CHAPTER 4

RISKS IN E-COMMERCE PAYMENT SECURITY

INDEX

4.1 INTRODUCTION

The steps that the IS Auditor follows during an audit of e-commerce (EC) payment security is, firstly, to gather information related to the area being audited. Secondly, it is to identify the risks prevalent in the environment being audited, and thirdly, to identify possible controls that may be implemented to mitigate the identified risks. The last step (for the purposes of this dissertation) is to develop an audit approach to serve as a framework for the area under review. Other steps in the audit approach includes audit testing and reporting on the results of the testing. All these steps are designed so that there is an inter-dependency between the steps. The output of each step will serve as the input of the following step. For example, the risk identification process can not take place effectively without the background information.

In Chapter 3 information was provided to serve as background to EC payment security. In that chapter it was shown that the nature of the EC environment results in specific risks. These risks and the controls implemented to minimise them, is the main focus of the IS audit. This chapter will provide more detail regarding security and the risks around EC payments. This risk identification process, described in section 4.4 below, serves a twofold purpose. Firstly, it is clear that the risk identification process is essential to developing the audit approach, because, without this risk identification process, the IS auditor cannot determine where the focus of a review should be. Secondly, the risk identification process also assists the auditor to obtain a better understanding of the environment being audited.

Once the risks described in this chapter have been identified, the next step will be to identify possible controls to mitigate the risks (control identification is addressed in Chapter 5). The risk and control identification will then provide the foundation that will enable the IS auditor to formulate the audit approach for the audit of EC payment security (the audit approach is addressed in Chapter 6).

This chapter will firstly provide examples of security issues in e-commerce payments. Thereafter the need for security will be stressed, and a definition of security and the implications of the Internet on security will be provided. The IS auditor will then be able to identify the risks (threats and concerns) prevalent in the EC payment security environment.

4.2 SECURITY AND E-COMMERCE (EC)

EC is widely viewed as threatening the privacy of an individual. Several surveys indicate considerable concern by users about their privacy online. This aspect was also highlighted in Chapters 1 and 3. Additional examples emphasising these concerns follow.

- "In March 1997, the Boston Consulting Group (BCG) surveyed 9,300 people about privacy concerns. BCG found 76% of respondents expressed concern about sites monitoring browsing on Net; 78% said privacy assurance would increase their willingness to disclose private information on Net. Without privacy assurance, BCG expect $6B of Web business compared with $12B if privacy were assured" (Kabay, 1998).
- The Lou Harris organisation surveyed 1,009 computer users in a United States national sample. "More than 50% of users are concerned about the release of their e-mail address by those responsible for the Web sites they visit. In general, observers feel that lack of consumer confidence is seriously limiting growth of e-commerce" (Kabay, 1998).
- In one large survey "70% of respondents were worried about safety of buying things online; 71% were more worried about Internet transfer of information than phone communications; and 42% said they refused to transmit registration information via the Internet. Several other observers report that lack of perceived privacy is a major block to the growth of e-commerce and that security is essential for e-commerce. Barriers to more effective e-commerce include poor security standards" (Kabay, 1998).

The 1998 FBI/Computer Security Institute survey found that "72% of security breaches resulted in financial loss. Although survey respondents reported net losses greater than $136 million, the monetary value of losses from information security breaches is difficult to estimate since companies are reluctant to admit compromise or loss due to concerns regarding client trust" (Zimits & Montano, 1998).

Table 1 below represents the average loss of different types of security attacks as presented in an FBI/CSI Computer Crime and Security survey (Zimits & Montano, 1998). This gives an indication of where the main focus of criminals resides when it comes to computer crime. This table shows that the main type of attack (where the

biggest losses are suffered) is through insiders such as employees. Although system penetration by an outsider is listed at the bottom of the table, it does not mean that this type of attack is not as serious. Companies may be reluctant to admit breach of their security by outsiders due to the possible impact of the negative publicity on their business.

Table 4.1 The Average Loss of Various Security Attacks

Type of Attack	Average Financial Loss ($)
Unauthorised Insider Access	$2,809,000
Theft of Proprietary Information	$1,677,000
Telecom Fraud	$539,000
Financial Fraud	$388,000
Sabotage	$86,000
System Penetration by Outsider	$86,000

Source: 1998/CSI/FBI Computer Crime & Security Survey

The following quote highlights the magnitude of the concern over Internet security. "A Net connection is a gateway to the external world, a doorway through which anyone with Internet access can attempt to break into your internal computer system" (Siebel & House, 1999).

Given this consensus (as highlighted above) that the Internet is not secure on its own (this will also be further highlighted below), this chapter focuses on the risks in this unsecure environment. This risk identification part is an important aspect for the IS auditor. This is also emphasised by Martin (2000). "E-commerce comes with its own set of challenges for auditors, and perhaps security is the most important of all." Auditors should be aware of security management issues and have a sound understanding of the various security risks and the tools available to be used in e-commerce sites to provide the necessary protection.

4.3 THE SECURITY IMPLICATIONS OF THE INTERNET AS AN OPEN NETWORK

This next section will provide background information that explains why the Internet is considered to be insecure. To understand the openness of the Internet is essential for the IS auditor so that this information will aid in the identification of the risks involved.

The Internet is considered a world-wide, global information infrastructure. Industry and governments aim to reduce overheads and shrink budgets but still need to continue to provide high levels of service to their customers and trading partners. In order to fulfill their promise "open networks must provide an efficient, highly scalable way to transmit quantities of information from point to point while doing so with a high degree of assurance" (Masse & Fernandes, 1997).

Open networks, such as the Internet, obey rules, which differ quite materially from the traditional, switched, point to point telecommunications infrastructure (Masse & Fernandes, 1997); (Rutgers, 1998). The telecommunications infrastructure is not extra-ordinarily secure and lends itself quite readily to both legal and illegal interception of traffic by such methods as wire tapping. Open networks like the Internet rely on their openness to achieve their ends: packets must be easily inspected by each node encountered on their route across the wired and networked globe so that they will be handed off in the probable direction of their intended destination (Rutgers, 1998); (Mehta, 1999). According to Oscar (1999) and the FDIC (1999) "The Internet is inherently insecure. By design, it is an open network, which facilitates the flow of information between computers". This openness is generally recognized as "providing a medium which is too insecure to permit digital commerce to flourish as it ought to do normally" (Masse & Fernandes, 1997).

According to Masse (Masse & Fernandes, 1997) "in order to flourish, commerce requires a communications medium, which is sufficiently secure, in relative terms, to assure both the integrity of the message and the authentication of its source and destination." This opinion is also shared by KPMG (1995).

In data communications however, the traditional authentication and verification tools no longer work. It is possible to verify that a message was received integrally in a point to point data communication by periodically transmitting data back to the sender for verification against the bits originally sent, but there is no way of knowing precisely who the reply is coming from (Vandenoever, 1995). As an example of data communications failure - every day clerks in businesses all over the world transmit faxes to the wrong destination by inadvertently keying in the wrong telephone number. No one knows this until the intended recipient denies receiving the message. In the case of the open network, communications may be diverted, copied, altered, replayed, rerouted, etc. The Internet is notoriously insecure. This aspect is

emphasised by McGhie & Maier (1998); Siegel (1997); Blunt (1997); Walder (1999); Hartman (2001); Kabay (1998); Baltimore (1999); Miller (2000); Masse & Fernandes (1997). The view of PWC (2000) on this aspect is that "the more open your network, the greater the chance that someone with malicious intent can break in and wreak havoc on the systems that run your business". This openness aspect will be elaborated upon below.

The Internet is the dominant and most important global example of an open network and there are a good number of examples in the retail sector of businesses doing well with Internet commerce at the present time. Many examples of such businesses were provided in Chapters 1 and 3.

Areas of concern over the use of open networks for commercial traffic relate to the health and financial sectors. There are formidable amounts of information recorded, stored and transmitted in the health care industry. The information is created and used by such diverse participants as medical professionals (doctors, nursing and para-medical staff), hospitals, clinics, insurance companies, governmental agencies, and patients. The same is true in the financial and accounting industry and the legal profession. Such information flows make up a very large component of business communications. These types of information require a higher standard of care. Medical, financial and legal information most frequently require to be reasonably protected from disclosure to the wrong parties. The present nature of Internet and other open networks fairly precludes their generalised use to carry such traffic. In fact, legal opinions have been given to the effect that "the Internet is not an appropriate medium for transmitting privileged information" (Masse & Fernandes, 1997). Zeus (2001) also shares this view. There are however ways to ensure that the confidentiality and integrity of messages is protected and these aspects will be highlighted in Chapter 5 - Controls.

Because the Internet has been designed to be 'open', the security aspect is also necessarily severely compromised. It is therefore necessary for the IS auditor to understand this inherent risk the weakness in security causes, because this knowledge will aid the IS auditor in the risk identification process as well as the subsequent control identification process (controls are addressed in Chapter 5). The risks will be identified in section 4.4 of this chapter.

4.4 INTERNET SECURITY - THREATS AND CONCERNS

4.4.1 THE NEED FOR INTERNET SECURITY

It is important to understand why we need security and the following paragraphs will highlight this importance. According to PWC (2000) "...there is no e-business without security". Feinmann (Feinmann et al, 1999) summarised the need for security as follows: "Not long ago only large corporations and companies needed to concern themselves with IT security issues. Their efforts to maintain ownership of information were the main focus of the field. This is no longer the case. Technology has become so prevalent that it affects almost every aspect of daily life. Computers are at the core of most businesses, ranging from trading systems used on the stock exchanges to the sports web page that delivers last night's scores. Computers are responsible for maintaining such things as bank accounts, medical records, and credit histories. Clearly, everyone who has a credit card or uses an Automated Teller Machine (ATM) must be concerned with the accuracy and privacy of their personal information; consequently, they must also be concerned with IT security."

According to Baltimore (1999) "we need information security not only to protect our assets, but also to enable us to take advantage of the new market opportunity. We need to have the same level of trust in the electronic world, as we have in the traditional world." The advantages of capturing a share of the e-commerce market have been highlighted in the previous chapters. For businesses that have a presence in this market on the Internet, the 'world' will be at their door and the consumers of the world are within their reach. The negative side is that "along with legitimate consumers, all kinds of malicious users may also be trying to gain access to on-line trader's information. Good security is therefore required" (Ghosh, 1999). The reason why web security requires special attention is mainly because the Internet is a two-way network, which allows organisations to publish information to users but also for criminals to access the equipment on which the information is stored. "The stunning growth of the Internet has spurred a new economy in which all aspects of the traditional payment infrastructure are being challenged." "... payment strategies are rapidly becoming a critical success component for companies buying and selling online" (Duques & Staglin, 2000). According to Ghosh (1997) "the number one rated concern for both businesses and consumers in establishing and participating in e-commerce is the potential loss of assets and privacy due to breaches in the security of commercial transactions and corporate computer systems."

There is a general opinion that the Internet environment is not secure and that the major concern for organisations doing business over the Internet is security of their systems and operations. This aspect is emphasised by McGhie & Maier (1998); Siegel (1997); Blunt (1997); Masse & Fernandes (1997); Walder (1999); Hartman (2001); Kabay (1998); Baltimore (1999); Miller (2000). In the same context "the lack of means for making secure electronic payments over the Internet is preventing the WWW from realising its full commercial potential" (Dixon, 1999).

"Today's business environment has different security requirements than traditional commerce" (PWCGlobal, 1999). According to PWC (1999) "the increasing use of the Internet – as an inexpensive virtual private network for electronic commerce… – has raised additional concerns about network security". "E-commerce generates some common IT risks, as well as some specific e-commerce risks" (Martin, 2000).

The following definitions are given to help understand security.

- "Security is about protecting valuable assets against loss, disclosure or damage" (Oliphant, 1999).
- "…security is about managing risk to mitigate some business information you are trying to protect from unauthorised parties, and it is also about decreasing the number of opportunities for the attacker to gain entry to your protected data". (Maung, 2001).
- Web security is defined as "a set of procedures, practices, and technologies for protecting web servers, web users, and their surrounding organisations. Security protects you against unexpected behaviour" (Garfinkel & Spafford, 1997).
- Security is dynamic: every month there are new types of attacks, new viruses, and/or newly published security breaches. Internal configurations are also modified with new applications (even new versions of operating systems or upgrades), and new hardware installed (modems on a workstation creating a "backdoor") (Martin, 2000).

These definitions have one thing in common and that is to show that security is about the protection of assets through minimising the risks, whether those assets are information, computer equipment, or any other assets required in a business environment. In an environment such as the Internet, information is a very valuable

resource. Effective security creates an environment that facilitates electronic commerce and private communications. This means not only creating a climate that is safe from robbery and fraud, but also a place where business transactions may take place under commonly accepted legal standards. Although an unsecured Internet will not stop electronic commerce, "the expectations are that the well-publicized lack of security on the Internet discourages business and consumer transactions" (Zimits & Montano, 1998).

4.4.2 BACKGROUND TO INTERNET SECURITY RISKS

To understand the risks regarding the Internet, this section continues with background information that emphasises the points highlighted in the previous section and so provides a broader and more detailed definition of risk. Thereafter it elaborates on the threats regarding the Internet. The specific risks are then listed and discussed in the remainder of this section.

The new global culture of electronic information exchange and networking poses a greater threat than ever before of fraud, e-mail eavesdropping and data theft for both companies and individuals. Enterprises around the world "are deploying a new generation of distributed, business-critical applications - enabling delivery of new products and services on an unprecedented scale - over intranets (employees), extranets (trading partners), and the Internet (worldwide customers and prospects). These applications must be operated in a high-availability, high-security environment, in order to gain customer confidence and allow enterprises to exploit the advantages of the electronic marketplace - faster time-to-market, lower distribution costs, and greater access to global customers" (Verisign, 1999).

According to Walder (1999) "the most obvious problem with Internet security is that as soon as you connect your network to the Internet, you are effectively opening a data pipe to the outside world. This is necessary to provide outbound connections for all your network clients, but is just as likely to allow unwelcome intruders to wander around your confidential data if you are not careful."

Information security is a major issue facing electronic societies (Masse & Fernandes, 1997). As the information highway transcends borders, locked doors are no longer sufficient to protect one of the corporation's most valuable assets - information. Information security is needed not only to protect assets, but also to enable

organisations to take advantage of this new market opportunity. "One of the major inhibitors for e-commerce on the Internet is security and privacy issues" (Mehta, 1999). The original intention of the Internet was for research and sharing of information, mainly by providing easy accessibility. Thus, openness was a focus, not security.

The above paragraphs have shown that security is a problem in the Internet environment. These problems must be narrowed down to specific risks. This is necessary so that the IS auditor will be able to analyse and understand each risk and determine what possible controls may be implemented to minimise those risks. The controls will be discussed in Chapter 5.

4.4.3 A DEFINITION OF RISK

Risk is be defined as

- "...uncertain future events that could influence the achievement of the organisation's objectives, including strategic, financial, and compliance objectives" (PWC, 2001).
- A vulnerability "is the susceptibility of a situation to being compromised. A threat (risk) is an action or tool which can exploit and expose a vulnerability and therefore compromise the integrity of a given system" (Flanagan & Safdie, 1997).
- The *Oxford Dictionary* (seventh edition) defines risk as "chance or possibility of loss or bad consequence; danger".
- Risk analysis according to the Canadian Institute of Chartered Accountants (CICA, 1986) involves "considering the damage which can result from an event of an unfavourable nature" and " the likelihood of such an event occurring".
- Another definition, provided as part of the preparation for students taking the CISA exam (CISA, 2001), states the following: "The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets".

From these definitions and the background information given in the prior sections, it is clear that risk is concerned with the protection of the assets of an organisation. These assets also include information and they (assets) are usually used in the day-to-day operations of the organisation. The loss of such assets may endanger the

continuity of an organisation or may negatively impact on the profitability of an organisation.

4.4.4 THREATS IN ELECTRONIC COMMERCE PAYMENT SECURITY

The following threats have been identified as the threats of EC payments.

1. Unauthorised access (Netscape, 1999); (FDIC, 1999); (Oscar, 1999).
2. Data alteration/Integrity (Netscape 1999); (Beck, 2001); (Maung, 2001); also noted by the British Standard on Information Security Management (BS 7799) as the threats related to information security; (Restell, 2001); as well as (GASSP, 1997); (LeClerc, 2001); (PWC, 2000); (IEC, 2000); (Dixon, 1999); (Dfat, 2000); (Mackey & Gossels, 2000); (CISA, 2001); (FDIC, 1999); (Oscar, 1999); (James, 1999).
3. Breach of confidentiality including Spoofing (Netscape 1999); (Beck, 2001); (Maung, 2001); also noted by the British Standard on Information Security Management (BS 7799) as the threats related to information security; (Restell, 2001) as well as (GASSP, 1997); (LeClerc, 2001); (PWC, 2000); (IEC, 2000); (Dixon, 1999); (Dfat, 2000); (Mackey & Gossels, 2000); (CISA, 2001); (FDIC, 1999); (Oscar, 1999); (James, 1999).
4. Denial of Service/Availability. (Netscape 1999); (Beck, 2001); (Maung, 2001); also noted by the British Standard on Information Security Management (BS 7799) as the threats related to information security; (Restell, 2001) as well as (GASSP, 1997); (LeClerc, 2001); (PWC, 2000); (IEC, 2000); (Dixon, 1999); (Dfat, 2000); (CISA, 2001); (Oscar, 1999).
5. Repudiation (Netscape, 1999); (FDIC, 1999); (Oscar, 1999); (James, 1999).
6. Client side and web side vulnerabilities (Netscape, 1999); (Beck, 2001); (Maung, 2001).
7. Authentication (IEC, 2000); (Dixon, 1999); (Dfat, 2000); (FDIC, 1999); (Oscar, 1999); (James, 1999).

The threats faced by business conducted through the Internet are not the same as those faced by storefront operations. Differences are in method, scale and geographical area. There may be hundreds of electronic attacks being mounted on key systems. Keeping up with the risks is challenging due to the Internet technology moving at a rapid pace. Problems are compounded since the technology is not mature. In addition, in the experience of the author, developments are typically made

without careful consideration to security. The risks listed above are explained in more detail in the paragraphs below. The IS auditor needs to understand the nature of each risk, which will enable the IS auditor to further identify controls available to address each risk. The control identification process will be addressed in detail in Chapter 5.

4.4.4.1 Unauthorised Access

For the purposes of this study, unauthorised access will be included with the other risks mentioned (e.g., integrity, confidentiality, denial of service, etc.) because the possible results of unauthorised access are data alteration, compromise of integrity, breach of confidentiality, denial of service and/or repudiation. In the next three sections (4.4.4.2 to 4.4.4) unauthorised access is an integral part of the discussion.

4.4.4.2 Data Alteration/Integrity

Integrity means "the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness" (GASSP, 1997). Data integrity issues are usually accidental or malicious (Mehta, 1999). However, data integrity issues are more likely to arise from system and communication errors. Another definition provided by PWCGlobal (1999) states that integrity concerns "... the prevention of unauthorised modification of information. Data integrity refers to the requirement that data in a file remains unchanged or that any data received matches exactly what was sent".

According to Dfat (2000) integrity means "ensuring that information in the message (including the identity of the sender and receiver) is not accidentally or deliberately modified." Ghosh (1997) is of the opinion that "violations in integrity of data sent over networks are often incidental and unintentional, but the potential to maliciously alter data in order to affect some outcome exists."

The risk of integrity therefore involves the maintenance of the completeness and accuracy of the data. In an Internet environment the possibility exists that data may be altered during transmission from the sender to the receiver. A message may be sent to one or more customers or organisations. There are also many communication points (e.g., routers, firewalls, etc.) between the sender and receiver where a

message may be altered. Controls are available to ensure that the integrity of data is maintained. The controls will be addressed in detail in Chapter 5.

4.4.4.3 Breach of Confidentiality Including Spoofing, Data Theft, and Fraud

Confidentiality means "the characteristic of data and information being disclosed only to authorised persons, entities and processes at authorised times and in the authorised manner" (GASSP, 1997). Data travelling over the Internet go through numerous intermediary sites and are routed considerably before reaching the final destination. A fixed path is not established for all messages passed between the message originator and its recipient. Thus, potential exists for people with the inclination to read information not intended for them. It is like sending a post card through surface mail. Additionally, the following is also stated regarding the Internet Protocol (IP). "IP is inherently insecure and provides opportunity for ill-intentioned individuals to read other people's transmissions" (Mehta, 1999). "One of the biggest fears that consumers have in online commerce is sending their credit card numbers over the Internet. It is quite easy for an interested party to eavesdrop on other people's Internet conversations" (Ghosh, 1999).

According to Mehta (1999) "the risks related to theft and fraud are probably more severe from Internet based transactions than when using traditional ways, especially in terms of scale." According to a joint survey by the FBI and the Computer Security Institute (CSI) of Fortune 500 companies (Mehta, 1999), "42 percent reported unauthorised use of their information systems, and 32 percent reported losing about $100 million due to security breaches, though not necessarily from the Internet." It is also important to note that electronic theft may be done from anywhere in the world. It becomes easier for a person to commit crime when hidden behind a curtain of electronic equipment such as routers, switches and wires. In addition, many companies may not have adequate controls to prevent and/or detect potential security breaches.

An example of spoofing (Netscape, 1999) occurs when "a virtual vandal creates a fake site masquerading as yours to steal data from unsuspecting customers or just disrupt your business." Spoofing is therefore also a way in which confidentiality may be compromised or in which fraudulent activity may take place.

Confidentiality involves the assurance that data is not disclosed to unauthorised persons. In the definitions and examples mentioned above, as well as from the previous two chapters, it becomes clear that privacy concerns are a major issue for EC. There are many possible ways in which privacy may be jeopardised, and these concerns need to be addressed to put customers and trading partners at ease when they deal with an organisation. There are controls available to ensure that the confidentiality of data is maintained and the controls will be addressed in Chapter 5.

4.4.4.4 Denial of Service/Availability

What is meant by availability is "the characteristic of data, information and information systems being accessible and usable on a timely basis in the required manner" (GASSP, 1997).

Denial of Service (DoS) attacks are defined (Mehta, 1999) as "launching an assault that would bring down the service that is offered to customers. Such attacks may cause loss of revenue when a company's key transaction server is brought down and customers cannot place orders." Netscape (1999) also agrees with this definition. This could also result in negative publicity when a Web-site has been altered. Unfortunately, it is difficult to defend against such attacks as infrastructural weaknesses are exploited. Knowledge of such attacks and other hacking/cracking related knowledge bases are well organised and published within the Internet community. A DoS "is aimed solely at making services unavailable. The attacks are particularly difficult to defend against because they exploit infrastructural weaknesses or flows in widely used protocols such as the Internet Protocol (IP). Strategically pinpointed attacks can bring down entire systems critical to the nation or organisation" (Ghosh, 1999).

DoS and availability is a concern and a risk because the unavailability of the medium used to conduct an organisation's business (in this case the computers) will result in a loss of revenue and/or customers. This will in turn have an impact on the long and/or short term profitability and continuity of the organisation.

4.4.4.5 Repudiation

Another concern is repudiation, especially for businesses where customers or business partners may deny that they transacted any business, when in reality, they

did (Mehta, 1999). For example, a customer orders a CD, and then denies to the vendor that such a request was ever made. In the Internet world, business parties may not know each other by face or reputation, or may not have had a prior business relationship. It would be difficult to positively confirm that a particular client did indeed request the transaction in question. Proper controls are needed to ensure for integrity and non-repudiation.

According to Dfat (2000), repudiation is summarised as follows: "The sender denies sending the message and the recipient disclaim receipt of the message".

Repudiation means that unnecessary costs may be incurred to prove that the transacting parties were the 'real' parties involved and therefore accountability is created. There are many ways to minimise and control repudiation risks and these will be addressed in the chapter on controls, Chapter 5.

4.4.4.6 Client side and web side vulnerabilities

Typical focus on e-commerce security has been on the transportation of information (Mehta, 1999). Often overlooked is the security of clients' PCs and Web servers. The biggest risk to clients connecting to the Internet is from the applications that are downloaded. These applications are typically downloaded by a click through to a Web-site that executes them within the PC. Such code typically animates Web pages. More and more Web sites are 'pushing' information to clients to make the Web servers more efficient. However, if the code downloaded has bugs or is malicious, risks could range from wiping clean the hard-drive to extracting information from the PC – often without the knowledge of the client. Though 'fixes' are constantly applied to the software, holes and vulnerabilities continue to emerge.

One of the obvious risks to Web servers mentioned above (4.3.4) is the denial of service attacks. Another issue is related to confidentiality of information that may be stored on Web servers, or areas that are accessible by Web servers such as database servers. If proper controls are not in place, this information could be retrieved, manipulated or destroyed.

Most security weaknesses of Web servers come from configuration issues. Typically, when installing the system, whether it is a firewall or an operating system, by default, a number of network services and protocols are made available. The more services

available, the more routes a hacker or cracker will have to penetrate the internal private network.

It is possible to protect data during transmission but this data will also be stored on a computer/server of an organisation. If this information is not protected at the server level, the integrity and confidentiality of the data are endangered and all controls implemented to protect the data during transmission will be rendered worthless. The controls related to client and web side vulnerabilities will be addressed in Chapter 5.

4.4.4.7 Authentication

Authentication involves the concern that "both parties quoted in the message are the actual parties to the transaction" (Dfat, 2000); (Held, 1997). This aspect has been addressed in the repudiation risk above because of the close link between the issues involved. For the purposes of this study authentication will be addressed in conjunction with repudiation issues.

4.4.5 RISKS RELATED TO SPECIFIC INTERNET PAYMENT METHODS

The main payment systems being used for Electronic Commerce (i.e. credit cards and electronic cash) have been mentioned in Chapter 3. The security problems affecting these two areas of Internet commerce are summarised in the following sections (4.4.5.1 and 4.4.5.2).

4.4.5.1 Credit Card Transactions

Confidential information, such as credit cards and personal details, may be intercepted during transmission over the Internet, for example when submitting an order form on the Web. The following statements emphasise the importance of credit cards in EC. "Protecting credit card numbers used in online transactions is the most often cited example of the need for web security" (Garfinkel & Spafford, 1997). "Credit card fraud is already a significant factor inhibiting consumer confidence in e-commerce" (Bohm et al, 2000). Duques (Duques & Staglin, 2000) states that "credit card fraud on the Internet is 12 times higher than at brick-and-mortar stores. Ensuring that business, merchants, and consumers have security and authentication services are critical to the widespread deployment of e-commerce."

The controls related to transmitted information is to ensure that

- it is inaccessible to anyone but sender and receiver (privacy/confidentiality),
- it has not been changed during transmission (integrity),
- the receiver will be sure it came from the sender and the sender will be sure the receiver is genuine (authenticity),
- the sender cannot deny he or she sent it (non-repudiation).

Without special software, all Internet traffic travels 'in the clear' and so anyone who monitors traffic is able to read it. This form of 'attack' is relatively easy to perpetrate using freely available "packet sniffing" software since the Internet has traditionally been a very 'open' network. "No special physical access is required (it is also possible to eavesdrop using network diagnostic hardware if you have physical access to the network cabling). Passwords and credit cards may be distinguished from the rest of the traffic using simple pattern matching algorithms" (Kabay, 1998). According to Ghosh (1997) "one of the biggest fears that consumers have in online commerce is sending their credit card numbers over the Internet".

Protecting transactions is only one element of the secure transaction problem. Once confidential information has been received from a client it must be protected on the server (client and web side vulnerabilities). Currently, Web servers are among the softest targets for hackers, largely due to the immaturity of the technology. The paragraphs above show that credit card concerns are very important. As has been highlighted in the previous chapters, credit card concerns are a limiting factor for the growth of EC. The risks mentioned in 4.3 above also apply to credit cards as one of the payment systems used for Internet transactions.

4.4.5.2 Electronic Cash

According to Warigan (1999) "security is perhaps the most critical aspect of electronic cash. It is the focus around which a successful electronic cash mechanism is structured and functions. The risks related specifically to electronic cash are summarised in the following few points.

- Electronic cash is loaded into a physical object, such as a smart card on a personal card computer. The data is secured by cryptographic methods. These

physical objects may be the subject of an attack (This is considered to be client and web side vulnerabilities).

- Electronic cash may be lost if the device e.g. computer that it is stored on crashes or if it is not protected by the owner or user (This will be considered under the client and web side vulnerabilities issues).
- The initiating system may be compromised resulting in the value of the cash to drop (This will be considered under the client and web side vulnerabilities issues).
- Software based electronic cash are susceptible to theft through hackers (This will be considered under the client and web side vulnerabilities issues).
- Privacy may be compromised by a lack of controls over electronic cash (This will be addressed under Confidentiality/ privacy issues).
- Electronic cash is protected through cryptographic solutions. All encryption or cryptographic mechanisms are breakable (Garfinkel & Spafford, 1997); (Warigan, 1999); (Ghosh, 1997).

Although electronic cash differs from credit cards in the sense that it is supposed to provide more anonymity, the main risks related to the use of this medium for electronic payments still revolves around the risks mentioned in section 4.4.3 above. The main security objective is to deter all or most people from attempting to compromise a secure mechanism and to make the cost of breaking such a mechanism higher than the benefit of doing so.

4.4.6 MANAGING THE RISK

The Internet's weakness (as an open network) is also its fundamental strength. The strength is that its openness makes it the ideal platform for global commerce and communications. The Internet offers the promise of inexpensive mass communication and provides economies of scale for low-cost distribution. This aspect has been highlighted in Chapters 1 and 3 of this study. However, the weakness of the Internet as highlighted above is that since it is open, communications are inherently difficult to secure. What is missing is the mechanism to guarantee the integrity and confidentiality of information and to provide protection against denial of service attacks, and to minimise exposures created by client and web side vulnerabilities. There are various controls available to address the risks highlighted in this chapter. These controls will be discussed in Chapter 5.

In the face of massive enthusiasm for the Internet, it must be stressed that 'all security is relative'. Any practical answer to the problems has to be a compromise between vulnerability and risk (e.g. there are some vulnerabilities which only a handful of people are currently skilled enough to exploit, which implies that the likelihood of the vulnerability materializing as an actual threat is relatively minor). The assessment of each threat must be weighed against what is at stake, the exposure faced by proceeding with the knowledge that some attacks are possible.

To manage business risk, the prudent business must therefore deal with risk by

- firstly, identifying the risks it runs (as described in section 4.4.4 above);
- secondly, avoiding those risks which may reasonably be avoided. This is done through the implementation of controls to minimise the risks- as described in Chapter 5);
- thirdly, shielding itself from the risks it cannot avoid principally by declining liability through contract or benefiting from so-called legislative safe-harbour provisions,
- and finally, accepting those risks which it can neither avoid nor deter by insuring, hedging, financing or otherwise providing for the impact of the risk on its business.

4.5 CONCLUSION

The approach to an IS audit of EC payment security involves a number of steps. It starts with the understanding of the environment and follows with the identification of risks. This chapter identified the unique risks in the EC payment environment. These risks stem from the fact that the Internet has been designed to be 'open', which increases the likelihood of manipulation. The need for security and control in this environment has also been highlighted. It has been established that the IS auditor needs to be aware of the inherent risks in an EC payment security environment so that it will enable him/her to identify such risks when an area involved in EC payments is being evaluated/reviewed. This chapter identified seven threats/risks in the EC payment security environment.

The IS auditor plays an important role in the risk management process through the risk identification process, and armed with knowledge of the risks, the IS auditor is able to perform the next step in the audit approach, which is to identify the controls

required to minimise or manage the risks identified. The ultimate objective of the audit is to form an opinion regarding the control environment.