Identification of Threats to Communication Security, Effects On Victims and Ways of Mitigating the Threats

Authors:
B. E. Okon., R. A. Umunnah.

ABSTRACT: Routine acquisition and aggregation of network data offer an opportunity to understand some of the forces that drive the internet. It also offers opportunity to detect and understand a variety of phenomena that are related to overtly questionable or malicious activities on the part of the user's and abusers.

In this research a revision of large threats to communication security, effects on victims and ways of mitigating such threats have been carried out. It is found that information in large corporate environment have made tremendous technical strides over the past years but as information becomes more available through the possession of computers and other computer related gadgets, attackers have discovered newer ways of breaking into our computer/network with the aim of gaining access to sensitive information, spreading viruses, worms, Trojan and inflicting distress through playful pranks. Organizations have learned the need for defensive measures against compromise of sensitive data and resources, such as virus defense, firewall, data encryption, logging, auditing, authorization, authentication and user education, to name a few. Technical risk management, vulnerability analysis and new threat research have all combined into a science.

Keywords: Network Data, Malicious Activities, Communication Security, Computer Related Gadgets.

University of Calabar
Calabar – Nigeria

1. INTRODUCTION

Computer users are facing all sort of security threats these days such as computer viruses, worms, Trojans, hacking, phishing, spyware etc. Almost every computer is challenged by more than one type of malicious attacks each day resulting in significant losses. Losses can stem, for example, from actions of supposedly trusted employees defrauding a system, from outside hackers, or careless data entry clerks. Precision in estimating computer security-related losses is not possible because many losses are never discovered, and others are "swept under the carpet".

Computer security breaches can be grouped into physical and logical breaches.

A physical breach of security involves actual damage to or loss of the computer hardware or media on which data are stored. A logical breach affects the data and software without physically affecting the hardware. Literature review reveals a stream of research on the cost of information systems security incidents [Cohen 1991, Orlandi 1991, Dobson 1994, Tarr 1995, Anderson 2001, Butler 2002,]. One of the problems with any logical breach of security is that the damage is invisible and its extent is unknown.

Although attacks originating from outside threat agents, such as hacking attempts or viruses, have gained a lot of publicity, the more risky attacks come from inside (Schultz, 2002).

Despite the likelihood of insider attacks and the potential magnitude of their impact, companies are still not doing enough to protect themselves against this kind of threat (Melara et al., 2003). Organizations can suffer from direct effects of this threat, resulting in financial losses (Furnell

and Phyo, 2003). Insiders are trusted and, therefore, have the necessary access to be able to exploit vulnerabilities more easily. To be sure, this has always been true – thieving or otherwise corrupt workers have undoubtedly existed since commerce itself – but the power of computers (and the inability to secure them in the best of circumstances) makes the problem far worse today (Bellovin, 2008). Surveys confirm this and reveal that current or former employees are the second greatest cyber-security threat, exceeded only by hackers (Greitzer et al., 2008). In addition, surveys reveal that the impact of security incidents is far greater than those caused by outsiders (Baker et al., 2008; Vadera et al., 2008). This are undoubtedly results obtained from compromised records (Baker et al., 2008), but also from indirect effects. These indirect effects include, for example: risks to reputation that could dramatically impact stock prices, or losing competitive advantage, due to loss of intellectual property (Sinclair and Smith, 2008).

The few models of and studies about insider attacks and related issues that are

available in scientific literature are a good start, but they are of little value in producing meaningful results that can help organizations reduce the frequency of and damage from insider attacks (Baker et al., 2008). There is a lack of appropriate definitions and contextual information, data for analysis, experimentation and, ultimately, validation of proposed solutions. This lack of data is driven by a variety of factors, the most prominent of which appears to be the sensitivity of the topic: organizations that have been the victims of insider

attacks tend to handle such (known) incidents as quietly as possible (Keromytis, 2008). Hence, this investigation is therefore conducted to identify persistent threats to communication security, effects on victims and ways of mitigating the threats.

2. EXPERIMENTATION

2.1 Materials

The following materials were used for the research.

2.1.1 Personal Computer (PC)

The personal computer (PC) is a device that performs computations and makes logical decisions at speeds millions (even billions) of times faster than human beings can. It has a storage capacity of 350Gigabyte, 3Gigabyte of installed memory (RAM), and 2 Gigahertz of processor speed.

2.1.2 Microsoft Security Essential Antivirus

Microsoft Security Essentials Anti-Virus Software is antivirus software that is very important to keep the personal computer safe and functioning efficiently. A virus, spyware or other malicious software tends to slow down the processing capability of our computer or even eat up some of its available memory. Not to mention the worst case scenario which is causing our personal computer to break down and crash.

This antivirus software was used to scan the personal computer for viruses, worms, trojans, botnet, adware, rootkits, spyware and other malicious codes.

2.1.3 Questionnaires

Questionnaires were drafted to seek people's response as regards the security concerns emanating from the Ministries, Departments and Agencies (MDAs) of the Cross River State Government, identifying potential threats, its effect on victims and counter measures. The questionnaire is divided into three sections A, B and C with a total of 30 items.

Section A seeks to know the name of the establishment, the establishment location and the type of job carried out by the establishment. Section B is the demographic information, which contains information on Sex, Age, Qualification and Occupation of the respondent. Section C seeks to know people's opinion on the Communication Security Threats encountered, effects of such threats and their counter measures.

2.1.4 Microsoft Office Excel 2010

Microsoft Excel is an electronic spreadsheet programme that was used to enter values and data into rows and columns then create numerical entries for calculations, charts and statistical analysis.

2.2 Methods

The methods used in the research involved the following with the associated materials;

2.2.1 Personal Computer

The personal computer was used for the following;

1. Installation of Microsoft Security Essential Antivirus Software.
2. Intrusion Detection/Prevention.
3. Manage Spreadsheet
   - Tabulate data
   - Sort and Filter data
   - Validate data
   - Create a chart

2.2.2 Microsoft Security Essentials Antivirus Software

Microsoft Security Essentials Antivirus Software Compact Disk was inserted on the CD ROM drive of the personal computer, the option to install automatically appears on the screen of the personal computer. The install option was selected and installations began and ended without human interaction. The "finish" installation option appeared at the end of the installation, this was clicked to complete the installation.

After the installation was completed, the "Scan my Computer" option was selected to scan the computer for threats. Potential threats were identified using results obtained from such scans and those threats identified were moved to quarantine and some removed.

2.2.3 Questionnaires And Interviews

A. Questionnaires

Five hundred copies of the questionnaire were distributed in the Ministries, Department and Agencies (MDA's) and other ICT businesses within Cross River State.

A total of four hundred and ten questionnaires were recovered while ninety of the questionnaire was not recovered. The overall response rate stands at eighty-two percent (82%). Information obtained from the questionnaires were tabulated, cleaned and analyzed using Microsoft Office Excel 2010.

B. Interviews

Interviews were conducted in the Ministries, Departments and Agencies (MDA's) and other ICT businesses within Cross River State. A total of forty-five respondent's were interviewed, thirty of the respondents were Higher Data Processing Officers (HDPO's) drawn from the Ministries Department and Agencies of the Cross River State Government and fifteen of the respondents were Computer Administrators in other ICT businesses within Cross River State. The questions asked included;

1. Name of the respondent
2. Qualification and job carried-out by the respondent
3. Type of operating system used by the respondent in his/her personal computer.
4. Functionality of the respondent Antivirus Software
5. How often the respondent updates his/her personal computer with the latest patches and service packs
6. How often the respondents scan his/her computer for threats
7. Results obtained by the respondent from reports of such scans (If any)
8. The effects of the malicious software on the respondent computer
9. The most common security threats encountered by the respondent within the MDA or ICT business
10. Suggestions on the best threat mitigation measures to be employed

2.2.4 Microsoft Office Excel 2010

The methods for the analysis include;

1. Tabulation
2. Data sorting and filtering
3. Data Validation
4. Data Cleaning

- Removal of invalid Data

5. Data representation (using Pie-chart)

3. RESULTS AND DISCUSSION

3.1 Identified Threats

A number of threats peculiar to the Ministries, Department and Agencies (MDA's) and other ICT businesses in Cross River State have been identified in this study.

3.1.1 Results From Questionnaires And Interviews

Here are some of the common security threats encountered:

1. **Human Error**: Intentional or not, people are security threats. Some examples of common human errors include:
   - Misplacing information.
   - Opening spam emails.
   - Failure to properly process information.
   - Improper disposal of documents (electronic and paper).
   - Sending email to someone other than the intended recipient (one of the dangers of auto fill!)
2. **Disgruntled Employees:** If your systems aren't secure, employees could be stealing all kinds of data before anyone notices it. There are a lot of reasons why a disgruntled employee might engage in these types of activities, including the fact that the employee seizes the opportunity and could use the money, or they feel the desire to take revenge on the company. Simple measures such as removing disc drives from computer towers can make a difference.
3. **Cyber Criminals:** Cyber criminals have developed a number of sneaky tactics to break into systems to get the information they want. It is simply the ability to hack into as many systems as possible. The tactics used by cyber criminals can be hard to catch, as many companies report that their systems had been invaded long before they knew anything was wrong.
4. **Property Theft/ Misplacement:** Information stored on laptops, USB keys and other portable devices increases security risks as these devices can be misplaced or stolen. These devices must be guarded by strong passwords and other recognition systems- facial scan, fingerprint, etc., in order to make sure information stays protected.
5. **Insufficient Network Security:** If your systems aren't properly guarded, it is easy for someone to break in. There are tons of ways that hackers weasel their way into your systems, so consulting a security or IT professional to find out which types of attacks you need to be on the lookout for is recommended. Find out which ones are most common and which ones could do the most damage, this way you can prioritize your actions.
6. **Accessibility:** When everyone has access to information in your organization, everyone could potentially steal that information. Sensitive information or information that doesn't pertain to one's job shouldn't be accessible to that employee. Clearly defined access roles make it easier to take control over sensitive information.
7. **Social Media:** The main security risk surrounding social media is personal information breaches and

the sharing of confidential information over these networks. Some people post work related information on a facebook wall post or when tweeting at someone, making the information available for a lot of people to see. There's a time and place for everything, and it's probably best not to have sensitive work related conversations with a colleague on a social media site.

8. **Physical Attacks:** Physical attacks can include an attacker coming in with an external hardware device like a USB drive and infiltrating a system that way. Thankfully, Microsoft has supplied us with group policy settings so we can set a policy in place that prohibits the use of any type of external storage device.
9. **Poor Password Policies:** When talking about password policies, we often think of complexity requirements. This can include number of characters, type of characters (letters, upper-case, lower-case, numbers, and special characters), how often the password should be changed, and failure thresholds. You might even consider having your users change the password every 90 days instead of every month because it cuts down on the chance that the user might write down their password. From a security standpoint, any passwords that are written down for someone else to possibly see are a potential hazard.
10. **Privileged Accounts And Social Engineering:** Microsoft has been telling us for years not to login with an account with administrative privileges and go web surfing, and checking our e-mail. Hence the "run as" feature that was so kindly given to us. While working with an account with non-admin rights, if we need to install a program, we can right-click and choose "run as" and only that one process will use the administrative token.
11. **Packet Sniffing:** when an intruder listens to the network traffic and analyses the packets having a possibility to read our incoming and outgoing information using obscure protocols (eg.FTP) in Voice over IP protocol also known as eavesdropping.
12. **Password Breaking:** where there are many methods, brute-force using rainbow tables or disguising as trusted entity sends requests to the target to confirm his username and password (also known as phishing).
13. **Man In The Middle Attack:** it's an attack where intruder attack someone who has already established a trusted communication, for instance subcontractor or another company we do business with, therefore because our network is too secure

intruder attacks less secure network we have connection with.

14. **Denial of Service Attack:** occurs where intruder is sending extremely high amount of packets/information so that our network/server can't handle it. Sometimes it may be caused by the number of users using certain services at the same time causing 'legitimate' denial of service.
15. **E-mail Attacks:** Imagine that you have just sat down to check your e-mail, and you receive an e-mail claiming to be from your bank or, better yet, from your HR department, claiming that a new policy is in place and it's required that you change your password for security reasons. You click on the link provided in the e-mail only to be directed to a site that looks alarmingly identical to your bank site or your internal HR site. At the site, it asks you to put in your current credentials for authorization. Spam and phishing attacks are classics in the online criminal's repertoire. But, as long as users keep falling for the tricks, the bad guys will just keep sending on the e-mails. These types of attacks can leave you wide open for some of more popular risks.
16. **Increased Malicious Malware:** We have all heard of malware infecting our systems. We usually only find out about it through scans because they are designed to infiltrate or damage a computer system without the user's consent. Although most of the malware is not malicious in nature and is usually referred to as spyware, the threat of malicious software infiltrating our machines is an ever-alarming one. Below is a list of intrusion detection scans conducted in the Ministries, Department and Agencies (MDA's) of the Cross River State Government using the Microsoft Security Essentials Anti-Virus Software.

- Win32/Virut.BN, Win32/Sality.AM, Win32/Sality.AT, Win32/Vobfus.E, Win32/Agent.FO, Win32/Conficker.B, Win32/Conficker.!inf, Win32/Sality.gen, Win32/VB.HA, Win32/Silly_P2P.B, Win32/Rimecud!inf, Win32:Elderado.B [Trj] (Engine-B), Win32/Vobfus!dll, Win32/Trojan-gen, Win32/Flot [Trj], Win32:Sality, "Win32:Sality-GR", "Bv:Autorun-S [Wrm]", "Bv:Autorun-A [Wrm]", "Inf:Autorun-gen2 [wrm]", "LNK: Runner", INF;Autorun-AX [wrm], "Win32:Rontokbr-L [wrm], "Win32:Confi [wrm]", "Win32: Delf-EVY [Trj]", Win32:Autorun-BHJ [wrm], Win32:Mirc-X [Trj], "INF:Autorun-CN [wrm]", "Win32:Vitro", "Win32:VXBehav", "Win32: Rootkit-gen [Rtk]", "Win32:Runouce-B [Trj]", "Win32: ConfiDrv-B

[Rtk]", Win32/Dorkbot!Ink, "VBS: Malware-gen", Win32:Optix.pro [Trj], Win32:SpyBot.S [wrm], Win32:Yanz.b [wrm], NVCPL.EXE, CRSS.EXE, SVHOST.EXE, Win32:AGOBOT.GH [wrm] (Crss.exe), W32/Agobot-S (ScvHost.exe), W32/Mydoom.I@mm [wrm] (Svhost.exe), INF/Autorun.gen, E:/Sggu.Pif, TSPY_ZBOT.BX, TSPY_ZBOT.QXC, BKDR_QUEJOB.BVL. TROJ_DLOADR.ZZJ, TROJ_MDROP.WMP, HackTool:Win32/Keygen.

17. Not Updating Patches

Of course most of these threats could be avoided altogether if everyone followed best practices and made sure that all of their patches are up to date. For the common end user, it's just a matter of keeping auto update turned on inside of Windows. For a larger organization, things may not be so simple. Patches and updates have to be tested before being rolled out on an active network to ensure there won't be any conflicts with other software that might be running. Sometimes, the software running may be detrimental to the functioning of the particular organization. Of course, this is where having a testing environment along with Windows Software Update Services can be key. With WSUS, administrators have more direct control over the type and time updates are applied to network systems. This not only controls precious bandwidth but also gives administrators control over yet another entry point into their networks. This might seem obvious, but neglect in this department can be catastrophic as it keeps the door wide open for all the exploits and vulnerabilities set forth by all the viruses, worms, and rootkits that malware and other types of attacks have lying in wait.

18. Third Party Applications

fair to say that Microsoft has put tremendous effort into adding a lot of security in the Windows operating system as well as its Microsoft Office applications. It seems that as our operating systems become more secure, attackers are beginning to focus more on application exploits rather than operating system exploits. Microsoft is generally great about routinely updating Internet Explorer to patch any security vulnerability. However, the vendors of many third-party applications are less security-minded or aware. Just think of how many independent developers there are out there offering freeware. Some of these programs present an opportunity we can expect hackers to take advantage of because most have not been written with security in mind and do not

automatically check for and download security updates.

3.1.2 Effects on Victims

1. Malware degrades system performance, infects files, resides in memory and will reinfect files thus exhibiting great resilience.
2. Malware renders system unstable, causes unexpected system error messages and automatic reboots.
3. Malware causes registry modification, therefore affecting the overall smooth operation of the personal computer, even causing inability to start windows.
4. Malware generates unusual system behavior, denial of service (DOS) attacks and grants unauthorized/ unauthenticated user's remote access to the personal computer.
5. Malware downloads codes from the internet, causing financial losses approximating millions of naira.
6. Malware embedded on chips infiltrate information from computers and result in theft of personal identifiable information that could then be used for future cyber crime.
7. Malware overwrites hard drives, erases CMOS and the flashable BIOS, therefore preventing system from booting.
8. Malware pilfers data from victim's e-mail address book, mixing and matching new senders and recipients for a new round of infection.
9. Malware corrupts data on user's computer, infects other computer, weakens computer security, or provides backdoors into protected networked computers.
10. Malware seriously impairs business operations, network use, and computer performance.
11. Malware causes time lost because of operational slowdown caused by the weight of a computer's parasitic population.
12. Malware exposes victims to undesirable content, notably graphic images inappropriate in the workplace.
13. Malware causes data-harvesting where private information is been distributed without victims knowledge; such data can be used in a number of different scams to drain user's banks accounts, make use of victims credit, or enact identity-theft crimes.
14. Malware reduces resource availability, production and possibly lead to compromise of the network.

15. The use of counterfeit network components which leads to exploitation of cyber infrastructure vulnerability and even network failure.
16. Effects of botnets which facilitates online schemes that steals sensitive data, or fund and deny access to other online resources.
17. Social engineering which leads to online theft of banking/brokering account credential and credit card number of individual and businesses that result in financial losses to victims.
18. Spyware compromises computer operations through hijacking and browser redirection or replace normal components of the operating system.
19. Intellectual property rights violations, including theft to trade secrets, digital piracy and trafficking counterfeit goods, also represents high criminal threats, resulting in billions of naira in losses annually.
20. Poorly manufactured computer chips that have been salvaged and repackaged infringe on intellectual property rights and could fail at critical times, posing a serious health and safety threats.
21. Threats to physical infrastructure, such as power failure (outages, spikes and brownouts), fire or flood which can destroy the entire computer centre.
22. Computer threats causes modification and disparity in financial, inventory and school grading system.
24. Compromise of encrypted data, by unauthorized user, therefore accessing content of data without the knowledge of the sender.

3.1.3 Mitigating Of Threats

1. Improved Operating System and Windows Firewall will help mitigate threats.
2. Keep systems updated with all the latest patches and service packs. If possible enable automatic updates on window systems.
3. Pay attention to Microsoft security advisories; implementing suggested mitigations before the patch becomes available could help alleviate exposure to zero day attack.
4. To prevent exploitation of remote code execution vulnerabilities, use tools like Microsoft DropMyRights to implement “least Privileges”.
5. Prevent vulnerable Active X component from running inside your Web-Browser via the “Killbit” mechanism.
6. Use antispyware scanner to detect Browser Helper Objects (BHO).
7. Use intrusion detection and prevention system, anti-virus, anti-spyware and malware detection software to block malicious HTML Script code.
8. Activate browser tools-popup stoppers, anti-phishing, plug-in monitors.

9. Consider using other browsers such as Mozilla Firefox, Google Chrome that do not support Active X technology.
10. Do not open attachments from unknown sources. Practice caution when opening unexpected e-mail attachment even from known sources.
11. Configure your system with enhanced security.
12. Use mail and web filtering systems at the network perimeter to prevent malicious office documents from reaching end-user systems.
13. Do not run email client on server or workstations with confidential information.
14. Do not run the email client as an administrative user, or other user account with elevated privileges.
15. Do not answer junk mails (Spam), even if you have the option to unsubscribe.
16. For secure email exchange, use digital signatures or/and encryption.
17. Configure operating Systems and browsers to prevent unintentional installations.
18. Enable logging/auditing to determine failed log-in attempts, who uses what services and when.
19. On centrally manage systems, use the principle of least privileges and limit installation of additional software by the end-user, when possible. This will make patch management and vulnerability management easier and more effective.
20. Users should be restricted from surfing any potentially dangerous URLs via URL blocking.
21. Users should not be allowed SMTP, POP or IMAP access to their personal or service provider mail servers. This helps prevent potentially unfiltered and unscanned content entering in an organization network via mail.
22. Do not use user-supplied inputs with file functions to avoid remote file inclusion attacks.
23. Join secure coding organizations, such as OWASP to boost skills and learn about secure coding.
24. Enable the windows firewall and/or install a 3rd party firewall on the host. Ensure that rules are applied to restrict access to windows machine except for those connections that are explicitly required.
25. Improve perimeter defense/monitoring log.
26. Enforce strong authentication, authorization and accounting (AAA) to prevent/block brute force attacks.
27. Avoid service interactions and misconfigurations.
32. Use vulnerability scanner to check whether your systems are patched against vulnerabilities.
33. Verify the presence of a patch by checking the registry key mentioned in the registry key modification section of the corresponding security advisory. Additionally, it is advisable to also make

sure the updated file versions mentioned in the advisory are installed on the system.

3.1.4 Other Results

Operating System

Table 1.1: Operating system type

S/N	System Type	Respondent
1	Windows 2000 workstation and Server	16
2	Windows XP Home and Professional	80
3	Windows Server 2003	9
4	Windows 7	196
5	Windows Vista	97
6	Linus/Unix/Mac Operating Systems	12

Result of information displayed on Table 1.1 is represented in the Figure below.

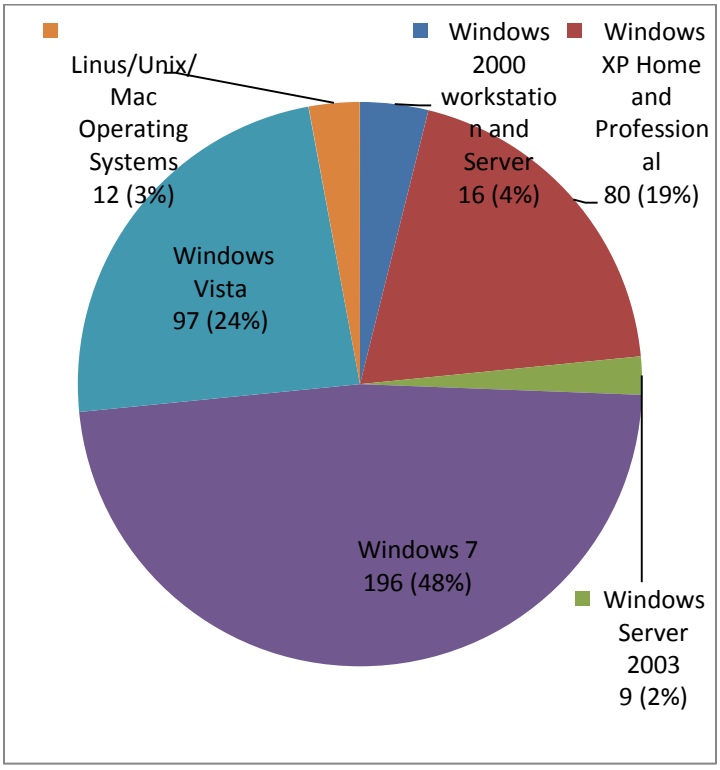

Fig. 1.1: Pie-chart showing operating system type

Most secured web browser

Table 2.1: Most secured web browser

S/N	Web Browser	Respondent
1	INTERNET EXPLORER	138
2	MOZILLA FIREFOX	256
3	GOOGLE CHROME	11
4	SAFARI	4
5	OTHERS	1

Result of information displayed on Table 2.1 is represented in the Figure below.

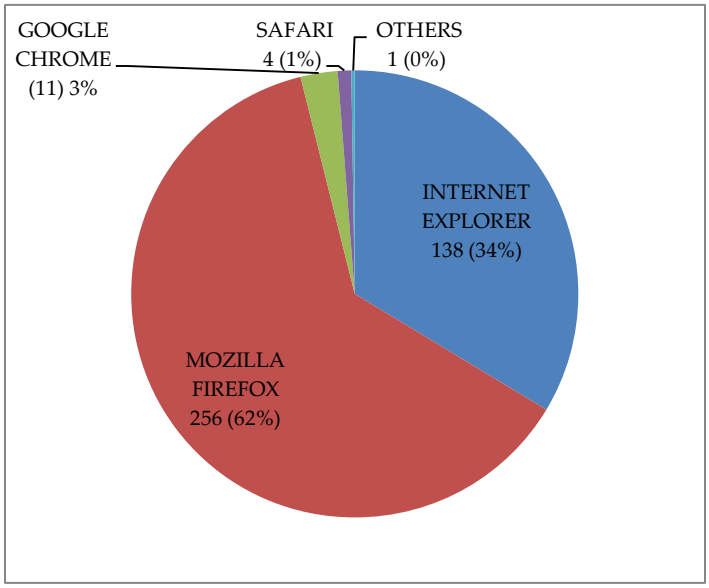

Fig. 2.1: Pie-chart showing most secured web browser

Browser with known vulnerability

Table 3.1: Browser with known vulnerability

S/N	Browser	Respondent
1	INTERNET EXPLORER	315
2	MOZILLA FIRFOX	2
3	GOOGLE CHROME	19
4	SAFARI	73
5	OTHERS	1

Result of information displayed on Table 3.1 is represented in the Figure below.

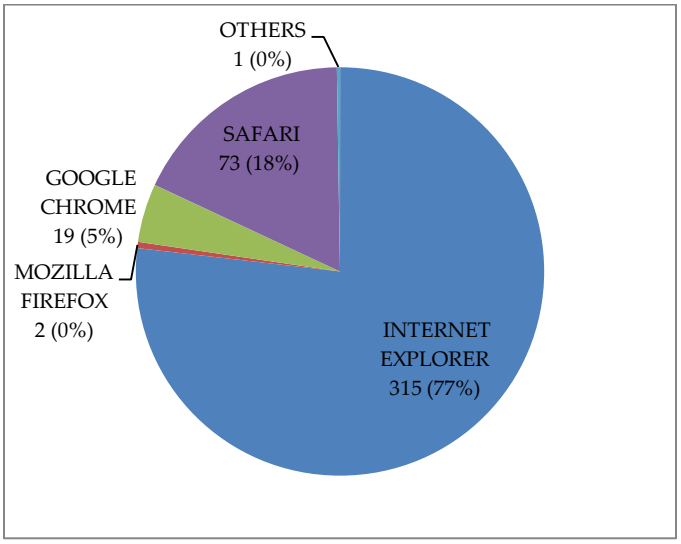

Fig. 3.1: Pie-chart showing browser with known vulnerability

Antivirus software used by users

Table 4.1: Antivirus software used by users

S/N	Antivirus Software	Respondent
1	BIT DEFENDER	19
2	MACAFEE	8
3	NORTON	52
4	KASPERSKY	9
5	ESET NOD32	41
6	AVG	22
7	G DATA	3
8	AVIRA	7
9	VIPRE	11
10	WEBROOT	2
11	AVAST	22
12	TREND MICRO TITANIUM	3
13	MICROSOFT ESSENTIALS	212

14	OTHERS	1

Result of information displayed on Table 4.1 is represented in the Figure below.

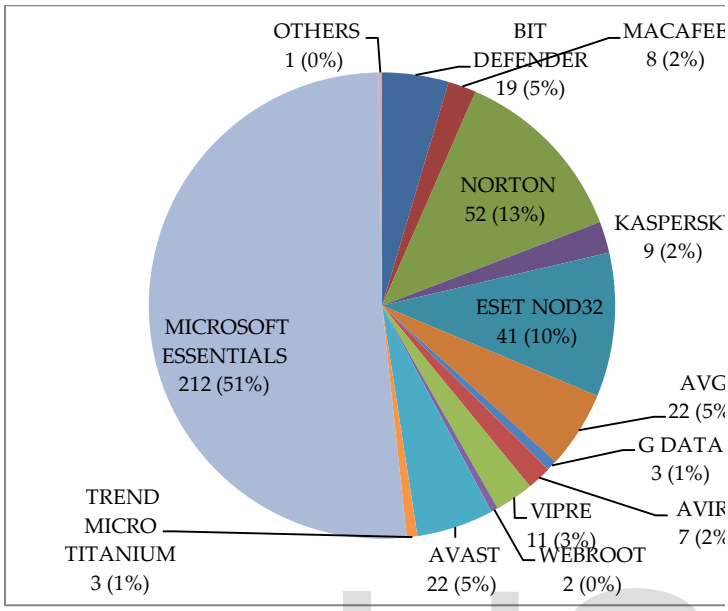

Fig. 4.1: Pie-chart showing antivirus software used by users

Best Measures Of Mitigating Security Threats

Table 5.1: Best measures of mitigating threats

S/N	Mitigating Measures	Respondent
1	USER EDUCATION	198
2	INTRUSION DETECTION/PREVENTION SYSTEM	58
3	USE OF FIREWALL	16
4	AUTHENTICATION	13
5	AUTHORIZATION	41
6	ACCOUNTING	7
7	REGULAR SYSTEM UPDATE	42
8	RESTRICTION OF UNNECCESSARY SERVICES	13
9	RESTRICTION OF MALICIOUS SITES	20
10	OTHERS	2

Result of information displayed on Table 5.1 is represented in the Figure below.

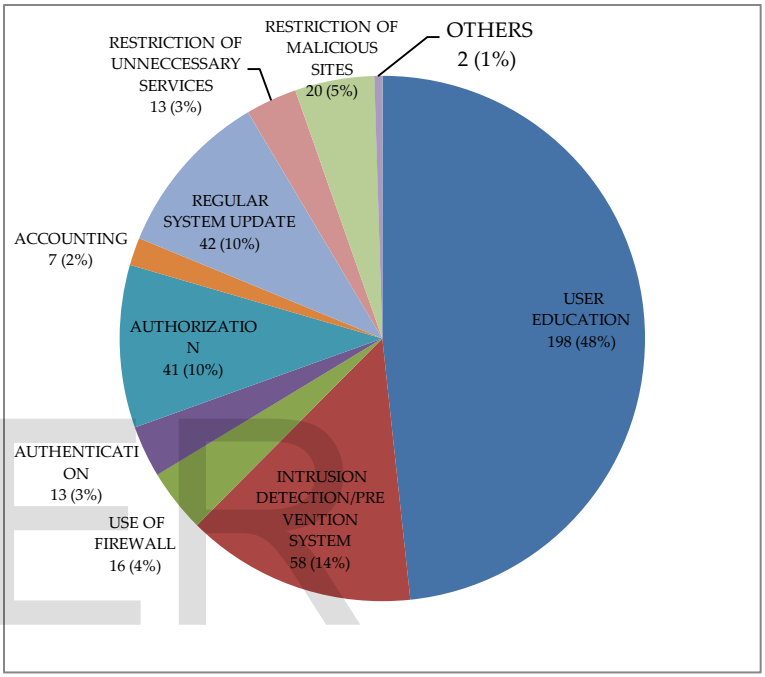

Fig. 5.1: Pie-chart showing best measures of mitigating threats

3.2 Discussion of Results

Results obtained from data analysis are discussed below.

Operating System

From the data analysis shown in Table 4.1, 48% of the respondent reported Windows7, 24% of the people interviewed used Windows Vista, 19% ticked Windows XP, 4% Windows 2000, 3% Linus/Unix/Mac operating System and 2% Windows Server 2003 operating system.

It can be deduced from this analysis that, greater number of respondents used Window 7 operating system.

Most Secured Web Browser

From the data analysis shown in Table 4.2, 62% of the respondents reported Mozilla Firefox as the most Secured Web Browser, 34% ticked Internet Explorer, 3% Google Chrome and only 1% Safari.

It can be deduced from this analysis that, greater number of respondents ticked Mozilla Firefox as the most secured web browser.

Browser With Known Vulnerability

From the data analysis shown in Table 4.3, 77% of the respondent's ticked Internet Explorer as the browser with known vulnerability, 18% reported Safari, and 5% Google Chrome, while none selected Mozilla Firefox.

It can be deduced from this analysis that, greater number of respondents ticked Internet Explorer as the web browser with known security vulnerability.

Antivirus Software Used By Users

From the data analysis shown in Table 4.4, 51% of the respondents reported Microsoft Security Essentials Antivirus Software, 13% used Norton, 10% ESET NOD32, 5% Avast, Bit Defender and AVG respectively, 3% selected Vipre, 2% MacAfee, Avira and Kaspersky respectively, while 1% G Data and Trend Micro Titanium.

It can be deduced from this analysis that, majority of the respondents uses Microsoft Security Essentials Antivirus Software.

Best Measures Of Mitigating Security Threats

From the data analysis shown in Table 4.5, 48% of the respondents reported user education, 14% ticked intrusion detection and prevention system, 10% Authorization and regular system update, 5% restriction of malicious sites, 4% the use of firewall, 3% authentication and restriction of unnecessary services, while 2% ticked accounting, and 1% selected others.

It can be deduced from this analysis that, greater number of respondents reported User Education as the best measure of mitigating potential security threats.

The results shown above are in good agreement with those obtained by [Cohen 1991, Orlandi 1991, Dobson 1994, Tarr 1995, Anderson 2001, Butler 2002] who identified common threats to computer security, effects on victims and certain security threats mitigating measures.

4. CONCLUSION

Communication security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, maliciously formed input data, poor application input validation, disclosure, destruction, modification,

disruption or distribution. The never ending process of communication security involves ongoing training, assessment, protection, monitoring & detection, incident response & repair, documentation, input validation, configuration management, session management, cryptography, parameter manipulation, exception management, auditing, logging, solid authentication and authorization strategy. This makes communication security an indispensable part of all the business operations across different domains.

The threat and risk assessment process is not a means to an end. It is a continual process that once started should be reviewed regularly to ensure that the protection mechanisms currently in place still meet the required objectives. The assessment should adequately address the security requirements of the organization in terms of integrity, availability and confidentiality. The threat and risk assessment should be an integral part of the overall life cycle of the infrastructure.

Organizations that do not perform a threat and risk analysis are leaving themselves open to situations that could disrupt, damage or destroy their ability to conduct business.

Therefore the importance of performing a threat and risk analysis must be realized by both the staff supporting the infrastructure and those that relies upon it for their business.

REFERENCES

1. Cohen, F., (1991): "A Cost Analysis of Typical Computer Viruses and Defenses," Computers & Security, Vol. 10, 1991, pp. 239-250.
2. Orlandi, E., (1991): "The Cost of Security," Proceeding of the 25th Annual IEEE International Carnahan Conference on Security Technology, Oct. 1991, pp. 192 –196.
3. Dobson, J., (1994): "Messages, Communication, Information Security and Value," Proceeding of the New Security Paradigms Workshop, IEEE, Aug. 1994, pp. 10-18.
4. Tarr, C.J., (1995): "Cost Effective Perimeter Security, Security and Detection," European Convention on Security and Detection, 1995, pp. 183-187.
5. Anderson, R., (2001): "Why Information Security is Hard- An Economic Perspective," 17th Annual Computer Security Applications Conference, Dec. 2001.
6. Butler, S. A., (2002) "Security Attribute Evaluation Method: A Cost-Benefit Approach," Proceedings of the 24th International Conference on Software Engineering, ACM, May 2002, pp. 232-240.
7. Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. Computers and Security 21 (6), pp. 526-531.
8. Melara, C. et al. (2003). A System Dynamics Model of an Insider Attack on an Information System. In Proceedings of the 21st International Conference of the System Dynamics Society (New York, USA, July 20-24).

9. Furnell, S.M., Phyo, A.H. (2003). Considering the Problem of Insider IT Misuse. Australian Journal of Information Systems 10 (2), pp. 134-138.
10. Bellovin, S.M. (2008). The Insider Attack Problem Nature and Scope. In Stolfo, S.J. et al. Insider Attack and Cyber Security, Beyond the hacker, New York, Springer Science, pp. 1-4.
11. Greitzer, F.L. et al. (2008): Combating the Insider Cyber Threat, IEEE Security and Privacy 6 (1), pp. 61-64.
12. W.H., Hylender, C.D. & Valentine, J.A. (2008): 2008 Data Breach Investigations Report. Obtained from www.verizonbusiness.com, October 2008.
13. Vadera et al. (2008): 2008 Information Security Breaches Survey. *Technical Report*.
14. Sinclair, S., Smith, S.W. (2008). Preventative Directions for Insider Threat Mitigation Via Access Control. In Stolfo, S.J. et al. Insider Attack and Cyber Security, Beyond the hacker, New York, Springer Science, pp. 165-193.
15. Keromytis, (2008). Hard Problems and Research Challenges Concluding Remarks. In Stolfo, S.J. et al. Insider Attack and Cyber Security, Beyond the hacker, New York, Springer Science, pp. 215-218.