Pakistan Journal of Applied Sciences 3(1): 17-22, 2003
© Copyright by the Science Publications, 2003

The Current Security Awareness and Reliability in Area Enterprise Networks

Dereje Yohannes and Zheng-Quan Xu
Huazhong University of Science and Technology, Department of Computer Science
Wuhan 430074, People's Republic of China

Abstract: Enterprises in both the public and the private sectors are aware of the needs of Internet security. It is interesting to know how both sectors take action to protect their Internet data and corporate systems. Internet security is recognized as the methods used by an enterprise to protect its corporate network from intrusion. The best way to keep an intruder from entering the network is to provide a security wall between the intruder and the corporate network. Since the intruders enter the network through a software program (such as a virus, Trojan horse, or worm) or a direct connection, firewalls, data encryption, and user authentication can restrain a hacker. While many tactics provide assurance of protection, carelessness can also be a key factor. As a result, awareness training and education should be used to remind staff that an Internet security breach could have a profound effect on the health of the enterprise and, hence, their job security.

Key Words: Security, Intrusion, Awareness, Virus, Firewall, Encryption and Training

Introduction

In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, network security has assumed increasing importance. Three trends have come together to conduct this short research on the awareness and reliability of Internet security in the local area enterprise networks. First, even though we conducted the research in local area enterprise networks, currently it is a universal issue and concern so it is to deploy a basic understanding to every enterprise networks on the awareness of internet security all over the world that are using Internet. Second, the explosive growth in computer systems and their interconnections via networks has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. This, in turn, has led to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks. Third, the disciplines of network security has matured, leading to the development of practical, readily available applications to enforce network security all over the world.

Therefore it is the aim and purpose of this paper to provide a practical survey of network security awareness and reliability. Here, the emphasis is on the often neglected but the most important aspect of computer security awareness and reliability. Reminding and increasing the network administrator's awareness in preventing illegitimate access, in Management and Maintenance of the Firewall, and in Security policy, Virus protection and Training of employees for strengthening the security are the main objectives of the research paper.

This short research paper begins with an overview of the statistical data obtained from the 35 randomly selected private and government enterprises that are located around Wuhan city. Next, it investigates the awareness and reliability of Internet security based on the collected data. And finally it stipulates an appropriate measure that should be taken by every enterprise networks to combat the current internet security breaches. Here, as we mentioned above the research is conducted in Wuhan city but it is clearly indicated as it is a universal problem and every enterprise networks all over the world share the problem especially in the awareness of Internet security and therefore it is hoped that the reader of this research paper will have a wider perspective on security awareness and reliability in general, and better understand how to reduce and manage risk personally, at home, and in the workplace.

Materials and Methods

The type of methodology used so as to collect appropriate information and data for the research is Questionnaire. A Questionnaire with sixteen (16) questions were prepared and dispatched to thirty five (35) randomly selected enterprises to achieve the objectives of the research. Since the very aim of the research is to assess the awareness and reliability of the current security tips of the area enterprise networks and stipulating effective measures for combating some of the current security breaches, the selected enterprises were encouraged so as to give us an appropriate and reliable information about their enterprise network.

Results Obtained from the Survey

Awareness in Preventing Illegitimate Access: From the questionnaires we dispatched to assess the awareness of enterprise networks to prevent an illegitimate access, we have got the following figures. Currently among the 35 enterprises 62.5% of them are using firewall and 25% of the enterprises are using user authentication systems for securing their organizational network but the rest 12.5% of the enterprises are not using any security tools and none of the enterprises are using either data encryption or digital certificate for the security purpose. From the statistical data we can also see that the demand of implementing the firewall for the security purpose is increasing year after year, as you can clearly see from the graph, during 1996 fiscal year none of the enterprises were using firewall but after 2000 almost 20 of the enterprises implemented the system. And in conjunction with that 37% of the enterprise networks are considering the necessity of the firewall and have the aim of incorporating the technology to their organizational networks. But surprisingly 6% of the enterprises have no plan to implement the firewall.

Questionnaire: What Internet (Network) Security Tools Your Organization is Using?

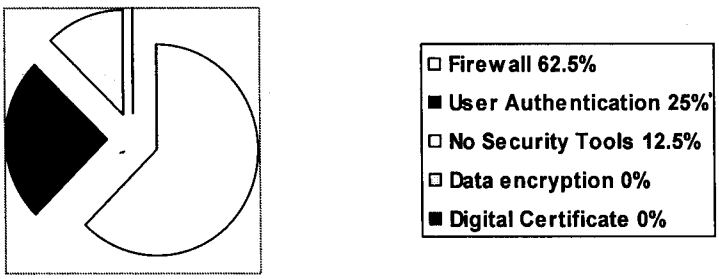

Fig. 1.1: Security Tools that the Enterprise Networks are Using

Questionnaire: - When You Implemented the Firewall for the Enterprise? (Fiscal Year)

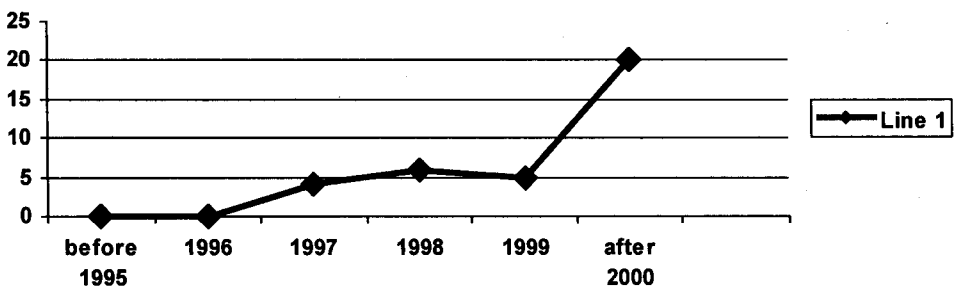

Fig. 1.2: Firewall Technology Implementation in Fiscal Year

Here the statistical data signifies, in today's world, most enterprises, regardless of size, believe that access to the Internet is imperative if they are going to compete effectively. Even though the benefits of connecting to the Internet are considerable, so are the risks. Actually when an enterprise connects its private network to the Internet, It physically connecting the network to well over 50,000 unknown networks and all of their users. While such connections open the door to many useful applications and provide great opportunities for information sharing, most private networks contain some information that should not be shared with outside users on the Internet. In addition, not all Internet users are involved in lawful activities. And it is not just only providing its employees access to external information and Internet services; it is also providing external users with a means to access the company's own private information. Horror stories abound in the media regarding companies that have had proprietary information stolen, modified, or otherwise compromised by attackers who gained access via the Internet. For this reason, according to the survey almost 87.5% of the enterprises that have ever contemplated connecting to the Internet has been forced to deal with the issue of network security.

While protecting the enterprise information may be the highest priority, protecting the integrity of the network is critical to protect the information that it contains. A breach in the integrity of the network can be extremely costly in time and effort, and it can open multiple avenues for continued attacks. Currently network packet sniffers, IP spoofing, password attacks, denial of service and application layer attacks are commonly used to compromise the integrity of every network.

When considering what to protect within the network, the main concern is to maintain the integrity of the physical network, the network software and any other network resources. This integrity involves the verifiable identity of computers and users, proper operation of the services that the network provides, and optimal network performance--all of these concerns are important in maintaining a productive network environment.

In response to these risks and other dangerous attacks firewall is the first line of defense for corporate networks and it is the best way to protect the enterprise network from illegitimate access that is why almost 62.5% of the enterprise networks are implementing and using the system. The system also provides a single point of defense between two networks it protects one network from the other. Usually, a firewall protects the company's private network from the public or shared networks to which it is connected. A firewall can be as simple as a router that filters packets or as complex as a multi-computer, multi-router solution that combines packet filtering and application-level proxy services.

Another line of defense is user authentication. Basically, a user must enter a password as a digital key to enter the computer system. User authentication can be

incorporated into a firewall, a particular application, a document, or a network operating system such as Novell NetWare and Windows NT. As you can see from the above statistical data here in Wuhan city from which the research is conducted 25% of the enterprise networks are using user authentication for securing their organizational networks.

The user authentication system works effectively if and only if every employee in the enterprise have a very strong and difficult to guess password as a digital key and every employee should have the habit of changing his/her password periodically for the purpose of preventing the stealing of passwords . From the research we conducted, 35% of the enterprises have employees that change their password continuously, 25% of the enterprises have employees that do not plan to change their password and 40% of the enterprises have employees that take the fact to consider.

Actually Passwords are a major vulnerability in most enterprises. It's not unusual for people to try to save time by sharing passwords or choosing a simple password. Weak passwords make it easy for unauthorized users to gain access. A potentially weaker spot in your network security may not be the user passwords, but the users. A carefree attitude toward passwords is what social engineers are banking on. It makes it that much easier to trick an employee into giving out their password over the phone or via email. Therefore, the network administrators should be aware of this fact and develop a password policy, requiring frequent password changes to prevent the stealing of passwords and educating users on social engineering tactics, and reinforce that they should never give out a password. Password cracking software is available to help find weak user passwords in your network. However, the software won't protect the company against an employee's negligent behavior. Often, educating employees is sufficient.

Here, firewall and user authentication are not the only security tools that protect the enterprise networks from an illegitimate access, there are also variety of technologies that an enterprise can employ to protect itself from unauthorized access. Data encryption, key management, digital certificates, Intrusion Detection Systems (IDS), virus detection, Virtual Private Networks (VPN) and Extranets are some of the most popular methods.

Therefore it is up to the network administrator to adapt and implement an appropriate security tool for the network so as to protect the enterprise from illegitimate access, dangerous internet attacks and security breaches. And these make the enterprise to be more competitive and effective.

Awareness in Management and Maintenance of the Firewall: From the research we conducted, we examined that 75 % of the enterprise network firewall systems are maintained and managed by the system manager whereas 25 % of the enterprise networks have no specific party to monitor the network.

From the survey that we performed, 60% of the enterprise networks faced no problems with their firewall system but the firewall system of 40 % of the enterprise networks were not going smoothly, the main reason for that was 37.5 % of the enterprise networks have a technical difficulty in maintaining and managing the firewall system. But the rest 62.5% of the enterprise networks were busy of other operations so that their firewall system was going wrong, but their technical level was sufficient to maintain and manage the firewall system. And among these enterprise networks 80% of them have a security policy for their firewall system and 5% of the enterprises have not established any security policy yet, but 15% of the enterprise networks are still analyzing its necessity.

From these statistical data what we conclude is that, many enterprise network managers believe that their networks are secure simply because they have installed a firewall system. Due to a false sense of security that many administrators feel because they have a firewall, the rigorous maintenance and management that is needed to ensure the security of a system is often overlooked.

It is important to think of installing a firewall as only the first step to secure the enterprise network. Once a firewall gateway is installed, the next question most administrators ask themselves is "how do I manage this device now that it is setup and running?" Unfortunately, as they try to solve that problem, many administrators commit a critical mistake that they need to avoid: they re-enable insecure management services.

Since the firewall is a bastion host, all of the insecure and unnecessary protocols and services have been disabled or removed. The list of common insecure protocols that are turned off includes SNMP, telnet and FTP –all 3 of these protocols are insecure because they send data and passwords unencrypted, which exposes the information to eavesdroppers. The security risk occurs because all 3 of these protocols are usually used to manage almost all operating system hosts, where critical system information can be exposed to a hacker.

Most system administrators often make mistakes during the initial install, leaving the firewall vulnerable from the start. Some of the most common mistakes observed during the research were:

- Not using a bastion host, this is a machine that has had its operating system hardened against an attack.
- Assuming that default software configurations are automatically secure.
- Allowing insecure protocols to be part of the enterprise network policy.
- Not testing the configuration sufficiently.

Here, even though installation mistakes can compromise the security of the network, the ongoing maintenance and support of the security system is much more important and warrants the bulk of every network administrator's attention.

Awareness in Security Policy, Virus Protection and Training: From the research that we performed, among the 35 enterprises that the survey was sent, 50% of the enterprise networks built a security policy for the whole of the company and 16.7% of the enterprises haven't yet build any security policy but the rest 33.3% of the networks considering the fact and have a plan to incorporate the policy for their enterprise networks.

According to the CSI (Computer Security Institute), "The findings of the '2001 Computer Crime and Security Survey' confirm that the threat from computer crime and other information security breaches due to the lack in the awareness of computer security policy continues unabated and that the financial toll is mounting." The following highlights are taken from this CSI/FBI survey: 85% of respondents...detected computer security breaches within a year, 186 respondents reported $377,828,700 in financial losses, the most serious financial losses occurred through theft of proprietary information (34 respondents reported $151,230,100),and 91% detected employee abuse of Internet access privileges.

Questionnaire: Who is Responsible to Maintain and Manage the Firewall?

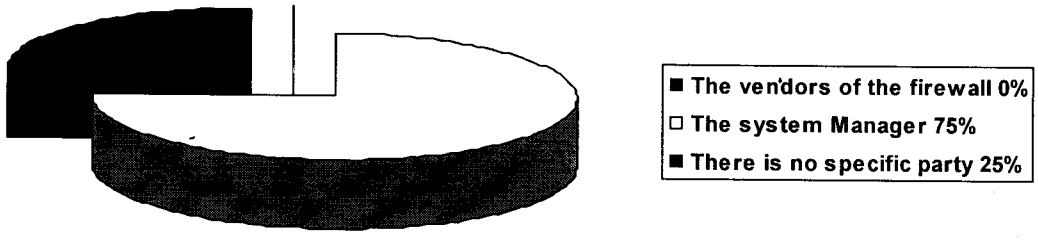

Fig. 1.3: Responsible Party for the Maintenance and Management of the Firewall

Questionnaire: Is the Maintenance and Management of the Firewall Going Smoothly?

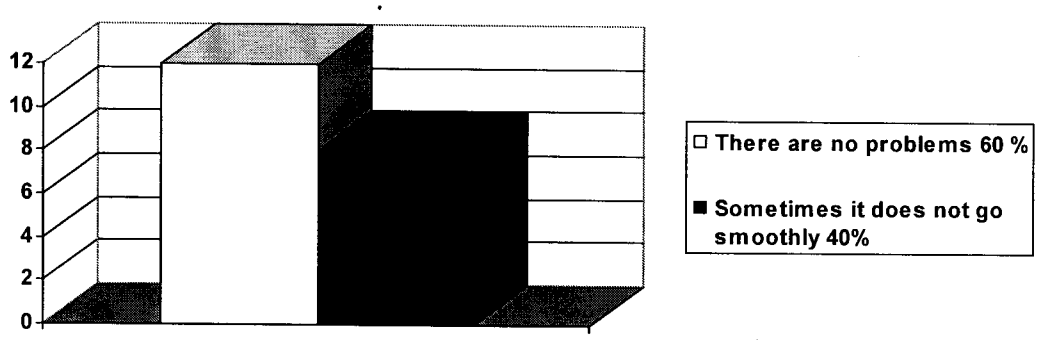

Fig. 1.4: Performance of the Firewall Technology

Questionnaire: Have You Built a Security Policy for the Whole of Your Company?

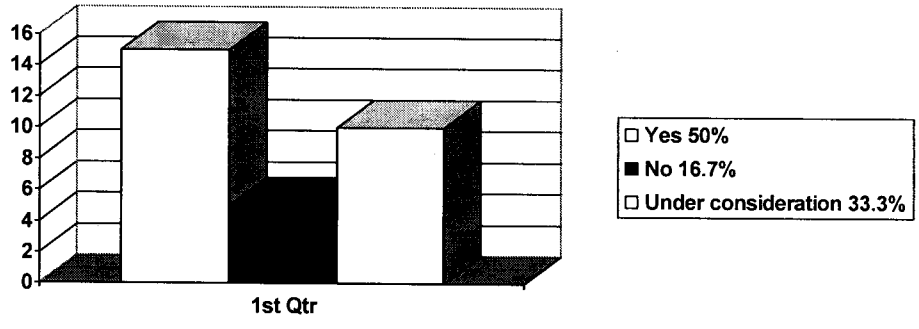

Fig. 1.5: Security Policy Assessments

The above statistical data can be used to help persuade organization executives of the need for a security awareness campaign. Actually, it is true that a sound security policy is the foundation of any successful security program. The policy defines the organization's overall posture toward security - whether it is very restrictive, allowing little or no leeway in access to data; or if is it more permissive, giving users more latitude in their actions. In either case, the policy must be the first step toward achieving an acceptable level of security.

But to what avail is even the best policy if those who are affected by it do not know of its existence or understand its contents? None! This is why security awareness (making users aware of what is expected of them in protecting the organization's data) is an

Questionnaire: How Often You Train Your Employees for the Latest Internet Attacks and Security Mechanisms?

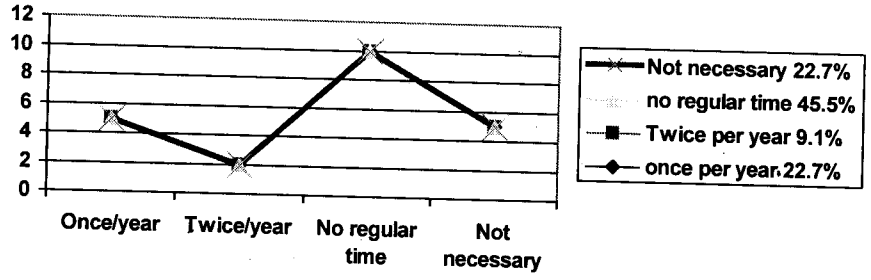

Fig. 1.6: Training Employees for the Latest Internet Attacks and Virus Protection

equally critical element in a successful security program. Without this awareness, users cannot be held responsible for failure to comply with policy; and may adversely affect the confidentiality, integrity and availability of the organization's information.

Users must not only know about the policy's existence, they must understand the contents of the policy, they must be aware of their responsibility in achieving the security objectives of the organization and they must be aware of the consequences for non-compliance. This user education can be accomplished most effectively through a well-designed security awareness program. For most organizations, security training should include initial new hire training followed by an annual refresher. Regardless of training employees for the latest security policy and virus protection, from the research we conducted only 8.6% of the enterprises have employees with a basic knowledge of virus protection, whereas 51.1% of the enterprises have some employees with a basic knowledge and 34.3% of the enterprises have no idea about this point. In connection with this, about 20% of the enterprise networks are implementing a training program so as to educate their employees but on the contrary 14.3% of the enterprise networks responded as training employees for virus protection and security policy at regular time is unnecessary. From those enterprises which implemented the training 45.5% of them have no regular time to educate their employees. 22.7% implement the training once per year and 9.1% of the enterprises implement the program twice per year. And 65.7% of the enterprises were failed to implement the training program due to lack of time and other reasons. Here from the statistical figure what we conclude is that most enterprise networks consider the implementation of training employees for virus protection and security policies as unnecessary and un useful task but despite the time, energy and money that companies funnel into products to maintain network security, their network's biggest threat is frequently from the inside. In addition to having basic security measures in place (such as firewalls, virus and mobile code protection and content filtering) companies also need to focus on training employees in order to reduce the impact of the human threat.

According to the 1999 Computer Security Institute/FBI Computer Crime and Security Survey, 38 percent of respondents had one to five security breaches originate within their organizations, while 16 percent had six to ten. Many security breaches occurred because untrained employees were unaware of how their computer use email or Internet impacted company security. Employees may fall prey to social engineering tactics, inadvertently downloading malicious code, or disgruntled employees may intentionally try to harm the company.

Employee email can cause several types of security breaches. If employees open unsolicited email attachments or do not scan attached documents for a virus before opening them, then the enterprise is vulnerable to virus attacks. Also, if companies rely on employees to keep their virus definitions updated, instead of pushing out new virus definitions automatically to ensure policy enforcement, they risk infection even if they do scan for viruses before opening attachments. By inadvertently allowing inappropriate email, sexual in nature or otherwise offensive, to be sent within the office, companies are vulnerable to legal action.

Employees spending time surfing for personal use also impact network security. The most common concern is that employees are wasting time. But there are other considerations. Just as with email, inappropriate Web surfing may lead to legal suits if an employee views sexually-explicit or discriminatory material online. And employees who excessively download MPEG or MP3 files risk slowing down the network.

Non-work-related surfing also increases the chances that an employee will visit a site using ActiveX or Java. These languages can be used to create malicious code that can communicate directly with the user's machine, giving hackers access to data and, potentially, the network. If employees download free software or screen savers from unknown sources, your system may be infected with a virus or Trojan horse, which may inflict damage ranging from file deletion to stealing passwords. However, experts say that larger and more popular sites that use these languages are fairly safe because the sites employ security measures.

Employees who don't know how to respond to potential security breaches, such as social engineering tactics, leave the company open to security attacks. Employees who are not properly trained or who are unhappy with their jobs are also more likely to divulge proprietary or otherwise sensitive information to unauthorized individuals, such as competitors.

And finally, so as to strengthen the security and increase the reliability of the enterprise the network administrator should give emphasis to the following important points that will avoid security breaches due to human factors

- Establish an Internet usage policy. Let employees know the enterprise's rules about personal use of email and the Internet. Developing Internet usage policies will also help IT managers to configure and monitor network security solutions more efficiently.

- Use technology that scans email for inappropriate content and logs Internet activity that falls outside the parameters set by management.
- Legal experts say that monitoring employees' email and Internet use can help to protect the enterprise in case of a lawsuit. Have a policy and a content-monitoring solution in place to show an effort to protect employees from harassment, for example.
- Train users to know when and how to download the latest anti-virus updates, as well as how to spot a potential virus. Teach employees how to scan documents before opening them.
- Patch known holes in software to reduce the chances of a virus entering from Web pages or email.
- Determine each employee's need to access sensitive information and restrict access to only what is necessary for their role in the enterprise.
- Warn employees of the dangers of downloading free software and screen savers.

The most effective, yet often neglected, method for addressing the "human factor" is to establish a policy of regular and consistent user training, with a focus on the enterprise's security objectives. Start by determining your policy needs and what level of training is required for each department. For example, IT security staffs need to have an in-depth understanding of the security products and systems that the enterprise uses, while non-technical staff and management can have a more general understanding of the security policy and virus protection.

Conclusion

In general when we compare the security awareness of the enterprise networks in Wuhan city with the rest of the world each Enterprise in both the public and private sectors uses almost similar security methods, but employ specific precautions that are prevalent to their type of business. Each enterprise has its own particular needs and requires certain safeguards to protect its data from damage.

Both the public and the private sectors have their own strengths and weaknesses on Internet security awareness and reliability. Each enterprise requires certain safeguards to protect their data while in transit. Developing a plan that has proportionately more strength than weakness is always the goal. However, since the Internet is still an untamed frontier that is still young and growing, for some of them it may take some time to develop stronger methods for data security.

Generally, today's Internet attacks are different from what they were just a couple of years ago. In addition to viruses, worms, and hackers, there is a new category of sophisticated and powerful threats that are known as "blended threats". What makes them so different is the fact that, unlike previous worm or virus outbreaks, blended threats can spread via several different avenues often discovering vulnerabilities on the fly and exploiting them. And they can be triggered automatically, without any human assistance.

The bottom line is that as today's threats are becoming more devious, the security measure and awareness have to become smarter. Although the enterprise may run anti-virus and have firewalls in place, threats at the network perimeter are especially difficult to prevent and repel – but very important to stop. Viruses, worms, malicious code, unauthorized network access and Denial of Service (DoS) attacks are often introduced into the enterprise through the Internet gateway, making it a highly vulnerable, yet often overlooked point in the network. To stay protected from all of the unpredictable threats coming from so many directions, the enterprise requires a timely security awareness, integrated solutions and overall improved security positioning at the gateway.

The future of Internet security, therefore, resides in human intervention and innovation. Implementing hardware and software solutions, as well as using human intervention to continually monitor the network, are two of the best ways to keep abreast of attacks from the outside. Every enterprise needs emerging technologies to protect privacy on the Internet. Depending on the type of business and the value of the data, an enterprise has the choice of using firewall, digital certificates, data encryption and network operating systems to protect their data while in transit, ensure the identity of a user and mask the data from unauthorized eyes. However, as technology continues to become more complex, the safeguards used today may be severely out of date tomorrow.

For this reason, enterprise network administrators should require their IT staff to stay abreast of innovations and new trends in the IT field by attending seminars and subscribing to computer publications. Most importantly, network administrators should make it a priority to sit in IT staff meetings, to read IT publications and to attend some of the training seminars.

And finally, Security awareness has never been more important and it's not the problem of a particular area or country rather it is universal concern. Therefore, as security threats become more complicated and enterprises become more inter-connected, it is imperative that organizations not only develop, but fully implement quality security awareness programs for the benefit of their users and organizations. By achieving this objective, the enterprises will have users that are "clued in" to the importance of information security and how it affects the organization, department and individual. Without this awareness, enterprise's users are "clueless" and an incident waiting to happen!

References

Douglas E. Comer, 1997. Computer networks and Internets, Prentice hall, Inc.

Douglas E. comer, 1995. Internetworking with TCP/IP vol. I, Prentice hall, Inc.

Introduction to Network Security, Matt Curtin, 1997. http://www.interhack.net/pubs/network- security/

Internet Security Issues, http://www.erin-it.com/security.html

James F. Kurose, 2001. Computer Networking, Higher education Press.

Overview of Computer Security Issues: http://www.madirish.net/tech.php?section=7 and article=70

Protect your assets, Barry R. Pekin, Nov. 2001. http://www.webchamber.com/Community/Security/Articles.asp?1

The New Definition of 'Network Security', 2002. http://enterprisesecurity.symantec.com

Ten Steps to Protect Your Enterprise from DoS Attacks, MAR27, 2001 http://enterprisesecurity.symantec.com

The Twenty Most Critical Internet Security Vulnerabilities, http://www.sans.org.

William Stallings, 2000. Networking Security Essentials, Prentice hall, Inc.