

E-business security in international perspective

N. L. Karmakar

School of Management, University of Western Sydney, Australia

Abstract

Security is a key barrier for reaping the full benefits of e-Business in an organisation. The term 'e-Business' is used in academic and business circles very frequently since the beginning of the new century. This is not just about commercial transactions over the Web, it is the overall strategy of redefining old business models using new technology to maximise customer value and profits. E-Commerce, an application of e-Business can be used to create virtual global trading collaborations among customers, suppliers, distributors and financial institutions. This radical shift in business paradigm is creating a huge market in cyberspace. The new world of e-Business has been the source of wealth creation for some developed countries, the USA in particular. It is projected that the USA will have up to \$7 trillion in online trade by 2006. In spite of this huge potential, it has some set backs that have questioned the reliability of the Web. In 2001, online fraud losses were more than \$700 million, or 1.14% of the total online sales of \$61.8 billion. The new technology is constantly developing to keep e-Business applications over the Internet safe and secured. The purpose of this paper is to explore major e-Business security issues from an international perspective. With the rising importance of e-Business, security will become an even more pressing concern.

Keywords: cryptography, cybercrime, digital economy, e-commerce, ethics, Internet, law, privacy.

'Do not figure on opponents not attacking; worry about your own lack of preparation'.

-----Book of the Five Rings

1 Introduction

Security issues in cyberspace to undertake e-Business are attracting attention in industries and governments around the globe. E-Business Security is related to



Internet security which is not about protecting hardware, it is about protecting information. The field of security in cyberspace focuses on designing measures that can enforce security policies, especially in the presence of malicious attack.

The Internet is the fastest growing, most user-friendly, and most commercially popular technology to date. This is based on an open network architecture, so information can be transferred freely and efficiently. While this greatly facilitates the development of e-Business applications, it also raises many security concerns. The Internet is the playground for hackers and lawbreakers. Fortunately, by using modern cryptographic techniques, we can make e-Business applications over the Internet safe and secure [1].

In this paper we have introduced some of the issues and measures taken to secure a website or network. Within a business framework, management develops a set of policies and procedures aimed at securing the network from external and internal threats [2]. The Internet is the source of digital economy and globalisation and thus gives rise to new threats to security, privacy, and ethics [3].

2 Security in general

In general, *security* is “the quality or state of being secure – to be free from danger” [4]. It means to be protected from adversaries-from those who would do harm, intestinally or otherwise. A successful organisation should have the multiple layers of security in place to protect its operations, such as *Physical Security*, *Personal Security*, *Operations Security*, *Communications Security*, *Network Security* and *Information Security* [5].

To protect the information and its related systems from danger, such tools as policy, awareness, training and education and technology are necessary. In short, security relates to controlling one’s environment for protection of data [6].

3 E-Business and e-commerce in a nutshell

E-Business is an integration of all the business processes required to buy and sell goods and services over the electronic platform known as the Internet. This is not a new concept: rather it is an evolution of traditional business practices taking advantage of the new technologies of the Internet age to enhance efficiency and productivity. IBM defines e-Business as “a secure, flexible and integrated approach to delivering differentiated business value by combining the systems and processes that run core business operations with the simplicity and reach made possible by Internet technology” [7]. It is vital to remember that e-Business is much more than e-Commerce which is defined as ‘buying and selling over digital media’ [8].

4 What is e-Business security?

E-Business Security may be defined as the *policies, procedures, practices*, and *technology* that must be in place to undertake business electronically via



networks with a reasonable assurance of safety. This assurance applies to all online activities, transmissions, and storage. It also applies to business partners, customers, regulators, insurers, or others who might be at risk in the event of a breach of that organisation's security. Ultimately, it may be court that is called on to decide whether reasonable security existed at the time of the breach [9].

With the advent of e-Business and increased use of the Internet, security has been a frequent headline in the news media. Many businesses and individuals alike routinely send sensitive data across the Internet. These data must be protected because network-enabled e-Business requires a high level of security in order to be successful. Unfortunately, the Internet was not originally designed to be a highly secure system. The good news is that a number of technologies have been developed to increase the security of the Internet and Web [10].

5 Privacy concerns in e-Business

Security and *privacy* are said to be two of the biggest challenges regarding e-Business. In reality, both are major concerns for any computerised environment including businesses, education, government and individuals. Privacy can be defined as 'the ability to manage information about oneself' [10]. The issue of privacy has become one of the hottest topics in e-Business security at the beginning of the twenty-first century. Many organisations are collecting, swapping, and selling personal information as a commodity and many individuals are aware of these practices and looking to governments for protection of their privacy. The ability to collect information as an individual, combine facts from separate sources, and merge it with other information has resulted in databases of information that were previously impossible to set up [5].

6 Ethics in e-Business

Due to the explosion of e-Business new industries are emerging and new business models are being invented. The new business environment includes new legal and ethical problems that the business people in the digital economy must be acquainted with in order to handle them properly and operate effectively. Ethics is a branch of philosophy that deals with what is considered to be right and wrong. *Ethics* has assumed a new dimension of importance as e-Business open-up a new spectrum of unregulated activities. Business people need guidelines as to what behaviours are reasonable under any given set of circumstances. E-Business is so new that the legal, ethical, and other public policy issues that are necessary for e-Business existence is still evolving [11].

7 Security threats in e-Business

There are many security threats in e-Business which face several challenges that are inherently not as challenging in traditional business. In [12], Kou lists the



potential threats and attacks to which commercial activities in networked environments may be vulnerable:

- Accessing unauthorised network resources
- Destroying information and network resources
- Altering, inserting, or modifying information
- Disclosing information to unauthorised people
- Causing networking services disruption or interruption
- Stealing information and network resources
- Denying services received, and denying information sent or received
- Claiming to have provided services that have not been administered and/or claiming to have sent or received information not given.

E-Business applications and technologies must address these security issues. It is helpful to break the threats into two categories- '*threats to data*' and '*threat to systems*'. Since the Internet is a network of networks, data that are transmitted via the Internet typically pass through a number of networks in order to reach their destination. At any point during the transmission, the data are subject to being intercepted. Once unauthorised individuals access the data, they are subject to misuse or alteration. The implications of intercepting data such as credit card numbers are obvious. However, other types of business data are equally important. For example, an organisation is subject to potential damage if its competitors could get access to sensitive e-mail correspondences.

As the Internet is an open network, it invites easily security threats related to systems. In theory, unless security measures are implemented, any computer on the Internet can access any server on the Internet. As a result, organisations must be careful to secure their systems against unauthorised access. Organisations that fail to take the proper precautions risk potential theft or loss of valuable data. An additional threat to systems comes from viruses that propagate across the Internet. Even if access to servers is restricted, those with access may mistakenly transmit dangerous viruses [10].

In a 2001 survey, 538 security professionals in US corporations on the risk of doing e-Business published by the Computer Security Institute and the FBI's Computer Intrusion Squad were asked "What security breaches or espionage occurred in your company in the past year?". Ninety three percent of the respondents reported computer viruses. These and other threats are summarised in Table 1 [13].

The total projected losses for 2001 due to security breaches were US\$377.8 million (up from US\$265.6 million in 2000) and losses from financial fraud are rising. The highest single loss (theft of proprietary information) in the 2002 CSI/FBI survey was US\$50 million (up from US\$10 million in 1997); the average loss was US\$4.6 million. The report states that the credit card information is the single most commonly traded financial instrument for attackers [14]. In 2003, 75% of the survey respondents of 530 acknowledged financial losses, but only 47% could quantify the losses [15]. For both individuals and organisations, credit card fraud is really scary [16]. There are however, some threats that US corporations rarely consider as top priority, while managers in other areas of the world must take them into consideration. Political



unrest and regional instability are two examples. Other examples of unique threats include natural disasters in areas prone to those, or civil unrest in other areas, all of which can cause business interruption.

Table 1: Computer Security Institute/FBI 2001 survey of security threats.

Security Breaches	% Of Respondents (<i>approx.</i>)
Computer virus	93
Insider abuse of Net Access	90
Unauthorised access by insiders	64
Laptop theft	61
System penetration	40
Theft of proprietary information	24
Sabotage	19
Financial Fraud	11
Telecom eavesdropping	11
Telecom Fraud	11
Active wiretap	3

Around the globe, security threats and concerns are similar. For example, a survey of security directors in an Asian corporation revealed that their top ten security issues were similar to those of their US counterparts [17].

7.1 Global trend in general

Senior representatives of more than 3,600 companies in 50 countries were interviewed during ‘Global Economic Crime Survey 2003’ by the PricewaterhouseCoopers [18]. The economic crime remains a significant threat with 37% respondents report significant economic crimes during the previous two years and the average loss per company was US\$2,199,930. The survey has identified that the gravest concerns for the future are asset misappropriation – the most visible of economic crimes and cybercrime. Looking forward over the next five years, 35% of companies expect their greatest economic crime risk to be asset misappropriation and 31% cybercrime. The cybercrime is still seen as a key risk for the future in North America (38%) and Western Europe (37%).

In ‘2001 Global *e.fr@ud. Survey*’ [19], KPMG Forensic & Litigation Services practices surveyed the world’s largest companies on the topics of e-fraud and security related issues in the world of e-Commerce in the following 12 countries:

Region	Countries
Asia Pacific	Australia, Hong Kong, India
Europe, Middle East and Africa (EMEA)	Belgium, Denmark, Germany, Italy, South Africa, Switzerland, United Kingdom
Americas	Canada, United States



In total, 1,253 completed questionnaires were included in the survey findings, although KPMG sent questionnaires on e-Commerce & e.fr@ud to more than 14,000 CEOs, CIOs, and other senior executives of the largest public and private companies of those countries. Hackers, Poor implementation of security policies, and the lack of employee awareness were identified by survey participants as the greatest to their e-Commerce systems and the responses were consistent for all participating countries. Survey respondents suggested also that security of their e-Commerce system could be most improved by the following:

- ✓ Regular system penetration testing (authorized hacking)
- ✓ Use of software specifically designed for security issues in an e-Commerce environment
- ✓ Increased use of encryption technology

In response to their views on public perception about e-Commerce security, 88% of respondents feel that the public perceives the traditional, more established “bricks and mortar” businesses as being more secure than e-Commerce based dot.com, companies. The participants identified concerns about the security and privacy of information and a lack of familiarity with technology as being the most important preventing the consumers from engaging in e-Commerce transactions.

In Australia, losses from computer crime have more than doubled in one year according to the ‘2003 Australian Computer Crime and Security Survey’ [20]. The huge losses, around AUS\$ 11.8 million (US\$ 9.1 million) over the 214 organizations surveyed, have stemmed primarily from financial fraud (AUS\$ 3.52 million), laptop theft (AUS\$ 2.25 million), virus, worm and Trojan infection (AUS\$ 2.23 million) and insider abuse of resources (AUS\$ 1.27 million). External attacks against computer networks are becoming more common in Australia.

8 Cyber-terrorism

Cyber-terrorism is the use of computers and the Internet to launch attacks and horrible acts that may directly harm or kill people [21]. Computer systems control airline traffic and transportation systems, water, oil pipelines, and energy. Therefore, disruptions in any one of these systems could cause loss of life or widespread chaos [9].

Internet population is huge, from about 50 million Internet users in 1997, there could be as many as 750 million by 2007 [22]. Growth in the number of users, online services, and devices connected to the Internet has made more computer crimes possible, profitable, and low-risk. The first half of 2002 saw a 28% increase in Internet attacks, and almost 2000, 000 of them were successful [23].

Fifty or more new computer viruses are created each week [24]. Using evidence from sophisticated malware hacker attacks, the FBI estimated that losses by US businesses had exceeded US\$7 billion in 2001 [25]. This estimate does not include the costs of fraud or damages by disgruntled employees.



8.1 Recent events

- UK customers of the US Bank MBNA are being targeted by an e-mail scam. Some of its customers have been sent fraudulent e-mails asking them for their online bank details. MBNA is just the latest of the High Street banks affected by the scam, known as *phishing*. It comes with a variety of subject lines such as “MBNA’s Official Notice,” “Attention all MBNA users” and “Official Notice for all users of MBNA.” The message says the bank is putting in a new security system to “help you avoid frequently fraud transactions and to keep your investments in safety”. It then advises people to reactivate their account by clicking on a link in the message. Any customers who tries to login through this fake page is very likely to have their personal bank information or identity stolen and relayed directly to the spammers [26].
- The sixth variation of the worm known as **SoBig.F** was transmitted in August 2003 through a pornographic website. It infected more than 145,260 computers worldwide, jamming with useless e-mails. Bill Gates believes that software is still not strong enough to connect devices together and there are too many viruses and security devices [27].
- A mass-mailing virus ‘MyDoom’ is dominating news headlines. The virus, which experts say is the fastest spreading e-mail worm in history, has left hundreds of thousands computers vulnerable to hackers and spammers. MyDoom causes no apparent damage to computers. However it leaves behind a program that could allow hackers to steal passwords or files that tracks keystrokes. It has three variants such as, MyDoom.A, My Doom.B & My Doom.C. The original MyDoom.A worm shut down its target, American Software Company ‘SCO’ by bombarding it with information requests. The third variant, MyDoom.C or Doomjuice, is similar to the MyDoom.B worm, which was designed to overload Microsoft’s website using same technique. The economic fallout has been estimated at US\$ 26.1 billion. The hunt for the creators has proved fruitless, but the focus is on Russia, where it first appeared. Microsoft and SCO have offered US\$500,000 reward for information leading to the prosecution of the creators of the virus [28, 29].

9 Key dimensions of e-Business security

There are six key dimensions of e-Business security:

- *Integrity* - the ability to ensure that information displayed on a Web site, or sent or received via the Internet has not been altered in any way by an unauthorised party.
- *Nonrepudiation* – the ability to ensure that e-Business participants do not deny (repudiate) their online actions.
- *Authenticity* – refers to the ability to verify an individual or business’s identity.



- *Confidentiality* – determines whether information shared online, such as through e-mail communication or an order process, can be viewed by anyone other than the intended recipient.
- *Privacy* - deals with the use of information shared during an online transaction. Consumers want to limit the extent to which their personal information can be divulged to other organizations, while merchants want to protect such information from falling into the wrong hands.
- *Availability* – determine whether a web site is accessible and operational at any given moment.

E-Business security is technology designed to protect these six dimensions, when any one of them is compromised, it is a security issue.

10 Encryption technology

Encryption provides the key to providing greater security, and various organisations are considering policies on cryptography. Encryption is the process of transforming plain text or data into *Cipher text* that cannot be read by anyone outside of the sender and the receiver. The purpose of encryption is (a) to secure stored information and (b) to secure information transmission. Encryption can provide four of the six dimensions of e-Business security:

- *Message integrity* – provided assurance that the message has not been altered.
- *Nonrepudiation* – provided the user from denying he or she sent the message
- *Authentication* – provides verification of the identity of the person (or machine) sending the message.
- *Confidentiality* – gives that others did not read the message.

There are a variety of different forms of encryption technology currently in use. They are

- ✓ Symmetric key encryption
- ✓ Public key cryptography
- ✓ Public key encryption using digital signatures and hash digests
- ✓ Digital envelope
- ✓ Digital certificates and public key infrastructure

Privacy of network communication is ensured by encryption. There is one other method that will facilitate higher levels of security in organisations undertaking e-Business using the Web or other networks. This is the implementation of *firewalls* and proxies within the system servers. Firewalls are an effective means of shielding private, secure, internal networks from nonsecure external networks. For example, firewalls are usually installed between an intranet and the Internet in order to prevent attack from the Internet. Like other security technology, they must be implemented correctly and in accordance with the overall security policy [30].

Security in e-Commerce generally employs procedures such as authentication, ensuring confidentiality, and the use of the cryptography to



communicate over open systems [31]. As more and more businesses go online, confidential files are increasingly exposed to the risk of infiltration [32].

Security and disaster recovery planning go hand in hand. A firm's solid reputation can be destroyed in a single day on the Internet. It is important to think through various disaster scenarios and have a plan for addressing each one [8].

11 E-Business privacy policy

It is important to develop a clear, concise, easily accessible privacy policy on an e-Business web site; the law varies significantly among countries worldwide with respect to protection of citizens' privacy. This is why many consumers fear Web-based shopping. But the European Union (EU) has adopted strict privacy laws. Although these legal principles apply only in the EU, their effect is far reaching. This is because the directive also prohibits the transfer of data from the EU to countries which do not have adequate data protection laws. Conversely, the import of data from such countries may also trigger the requirement of the importer to abide by the EU directive. This is one of the factors putting pressure on countries such as Australia to improve their privacy protection laws. In terms of e-mail generally, the tragic events of 9/11 (11 September 2001) in New York have led to government increasing their powers to monitor e-mail traffic around the world consequently diluting privacy.

Many of the threats to privacy are not new. Many privacy organisations are fighting for setting standards on the Internet, but as the Internet does not belong to anyone in particular it is not possible to enforce standards. New standards evolve slowly and need to bring advantages to the user in order to be accepted [33]. For this reason, ethical and legal controls are an important part of e-Business security. However, the law is slow to evolve due to the global nature of e-Business. Again the technology involving the Internet is evolving rapidly. Although legal protection is necessary and desirable, trust and confidence in e-Business must be reassured again and again through robust security technologies and ethical standards.

Many organisations take ethics seriously and produce a document guiding the behaviour of its members or employees. Some corporations require new employees to read its code of ethics and sign a promise to abide by it.

12 E-Business security plan

Security is a combination of technical, administrative, and physical controls. A security plan identifies and organises the security activities. The plan is both a description of the current situation and a plan for improvement. A security plan must state the organization's policy on security [34].

A security plan is a very comprehensive document; its creation typically requires the involvement of key information technology personnel as well as end users and management. In order to minimize security threats, e-Business firms must develop a coherent corporate policy that takes into account the nature of the



risks, the information assets that need protecting, and the procedures and technologies required to address the risk, as well as implementation and auditing mechanisms. Public laws and active enforcement of cybercrime statutes are also required to both raise the costs of illegal behaviour on the Internet and guard against corporate abuse of information [35].

13 Conclusions

Recent advances in IT have been and continue to be a driving force in business innovation in general and e-Business in particular. The flow of information over the Internet must be safe and secure so that consumers can take part in e-Business without hesitation. In general, Internet security for building secure e-Business Systems is a growing concern. Contemporary security issues and technologies have been discussed. Most of the countries are not fully prepared to face security challenges. It will take time to develop a uniform cyber law to safeguard e-Business worldwide.

With the emergence of Homeland Security initiatives in 2002 and the National Strategy to secure cyberspace in 2003(both in the USA), the demand for trained information security professionals far exceeds the supply. Securing cyberspace is an extraordinary difficult challenge to undertake e-Business. Despite security breaches e-Business is growing. It will never be possible to eradicate crimes in cyberspace completely, but new evolving security technologies along with policy, procedures and law should keep threats as minimum as possible or manageable. Security breaches will remain a formidable and costly issue which can be countered by effective controls, a strong culture of prevention and deterrence and assertive action when cases arise.

Acknowledgements

The author expresses his gratitude to the Research Management and Training, College of Law and Business, University of Western Sydney for supporting this research partly under the CLAB Research Activity Support Scheme. He remembers the loving support of his children Indira & Bikram and wife Mitra during the preparation of the manuscript.

References

- [1] Chan, H., Raymond, L., Dillon, T., & Chang, E., E-Commerce: Fundamentals and Applications, John Wiley & Sons. 2001
- [2] Chaudhury, A., & Kuilboer, J., E-Business and e-Commerce Infrastructure: Technologies Supporting the e-Business Initiative, McGraw-Hill/Irwin, 2002.
- [3] Karmakar, N. L., Digital Security, Privacy & Law in Cyberspace: A Global Overview, Proceedings of the e-society 2003: IADIS International Conference, Lisbon, Portugal, June 3-6, Vol.1, pp 528-535, 2003.



- [4] Webster, M, "security," available from the World Wide Web <http://www.m-w.com/cgi-bin/dictionary>, 1 February 2002.
- [5] Whiteman, M.E. & Mattford, H.J., *Principles of Information Security*, Thomson. 2003.
- [6] Hoffman, D., Novak, T. P., & Peralta, M., Building consumer trust online, *Communications of the ACM* **42**(4), pp.80-85, 1999.
- [7] Alter, S., *Information Systems: The Foundation of E-Business*, 4th edition, Prentice Hall, pp. 6, 2002.
- [8] Kalakota, R., & Robinson, M., *e-Business 2.0 – Roadmap for Success*, Addison-Wesley, 2001.
- [9] Volonino, L., & Robinson, S., R., *Principles and Practice of Information Security*, Prentice Hall, 2004.
- [10] Van Slyke, C., and Belanger, F., *E-Business Technologies: Supporting the Net-Enhanced Organization*, John Wiley & Sons. 2003.
- [11] Turban, E. et al., *Electronic Commerce: A Managerial Perspective*, Prentice Hall, 2002.
- [12] Kou, W., *Networking Security and Standards*, Kluwer Academic Publishers, 1997.
- [13] Computer Security Institute, 2001 Computer Crime and Security Survey, <http://www.gocsi.com/forms/fbi/pdf.html>, July 2001.
- [14] Computer Security Institute, 2002 CSI/FBI Computer Crime and Security Survey, <http://www.gocsi.com/forms/fbi/pdf.html>, Spring 2002.
- [15] Computer Security Institute, 2003 CSI/FBI Computer Crime and Security Survey, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf, 2003.
- [16] McNurlin, B. C. & Sprague, Jr., *Information Systems Management in Practice* (6th ed), Prentice Hall, 2004.
- [17] Source: The Threat from the Net, *Asian Business* **36**(11), pp. 34.
- [18] PricewaterhouseCoopers, economic crime survey 2003, available at <http://www.pwc.com/extweb/insights.nsf/docid/662DCF05C90F69E680256D6E0052125A> 2003.
- [19] KPMG, 2001 Global e.fr@d.survey, available at <http://www.aic.gov.au/research/fraud/surveys.html>, 2001.
- [20] Gray, P., Australian computer crime losses double, Survey at <http://www.zdnet.com.au/news/security/0,2000061744,20274402,00.htm>, 12May 2003.
- [21] Dasgupta, P, **Cyber** Terrorism, *The Statesman* (India), May 24, 2002.
- [22] Turban E, McLean, E, and Wetherbe, J., *Information Technology for Management: Transforming Business in the Digital Economy* (3rd Edition). John Wiley & Sons, 2002.
- [23] Barbara, M., Internet Attacks On Companies Up 28 Percent Report Says, *The Washington Post*, P. E5, July 8, 2002.
- [24] Vise, D. A., & Daniel E., FBI Warns of Cyber-Attack Threat: U.S. 'Very Concerned' About Vulnerability of Infrastructure, *The Washington Post*, P. A16, March 21, 2001.
- [25] Fonseca, B., IT Security Under the Gun, *IT World*, March 12, 2001. <http://www.itworld.com/Sec/3832/itwnws010312security/>



- [26] BBC News World Edition, E-mail scam hits MBNA customers, <http://news.bbc.co.uk/2/hi/technology/3518411.stm?headline=E-mail~scam~hits~MBNA~customers>, accessed on February 25, 2004.
- [27] IT Today, Gates says software needs better security, *The Australian*, Tuesday, September 2, pp. 37, 2003.
- [28] Mills, K., Net virus in the back door, *The Australian*, Wednesday, February 2004.
- [29] AFP, Hackers hit website as virus continues to spread, *The Sydney Morning Herald*, pp. 4, Monday, February 2, 2004.
- [30] Goldman, J. E. & Rawles, P. T, *Applied Data Communications: A Business Oriented Approach*, Wiley, 2004.
- [31] Awad, E., *Electronic Commerce: From Vision to Fulfillment*, Prentice Hall, New Jersey, 2002.
- [32] Besserglik, B., Spotlight turned on cyber crime, *The Australian IT/Cutting Edge (The Australian)* Tuesday, pp.3, May 16, 2000.
- [33] Amor, E., *The E-Business Revolution: Living and Working in an Interconnected World*, Prentice Hall PTR, 2000.
- [34] Pfleeger, C. P. and Pfleeger, S. L., *Security in Computing* (3rd ed), Prentice Hall, PTR, 2003.
- [35] Laudon, K. C. and Traver, C. G., *E-Commerce: business, technology, society*, Addison Wesley, 2002.

