Identifying risks in e-commerce payment security for use by the IS auditor

PS Bezuidenhout
Department of Auditing
University of Pretoria

JD Gloeck
Department of Auditing
University of Pretoria

ABSTRACT

The emergence and growth of business conducted through the Internet has given rise to numerous concerns. Both business and customers alike are facing additional risks in this environment. The Information Systems Auditor (IS auditor) plays an important role in contributing towards managements' efforts to manage the electronic commerce (EC) environment and more specific Internet security and Internet payments. This article investigates the role of the IS auditor in the EC environment and seeks to contribute towards the development of knowledge on the topic by identifying, describing and discussing the major risks associated with EC payment security and Internet payment methods.

This is the first of two articles on the IS auditor in the EC environment. The second article uses the risk model developed in this paper to develop a suitable audit approach for the IS auditor in the mentioned environment.

Key words

Audit of… information systems, internet security, internet payment; e-commerce;information systems auditor/audit; internet payment security; internet payment methods; internet risk management; internet security risks

1 THE EXPANSION OF THE INTERNET AND ELECTRONIC COMMERCE (EC)

The emergence of markets on the Internet has had a dramatic impact upon the traditional ways of doing business. The Internet provides a network that allows individuals and enterprises to connect in a way never before believed possible. It provides a framework that allows the convergence of voice, data, and broadcast, all of which have been (and mostly still are) discrete. It brings customers and merchants closer together. Yet, it also introduces new questions, such as the following:

- How is the customer to know to whom he is giving his credit card detail?
- What if the customer wishes to pay with cash?
- How does the merchant know that this is a legitimate customer order?
- What physical evidence does either customer or merchant have of an order being placed or paid?

As mundane as these problems may appear, they represent a formidable challenge to the growth of electronic-commerce (EC). If EC is to enjoy sustainable growth, it is necessary to find in the electronic world of the Internet, answers to these questions. Both customers and merchants must have the same level of confidence in purchase and sales transactions conducted through the Internet as they do when they buy or sell goods over the counter, by mail, or over the phone.

Internet payment security therefore plays a very important role in the EC process.

According to Denny (1997) "…one of the biggest challenges in the development of electronic commerce has been for banks and merchants to overcome the issues of customer identification and account verification for online purchases." While the credit card systems have a process in place to verify and authorise transactions, the Internet poses challenges for merchants to not only validate that funds are available in an account, but to positively identify that the customer is in fact authorised to use that account for purchases.

In the physical world, merchants validate the identity of the account holder by comparing the signature on the credit card with the signature on the sales slip. But in a virtual world, where the customer is not present, the merchant does not know if that person is authorised to use the account number provided for the transaction. The danger in the EC environment is that, without additional controls, the exposure to losses from fraudulent usage is exponentially greater.

The Information Systems (IS) auditor plays an important role by understanding the issues, analysing the effects of these issues on the risks and controls in an organisation, and recommending solutions. In order for an auditor to fully understand the risks, impact, and possible controls available in Internet payment security systems it is necessary to understand the EC environment, including Internet payment security.

The purpose of this article is to identify and present details of the risks in EC payment security in relation to the IS auditor. In order to achieve this, it is necessary to first identify the importance of EC to the IS auditor, secondly, to provide a description of the role of the IS auditor, including management's expectations, and thirdly to provide the relevant details of security and risks in this environment. Finally, details of EC payment security and the risks prevalent in EC payment security will be presented.

Risk is 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) (1984) 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 Certified Information Systems Auditor (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 information given in prior sections, it is clear that risk is related to 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.

2 EC AND THE IS AUDITOR

2.1 Introduction

The IS auditor is not synonym with the external auditor who expresses an independent opinion on the financial statements. It is therefore essential to firstly provide a short definition of the role of IS audit in a general context before the role of IS audit in a specific environment such as EC payment security will be described. The following definition (based on the concepts promulgated in "Internal Control – Integrated Framework" developed by the Committee of Sponsoring Organisations (COSO) of the Treadway Commission's Internal Control - Integrated Framework (USA may be considered as the mission of the IS auditor (Paliotta, 1999).

> Using appropriate technological tools and expertise, evaluate the adequacy and effectiveness of control systems addressed to the risks emanating from an organisation's application of technology in support of its business objectives and proactively work with management to identify risks and control objectives in the application of emerging technologies in support of strategic objectives.

The role of the IS auditor is therefore regarded as evaluating the risks and controls in the IS environment as part of their responsibility to management of the organisation and other interested parties. This role may either be performed in the capacity of an external or an internal auditor.

2.2 The importance of IS auditor involvement in EC

Whilst no universal definition of EC exists, it is clear that it is all about the method of communicating over networks between buyers and sellers of goods or services. In order to achieve this, new technologies are constantly evolving. It is important that they are understood together with the related management issues of security and control. The Institute of Chartered Accountants of Scotland (ICAS, 1998) states that:

> The extent of electronic trading is presenting businesses with unique challenges and presents the audit profession with a number of similar challenges and opportunities. Successfully managing the transition to EC demands overcoming a number of significant issues, including not only making the technology work, but also re-engineering existing business models and business processes. The change can so fundamentally affect an organisation that the evolution involves all aspects of the business from procurement to marketing and from finance to the audit.

As soon as an organisation considers EC and challenges their own business model, it provides auditors with an ideal opportunity to reassess the way the audit is carried out. To understand the risks, auditors need to ensure that the business processes being developed support the client's strategies, and that control procedures are integrated from the start. Because the business is susceptible to fundamental change, so are the risks involved.

The risks and concerns as identified by the ICAS (1998) include the following:

- In the rush to the Web, it is important that the business does not overlook the issue of financial control of the process. Financial control contains several key elements including the security of systems underlying the process and the accuracy of information.

- The most notable issue concerning consumers and businesses alike regarding EC is security, especially that of the Internet. The Internet is known for its lack of security. Unless encrypted during transmission, messages can be intercepted and read by third parties. In the case of sensitive information, such as credit card numbers, unintentional disclosure to unauthorised parties could result in significant financial loss.

- New ways to conduct electronic business often means connecting to other public or private networks. Trusted business partners are not the only ones shown the way to client's electronic systems: electronic vandals, criminals and other threats are also given access. The advent of the "Secure EC" Bill in the UK brings further risk in that it suggests that the government retains the right to access encrypted information without the knowledge of the business, and prevents service providers from tipping them off.
- Evaluation of the security environment surrounding a client's systems becomes key to providing audit assurance that the data which forms the basis of the financial statements is complete and accurate. Auditors have traditionally reviewed data file access and program change controls. In an EC environment, this has expanded to cover increasingly detailed controls such as application, access and authentication controls as well as physical and logical access.
- A significant impact of EC on businesses is that there is less margin for error - transactions have to be right first time, every time - especially those where funds are being transferred. This combined with the implicit loss of paper trail, means that processes have to be well controlled and have a clear electronic audit trail. For example, current requirements to hold financial information for a period of time extend to electronic information. This has significant ramifications in an electronic environment and would require historical information to be recoverable even if systems have changed. Recoverability and contingency planning in the event of disaster are also significant concerns.

In future, an explosion of EC will require all auditors to have a greater understanding of the types of risks this kind of trading brings.

Further evidence of the importance of EC as seen by the Accounting Associations is found in the following statements (Elliott & Pallais, 1997):

- "With accounting and auditing income flat for the last seven years, the CPA (Certified Public Accountant) profession's greatest opportunity for growth lies in new assurance services. (This includes the EC area).
- A variety of research would also help the profession's expansion into new assurance services. One of the kinds of research mentioned is criteria for assessing the integrity and security of electronic commerce. The estimated market for electronic commerce assurance services alone is between $ 1bn and $11bn. Systems and information technology naturally plays a prominent role in the new assurance services. They are part of how information for decision making is gathered and deployed and used in transactions. More opportunities will open up as the information technology revolution continues. Practitioners' information technology skills and knowledge will affect not only the range of new assurance services they can avail themselves of, but also the way they adapt their traditional services to changing circumstances."

These examples highlight the importance of EC for business and also indicate which role the IS auditor should play in EC.

2.3 The Role of IS Audit in EC Environments

EC integrates many technologies, both in hardware and software. In addition, information protection mechanisms must be included in the design. Implementation and maintenance of the network architecture must provide more secure and manageable access to public services and reduce associated risks. The protection mechanisms, which are part of the total EC picture, may include firewalls, data encryption, digital signatures, and time stamping.

Tibaldeo (Tibaldeo & Buben, 1996) is of the opinion that "…most IS professionals are familiar with several electronic based payment systems such as credit cards, direct deposits, and bank-to-bank transfers". The media and Hollywood films are probably responsible for escalating people's expectations regarding these payment systems. These films produce a perception of electronic payment methods involving virtual reality and biometric authentication systems. Tibaldeo (1996) further believes that "…although authenticating purchases at the virtual grocery store by way of retina scan may be far into the future, technology conscious merchants and consumers are carefully watching the development of several forms of electronic payment. Several emerging electronic payment models such as digital cash, electronic checks, encrypted credit cards, and third-party processing transactions are poised to take the Internet by storm". IS audit professionals need to understand how the strengths and drawbacks of these models compare.

There are other aspects relating to the controls in Internet related systems that could affect the auditor. The Internet today is a vast frontier of unknown elements including new types of software, new discoveries of security flaws, and unfriendly neighbours. The most secure technical solution to preventing attacks launched from the Internet is to unplug the network from the computer. This solution is not viable in today's business climate. Rather, the components that comprise EC systems must be adequately secured.

The role of the IS auditor in EC is defined as follows:

> Electronic commerce presents the IS auditor with challenges and opportunities. Its emergence will cause people to rethink the way organisations do business, and will force them to focus on enterprise-wide issues and technological solutions. A focus on business processes will be necessary to understand and evaluate an organisation's electronic commerce strategy (including electronic commerce objectives and investments), process re-engineering strategies, change management issues, and operational improvements that affect business transactions. A focus on technology considerations will be necessary for evaluating connectivity/hardware issues, information protection strategies, and application quality considerations (Tibaldeo & Buben, 1996*)*.

Paliotta (1995) is of the opinion that "…auditors need to take an objective look at the new technological advances, evaluate the risks associated with them, and work with management to establish controls that reasonably assure the new technological world order will be a safe place to 'live' in." The risks can be, and must be controlled.

Today's IS auditors are living in exciting and interesting technological times. Technological advances provide major competitive advantages to those with the ability to harness, utilise and control them – or they are a curse to those who cannot. With opportunity comes threat, and the audit, control, and security professionals will have an important role in helping management safely navigate through the new world order and to use it to its best advantage.

The question now arises: What is being done by auditors all over the world to address the risks of Internet related systems, and to provide assurance to customers and management in this regard?

2.4 IS Audit and Management Expectations

Executive management's focus on information technology varies dramatically depending on the mission of the organisation, the industry, the culture, and whether technology is a product or service provided or consumed by the organisation. The auditor's role within an organisation may also vary greatly depending on executive management expectations of audit and the state of controls within the organisation. In general, management expects auditors to assess controls, rather than define or prescribe them. Management should also regard information as a major organisation asset, the protection of which must preoccupy all executive managers.

Senior management has a responsibility to establish effective control over information and information systems (CICA, 1986; ISACA, 1999; Menkus, 1998). Discharge of this responsibility involves the exercise of management practices, which are as applicable to information systems as they are to other activities of the entity, and is summarised as follows (CICA, 1986); (Oliphant, 1998):

- Establishment of objectives and policies for each role and function.
- Assignment of the related responsibilities.
- Development of a comprehensive plan for the achievement of the information system's objectives and policies for the entity.
- Monitoring of activities against the company objectives, policies, and plans.

The following statements defines the responsibility for control:

- The directors should report on the maintenance of an effective system of internal controls. This is a requirement of the King report on Corporate Governance in South Africa (IOD, 2002: 33).
- Ensuring the integrity of the corporation's accounting and financial reporting systems, including appropriate systems of control (OECD, 1999).
- It is the responsibility of the audited body (Audit Commission, 2000) to:
  - Put in place proper arrangements to ensure the proper conduct of its financial affairs, and to monitor their adequacy and effectiveness in practice.
  - Develop and implement systems of internal control, including systems of internal financial control and to put in place proper arrangements to monitor their adequacy and effectiveness in practice.
  - Ensure its affairs are in accordance with proper standards of financial conduct and to prevent and detect fraud and corruption.
- Management, through its enterprise governance, must ensure that due diligence is exercised by all individuals involved in the management, use, design, development, maintenance and/or operation of information systems (ISACA, 1999).
- Organisations must satisfy the quality, fiduciary and security requirements for their information, as for all assets. According to the Information Systems Audit and Control Association (ISACA, 1999):
  Management must also optimise the use of available resources, including data, application systems, technology, facilities and people. To discharge these responsibilities, as well as to achieve its objectives, management must understand the status of its own IT systems and decide what security and control they should provide. Management must ensure that an internal control system or framework is in place which supports the business processes, makes it clear how each individual control activity satisfies the information requirements and impacts the IT resources.

- "Control of information systems is the responsibility of senior management" (CICA, 1986). The inherent partnership between auditors and management requires that the auditors understand management's concerns, ensuring that the organisation's structure addresses business objectives including:

- Quality of the organisation's products and services
- Customer and business partner satisfaction
- Cost management, revenue/profit maximisation, and effective and efficient operations
- Information management for integrity, availability and privacy
- Safeguarding of assets including information assets
- Regulatory and internal compliance
- Business continuity
- Fraud prevention and detection
- Technology innovation appropriate to the organisation's objectives
- Accurate and timely financial reporting.

From these statements, the responsibility of the IS auditor is defined as to consider the activities and assets that would interest a third-party stakeholder or management in the organisation – one who understands IT issues, opportunities, and potential problem areas, and who has a strong interest in the organisation's performance. The auditor must then develop an understanding with executive management about the relevance of each of these areas, with some measure of their importance or potential risk, comprehending the degree of technical complexity involved in assessing them and providing audit results.

The responsibilities of the internal and external auditor towards management and external parties respectively are defined by Wilson and Root (1983) as: "Internal auditors provide boards of directors and companies' management with assurance as to the sufficiency of the authorised control techniques to accomplish business goals and the degree of compliance therewith." External auditors "…provide assurance to stockholders, creditors and others regarding the fairness of the information contained in the financial statements."

The ICAEW's booklet (ICAEW, 2000) on "Internal Audit and its Value" highlights three areas in which internal audit assist management of organisations, namely:

- meet their corporate governance responsibilities;
- assess and manage business risk;
- ensure adequate systems of internal controls.

According to Miller (1999):

> Stakeholders expect Internal Auditors to ensure that the organisation's assets are safeguarded. This extends to critical information security. The Internal auditor may well be the person with the broadest perspectives and knowledge base when it comes to understanding the control environment and the control systems that provide infrastructure protection. For the current audit evolution to be complete, Internal Auditors must recognise the elements of information security as key in providing reliable evidence about infrastructure protection and assurance.

The following statements further highlight the relationship between IS audit and management:

- "Nobody understands the changing audit environment better than IS auditors who deal with new and emerging technologies and objectives and techniques that did not exist the day before" (Garitte, 1998).
- Garitte (1998) is also of the opinion that. "Auditors should address management as experts in neither technology nor controls, but as business strategists who are keenly aware of the organisation's dependence on information, technology, and the controls that assure integrity. Auditors apply their expertise to provide the assurances management needs in terms of the integrity of information assets"
- According to Sayana (2002): "Information systems are the livelihood of any large business. As in years past, computer systems do not merely record business transactions, but actually drive the key business processes of the enterprise. In such a scenario, senior management and business managers do have concerns about information systems. The purpose of the IS audit is to provide feedback, assurances and suggestions."
- "In taking responsibility for internal controls, management must also take responsibility for IS controls. While management may be familiar with some technologies, their knowledge is short lived due to the constant change of systems. This should result in greater reliance of management on IS audit and control professionals" (Owen, 1994).

From the above it is clear that executive management therefore need not understand technical language or the details of technical tasks performed by auditors. Auditors, however, must understand management's perspectives and keep management aware of key technology issues. In short, auditors must show understanding of the significant business issues and the technology components that support them, and gather supporting evidence.

The Australian Guidance Statement number AGS1056 from the Australian Accounting Research Foundation (AARF) (2000) states that: "Management is responsible for developing an e-com strategy to address risks and opportunities arising from its e-com activities." "Ordinarily management will identify e-com business risks, and will address those risks through the implementation of appropriate security and internal control measures. The auditor considers e-com business risks in so far as they impact on audit risk."

In summary, auditors must also ensure that appropriate audit resources are applied to those issues that concern executive management. They must bring new information, positive or negative, to management's attention in such a way that management will understand its importance and act appropriately.

From the above it is clear that technology brings risks along with its potential rewards, and IS auditing also has a responsibility to increase awareness of technological risk and control issues. The IS auditors should help to educate the rest of the organisation regarding these risks and controls in order to assure that the implementation of new technologies will achieve the corporate objectives without placing the organisation in an unacceptable risk position.

2.5 Steps in an Information Systems Audit

The steps that the IS auditor follows during an audit of EC payment security is (Bezuidenhout, 2002), firstly, to gather information related to the environment 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. Other steps in the audit approach include developing an audit approach to serve as a framework for the environment under review, audit testing and reporting on the results of the tests. 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 sufficient information regarding the environment to be audited.

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 article will provide more detail regarding security and the risks around EC payments. The risks identified and described in section 4 and 5 below, serve a twofold purpose. Firstly, it becomes clear that the risk identification process is essential to the IS audit, because, without this risk identification process, the IS auditor cannot determine where the focus of a review should be. Secondly, risk identification also assists the auditor to obtain a better understanding of the environment being audited.

The next section of this article will firstly provide examples of security issues in EC 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. This knowledge will enable the IS auditor to identify the risks (threats and concerns) prevalent in the EC payment security environment.

3 SECURITY AND EC

3.1 Examples of EC security issues

EC is widely viewed as threatening the privacy of an individual. Several surveys indicate considerable concern by users about their privacy online. 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 2002 FBI/Computer Security Institute (CSI) survey "…confirm that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting” (CSI, 2002). The survey is based on responses from 503 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities.

Highlights of the "2002 Computer Crime and Security Survey" include (CSI, 2002):

- Ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.
- Eighty percent acknowledged financial losses due to computer breaches.
- Forty-four percent (223 respondents) were willing and/or able to quantify their financial losses. These 223 respondents reported $455,848,000 in financial losses.
- As in previous years, the most serious financial losses occurred through theft of proprietary information (26 respondents reported $170,827,000) and financial fraud (25 respondents reported $115,753,000).
- For the fifth year in a row, more respondents (74%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (33%).
- Thirty-four percent reported the intrusions to law enforcement. (In 1996, only 16% acknowledged reporting intrusions to law enforcement.)

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 article focuses on the risks in this unsecured 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 risks and the tools available to be used in EC sites to provide the necessary protection.

3.2 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 Baltimore (1999); Blunt (1997); Hartman (2001); Kabay (1998); Masse & Fernandes (1997); McGhie & Maier (1998); Miller (2000); Siegel (1997); Walder (1999); . 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 EC at the present time. To illustrate this the following example is quoted:

> Companies are quickly moving to utilise the expanded opportunities created by the Internet. For instance, Cisco systems, Dell computers, and Boeing's spare parts business report almost immediate benefits after putting their ordering and customer service operations on the Internet. They are so convinced of its benefit to their own companies and their customers that they believe most of their business will involve the Internet in the next three to five years (US Department of Commerce, 1998).

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.

Because the Internet has been designed to be 'open', the security aspect is also 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. The risks will be identified in section 4 of this article.

3.3 Internet Security - Risks and Concerns

3.3.1 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 sections. 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" (PWC, 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).

3.3.2 Understanding Internet Security Risks

To understand the risks regarding the Internet, this section provides more information to emphasise the points highlighted in the previous section and thereby providing a broader and more detailed definition of risk. The specific risks of EC payment security are subsequently listed and discussed in sections 4 and 5.

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 the 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.

4 RISKS IN EC PAYMENT SECURITY

4.1 EC payment risks

The following risks have been identified with regard to EC payments.

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

Authentication (Dfat, 2000; Dixon, 1999; FDIC, 1999; IEC, 2000; James, 1999; Oscar, 1999).

The risks 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 authors, 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.

4.2 Unauthorised Access

For the purposes of this article, 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 unauthorised access is an integral part of the discussion.

4.3 Data Alteration/Integrity

Integrity means "…the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness"

(GASSP, 1997). Losses of data integrity 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 PWC (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."

Data 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.

4.4 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 traveling 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, the 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 listed above, 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.

4.5 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.

4.6 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 results in unnecessary costs to be incurred to prove that the transacting parties were the 'real' parties involved and thereby establish accountability .

4.7 Client Side and Web Side Vulnerabilities

Typical focus on EC 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 listed above (4.5) 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.

4.8 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 article authentication will be addressed in conjunction with repudiation issues.

5 RISKS RELATED TO SPECIFIC INTERNET PAYMENT METHODS

5.1 Credit Card Transactions

Confidential information, such as credit card numbers and personal details, may be intercepted during transmission over the Internet (for example when submitting an order form on the Internet). 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 should ensure that:

- it is inaccessible to anyone but sender and receiver (privacy/confidentiality),
- it has not been changed during transmission (integrity),
- the receiver will know it came from the sender and the sender will know 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 (see 4.6 - 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 previously, credit card concerns are a limiting factor for the growth of EC. The risks described , also apply to credit cards as one of the payment systems used for Internet transactions.

5.2 Electronic Cash

Electronic or digital cash is an electronic replacement for paper currency and coins. It provides the ability to transfer value, in the form of digital tokens, between a buyer and a seller in exchange for goods or services, ideally without an intervening third-party validation and clearing of each transaction. Either cryptographic authentication or tamperproof hardware (such as a smart card) is required to prevent double spending or counterfeiting.

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 onto 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.
- 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.
- The initiating system may be compromised resulting in the value of the cash to drop.
- Software based electronic cash are susceptible to theft through hackers.
- Privacy may be compromised by a lack of controls over electronic cash.
- 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 already mentioned . 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.

6 MANAGING THE RISK

Whilst it may sound contradictory, 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. However, the weakness of the Internet as highlighted above is that since it is open, communications are inherently difficult to secure. What still needs to be fully developed, is a mechanism to guarantee the integrity and confidentiality of information, 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 article. The identification of controls fall outside the scope of this article, but more details on the controls in EC payment security are provided by Bezuidenhout (2002).

In the face of the massive enthusiasm for the Internet, it must be stressed that 'all security is relative'. Any practical answer to the above problems has to strike 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 and 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.
- Secondly, avoiding those risks which may reasonably be avoided. This is done through the implementation of controls to minimise the risks.
- 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.

7 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 is followed with the identification of specific risks. This article identified the unique risks in the EC payment environment. These risks stem from the fact that the Internet has been designed to be 'open', thereby increasing the likelihood of manipulation. The article also highlighted the need for security and control in this environment. 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.

By identifying and discussing the major risks in the EC payment security environment, this article aims to contribute towards the common body of knowledge available to the IS auditor when performing an IS audit in this environment.

REFERENCES

AARF (Australian Accounting Research Foundation). 2000. *Electronic Commerce: Audit Risk Assessments and Control Considerations*. AGS 1056. Australian Accounting Research Foundation. Melbourne. p10.

Audit Commission. 2000. Who Audits the Auditors? [Online]. Available at Internet: http://www.audit-commission.gov.uk/publications/general.shtml. Date visited: 12 January 2001.

Baltimore. 1999. 'Global e-security'. [Online]. Available at Internet: http://www.baltimore.com. Date visited: 27 April 2000.

Beck, D.F. 2001. 'A Review of Cybersecurity Risk Factors'. [Online]. Available at Internet: http://www/sans.org/infosecFAQ/securitybasics/risk.htm. Date visited: 27 July 2001.

Bezuidenhout, P.S. 2002. An Audit Approach Of The Information Systems Auditor In An Electronic Commerce Environment With Emphasis On Internet Payment Security. University of Pretoria. Pretoria.

Blunt. J. 1997. Internet Security: An Oxymoron. [Online]. Available at Internet: http://www.decus.org/decus/pubs/magazine. Date visited: 26 June 1998.

Bohm, N., Brown, I. & Gladman, B. 2000. 'Maintaining consumer confidence in electronic payment mechanisms'. [Online]. Available at Internet: http://elj.warwick.ac.uk/jilt/00-3/. Date visited: 22 February 2001.

CICA (The Canadian Institute of Chartered Accountants). 1986. *Computer Control Guidelines*. The Canadian Institute of Chartered Accountants. Canada. p24.

CISA (Certified Information Systems Auditor). 2001. 'CISA Review Technical Information Manual'. Information Systems Audit and Control Association. Rolling Meadows, Illinois. pp24 - 25.

CSI (FBI/Computer Security Institute). 2002. 'Cyber crime bleeds U.S. corporations, survey shows; financial losses from attacks climb for third year in a row'. [Online]. Available at Internet: http://www.gocsi.com/press/20020407.html. Date visited: 15 February 2003.

Denny S. 1997. The Electronic Commerce Challenge. [Online]. Available at Internet: http://www.denny.dc3.com. Date visited: 18 January 1999.

Dfat (Department of Foreign Affairs and Trade). 2000. 'Electronic Commerce – An Australian Customs Perspective'. [Online]. Available at Internet: http://www.dfat.gov.au/apec/ecom/custec1.html. Date visited: 25 June 2001.

Dixon, K.L. 1999. 'Electronic Commerce Security'. [Online]. Available at Internet http://www.aph.gov.au/library/pubs/rp/1998-99/99rp12.htm. Date visited: 19 June 2001.

Duques, R & Staglin, G.K. 2000. 'E-Commerce whitepaper'. [Online]. Available at Internet http://www.eoneglobal.com/whtpaper.html. Date visited 25 June 2001.

Elliott, R. & Pallais, D. M. 1997. Are you Ready for Assurance Services? *AICPA Journal of Accounting,* June 1997: pp47-51.

FDIC (Federal Deposit Insurance Corporation). 1999. 'Security Risks Associated With The Internet'. [Online]. Available at Internet: http://www.spicersweb.net/fdic.htm. Date visited: 12 October 2001.

Feinman, T., Goldman, D., Wong, R. & Cooper, N. 1999. 'Security Basics: A White Paper' [Online]. Available at Internet http:www.itaudit.org/forum/security. Date visited: 31 July 2001.

Flanagan, T. & Safdie, E. 1997. 'Internet Security Primer'. [Online]. Available at Internet http://www.techguide.com. Date visited: 28 October 2000.

Garfinkel, S. & Spafford, G. 1997. 'Web security & Commerce'. O'Reilly & Associates Inc: First Edition, June 1997. USA. p3.

Garitte, J. P. 1998. Keeping exec mgmt focus on IT part I. [Online]. Available at Internet: http://www.itaudit.org. Date visited: 6 March 2000.

GASSP (Generally Accepted System Security Principles). 1997 [Online]. Available at Internet: http://web.mit.edu/security/www/gassp1.html. Date visited: 28 August 2001.

Ghosh, A.K. 1997. 'E-commerce Security'. John Wiley & Sons. USA. pp 9-13.

Ghosh, A.K. 1999. 'Securing E-Commerce: A systematic Approach'. [Online]. Available at Internet: http://www.rstcorp.com/~anup aghosh@rstcorp.com. Date visited: 18 January 1999.

Hartman, S. 2001. 'Securing E-Commerce: An Overview of Defense In-depth'. [Online]. Available at Internet: http://www/sans.org/infosecFAQ/start/sec_ecom.htm. Date visited: 27 July 2001.

Held, G. 1997. 'Electronic Commerce'. *EDP Auditing - Auerbach Publications*. p7.

Held, G. 1994. 'Securing electronic messages'. *EDP Auditing - Auerbach Publications*. Warren Gorham & Lamont. p5.

ICAEW (Institute of Chartered Accountants of England & Wales). 2000. The Internal Audit Role in Singapore Listed Companies. [Online]. Available at Internet: http://www.gt.com.sg/art_ia.doc. Date visited: 2 December 2001.

ICAS (The Institute of Chartered Accountants in Scotland). 1998. [Online]. Discussion paper on Electronic Commerce. Available at Internet: http://www.icas.org.uk/members/servicesfrom. Date visited: 14 July 1999.

IEC (International Engineering Consortium). 2000. 'Internet Security'. [Online]. Available at Internet: http://www.iec.org/online/tutorials/int_sec/index.html. Date visited: 25 July 2001.

IOD (Institute of Directors). 2002. *King Report on Corporate Governance for South Africa*. Institute of Directors. March 2002. Parktown.

ISACA (Information Systems Audit and Control Association). 1999. *Control Objectives for Information and Related Technology* (COBIT) Framework – Executive Overview. Published by the Information Systems Audit and Control Association. Rolling Meadows, Illinois. p1.

James, M.L. 1999. 'Electronic Commerce: Security Issues'. [Online]. Available at Internet: http://www.aph.gov.au/library/pubs/rp/1998-99/99rp12.htm. Date visited: 17 July 2001.

Kabay, M.E. 1998. 'Identification, Authentication and Authorization on the World Wide Web'. [Online]. Available at Internet: http:www.icsa.com Date visited: 03 February 2000.

KPMG. 1995. *Secure Commerce in the Information Age*. KPMG International Headquarters. p12.

LeClerc, R. 2001. 'Audit and Security Control Issues when Conducting Information Security Reviews'. [Online]. Available at Internet: http://www.sans.org/infosecFAQ/securitybasics. Date visited: 28 July 2001.

Mackey, R. & Gossels, J. 2000. 'Mastering Fundamentals, Part 1' [Online]. Available at Internet: http://www.infosecuritymag.com/articles/january00/features3. Date visited: 21 August 2001.

Martin, D. 2000. 'Auditing Electronic Commerce Activities: Security Tools That Should be in Place'. [Online]. Available at Internet http://www.itaudit.org. Date visited: 06 July 2001.

Masse, D.G. & Fernandes, A.D. 1997. 'Economic Modelling and Risk Management In Public Key Infrastructures'. [Online]. Available at Internet: http://www.masse.org. Date visited: 7 June 2000.

Maung, P. 2001. 'Preparing for a Web Security Review'. [Online]. Available at Internet: http://www/sans.org/ infosecFAQ/audit/web _review.htm. Date visited 27 July 2001.

McGhie, L.L. & Maier, P.Q. 1998. 'Security Management For The World Wide Web". *Auerbach Publications*. 82-10-50. p1.

Mehta, R. 1999. 'Secure E-Business'. *ISACA Journal*. Volume I 2000. p32-37.

Menkus, B. 1998. IS Auditing and EDPACS at 25 years. EDPACS. May 1998. Auerbach Publications. p9-15.

Miller, J. 2000. 'Information Systems Security: Lessons Learned'. [Online]. Available at Internet: http://www.sana.org/infosecFAQ. Date visited: 27 July 2001.

Miller, L.N. 1999. Internal Audit's Critical Role – Part A. [Online]. Available at Internet: http://www.itaudit.org. Date visited: 6 March 2000.

Netscape. 1999. 'Securing your site for E-Commerce'. [Online]. Available at Internet http://home.netscape.com/ directorysc. Date visited: 7 December 1999.

OECD (Organisation for Economic Co-operation and Development). 1999. The OECD Principles of Corporate Governance. [Online]. Available at Internet: http://www.oecd.org/EN/home/0,,EN-home-28-nodirectorate-no-no--28,FF.html. Date visited: 7 January 2002.

Oliphant, A. 1998. An introduction to Computer Auditing. [Online]. Available at Internet: http://www.itaudit.org. Date visited: 15 July 2000.

Oliphant, A. 1999. 'Managing Information Security'. [Online]. Available at Internet: http://www.itaudit.org. Date visited: 06 July 2001.

Oscar. 1999. 'E-Commerce Risks – Security and Business' [Online]. Available at Internet: http://oscar.cprost.sfu.ca/~isp253/992/netbucks/risks.htm. Date visited: 12 October 2001.

Owen, L. 1994. The Future of Information Systems Audit and Control. IS Audit & Control Journal. Volume IV. 1994. Information Systems Audit and Control Association.

Oxford Dictionary. 1984. *The pocket Oxford Dictionary*. Seventh edition. Clarendon Press. Oxford.

Paliotta, A.R. 1995. Protecting the Electronic Environment in the 'New Technological World Order'. *ISACA Journal.* Volume VI. *1995*. p6.

Paliotta, A.R. 1999. A personal view of a World Class IT Auditing Function. [Online]. Available at Internet: http://www.itaudit.org. Date visited: 6 March 2000.

PWC (PricewaterhouseCoopers). 1998. *Technology Forecast: 1999* Published by PWC Technology Centre, California, USA, October 1998.

PWC (PricewaterhouseCoopers). 1999. Electronic Business Outlook. [Online]. Available at Internet: http://www.e-business.pwcglobal.com. Date visited: 20 August 2000.

PWC (PricewaterhouseCoopers). 2000. 'Securing the Internet Economy'. *Infoworld*. p3.

PWC (PricewaterhouseCoopers). 2001. 'Risk Management Forecast'. *PricewaterhouseCoopers LLP*. p7.

Restell, P. 2001. 'BS 7799 - Information Security Management'. [Online]. Available at Internet: http://www.bsi-global.com. Date visited: 28 July 2001.

Rutgers. 1998. 'Risks and Securities of On-line Information Flows'. [Online]. Available at Internet: http://www.rutgers.edu/Accounting/raw/mikos. Date visited: 27 October 1998.

Sayana, S.A. 2002. The IS Audit Process. *Information Systems Audit and Control Journal*. Volume 1. 2002. Published by the Information Systems Audit and Control Association.

Siebel, T.M. & House, P. 1999. 'Cyber Rules - Strategies for Excelling at E-business'. *Currency and Doubleday*. May 1999. New York. p50.

Siegel, C.A. 1997. 'Managing Risk in Electronic Commerce". *Auerbach Publications*. 82-10-26. p1.

Tibaldeo, G. & Buben, D. 1996. Cashing in on Technology: A Primer on Electronic Payment Systems. *IS Audit & Control Journal.* Volume VI. 1996. p14-18.

US Department of Commerce. 1998. The Emerging Digital Economy – Chapter 1 [Online]. Available at Internet: Http://www.ecommerce.gov/viewhtml.htm. Date visited: 2 June 1999.

Vandenoever, C. 1995. "Information Protection, your Business and the Internet". Deloitte &Touche LLP.

Verisign. 1999. 'Securing Your Web Site For Business'. [Online]. Available at Internet: http://www.verisign.com/rsc/gd/srv. Date visited: 8 October 1999.

Walder, B. 1999. 'Internet Security'. [Online]. Available at Internet: http://www.nss.co.uk. Date visited: 23 July 2001.

Warigan, S. 1999. 'Commercial, Privacy Protection, Regulatory, and Security Implications of Electronic Cash'. *Auerbach Publications*. CRC Press LLC. pp 16-19.

Wilson, J.D. & Root, S.J. 1983. *Internal Auditing Manual*. Warren Gorham & Lamont: 1-1 to 1-23.

Zeus. 2001. 'Increasing Security, Reducing Workload'. [Online]. Available at Internet: http://www.zeus.co.uk/library/articles/security.html. Date visited: 12 October 2001.

Zimits, E.C. & Montano, C. 1998. 'Public Key Infrastructure: Unlocking the Internet's Economic Potential'. [Online]. Available at Internet: http://www.iword.com/iword32/istory32.html. Date visited: 14 August 1999.