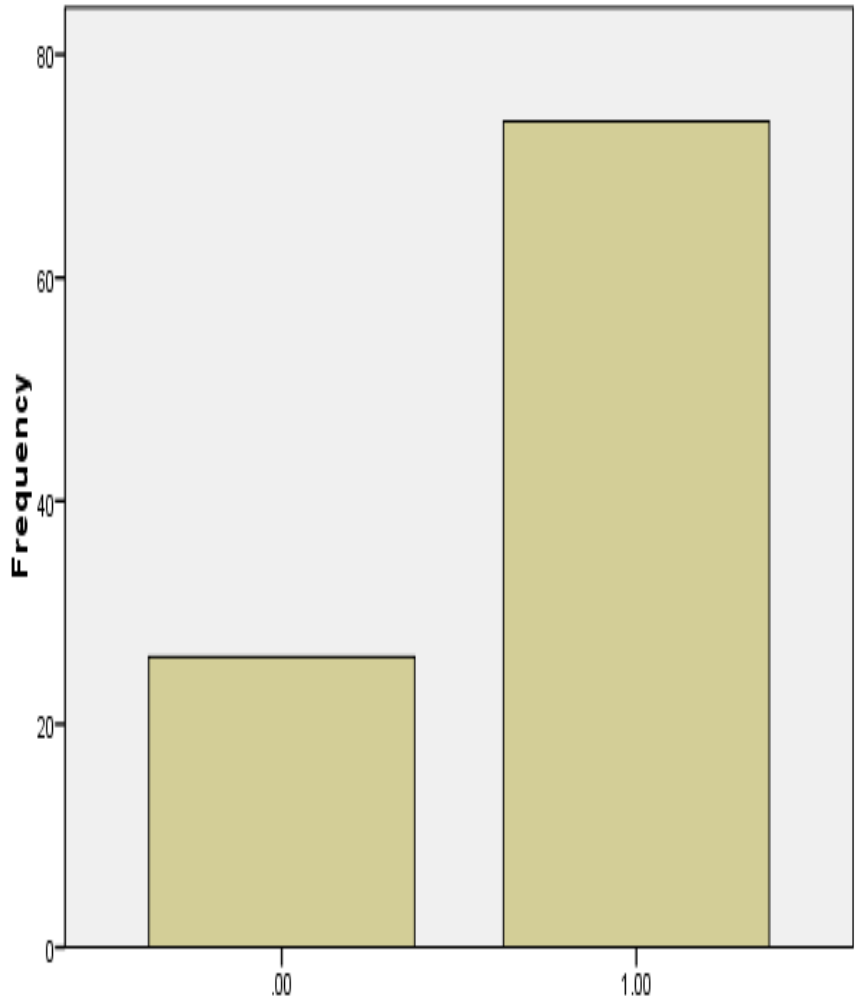

Figure 4.4: Percentage Analysis of the Respondents that Loss Data/Information Due To Attacks

4.2.5 Cost of Investment on Cyber Security Vs. Cost of Loss/Restoration of Data and Information

As shown in Figure 5, the cost due to data loss and retrieval after attack is extremely high compared to cost of securing of cyber security. Hence, the benefit of cyber security outweighs its cost. Every business owners must strive to invest on security online to ensure their continuous profitability.

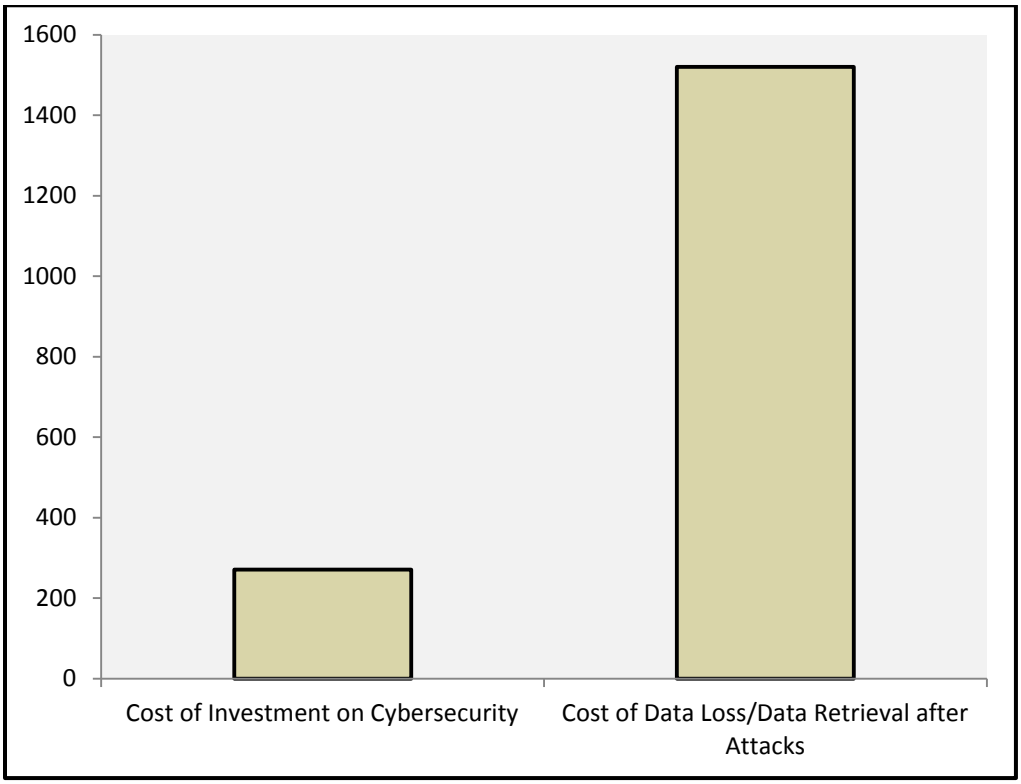

Figure 4.5: Percentage Analysis of the Respondents on Cost of Investment on Cyber security vs. Cost of Loss and Restoration of Data/Information

5.1 CONCLUSION

In conclusion, the results of the analysis have shown that 78% of respondents were involved in online business, while 63% of them suffer regular attacks on their businesses. Dues to these attacks, losses were recorded. While 74% acknowledged loss of data and information on their businesses, 57 % showed that they lost customers in the process of such attacks. Hence, it is a good thing to prevent these attacks by budgeting significantly on investment on cyber security.

5.2 RECOMMENDATION

For any SME to continue business online such must invest significantly on cyber security otherwise the business may not continue due to attacks.

For further study research work can consider large scale industries.

REFERENCES

1. Alese, B.K. (2004); "Elliptic Cryptographic System" (A P. hd Thesis at the Department of Computer Sc. Federal University of Technology, Akure.) Bagchi, K., & Udo, G. (2003). An analysis of the growth of computer and Internet security breaches. Communications of the Association for Information Systems, 12(1), 46.

2. Coffman, K. G., & Odlyzko, A. M. (2002). Growth of the Internet. Optical Fiber Telecommunications IV B: Systems and Impairments, IP Kaminow and T. Li, eds, 17-56.

3. Cotton, M., & Vegoda, L. (2010). Special Use IPv4 Addresses (No. RFC 5735).

4. Daya, B. (2013). Network security: History, importance, and future.University of Florida Department of Electrical and Computer Engineering. Daniel G. James (2000). Statistical Analysis of Internet Security Threats
5. Gabriel, J.A. (2015). "A Multivariate Polynomial Based Post-quantum Cryptographic System for Securing of Information over Enterprise Network". a Ph.D. Thesis at the Department of Computer Sc. Federal University of Technology, Akure.
6. Gallaugher, P. A. J. M. (1997). Factors affecting the adoption of an Internet-based sales presence for small businesses. The Information Society, 13(1), 55-74.
7. Householder, A., Houle, K., & Dougherty, C. (2002). Computer attack trends challenge Internet security. Computer, 35(4), 5-7.
8. Howard, J. D. (1997). An analysis of security incidents on the Internet 1989-1995. Carnegie-Mellon Univ Pittsburgh PA.
9. Hunt, R. (1998). Internet/Intranet firewall security—policy, architecture and transaction services. Computer Communications, 21(13), 1107-1123.
10. Kim, W., Jeong, O. R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. Information systems, 36(3), 675-705
11. Kende, M. (2012). How the Internet continues to sustain growth and innovation. Retrieved from: http://www.internetsociety.org/sites/default/files/How, 20. Accessed on 12/4/2016
12. Department of Commerce Internet Policy Task force (2011). CyberScurity, Innovation and the Internet Economy (DOCIPTF)
13. McDaniel, P., & Rubin, A. (2008). 2008 IEEE Symposium on Security and Privacy (Conference Closing). Sonicwall, Inc. (2001): Internet Security Issues and Solutions for Small and Medium Business Szor, P. (2005). The art of computer virus research and defense. Pearson Education.
14. Wymer, S. A., & Regan, E. A. (2005). Factors influencing e-commerce adoption and use by small and medium businesses. Electronic Markets,15(4), 438-453.