Modified Small Business Network Security

[1]Md. Belayet Ali, [2]Oveget Das, [3]Md. Shamim Hossain

[1]Department of Computer Science & Engineering,
Mawlana Bhashani Science & Technology University
Tangail, Bangladesh

[2]Department of Computer Science & Engineering,
Mawlana Bhashani Science & Technology University
Tangail, Bangladesh

[3]Department of Computer Science & Engineering,
Mawlana Bhashani Science & Technology University
Tangail, Bangladesh

*Abstract:-***This paper covers some likely threats and effective steps for a secure small business. It also involves a flowchart to comprehend the overall small business network security easily and we identify a set of security issues and apply appropriate techniques to satisfy the corresponding security requirements. In respect of all, this document is strong enough for any small business network security.**

Keywords: - **Firewall, Antivirus, Back-up, Flowchart, Remote Access VPN and Site-to-Site VPN.**

I. INTRODUCTION

Today more than ever, good network security is vital to businesses of all sizes. With broadband usage swiftly becoming a standard in the business world and network security hazards on the rise, except dedicated IT team small businesses are confronted with the great challenge of defending their networks from threats because it may hurt if we don't know about the security [1]. However, in order to meet this challenge, small businesses must initial face a greater challenge: apprehending and acknowledging the threats? The purpose of this paper is to make available small business owners and network administrators with a better apprehending of security significances and to summarize the actions that can be taken to make sure the safety of networks and their data.

This paper is organized as follows: Section 2 gives the brief introduction to the background of small business network security. In Section 3 the threats issue are explained. In Section 4 describes the protection for avoiding risk . Section 5 gives eleven steps to a secure small business network. Section 6 gives the graphical view of proposed work. Section 7 gives the evolution of the proposed work. Finally Section 8 concludes with a scope for further research.

II. BACKGROUND

A. Small Businesses Defenseless

Probably the owner's false sense of security and lack of efficiency in protecting their networks is the greatest threats to small business networks. Very often network security is considered as trivial matter that's why they try to push network security down the priority list in favor of more pressing matters, and in many cases, network security is not a concern at all.

To better realize the ruthlessness of this phenomenon, consider the following research results:

- According a survey conveyed by the National Cyber Security Alliance, "More than 30% of those polled by the National Cyber Security Alliance (NCSA) think they'll take a bolt of lightning through the chest before they see their computers violated in an Internet attack [2].

- The SANS/Internet Storm Center publishes a statistic reporting the average time a "clean" (unpatched and undefended) system can be connected to the Internet before being attacked or scanned. Recent data indicated an average of 20-30 minutes [3].

New threats continue to grasp every day, and "lightning" can strike, whether in the form of lowered productivity due to spam, or priceless information such as customer credit card numbers that end up in the wrong hands.
Many small business owners do not give importance the network security concerns, believing and claiming that

because of company's size and insignificance hackers won't target the network . This is not very prudential approach .It is nothing but absolutely misguided approach. Strict regulations such as the Sarbanes-Oxley Act require enterprises to invest more in information security. Enterprises are conscious about various kinds of threats and very often employ in house specialists to protect from such kind of threats .The companies which have large networks own complex firewall and intrusion prevention system are to be updated and maintained regularly. Though small businesses don't have manpower, time, enough money as like as enterprise network security system, they should not ignore security threats.

A good example of the vulnerability of small networks in comparison to enterprises is the effect of the My. Doom worm (released in January 2004). According to the Internet Security Alliance data, one out of three small businesses was affected, while only one out of six enterprises was affected.

It is not always personal. As you will learn later, most attacks and security threats are aimed at the general public and not directed at any specific company or network. A hacker can run a software program that scans networks and IP ranges, looking for potential weaknesses. When such weaknesses are found, the hacker can take over the machines or infect them, in order to use them as a "zombie army" in larger scale attacks.

B. When Someone Hacked

Strange pop-up windows, unauthorized software, sluggish systems, mysteriously changed passwords, programs running automatically, or unofficial content posted to your website are all signs that your small business network has been hacked. If you suspect that your network security has been compromised, don't panic! You can use the following five steps to get rid of attacks.

1) Testify the attack on your network. You should gather as much information as early as possible. Confirm which systems were compromised, determine the IP addresses that were used in the attack, and identify the type of attack. Use the administration tools available in your routers and firewalls. If devices on your network can provide traffic flow records, these records can help to investigate.

2) Include the damage and preserve your business assets. Your initial reaction may be to take your entire network offline but that could actually cause additional damage to your company's operations, not to mention relationships with customers and reputation in the marketplace. Instead, strategically isolate and take offline just the impacted applications; or, if necessary, take down the servers or computers those applications live on. This will quarantine the affected applications and devices while still allowing your company to continue to do business. You may need to delete any offensive content left on your site or wipe your systems clean of malware, but you also need to preserve evidence of the crime that was committed against your company.

3) Come to a decision if you need to make a public statement about the incident. Depending on the kind of attack and the damage your network sustained, you may need to communicate with customers, partners, or authorities. For example, If customer or partner data was affected, you'll need to notify them that their information was compromised. Again, consult first with your lawyer and public relations professional before issuing any sort of public announcements.

4) Cleanse and restore the affected systems. If more than one computer or server was hit in the security attack, you should first prioritize the order in which you'll clean and then restore them to their previous states—starting with business-critical systems, of course. Replace the current, compromised data, configurations, and applications with the most recent clean backup. Change the passwords for all affected systems, users, and applications, including the root password. At the same time, require that all passwords companywide be changed, even on systems that weren't impacted by the attack. Make sure, too, that no passwords are set to a default or "admin."

5) Lock up the vulnerability used to access your network and amp up security. Make sure you fix the hole that was used to gain access to your network, whether it was a configuration error, an email download, or other vulnerability. You should also enhance your network security. For example, check for new security patches and update all systems and software to the most current versions and make sure the security settings on all of your network hardware and software are set appropriately.

III. THREATS ISSUES

Like any technology, Internet sanctuary threats are altering and sprouting at all times. Hackers adjust their methods and flourish them to take advantage of both technological vulnerabilities and psychological weaknesses of employees. Some Current threats are:

A. *Security Holes or Vulnerabilities:* New network vulnerabilities and security attacks are continually cropping up. Technology vendors discover new holes and release patches to their products' firmware and software on a regular basis. But attackers are moving just as fast to exploit those holes and invent new ways to break into your network.

B. *Direct Attack:* Though less common in the small business world, direct attacks do exist. A Displeased worker, a very dejected customer, or a rival with network knowledge can try to hack into the network with different intentions. From simple inquisitiveness to data theft, many reasons can cause a hacker to come knocking on your office network door.

C. *Viruses:* A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. Viruses can be transmitted as attachments to an e-mail note or in a downloaded file, or be present on a diskette or CD. The user activates the code unknowingly, thus infecting their system with the virus. Viruses often use the victim's address book to email themselves to other mailboxes. Viruses can range from merely annoying to dangerously destructive [1].

D. *Worms:* A virus that replicates itself by resending itself as an e-mail attachment or as part of a network message is known as a worm. Worms are programs that replicate themselves from system to system without the use of a host file. This is in contrast to viruses, which requires the spreading of an infected host file. Although worms generally exist inside of other files, often Word or Excel documents, there is a difference between how worms and viruses use the host file. Usually the worm will release a document that already has the "worm" macro inside the document. The entire document will travel from computer to computer, so the entire document should be considered the worm W32.Mydoom.AX@mm is an example of a worm.

E. *Trojan Horses:* A Trojan horse is a software that appears to perform a desirable function for the user prior to run or install, but steals information or harms the system. It captures passwords and other personal information, and which can also allow an unauthorized remote user to gain access to the system where the Trojan is installed [7]. Furthermore firewall provides additional protection against Trojan Horses as it will block the unauthorized e-mailing of the key-log file to its intended recipient, and alert you of the Trojan horse's attempt to do so.

F. *Spyware:* Spyware is a type of malware that can be installed on computer, and which collects small pieces of information about users without their knowledge. The presence of spyware is typically hidden from the user, and can be difficult to detect. Typically, spyware is secretly installed on the user's personal computers to change computer settings, resulting in slow connection speeds, different home pages, and/or loss of Internet connection or functionality of other programs.

G. *Spam:* Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Due to the current rise of malicious software delivered by spam messages, as well as "phishing". Phishing is a method used to acquire personal information such as passwords, bank account and credit card numbers, and more, through sophisticated email messages that claim to have come from a specific provider (eBay for example) and appear quite authentic to the unsuspecting recipient.

IV. PROTECTION

If you have read this far, you have passed the toughest challenge for small business network owners. You should now have a pretty clear picture of what the possible threats are and how they can harm your network. The next step is to evaluate the risks and allocate the resources:

- **Assess your needs and invest correctly:** Consider the harm that could be caused if a competitor retrieved customer information. Think of the damage to your business that can be done by Web site downtime.

- **Don't go overboard:** Investing valuable time and money in resources you do not need. For example, a home-based business of three employees does not necessarily require content filtering to avoid questionable content online.

- **Outsource whenever possible:** Many ISPs offer security services for small as well as large networks. Check what security management options then can provide. Network security consultants as well as companies dedicated to network security service provisioning can be very helpful if you do not have an IT staff.

V. ELEVEN STEPS TO A SECURE SMALL BUSINESS NETWORK

There were ten steps in the existing paper [1]. But those ten steps are not strong enough for paper security. In this context we have proposed another new security step as physical security deposit box which plays vital role in the small business security.

The modified existing steps including proposed step are as follows:

A. Consciousness: Consciousness is not only important, it is the *most* important and first skill that *must* develop in order to achieve any lasting and significant growth. Be sure to check the availability of security updates and software patches. Augment awareness in own self, workers and environment. Have them read this document, if necessary. Make sure they do not bring unprotected mobile devices into the network, that they do not open unexpected email attachments, and so on.

B. Safety policy: In business, a security policy is a document that states in writing how a company plans to protect the company's physical and information technology (IT) assets. A security policy is often considered to be a "living document", meaning that the document is never finished, but is continuously updated as technology and employee requirements change. A company's security policy may include an acceptable use policy, a description of how the company plans to educate its employees about protecting the company's assets, an explanation of how security measurements will be carried out and enforced, and a procedure for evaluating the effectiveness of the security policy to ensure that necessary corrections will be made.

C. Physical security deposit box: In an ideal world, the smart business owner, when making their business plan, would go out and purchase a security deposit box with the same bank or credit union they received an approval for a business loan. To legally protect new business owners from tax audits or the destruction of important information, the new business owner would store their business plan and insurance premium paperwork in the security deposit box divided into organized files along with countless other legal paperwork .With a physical security box, small businesses do not have to worry about the threats of online hackers trying to find private financial and personal information pertaining to your business. It would also be wise, if you choose to purchase a security box and not have one through a bank or community credit union, to store the box outside the business's location, this way employers cannot get to it in anyway[6].

D. Firewell: A firewall is a security device that can be a software program or a dedicated network appliance. The main purpose of a firewall is to separate a secure area from a less secure area [4]. A firewall acts as the security guard between your network and the Internet. Software firewalls, also sometimes called personal firewalls that are installed directly on the computer are required in cases where the machine leaves the office, or where it is the only computer in the business. Hardware firewalls installed on firewall dedicated machines are required in networks comprised of a number of computers.

Firewalls differ from one another: some provide in-depth firewall protection and additional security services, while others simply provide Internet connection sharing with NAT translation, allowing only very basic protection. The main purpose of a firewall is to keep out unwanted traffic, such as a computer worm attempting to infect computers with a specific vulnerability. Note that some firewalls can also be used to block specified outgoing traffic, such as file sharing programs, and to block specified incoming traffic, such as instant messengers or any other service the firewall administrator chooses to block.

Many hardware firewalls offer additional services such as email antivirus and antispam filtering, content filtering, and secure wireless access point (AP) options. When selecting a firewall, define the requirements of your business. Many firewall vendors provide customizable firewalls with pricing depending on the range of services you select. If you can, get technical assistance from a local network security service provider. Firewalls are vital to network management. Without this control over computer and network access, large networks could not store sensitive data intended for selective retrieval. Firewalls are also very important for home broadband users - without a home version of one of these products; your personal data is at risk.

E. Antivirus: Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. In addition to implementing AV solutions on each machine, it is important to have an AV gateway: a local or remote machine where email messages are scanned for viruses while they are being downloaded to the client computer. It is crucial to keep the antivirus software updated at all times, as new viruses are found almost every day. Do not forget that simply having the software is not enough. Schedule an automatic scan if possible. If not, then set a reminder to ensure that you and other office employees run the scan on their computers periodically.

F. Patches and Updates: Microsoft and other software vendors provide updates that are meant to fix bugs and patch Potential security holes in their software. Make sure you regularly check for updates. You can even decide on a specific day (once in two weeks is usually enough) on which to remind yourself and your employees to run the software updates or check the software manufacturer Web site for any updates that may be available.

G. Backup: In information technology, a backup or the process of backing up is making copies of data which may be used to *restore* the original after a data loss event. By using Backup, you can create a duplicate copy of the data on your hard disk and then archive it on another storage device, such as a hard disk or a tape. . The primary purpose is to recover data after its loss, be it by data deletion or corruption. Data loss is a very common experience of computer users. 67% of Internet users have suffered serious data loss. If possible, encrypt sensitive information and always keep a non-rewritable copy (CD-ROM) of the files in a safe location.

Using Backup, you can:

- Archive selected files and folders on your hard disk.
- Restore the archived files and folders to your hard disk or any other disk you can access.
- Make a copy of your computer's System State data.
- Use Automated System Recovery (ASR) to create a backup set that contains the System State data, system services, and all disks associated with the operating system components.
- Create a log of what files were backed up and when the backup was performed.
- Make a copy of your computer's system partition, boot partition, and the files needed to start up your system in case of a computer or network failure.
- Schedule regular backups to keep your archived data up-to-date.

H. ISP and/or Gateway Failover: The businesses what are massively dependent on Internet connectivity, it is crucial to have a backup Internet connection and a backup firewall/gateway to conserve connectivity and production in the event that your primary Internet connection goes offline or the main firewall/gateway malfunctions. Numerous firewall gateways offer smooth and automated failover and ISP backup options. If temporary connectivity loss means potential profit loss, be sure to have failover options.

I. Antispam and Antispyware: Spam filtering can be implemented on the mail server, on the firewall/gateway, or on the machine receiving the messages. The antispam software acts as filter that scans the e-mails sent to your machine. Whenever it detects a bulk mail or unsolicited content in your mainframe, it sends the e-mail directly to the spam bin instead of delivering it to the message inbox [5].
Spyware can be removed by using antispyware software on the local machine. You may want to include this in your weekly or bi-weekly routine of updates and scans, and scan your network computers for spyware, as well as viruses and worms.

J. Blocking Specific Sites, IM Clients, and File Sharing Programs: The best way to deal with questionable sites online, IM conversations during work hours, and bandwidth-wasting file sharing is to enforce their exclusion on the gateway. Some firewalls allow you to select specific services to which access should be blocked and to filter Web sites by address and/or by category.

K. Remote Access VPN and Site-to-Site VPN: Virtual private network (VPN) technology allows you to connect two or more networks in a private connection, creating a tunnel of encrypted data between the two points. This technology was adopted to replace expensive private networks (such as frame relay) with increasing popular and available broadband Internet connections. VPNs provide privacy and encryption for the data as it is transferred over the Internet. This is especially useful if you have two or more branches in your business or would like to access your office network remotely. For example: Suppose, two regional office are connected with a head office through internet as well as remote user or roaming user .That's why a remote user doesn't have to carry confidential information on his laptop when visiting abroad. He has to do is connect to the Internet and access the data in the office through a secure connection.VPN Connectivity overview is shown below:

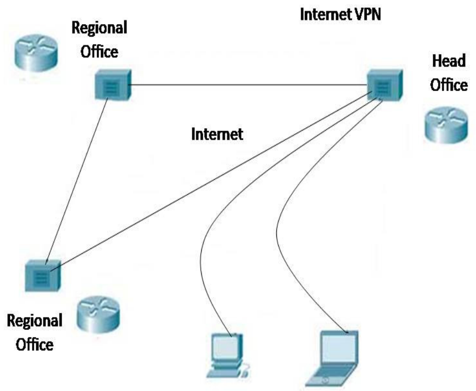

Figure 1: VPN Connectivity

VI. PROPOSED WORK

Our Proposed work is a flow chart of small business network security as well as a physical deposit box. The flow chart is:

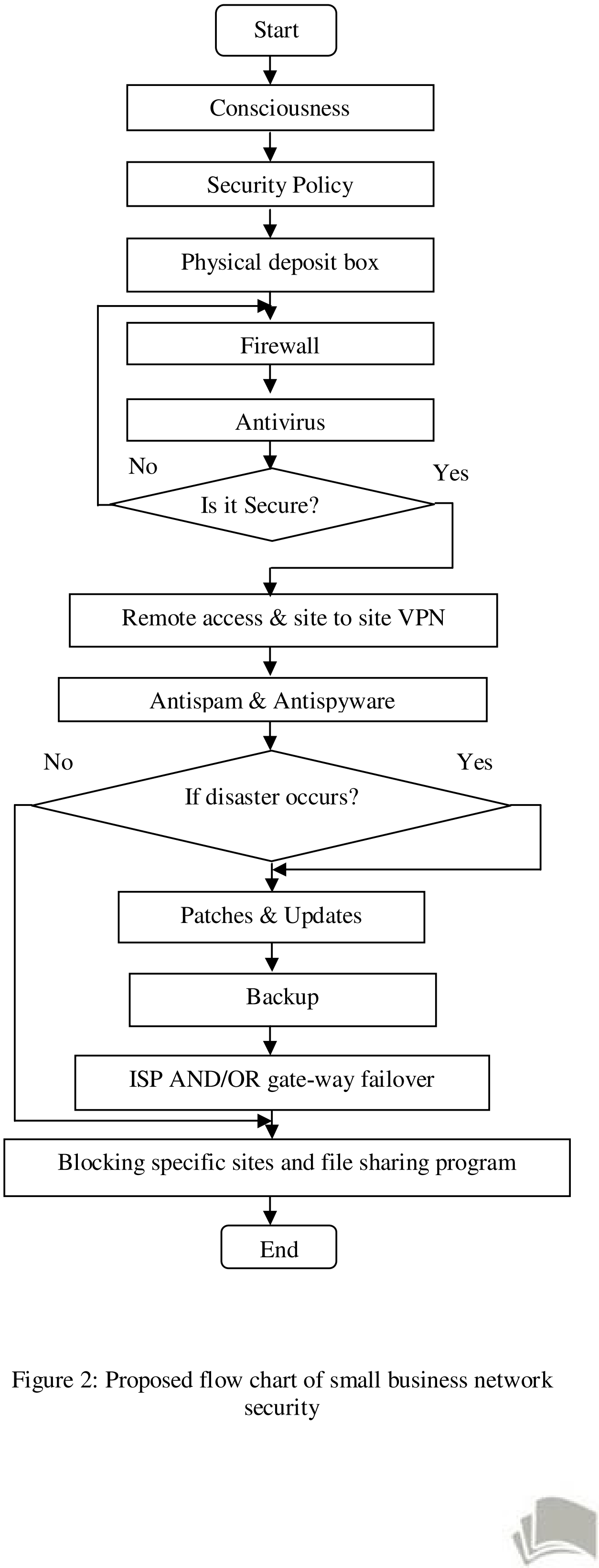

Figure 2: Proposed flow chart of small business network security

VII. EVALUATION OF PROPOSED WORK

The flow chart we have proposed, it is convenient enough to make anyone understand at a glance. We can hope that our proposed works are better than existing approaches[1] because such kind of flow chart is yet to be mentioned. Besides it, Physical deposit box is another important element in the realm of business security. A deposit box is used to legally protect new business owner would be store their business plan and insurance premium paperwork in the security deposit box.

VIII. CONCLUSION

On the basis of research on actual needs, we have proposed "Small Business network Security" flowchart, security deposit box, and elaborate discussion including a well example of VPN. This paper specifically addresses the solution of Network Business Security and gives the description of network business security threats.

REFERENCES

[1] Small Business Network Security 101 by Ilana Nijnik
[2] Poll: Lightning strike more likely than breach - http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1011092,00.html
[3] Survival Time History - http://isc.sans.org/survivalhistory.php
[4] Firewall, http://whatismyipaddress.com/firewall
[5] Antispam and Antispyware, http://www.sea-online.net/534882-Antispam-and-Antispyware-Protect-Your-Computer-Against-Intruders-How-do-They-Work-How-to-Use-Them-Pros-an-Cons.html
[6] why-small-businesses-need-a-physical-security-deposit-box, http://financewand.com/why-small-businesses-need-a-physical-security-deposit-box.html
[7] Security Assessments, http://kuszynski.com/Security/index.html
[8] Design and implementation of system and network security for an enterprise with worldwide branches, By Seifedine Kadry, Wassim Hassan