Internet firewall environment: an audit perspective

AM Bouwer & H de Jager

School of Accountancy
University of Pretoria

ABSTRACT

The aim of this article is to introduce auditors to the Internet, and more specifically to security implications for companies online. The article will look at firewalls as a control measure to protect these companies against the risks of the Internet environment. Guidance will also be given to auditors facing the challenge of auditing Internet firewall environments.

Key words: computer, firewall, hackers, Internet, networks, password, security.

1 INTRODUCTION

The phenomenal expansion of the Internet, estimated at growing from 23 500 web pages in June 1995 to 650 000 web pages during January 1997 (Grey 1998:1), has introduced millions to its vast resources. It has created a new dimension for various kinds of computer users in which information can be obtained and business conducted. Included in this group of users are, however, many "cyber bandits."

These pirates attack indiscriminately and without remorse. All organisations or individuals connected to the Internet are potential targets. These bandits can and must be deterred by the construction of well designed and trusted defences against their attacks. Like an impregnable fortress, a properly designed and maintained firewall can provide a significant protective barrier to these vandals (LaBar 1995:1).

In this new and dynamic environment, auditors will be expected to provide guidance to clients on the security implications of the Internet and, once security measures such as firewalls have been implemented, auditors will also be expected to audit and evaluate the adequacy and effectiveness of the security in an Internet firewall environment.

2 THE INTERNET

The Internet, the global network of networks, is currently a hot topic of discussion in the media and could be described as the latest frontier beckoning explorers. Its recent growth is astounding and even surprising considering the fact that it has been in existence for over 20 years. (Duncan 1994:1). Its impact on society can be compared to that of the invention of the telephone.

The US stock market was gripped by Internet mania in 1995. An example of this phenomenon is that of Netscape, a company which develops tools for navigating the Internet's World Wide Web. It went public during August of 1995, at a stock price of US $ 28. By 30 November of the same year it was standing at US $ 140 after gaining US $ 29 in the previous two days.

There is little doubt that the Internet is a major communications breakthrough. It connects the world through the communication of news and it allows citizens of the world to talk to one another. The Internet will also create an entirely new electronic marketplace that will allow businesses to reach customers directly, world wide.

The Internet is also propelling the sales of personal computers and peripheral devices. The latest way of thinking sees a move towards the production of a low-cost network computer that will utilise the processing power available on the Internet instead of providing such power in the personal computer. Such a

network computer will contain the random access memory (RAM) needed by each computer, but less expensive processors will be needed. This could have a major impact on current personal computer sales as such computers could be made available at prices as low as R 3500.00 (US $ 500). The significance of such low priced computers is that many more people will be able to afford home computers which in turn will make the Internet population, or so called "netizens", so much bigger.

The prospective sales market of businesses intending to function via the Internet could increase dramatically. Another factor which makes low cost computers very attractive is the upwardly spiralling cost of keeping up to date with computer hardware and software developments. Recent years have seen the life span of personal computer equipment shrinking at an astounding rate. A 486 processor which was state of the art technology as little as three years ago is now seen by many as a redundant piece of equipment and a pentium processor is now seen as entry level equipment. Although more powerful processors do provide users with increased processing power, the processing power is mainly needed due to the development of increasingly resource hungry software. It could therefore be argued that the main benefactors of these technological advancements are the developers and suppliers of computer hardware and software. A $500.00 computer could be a means of stopping this snowball effect, as such a computer could be used to access applications and storage space on the Internet instead of users having to invest in software and hardware for each individual computer (Cangemi 1996:1).

Bill Gates, chairman of Microsoft, the world's leading personal computer software company, has clearly seen the potential threat to his company and dismissed the idea of a US $ 500 network computer as "stupid" in the *London Financial Times*. Oracle Systems, however, already brought its low cost network computer to the market during 1997.

2.1 History and background

According to Hauben (1995:1) the Internet evolved from the US Defence Force Advanced Research Projects Agency Network (ARPANET). From an in-depth study of the development of the ARPANET he concludes that it is fundamentally connected to, and born of, computer science, rather than of the military.

In the early 1970s, ARPA directed Stanford University to begin experimentation in multiple network packet-switching technology. Packet-switching technology was very effective when network connections were unreliable. In 1977 an experiment among four government networks demonstrated the feasibility of the technology. This research resulted in the development of the TCP/IP protocol suite. TCP/IP stands for Transmission Control Protocol/Internet Protocol; and by January 1983 it had become the standard communications protocol.

During 1985 the National Science Foundation (NSF) established its own network, the NSFNET, as part of the SuperComputer's program. By 1990 the NSFNET became the dominant network, leading to the downfall of the ARPANET. The regional networks using the NSFNET backbone created the foundation of the Internet as we know it today. The NSF's primary focus was research and development and it resisted allowing access to commercial users. During the 1980s, however, the NSF advised the regional networks that they had to become self sustaining. This sparked the creation of commercial Internet providers in 1991. Commercial use of the Internet was finally possible (Hauben 1995:2).

2.2 Transmission control protocol/ internet protocol (tcp/ip)

The Internet uses TCP/IP as its communication protocol. TCP/IP is the usual shorthand phrase for a collection of protocols. It was originally developed by the ARPA project team and was deployed on the old ARPANET in 1983. A schematic diagram of the TCP/IP protocol is presented in figure 1. Each row represents a different protocol layer. The top layers contain the applications, WWW, telnet, e-mail etc., which call the lower layers to fetch and deliver the data. In this level one typically finds TCP or User Datagram Protocol (UDP). UDP is similar to TCP only somewhat less secure, as it performs no handshakes and contains no sequence numbers.

In the middle is the Internet Protocol (IP), which is a packet multiplexer. Messages from higher level protocols have an IP header, and are sent to the device drivers for transmission. Finally, the Internet Control Message Protocol

(ICMP), has the purpose of influencing TCP and UDP connections. It identifies the best route to a destination, reports network problems and handles ping requests. Ping is a program used by network administrators to determine if a network machine is "alive" (Cheswick & Bellovin 1994:19-20).

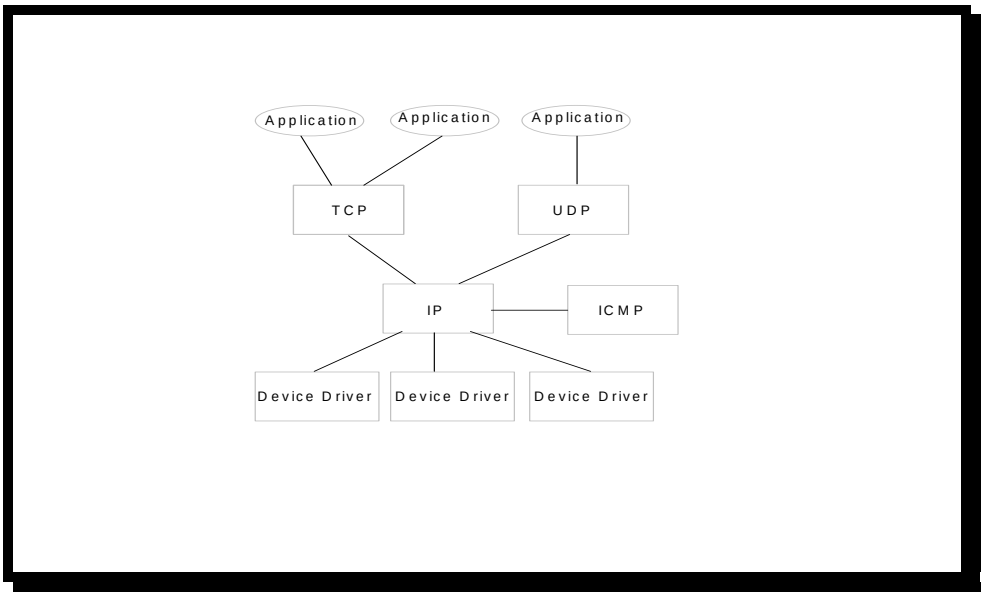


Figure 1 A schematic diagram of the different layers found in the TCP/IP protocol suite. (Cheswick & Bellovin 1994:19)

2.2.1 The Future of The Internet

It is a fact that the day that we, as a society, entered the information age was also the day that we ceased to be able to live without the technology we have created. Current trends project figures of 125 million users on the Internet by the year 2000. These same projections estimate that by 2010, a billion users will be online. (Schwartau 1996:10)

A rather more sobering question could be that of the role of business on the Internet. As can be seen from the above discussions, it is quite clear that many people are currently successfully utilising the Internet. Most people are also generally satisfied with, and excited about the services provided and the information available on the Internet. The one area of the Internet that still has to prove its value is that of its ability to facilitate business transactions. In most journals the lower than expected growth of business over the Internet is ascribed mainly to users' fear of inadequate security. An example can be found in the article "Business Online: When will the Internet grow up?", *Information Technology Review* (Heydenrych 1996:12). Heydenrych concludes that business will not only have to address clients' fears but will also have to adopt a significantly more proactive approach towards ensuring security and confidentiality in the Internet arena.

It can be argued that the Internet has brought many positive advances to the world. It is, however, also abundantly clear that this communication medium has altered the potential risk profile of individuals and businesses alike. Let's investigate the major risks that need to be addressed in an Internet environment.

3 INTERNET SECURITY RISKS

Any computer employed by a business faces security risks. These risks exist because each computer can house information resources which are valuable to their owners and in many cases to the business' competitors or enemies. The computer's processing capabilities are also valuable to many who do not own the machine or its software. The probability of computer security risks materialising is significantly bigger for computers connected to a network such as the Internet. More attack access points exist,

information flows through more machines and many more services, such as File Transfer (FTP), Mail, disk access, remote execution etc. are provided (Cheswick & Bellovin 1994:xi).

Commerce over the Internet is a risky business according to Knowles (1995:17). She is of the opinion that business via the Internet will only be low risk when all transactions can be authenticated by a trusted system or device. In the meantime, however, even the most security conscious company has to beware. Had they been more careful, Citicorp, a US bank, would not have lost $400,000 and have had to recover $12 million in illegal transfers after having its computer network infiltrated 40 times in five months. From Carnegie Mellon University's famed Computer Emergency Response Team (CERT), it is reported that they received 29,850 e-mail messages and 3,664 hot-line calls reporting computer security incidents or requesting information during 1995. The staff handled 2,241 computer security incidents affecting 40,241 sites (CERT 1995:1).

Closer to home, Telkom reported in the *Computer Week* of 8 July 1996 that "international fraud targeting Telkom's network resulted in direct losses of at least R200 million, and resulted in the arrest of at least 160 people". According to Vernon Fryer, senior superintendent and head of the computer crime investigations unit at the SA Police Service, a syndicate defrauded Telkom by using software downloaded from the Internet to hack into the company's network. A Telkom official added that, with the advent of the Internet, Telkom would have to advance its anti-crime programmes.

The Computer Security Institute reports that one of every five Internet sites has suffered a security breach . This finding is based on the results from a recent survey done on Internet Security. Information security professionals in 320 Fortune 500 corporations, government agencies and universities participated in this survey, which revealed that company security policies lag behind the use of technology. Many experts fear that the reality is even worse than the survey suggests They say many companies refuse to admit their security breaches, or are oblivious of them.

According to Fred Trickey, Data Security Administrator at Columbia University, system intrusion is only one type of Internet security transgression. If other types of incidents, like virus contamination through FTP downloads or company information disclosed through e-mail, the number of incidents to be included in the data might be closer to half of all connected sites. An interesting piece of information revealed by this survey is that 78% of the companies are connected to the Internet and that 50% of those provide high risk features such as FTP and WWW access to all employees. More than 60% of these sites do not have a firewall in place, although 70% of those without a firewall intend to install one in the near future (Chapman 1996:9).

A similar information security survey done in South Africa, *The 2nd Annual Ernst & Young / Financial Mail Information Security Survey*, found that South Africa is even worse off than the US. Ernst & Young audit partner John Davis is of the opinion that the results of this survey contrast with a similar survey conducted in the US, where it was found that information security is finally on corporate agendas. Where breaches in information security are likely to worsen as more corporates link their computers to the Internet, SA executives continue to ignore the problem (Davis 1996:82). The key survey findings were as follows:

- Management's attention to information security has not improved since the 1995 survey.

- More than 30% of respondents still indicated apathy towards security by senior management, and management awareness was still noted as an obstacle to information security.

- Organisations are increasingly dissatisfied with their information security administration.

- Organisations are increasingly embracing client/server technology and processing on LAN's and UNIX-based systems. A growing number of organisations are, however, not satisfied with the overall security of these client/server environments. Client/server technology makes it possible for many users to share applications and computer resources at the same time. Many of the services available on the Internet are based on this technology.

- Concern over Internet security is increasing in tandem with business use of its facilities. Two in three Internet-connected organisations reported break-ins to their organisations through the Internet during 1995/96.

- More than 33% of respondents encountered a virus over the same period.

- Business continuity planning is receiving ongoing attention, with over 90% of respondents indicating having some type of backup strategy in place.

- Over the period 1994 to 1996, almost 50% of the organisations surveyed suffered an information security related financial loss.

- Less than 50% of respondents have formal information security policies, and only 50% of those have on-going security awareness and education programmes for employees.

- The major obstacles to effective information security are a lack of human resources and a dearth of proven information security tools and solutions (Ernst & Young/Financial Mail 1996:2).

As organisations connect to the Internet or Information Superhighway, they will find that they are exposed to a multiplicity of security threats. Enterprise networks today are fairly contained. There are not 40 million people knocking at their door and they do not have 167 different countries connected to their network, which can be the case once you go online.

The threat multiplier of the Internet can be likened to connecting to a "criminal centre". The Internet is anarchistic and chaotic. The Internet has recently been proven to be a tool for terrorism. Associated Press reported that terrorism groups are using the Internet as a prime means of communication. Like all weapons, the Internet can be used for good or evil. It is up to us to learn how to outpace our enemies in the mastery of this weapon.

All too often management asks, "Why do we need to secure things? Why do we need to spend money on things that hit the bottom line?" The results of a study performed by the Defence Information Systems Administration (DISA) are staggering. They launched 8932 dedicated attacks from the Internet on military computers and found that 88% (7860) could be penetrated within 10 minutes. Of the almost 8000 successful attacks, only 390 were detected and only 22 were reported. This gives some indication of what it could be like on the Internet. These figures suggest that for every single external remote breach of security, there are 399 more of which we are unaware (Schwartau 1996:10).

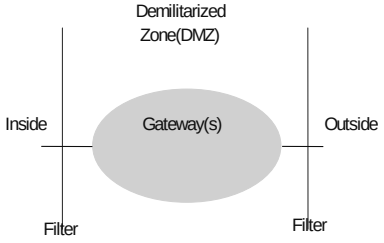
4 SECURING AN INTERNET CONNECTION

It is easy to secure a computer system. You merely have to disconnect all dial-up connections and permit only direct-wired terminals, put the machine and its terminals in a shielded room and post a guard at the door (Grampp & Morris 1984:12). Few computer systems are run that way today. Security is in general a trade-off with convenience in which some loss of security is inevitably suffered.

As discussed previously, a business connected to the Internet faces many risks. A cost effective balance between security, efficiency and client service must therefore be found. Since connection to the Internet is in many cases initiated by a business because it wants to communicate and transact with clients and other business partners, it is necessary to trust the machines of those business partners. Although trusting outside machines lies at the heart of Internet security risks, it also provides us with a security strategy which is fast becoming the most popular and effective means of securing one's internal networks.

An Internet connection can be configured in such a way that only one machine, the firewall gateway, needs to communicate with the outside world. Computers situated on the internal networks only have to trust the firewall while the firewall's sole purpose is to protect the internal networks from unauthorised entrants.

Although other security methods also exist to



protect a business' Internet connection, firewalls are the most common and flexible (Cheswick & Bellovin 1994:xii). In most instances where an Internet connection poses a significant threat to the audit engagement's control risk and/or audit risk, auditors are likely to encounter a firewall as the most important control measure for mitigating the control and/or audit risk. For this reason this article will focus on firewalls and the manner in which the audit of an Internet firewall environment should be approached. In order to understand the concept and functioning of a firewall we will now investigate the nature of this security measure a little more closely.

5 A FIREWALL OVERVIEW

Broadly speaking, a firewall is a system or group of systems that enforce an access control policy between networks. More specifically, a firewall is a collection of components or a system placed between an entity's private network and a public network such as the Internet. It possesses the following properties:

- all traffic from inside to outside, and vice-versa, must pass through it;
- only authorised traffic, as defined by the local security policy, is allowed to pass through it; and
- the system itself is immune to penetration.

In summary, a firewall is a mechanism used to protect a trusted network from an untrusted network such as the Internet (National Computer Security Association 1995:3).

Another definition of a firewall is as an access control policy concerning networks. Firewalls often have two functions: one to allow certain classes of traffic across the firewall, and the other to block specific traffic from gaining access to the protected network (LaBar 1995:1). LaBar also believes strongly that a firewall must form part of the overall organisational security architecture.

One important term that is often used in conjunction with a firewall is *gateway*. Internet firewalls are often referred to as secure Internet gateways. But there is a more specific use of the term gateway. As one can see from Figure 2, a firewall consists of several different components, including filters or screens that block transmission of certain classes of traffic. A gateway is a machine or set of machines that provide relay services to compensate for the effects of the filter. The network occupied by the gateway is often referred to as the demilitarised zone (DMZ) (Cheswick & Bellovin 1994:52).

Figure 2: A Firewall schematic (Cheswick & Bellovin 1994:52)

A final fact upon which all authors on the subject agree, is that no firewall can be secure without an established formal security policy. The organisation must know what it wants to achieve before implementing the firewall. The firewall cannot make this decision for the organisation or its networks.

5.1 Types of firewalls

According to LaBar (1995:4), types of firewalls are split up according to where on the protocol layer the firewall operates. The protocol layers referred to are those specified by the ISO OSI Reference Model. Table 1 depicts this reference model as follows:

Layer	Action
7	Application. Firewalls on this level employ software to analyse and filter traffic flowing through them.
6	Presentation
5	Session
4	Transport
3	Network. Firewalls on this level typically employ routers to filter traffic based upon addresses and port numbers.
2	Data Link
1	Physical devices

Table 1 The OSI ISO Reference Model

Typically, on the network layer one finds routers (hardware) that filter traffic passing through them, based upon the source address, destination address and port numbers.

On the application layer one finds firewalls that provide better security than network level firewalls. These firewalls employ software that examines the traffic that passes through them more closely. LaBar's experience has shown that, in practice, network and application level firewalls are installed together, because their characteristics complement each other, thereby making a more secure firewall.

Cheswick and Bellovin (1994:51) classify firewalls into three categories: packet filtering, application gateways and circuit gateways. Their classification of the first two types of firewalls is basically the same as LaBar, but they also identify another type of firewall, namely the circuit gateway which relays information at the connection level. Once a connection is established on behalf of a client, the proxy simply copies packets from one network interface to the other. According to them it is not unusual to see a combination of these firewalls implemented. The firewall is sometimes referred to as a proxy. A proxy is the application on the router or the host, which makes the access decisions based upon the firewall's security policy.

5.2 Situating firewalls

A firewall is traditionally placed between an organisation's computer network and the outside world. Depending on the sensitivity of information kept on internal networks, firewalls may also be found within an organisation's own networks.

Many good reasons exist for the implementation of a firewall. Its purpose is to protect the internal network from uncontrolled access from the outside world. The matter of transitive trust must be kept in mind, however. Transitive trust refers to the risk of uncontrolled access to an internal network through another, trusted network, which has been compromised. It is necessary to consider all access paths to the internal network before deciding on the positioning of the firewall (Cheswick & Bellovin 1994:52).

Figure 3 contains a few examples of networks connected to each other, either directly or indirectly through the Internet. The arrows indicate the placements of firewalls, with the arrow pointing to the untrusted networks. The dotted lines indicate the potential result of transitive trust.
.

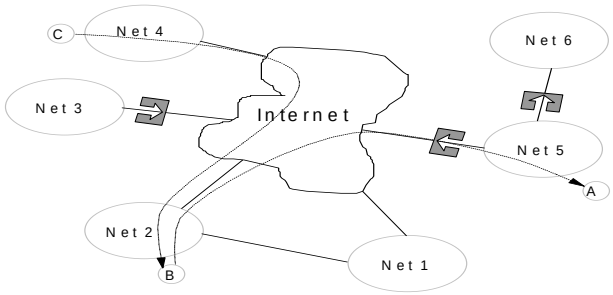


Figure 3 Positioning firewalls and transitive trust (Cheswick & Bellovin 1994:54).

Although Net 5 in figure 3 is protected by a firewall against unauthorised access from both the Internet and from Net 6, a seemingly internal network, machine A could be compromised if it trusted machine B. This could happen if machine C compromised machine B, which has no firewall between itself and the Internet, and then accessed machine A, impersonating the trusted machine B. The consequence of transitive trust is that, no matter how strong a network's security or how well its firewall has been placed, if machines outside the firewall need to be trusted, one also needs to trust those machines' security measures (Cheswick & Bellovin 1994:53-54).

5.3 Limitations of a firewall

If one looks at the protocol layer as depicted in table 1, it is clear that a firewall is a very strong defence against attacks from the lower layers. A circuit-level gateway is more or less immune against attacks from the network level. In contrast, firewalls provide almost no protection against attacks from the higher layers. If the proxy or code used to operate the firewall is full of bugs, no firewall in the world will be able to secure the internal network.

Firewalls are powerful tools with which to achieve certain security objectives. However, there are many things they cannot do and it is important to be aware of this. There are few greater dangers than to live in a vulnerable world while under the impression that all is safe and secure.

An interesting question is what protection a firewall provides against attacks from its own layer. The answer depends on how carefully the gateway code has been written. A mail gateway, which runs at the application level, must therefore be extremely careful to implement all of the mail protocols and other functions absolutely correctly. On this level the greatest danger is human error or oversight. Extensive quality control and testing procedures are called for.

Flaws in the code of services provided on the host can never be foreseen in all cases. Even if one could eliminate all the current flaws, one would still be vulnerable to next year's flaws. At best, a firewall provides a convenient single place to apply a corrective filter (Cheswick & Bellovin 1994:82-83).

6 AUDITING AN INTERNET FIREWALL ENVIRONMENT

An Internet firewall environment has been shown to contain the same characteristics as traditional computer network environments, only on a substantially larger scale. It can therefore be assumed that the same audit principles will apply in both environments. In order to design an audit programme for an Internet firewall environment, the auditor must comply with generally accepted audit standards. These standards include obtaining a detailed knowledge and understanding of the Computer Information System (CIS) and the environment in which it functions. Once such knowledge and understanding has been obtained, the auditor will be in a position to determine the objectives of the system's internal controls (SAAS 4011 1998:4).

6.1 Audit approach

In developing a set of audit procedures, the auditor must take into account his/her acquired knowledge and understanding of the internal control objectives, which will enable him/her to evaluate the environment's achievement of its control objectives. The audit approach should not be to determine the technical efficiency of the firewall but to determine if the firewall is achieving its

objective of securing the business' internal network.

Furthermore, the audit of an Internet firewall environment can easily focus on security alone. Auditors must ensure that they are not intimidated by the technical nature of an Internet firewall environment. As discussed earlier, the same risks and internal control objectives exist in this environment as did in more traditional computer environments. The same audit principles still exist and it follows that a similar audit approach should be followed.

In developing this audit approach, the auditor must consider the impact of general controls and applications controls on the audit engagement as a whole (SAAS 4011 1998:7). In this case the auditor must determine the impact of an insecure Internet connection or an inappropriate implementation of a firewall on his/her audit risk.

Based on this approach, we will now examine the steps necessary to perform an audit of an Internet firewall environment.

6.1.1 Study and understand the specific internet firewall environment

An analysis of all services offered and protocols used on the host as well as the firewall topology, must be studied and documented thoroughly. The best approach to understanding the firewall is to study the firewall's user manuals and parameter printouts. In other words, find out what the firewall can protect against and then determine how the parameters of the specific implementation are set. This is of utmost importance to ensure that the audit programme will be applied correctly in the specific environment.

6.1.2 Study and understand internet security risks

Keep in mind that the Internet is a dynamic environment which changes constantly. Keeping up to date with Internet security risks can be done effectively by visiting the various Internet discussion sites on Internet security and firewalls.

6.1.3 Perform a risk analysis on the specific internet business environment

From a business point of view, the security over authentication of messages could be more important in an environment where financial transactions are being concluded over the Internet, than it would be for an environment where the Internet host is primarily used to advertise the company's products. From a security point of view, however, any access to an Internet host could be potentially dangerous. Once an Internet user has logged onto an Internet host, he or she could alter or destroy data if the host's security is inadequate.

When an auditor performs this risk analysis, certain distinctive trends in Internet security risks must be kept in mind. Research has shown that most security risks could be grouped into a few categories. A summary of these categories is as follows:

a) Security Policy

The importance of a well defined and formal security policy in an Internet firewall environment can not be over emphasised. Most Internet security risks can only be controlled effectively if a policy exists that addresses the issue of who, what, where and when access to and from the host can be allowed. As a measure of its importance, the security policy forms one of the building blocks upon which the Department of Defence Trusted Computer System Evaluation Criteria have been developed (DoD 1985a). This security policy must be documented and approved at top management level. Security measures implemented in an Internet firewall environment must exactly reflect this policy.

b) Address Spoofing

Many protocols can be abused to change the address of the sender in messages being transmitted to the host. If the Internet firewall environment relies on the address of the sender to authenticate any information received, big risks may exist. An auditor must identify those services and access to sensitive information provided at the business' Internet site. The question must then be asked how access to those services and information is authenticated, keeping in mind that spoofing could have taken place.

c) Port Number Spoofing

In the same fashion as address spoofing, port numbers can be changed in many protocols. This effectively allows the sender to abuse the information about his or her status or objectives. Because the Internet uses, but does not enforce, certain standard ports for specific Internet services, this could lead to great dangers if authentication is based on port numbers.

d) Passwords

Most password systems have major inherent weaknesses, but they are by far the most practical solution available. In an Internet environment they are once again the axis on which security turns. It is not surprising that most compromises of an Internet host take place due to password security failures.

Without a strong and regularly tested password system in place, an Internet environment is open to abuse, even with a firewall in place.

e) Software Bugs

If one notes the frequency of Internet security risks caused by weaknesses inherent to the software, one can not but distrust all software programs. No external software can be trusted to provide the level of security required in an Internet firewall environment. All software, be it WWW, FTP or telnet, must be treated as hostile until proven otherwise. The auditor should evaluate the risk of software bugs by referring to the origin of the software (eg. Purchased firewalls vs home grown software) and the process of quality and change control within the CIS environment.

f) Hackers

Many Internet security weaknesses can be exploited by hackers. In the Internet environment the term "hacker" is synonymous with an intelligent or inventive person who has manipulative powers over business. In the opinion of many specialists in the field, hackers are no more than modern day criminals. The fact of the matter is that hackers only exist because of weak security policies or badly implemented security policies and software. We allow hackers to threaten our assets.

The auditor must evaluate the probability that hackers might target the Internet site. Financial institutions might for instance carry bigger risks due to the potential manipulation of financial instruments once a successful hack has been performed. A site might also hold data valuable to criminals, such as credit card numbers, client information etc.

g) Denial of Service

Many attacks on a machine will do little more than result in the machine or service being unable to perform optimally or at all. Hackers have shown the tendency to perform denial of service attacks on hosts just to prove they could do it, because they became frustrated with not achieving their ultimate goal or to hide their tracks. The impact of such an attack could be much greater than expected. A modern business which is unable to communicate or process its transactions is a business in serious trouble. It is clear that these kinds of attacks must be catered for in any disaster recovery plan. The auditor must evaluate the impact a denial of service attack will have on the business owning the Internet connection.

h) Network Monitoring

Many of the control objectives in an Internet firewall environment refer to effective monitoring of services, messages and logs to protect against risks or to detect an intrusion before serious damage can be done. No firewall environment can be classified as operating effectively without a well defined set of audit logs and monitoring tools in place. After the complete and accurate implementation of a firewall, this is probably the most significant aspect of maintaining adequate security in an Internet firewall environment. The auditor must evaluate the risk of not identifying unauthorised intrusion into the Internet firewall environment.

6.2 Performing the audit

Once the Internet security risks have been identified, the auditor must develop an audit programme that will ensure that control over these risks is tested for effectiveness and consistency. This is done by setting control objectives for each identified security risk and developing audit procedures to test the achievement of those objectives.

When the audit procedures are performed, the auditor must ensure that he or she has adequate access to the Internet host. An audit in an Internet firewall environment can only be directly performed. This is due to the fact that

most firewalls are parameter driven and the auditing of the parameter settings must be done through physical checking of the particular setting or through simulated audit tests.

The auditing of an Internet firewall environment can be performed very effectively with the help of automated auditing techniques. Computer programs that check for vulnerable settings or files can give the auditor a quick view of the general status of the environment. A few of these programs, which are in many cases freely available from the Internet, are as follows:

- TAMU is a collection of tools that can be used to build a firewall as well as to identify attack signatures.

Available for ftp from
ftp://NET.TAMU.EDU/pub/security/TAMU

- COPS is another auditing package along the lines of the scripts included in TAMU.

Available for ftp from
ftp://*FTP.CERT.ORG/pub/tools/cops*

- Tripwire is a package that, inter alia, evaluates a system and checks for altered files.

Available for ftp from
ftp://*FTP.CS.PURDUE.EDU/pub/spaf/COAST/Tripwire*

- The ISS package is a network vulnerability programme that can probe whole networks for vulnerabilities. The ISS package was initially made available as shareware but current versions are commercially available from the suppliers. Demonstration software can still be obtained free of charge.

Available for ftp from
ftp://*FTP.UU.NET/usenet/comp.sources.misc/volume39/iss* or
ftp://*AQL.GATECH.EDU/pub/security/iss*

- Crack is a program that attempts to crack passwords and the cracklib library provides routines to check the safety of a proposed password.

Available for ftp from
ftp://*FTP.CERT.ORG/pub/tools/crack*

It is, however, of utmost importance that the auditor also understand the specific Internet firewall environment and its control objectives. Due to the individual characteristics of every environment, as well as the dynamic nature of the Internet, a computer program might not always identify all critical risks. An auditor who relies only on the results of such a program might be running a real risk of expressing an inappropriate opinion.

7 CONCLUSION

Based on the astounding expansion of the Internet and the predicted growth of business on the Internet, it is reasonably certain that most computer auditors will soon be confronted by Internet firewall environments. The auditor will be expected to assist in the development of a complete and accurate security policy for firewalls, and management will expect of the auditor to verify that the security policy has been implemented correctly and completely by the firewall.

To perform these functions an auditor needs to have a thorough knowledge and understanding of Internet security issues. Based on the limited available literature on the auditing of Internet firewall environments, it can be concluded that the auditing profession has not yet adequately addressed its duties in this regard. Considering the growth experienced on the Internet, this profession has a lot of catching up to do.

A paradigm shift also has to take place in the traditional audit approach to computer security. Although the securing of networks is not new to computer auditors, the Internet introduced another subtle, but big, difference to traditional network security. Where system administrators and auditors have previously only had to deal with employees of an organisation, they now have to protect the network from external people. Not only must Internet users be allowed through the firewall, but they are invited through advertising to visit the Internet host. No longer can these system administrators and auditors take the traditional uncompromising stance towards users of the network. It could be concluded that these people will, for the first time, have to understand and become involved in customer service. A balance between network security

and satisfying customers' needs has to be found.

The ubiquity of the Internet has ensured that security risks have been widely exposed. It could be concluded that, with the advent of the Internet, management became more aware of computer security risks in general.

This will obviously ease auditors' task of convincing management to implement effective security policies and procedures. It also places a burden on auditors to only recommend practical and cost beneficial security measures to management. The Internet and its security risks have been manipulated by many consultants to create paranoia in management in order to sell their products. It has become increasingly important for auditors to maintain their independence and assist management in seeing a clear picture regarding Internet security risks and control measures.

References:

CERT. 1995. CERT Coordination Center 1995 Annual Repor,. *Computer Emergency Response Team.* Available for http on *http://www.cert.org/cert.report.95.html*

Cangemi, Michael P. 1996. *Issues and Comments*, IS Audit and Control Journal, Vol. 11, p. 1.

Chapman, Christy. 1996. *Security over the Internet*, Internal Auditor, February 1996, p. 9.

Cheswick, William R. & Bellovin, Steven M. 1994. *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley Publishing Company, New York.

Davis, John. 1996. *Crimewatch*, Financial Mail, January 26, p. 82.

DoD. 1985. *Department of Defence Trusted Computer System Evaluation Criteria*, DoD 5200.28-STD, DOD Computer Security Center, Available for ftp from *ftp://ftp/cert/org/pub/info/orange-book.z*

Duncan, Rebecca J. 1994. *Addressing the Issues: Internet Security*, DATAPRO, Vol. 5850, p. 1, McGraw-Hill.

Ernst &Young/Financial Mail. 1996. *Key Survey Findings*, 2nd Annual Ernst & Young / Financial Mail Information Security Survey, January 1996.

Grampp, Fred T. & Morris, Robert H. 1984. *UNIX operating system security.* AT&T-Bell Laboratories Technical Journal, October 1984.

Grey, Matthew. 1998. *Web Growth Summary*, Available for http from *http://www.mit.edu/people/mkgray/net/web-growth-summary.html*

Hauben, Michael. 1995. *The Netizens and the Wonderful World of the Net: An Anthology.* Available for http from *http://www.cs.columbia.edu/~hauben/netbook/*

Heydenrych, F. 1996. *When will business on the Internet grow up?*, Information Technology Review, Vol. 3, No. 2, p. 12, March 1996.

Knowles, Anne. 1995 *Risky Business*, PC Week Online, Available for http from *http://www.pcweek.com/archive/40/pcwk0032.htm,* 10 September 1995.

Krick, John H. 1994. *Introduction to the Internet*, DATAPRO, Vol. 1420, MacGraw-Hill Inc, NJ 08075 USA

LaBar, D. 1995. *Packet Filtering in Internet Firewalls.* Available for ftp from f*tp.cert.org/pub/firewall.zip*

National Computer Security Association. 1996. *NCSA Firewall Policy Guide Version 1.01*, Available for ftp on *ftp.ncsa.com as /pub/~fwpgv101*

SAAS 4011. 1998. *Risk Assessments and Internal Control - Computer Information Systems and Characteristics and Considerations*,The South African Institute of Chartered Accountants, Statement of South African Auditing Standards, April 1998.

Schwartau, W. 1996. *Information Warfare: Chaos on the Electronic Superhighway*, IS Audit and Control Journal, Vol. 1, p. 10 1996.