

Information Security Challenges Facing TEISME Business Operations in the UK

Charles A. SHONIREGUN
Sonny NWANKWO
Chris IMAFIDON
Peter WYNARCZYK

One of the major challenges facing the technologically advanced world is how businesses can function through vast interrelated and complex network, without sacrificing human creativity and individuality. Against a backdrop of psychedelic change the Technology Enabled Information Small Medium Enterprises (TEISMEs) must create plan and control their business operations to achieve high goals. TEISMEs are SMEs that provide services based on 80% electronic transmission of sensitive and non-sensitive information and 20% human interaction, within their normal course of business operations. By our definition, the amalgamation of Technology Enabled Information (TEI) and Small Medium Enterprises (SMEs) has given birth to TEISMEs. The TEISMEs business operation relies exceptionally and heavily on information transfer via the internet. This paper discusses the information security challenges facing TEISMEs business operations in UK. A questionnaire survey was conducted to find out how safe and what security control measures are used by TEISMEs as a result of their reliance on TEI. The question posed by this paper is that, 'can absolute security be attainable on TEISME business operations or not'.

Keywords

- Internet-eC
 - information security
 - social engineering
 - TEISMEs
 - virus
-

The economic challenges of information security will be pervasive, on both businesses and the society. For those businesses that fully exploit the potential of TEI, the possibility of breakpoint changes that so radically alter customer expectations and re-define the market or create entirely new markets will be noticed. The information security challenges facing TEISMEs business operations will impacts the safety of information transfer on the internet. In everyday life goods are paid for in a number of ways, either by cash, cheque or electronic payments via credit or debit card. All other businesses, including those that try to ignore the TEI, will then be impacted by changes in the market and customer expectations.

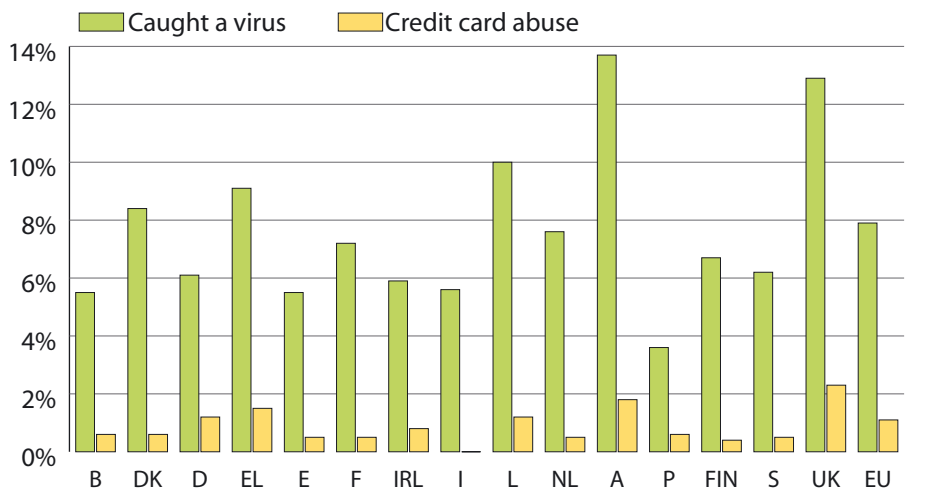
The term security describes the capability of TEI to ensure confidentiality, integrity and authenticity of transmitted and stored data against threads or attacks [1]. Information security is definitely an issue. *How and where do we draw the line and how do we ensure that what is behind the line is safe?* We are going to need that kind of technological breakthrough to really make advance [2] or to have a risk assessment that will give an accurate projection where others have failed. Traditionally security was used by businesses to protect property of a physical nature, by the use of a security guard or an alarm system. In today's world the security guard and an alarm system still serve as an effective deterrent to the common thief. They do nothing however to protect business organisations against the unauthorised access and deprivation of information, by hackers (cyber terrorists) via the Internet, which happens under their very noses. A study by the Department of Trade and Industry (DTI) (2002) has concluded that, *nearly two thirds of small businesses with crucial or sensitive information have suffered serious breaches of security* [3, 4]. These studies and the statistics highlighted the very real risk of an attack on a web site and the scale of the problem, which unfortunately seems to be spiralling out of control. The computers and services providers server are seen to be targets that can be attacked ('do to'), or tools that can be used ('do...with, on, or from'). From this perspective, computer security is distinguished from information security. Chiswick et al., (1994), defined computer security as [5]:

'keeping anyone from doing things you do not want them to do to, with, on or from your computers or any peripheral devices.'

A report published by the DTI in April 2002, found that computer hacking, cyber fraud, and software bugs are costing Britain up to £10 billion a year. According to the DTI, 50% of all businesses were victims of such attacks compared with 25% in 2000 and less than 1 in 5 in 1998. The report found that attacks by hackers on

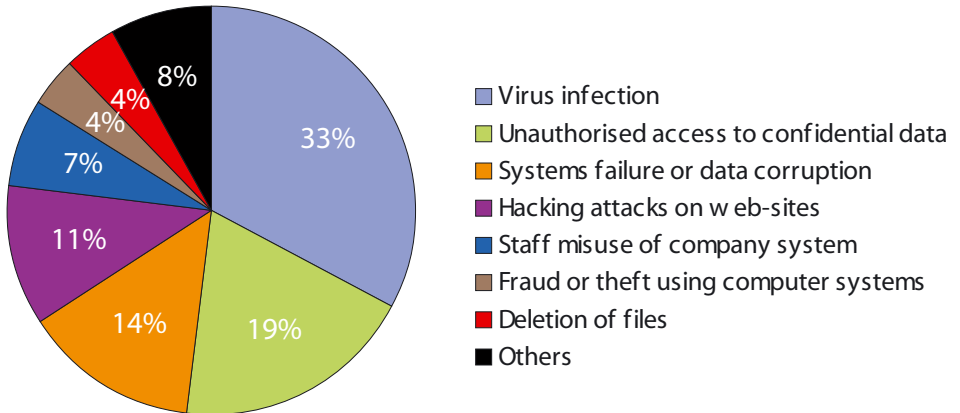
SMEs more tripled in the past years and 4 out of 5 the businesses have been victim of virus or fraud in 2001. The average cost of each security lapse is £30,000, and fraud and hacking had cost well over £500,000 [6] (see Table 1 for current average cost of worst security incident). In relation to a security of TEISME networks there is little data available on this understandably confidential subject. One of the few is the number of secure socket layer (SSL) servers. The OECD found that, on a per-capita basis, the USA had six times as secure servers as the EU [7]. The Figure 1 below shows that the percentages of credit cards abused has been relatively low compare to virus attacks on businesses among the 16 countries survey by Netcraft and Eurobarometer in 2000.

Figure 1 Security Problems of Credit Cards and Viruses (% Internet Users) (Adopted from Netcraft and Eurobarometer, 2000) [7]



Furthermore, due to all the fraudulent acts that have taken place, businesses are trying to make their TEI more secure, but the root problem is that majority of internet business users do not possess technical knowledge and lack the know how on security for their systems. The Netcraft and Eurobarometer (2000) results presented in Figure 1 shows similar outcomes to the a survey conducted by the DTI 'Information Security Breaches Survey 2002', with an estimated 33% viruses, indeed, viruses are still the most profound security breaches reported so far (see Figure 2 below).

Figure 2 DTI Information Security Breaches Survey 2002 (Adopted from DTI) [3]



The unprotected systems are fair game for hackers who would use them as attack platforms in order to promote their own goals. The increasing numbers of TEISME who do not take the necessary steps to protect their own systems are further compounds with unprotected systems problems. However, even though orders are sent through secure applications, many businesses still print out orders on paper, which could be stolen or copied easily. Unless businesses streamline their order and payment processes and connect back office applications, the security of front end might not lead to fully secure transactions. We shall now look at the various concerns of TEISME with regards to TEI. The risk of a computer virus attack is increasing at an alarming level. E-mail service provider MessageLabs saw the number of hostile e-mail attachments triple between 2001 and 2002. In the early months of 2001, MessageLabs found that 1 in every 1053 emails coming through their company's gateway had a malicious attachment. One year later the frequency was 1 in 325 [3].

3

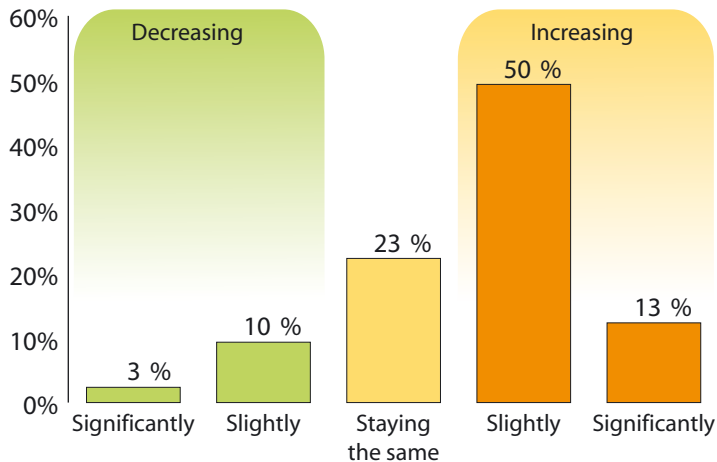
Sheared Threats

Horton et al (2000) states that there are risks involved in sharing information and also no aspect of internet-eC is independent of other critical factors, and that massive amount of information are transmitted continuously to help maintain vital services and economic well-being [8]. TEISMEs needs to identify what Horton et al (2000) called 'a complete threat population' when assessing threats of information security. However, Martin (2000) identifies seven key risks, which can threaten TEISME business operations. These seven key risks are discussed below:

Fraud

Fraud has a worldwide impact and is highly publicised in many internet-eC research reports. In the third quarter of 2000, and again in the third quarter of 2001, Gartner surveyed online retailers with the largest transaction volumes across several industries regarding electronic payment issues, including the issue of online fraud. Online fraud rates have held steady since 2000, despite significant efforts by merchants, card issuers and law enforcement to curb fraud. In 2000, online fraud losses were 1.13% of \$44.2 billion in annual online sales. In 2001, some \$700 million was lost, representing 1.14% of \$61.8 billion in online sales [9]. These figures in Figure 3 below do not include additional labour and fees spent on fraud investigations or merchant fines that are sometimes imposed by credit card companies for high levels of charge-back, which include outright fraud and other disputes 'Is Internet transaction fraud increasing or decreasing?'.

Figure 3 Merchants' view of Online Fraud Trends (Adopted from Gartner Survey 2001) [10]



Although the fraud nature of fraud in questioned can be committed by a member of staff or by people outside the TEISME business operations (they may be parties in a foreign country) using the website as a tool. The following fraudulent activities are most commonly encountered by TEISMEs:

- Unauthorised movement of money (e.g. making payment to fictitious suppliers located in areas (safe havens) where recovery of money is difficult (e.g. Switzerland))
- Misrepresentation of company tenderers
- Corruption of the electronic ordering or invoicing
- Duplication of payment
- Denying an order was placed/received
- Denying receipt of goods
- Denying that payment was received or falsely declaring that a payment was made.

The fact that some of the TEISME's employee themselves, and many handsomely paid, are largely involved in fraud, we strongly suggests that TEISME's business operational security is unattainable. According to Smith (1998) total security can never be guaranteed either in physical world or the virtual universe of open networks, so companies looking at internet-eC need to evaluate the level of fraud that they can expect, bearing in mind that the risk of fraud losses on commercial transactions is comparatively small [10]. This raises the question of the security of the Internet-eC. There are many types of fraud, the most significant of which has been seen by the introduction of credit and debit cards to our society, which has seen the crime of Internet fraud. Fraud can take place at a retail outlet when an unauthorised user (a person whose name is not specified on the card, but pretends to be that person whose name is specified) of a credit or debit card uses it to purchase goods or service. In much the same way, fraud can take place on the Internet, and this is what is known as Internet Fraud.

Internet crime is the most significant problem Visa is dealing with in Europe'

—John Prideau (Visa: Executive Vice President, 2000)

The situation has also been made worse by the fact that when ordering goods by credit card, they can be delivered to an alternative address or/ addresses, whereas before, when paying for goods using this method, any goods ordered had to be delivered to the card holders address.

Loss of privacy/confidentiality

The success of TEISMEs business operations largely depends on information on the Internet. But customers are increasingly concerned about the amount of information required and the degree of security the TEISMEs and their service provider applies to the information. The result is that if people who provide the information are less confident that the information they provide is not adequately protected, then they may not be willing to provide it next time they visit the TEISME's website. The information at risk includes customer's name, contact details, previous purchases, services provided, criminal or medical records etc.

According to Gosh et al., (2001), when engaging in transactions or simply communicating over the Internet, most people naively assume that their message remains private. In fact, it is quite easy for an interested party to eavesdrop on other people's Internet conversations. While the electronic age has made communication arguably easier, it has made intercepting communications easier for unknown third parties [11]. The TEI introduces technology that poses new challenges to TEISMEs business operations. On-line activities can be recorded to track, which files or Web sites one has visited. Such information are collected by both TEISMEs and their internet service provider. The e-mail addresses can be collected for 'spamming' — the practice of sending unsolicited e-mail and other electronic communication to TEISMEs and their customers, which leads many hours of filtering these unwanted messages [12, 13] and not cost effective on the long run.

'The right to privacy is the right of the individual to decide for himself how much he/she will share with others his/her thoughts, feelings, and the facts of his/her personal life... Actually what is private varies from day to day and setting to setting.'

—*Off of Sci & Tech of the Exe Off of the US President (1999)*

Globally speaking, not all countries see information as the property of the collector. In 1995, the European Parliament announced a directive stipulating that individuals on whom information is collected be made aware of the users of the information, the purpose for the collection, to whom the information may be disclosed, right of access, and correction. On-line businesses constantly gather and use demographic information from users who are afraid that their personal data, including credit card numbers or their behaviour on the Net, many be sold, used, or revealed in appropriate manner. Such fears keep many consumers from shopping on-line [14, 15].

Lack of Authentication

Lack of authentication refers to a transaction without being authorised to do so. Because of the sheer mass of information being circulated during TEISMEs business operations and the concerns over the amount of information requires the degree of security applies to the information, it becomes important to provide adequate authority to customers who are involved business transactions. However, once a transaction has been accepted over the network, it becomes legally binding and liability is created for a party involved in the transaction. The risk here is that because 'the paper-based controls are limited to allow reconciliation, the authentication process may well accept the unauthorised party indefinitely and go undetected'. The risks may result from corruption of a list of signatories, creation of fictitious supplies (masquerade), unauthorised ordering or approving a transaction etc.

'Security analysts agree that most computer fraud is accomplished by traditional methods, involving physical access to sensitive data. Nonetheless the public perception of data networks is of an electronic world plagued by swarms of ingenious hackers.'

—*ISOCOR (1999) Marking the Commercial Superhighway Happen', January.*

Authentication is proving that you are who you say you are. This is a concern for both TEISMEs and their consumers. The pure number of virtual retail outlets offering goods at discounted prices is like a paradise for bargain hunters everywhere. Some of the web sites advertising these goods or service have never been heard of before and are not established retailers. A few cases have been reported where virtual shops have been created, that are remarkably similar to well-known companies, tricking the customer in believing that they are an established retailer and accept payments for goods or services that they never intend to deliver or where the description of an item is significantly different to that advertised (also an aspect of fraud). The subject of authenticity also arises in e-mail spoofing, when a user receives an e-mail that appears to have originated from one person, but is actu-

ally sent from another person trying to impersonate a third individual. The goal of e-mail spoofing is to trick the user into divulging information or replying with information that is confidential.

Repudiation

In certain circumstances, the TEISME transaction conducted over the network system indicates that buying and selling have taken place, but one of the parties repudiates or denies it. This can result to invalid contracts, TEISME not being paid for goods and services delivered or customers not receiving services/goods already paid for. In turn, this can create liabilities that can result in a company going out of business.

Corruption of data

This is the violation of data integrity. According to Gosh et al., (2001), the data integrity attacks are not often discussed in the context of internet, they are nevertheless of concern to the internet-eC community as it impacts upon TEISME business operations transactions. The violations in the information sent over networks are often incidental and unintentional, but the potential to maliciously alter the information in order to affect some outcome do exist in different ways. This argument has been supported by Martin (2000), that the commonly held view is that risks involve activities that can be performed remotely through web resources; the reality, however, is that almost all corruptions are conducted within the system. Examples of malicious damage that can be done by hackers, staff, clients or suppliers range from amending catalogue without authorisation, destruction of audit trail through tampering with the ordering process, to disrupting online tendering, posting inaccurate information online (e.g. stock information). This suggests that corrupt data may render TEISMEs business contract invalid [11, 16].

Business operation interruptions/denial of service

The TEISMEs business operations interruptions are considered as a key risk because they are tantamount to a denial of service (i.e. making services unavailable), the ultimate internet security nemesis. The business interruption or denial of service can lead to financial crisis and lawsuits. For example, Internet providers that depend on BT communication system may be denied services to their clients if there is a major breakdown in the BT communication system. Thus the major risks to be considered by TEISMEs include the following denial of security tools, infrastructure failure (e.g. due to lack of resources), how to assess the claim and who will pay compensation.

Inadequate funding

Inadequate funding is classified as a risk element for e-commerce businesses because both the software or hardware that make up TEI are regularly changing which means that TEISMEs will need to be kept up to date with the advancement in TEI which eventually will cost TEISME to continuously upgrading their TEI. This demands substantial investment as well as the business process being re-engineered.

4

Social Engineering

Social engineering is one of the hardest attacks to stop and inevitable risk of all to TEISMEs and their customers. It takes advantage of the weakest element in the security chain—people. Why attempting to hack into a system when you can probably get the information such as login password from the help desk or the service provider's staff? Social engineering is defined as an outsider trying to trick legitimate personnel into disclosing information or granting inappropriate access [17]. The human based social engineering adopts the low-tech approach. An example of a human based social engineering is when a hacker phone up a help desk to gain vital information from the technical support staff. This is surprisingly easy to do since most people are inherently trusting and would disclose sensitive information to their friend(s) unknowingly. There is a misplace if trust that free discussion at lunch time or at dinner even among friends in a social gathering can led to information which provides clues to some vital security breaches. So the argument that arises here is that how do TEISMEs employees know when in breach of security information.

5

Discussion

According to Horton et al., (2000), thousands of unauthorised attempts are made to intrude into systems that control key information resources and infrastructure components, including power grids, communication networks, banks, transportation systems, and defence facilities [8]. *No businesses that uses the internet or other shared networks or depends on other infrastructure components are immune to any attacks.* But some TEISMEs enable intruders to gain 'system administrator status', download sensitive files such as passwords, implant 'sniffers' (or what is dubbed here as internet dogs or spy-ware) to copy transactions, insert 'trap doors' to permit easy return, or implant program that can be activated later for a variety of purposes. The Hackers have been around for approximately twenty years, shortly before the more commercial use of the internet began. They are comparable to modern day burglar, except with one significant difference, a hacker does not have to be physi-

cally present at the scene of a crime. All that is required for any intrusion to take place is the use of a computer terminal that has an internet connection, location of where the unauthorised entry or appropriation of property or information is to take place and the appropriate software and techniques of accessing internal networks and personal computers. Hackers continue to develop new software and various techniques for accessing internal networks and personal computers. The web site www.alt2600.com provides information on the latest sites attacked by hackers and the links to tools that they use. More hacking software are now readily available on the Internet for free. For example, Portscan 1.2 is a utility, which allows the user to scan ports on any target system. The user specifies the target IP address. The program then scans all ports between 1 and 65536. The resulting information can then be used to find loopholes in a security set-up. Another tool similar to this is IP-Prober; it allows open ports to be scanned in order to gain entrance to a network. Password cracking represents another method hackers use to enter networks. Again several tools for cracking passwords and codes can be found throughout the Internet. The majority of these tools work by generating potential password combinations including both letter and number codes. The majority of these software tools can repeat this process, millions of times. As a consequence, the number of UK businesses that suffered a security breach continues to rise. The Table 1 below shows the average cost of worst security incident [18] and the ranges are quoted because of the inherent uncertainty involved in extrapolation.

Table 1 Average cost of worst security incident (Adopted from PricewaterhouseCoopers [19])

	Overall	Large businesses
Disruption to business	£5,000–£10,000 Over 1–2 days	£50,000–£150,000 Over 1–3 days
Time spent responding to incident	£500–£1,000 Over 2–4 man days	£3,000–£6,000 Over 10–20 man days
Direct cash spent responding to incident	£1,000–£2,000	£5,000–£10,000
Direct financial loss (e.g. loss of assets, fines etc.)	£200–£500	£2,000–£4,000
Damage to reputation	£100–£300	£5,000–£20,000
Total cost of worst incident on average	£7,000–£14,000	£65,000–£190,000

An online questionnaire survey was conducted within TEISMES in the UK, to find out how safe and what security control measures are used by TEISMES as result of their reliance on TEL. The Table 1 presented the outcomes of the 400 TEISMES directors / managing directors that participated in the survey. We received 118 questionnaires out of 400. The first question we asked the 118 TEISMES directors / managing directors, was 'do they consider the internet to be safe for their business operations'. The responses to this question was 80 (92%) out the 118 TEISMES Directors and/or Managing Directors agreed that the internet is not safe to transact business operations, then the question that this result posed is that why are the

TEISMES still doing business on the internet. When asked the second question was about the security control measures they adopted, the survey revealed that the types of security control measures adopted by the TEISMES are combinatory security control measures (see Table 2).

Table 2 Security control measures

	Public key encryption	Firewall	Digital signature	Password	Keystroke	Email sniffing	Personal Identity (ID)
Yes	98	82	7	118	5	21	118
No	20	36	111	0	113	97	0

The survey result shows that Password and Personal identity accounts for 118 (100%) of the most common security control measure adopted while the use of Public key encryption shows 98 (83%) with 20 (17%) 'No', Firewall 82 (69%) 'Yes' with 36 'No', Digital signature 7 (6%) 'Yes' with 111 (96%) 'No', Keystroke 5 (4%) 'Yes' with 113 (96%) 'No', and Email sniffing 21 (18%) 'Yes' with 97 (82%) 'No'.

However, the analysis presented in Table 2 shows that TEISMES used a combination of security measures to protect their business operations. This view is supported by Brent Huston (2002) who claims that security in modern world relies completely on layers of defence referred to in the military world, as 'defence in depth'. The defence in depth goes beyond platforms, products, and patches and the protection of assets can no longer be left to simple single-point solutions. He considered the firewall security systems as nothing more than a little speed bump unless it forms an integral part of an overall security solution integrated with components that enhance and support its position. He suggested the use of Network intrusion sensors, host-based hardening and monitoring, network access lists on perimeter devices, and log watching accessories all combined with hardware tokens, honey pots, and a myriad of other devices, products, and strategies to create an effective technical security bastion [20]. Brent Huston's view strongly supports the hypothesis that 'absolute security is unattainable'. The number of attacks from outside crackers is catching up to the frequency of unauthorised access from insiders. Insider attacks also rose for the third straight year, with 55% of the respondents reporting incidents, a 10% increase from last year [21]. Indeed, many companies have opened themselves to attack by installing a firewall without dedicating resources to manage it effectively. Effective security requires an adequate budget, staff training, and management support. A firewall is not a one-time silver bullet. The most recent security lapse has been exposed, the potential risk to TEISME business operations and merchants who share web servers with other businesses, is that, it is possible to locate and compromise a private key that is encrypted and buried in the disc storage of web server. This discovery offers the possibility that a hacker with access to TEISME business's server or their merchants server could locate cryptographic key that would allow access to secure credit card numbers.

Internet security demands attention at multiple levels. Although biometrics is still relatively expensive and immature but the integrated multiple biometrics features such as fingerprints, palm prints, facial features and voice patterns to authenticate a person's identity and verify his or her eligibility to access the internet are in the development stage [22]. Most of the time when security on the internet is mentioned, it is assumed that the data is safe from hacker or unauthorised third parties. But '*what exactly does security on the internet cover?*' and '*Is it just unauthorised access of data or more?*', Many researcher have highlighted six criteria that the internet has to satisfy in order to be considered 'secure' i.e. confidentiality, authenticity, integrity, non-repudiation, access control and availability but what has no yet been emphases upon is that the internet can not be 100 per cent secure. However, no insurance companies in the UK are willing to insure TEISMEs business operational risks but to insure the risks that may be encountered electronically will foster trust. So can absolute security be attainable on TEISME business operations or not, what we believed is that only the future technology advancement can answer this question, but who knows and that is if.

REFERENCES

1. Pfleeger, C.P., (1997), 'Security in Computing', 2nd Edition, Prentice-Hall Englewood Cliffs, NJ.
2. Bond, B., (2000), 'The e.volving New e.conomy - A Roundtable with Gartner Analysts, Gartner Special Report, eAI Journal, pp 16–20, Oct.
3. Department of Trade Industry (DTI)., (2002), 'Information Security Breaches Survey', p. 20 <http://ukonlineforbusiness.gov.uk/cms/template/infor-security.jsp?id=213097> (Accessed date 8 Jan 2003).
4. CERT Research, (2001), 'International CERT Conference on Computer Security and Information Assurance', Omaha, NE USA, August.
5. Chiswick et al., Firewalls, and Internet Security, Pub Addison Wesley Professional Computer Series, 1994
6. Fraud Advisory Panel (FAP) Technical Report, (2003), 'The fraud Cybercrime advisory, What every SME panel should know', Chartered Accountants' Hall. <http://www.fraudadvisorypanel.org/pdf/Cybercrime%20what%20every%20SME%20should%20know.pdf> (Accessed date: 23 Sept 2003)
7. Netcraft and Eurobarometer, (2001), 'e-Europe 2002 Impacts and Priorities', Commission of the European Communities, Brussels, 140 Final: Communication from the Commission to the Council and the European Parliament http://www.ekt.gr/ncpfp5/ist/info/material/eeurope/impact_en.pdf (Accessed date: 13 Nov 2003)
8. Horton, T.R., LeGrand, C.H., Murray, W.H., Ozier, W.J., and Parker, D.B. (2000), 'Risk Management - Managing Information Security Risks', Part 1 Vol. # 3 August 15, 2000 and Part 2, Vol. # 3 October 15, <http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=25> (Accessed date: 10 November, 2001).
9. Kerr, K., and Litan, A., (2002), 'Online Transaction Fraud and Prevention Get More Sophisticated: Companies, Markets, Forces', Gartnerg2, <http://www.gartnerg2.com/research/rpt-0102-0013.asp> (Accessed date: 6 Nov 2003).
10. Smith, A.M. (1998), 'Electronic Commerce', In Institute of Directors, Directors Publications, p.62.

11. Gosh, A. K. and Swaminatha, T. A., (2001), 'Software security and privacy risks in mobile e-commerce', *Communications of the ACM*, February, V44 i2
12. Cranor, L.F., and LaMacchia, B.A., (1998), 'Spam!' *Communication of the ACM* 41, no 8, August.
13. Loudon, K. C. and Loudon, J. P., (1999), 'Essentials of Management Information System', 3rd ed., Prentice Hall, Inc.
14. Haag, S., Cummings, M., Dawkins, J., (2000), 'Management Information Systems, For the Information Age', Ed 2nd.
15. Turban et al., (2000), 'Electronic Commerce, A Managerial Perspective', Pub Prentice Hall.
16. Martin, C., (2000), 'An International and Strategic Networks: An SME Perspective', Paper presented at the 5th International Manufacturing Research Symposium International and Strategic Network Development, The Centre for International Manufacturing, Cambridge University September.
17. Gragg, D., (2003) 'A multi-level defence against social engineering' SANS Institute, <http://www.sans.org/rr/papers/51/920.pdf> (Accessed Date: 18 Sept 2003)
18. Shoniregun C.A. (2002), 'The Future of Internet Security', *Communication of The ACM: Ubiquity*, Volume 3, Issue 37, p 1, Oct 29.
19. PricewaterhouseCoopers, (2004), 'Information Security Breaches Survey 2004 Technical Report', in association with Computer Associates, Entrust and Microsoft DTI recommendation, <http://www.pwc.com/images/gx/eng/about/svcs/grms/2004TechnicalReport.pdf> (Accessed date: 23 March 2004).
20. Huston, B. (2002), 'A Higher view of Defence in Depth', <http://www.itworld.comh/nl/securitystrat/02202002/>
21. BMRB Research Group, (2000) 'Internet Monitor', International Research Report, Oct.
22. Shoniregun, C. A., (2004), 'Are existing internet security measures guaranteed to protect user identity in the financial services industry?' *International Journal of Services, Technology and Management (IJSTM)*, Volume 4, pp194–215.