



Information systems security in the age of electronic commerce

J. Biggam & A. Hogarth

*Department of Business Information Management,
Faculty of Business,
Glasgow Caledonian University, Scotland*

Abstract

The Internet is a global facility that is gaining in popularity and usage. Its users are diverse and many, ranging from those interested simply in discussing their favourite films, to groups highlighting human rights issues. Increasingly, and perhaps inevitably, there is a major movement to exploit the Internet for business purposes ("E-Commerce"). The aims of this paper are to identify the main stakeholders in the security of computer-based information systems, the problems of tackling computer security and to advise on issues pertinent to advancing business use of the Internet.

1 Introduction

Security is a concept that is central to all societies. Countries invest a large proportion of their gross national product on military protection (from purchasing the latest fighter aircraft, to developing new types of "smart" missiles); in cities and towns, we have police forces to "protect and serve" local communities; and at a personal level, individuals acquire a multitude of security habits and recommendations to protect themselves: insuring their homes against damage, installing fire/house alarms, purchasing personal insurance in the event of ill-health, wearing of appropriate clothing to counter different types of weather, applying sun cream to avoid harmful effects of sunburn, learning martial arts to defend against physical violence, etc. Thus, it is a simple matter to appreciate the importance of security to the physical and psychological well-being of society, not only to the individual, but also to society as a whole.



284 *Management Information Systems*

Security is also a concept that has gained much attention and publicity within the computing environment (Biggam and Eadie [1]; Joch [2]; Lucas and Rolfe [3]; Harrison [4]). The media view computer security as a “sexy” topic and regularly highlight areas that make good “copy”: hacking, viruses, computer fraud, the millenium bug (e.g. Herald [5]). Rarely does the media consider computer security from a sober, mature perspective. The proliferation of computer security conferences testifies to the importance of security to the business community. Similarly, the volume of government (CCTA [6]; NCC [7]), academic (Gollman [8]), and business literature (ICL [9]) on the subject matter underlines the value which society places upon the protection of our computer-based information systems.

Yet, survey after survey (Audit Commission [10]; NCC [7]; Lohr [11]; NCC [12]) consistently reveals that computer-based information systems regularly suffer from breaches, both physical (e.g. computer theft) and logical (e.g. virus infections). Given the plethora of security hardware and software devices, including guidance from a wealth of venerable bodies (e.g. National Computer Centre, FBI, etc.), supported by legal avenues (e.g. Computer Misuse Act 1990, Data Protection Act 1984, etc.), why is it that we still suffer from consistent computer security breaches ? And what are the implications for our computer-based information systems in this new age of E-commerce ?

The purpose of this paper is to:

- Identify the main stakeholders in the security of computer-based information systems
- Outline key reasons why computer systems remain vulnerable
- Highlight security issues pertinent to the Internet and E-commerce
- Offer advice on encouraging business use of the Internet.

2 Information Systems Security: The Main Stakeholders

Stakeholders (Checkland [13]), in the context of computer security, are those individuals or groups who either have a significant influence on the security of an environment or who themselves are affected by such security, or lack of, in an environment. Obvious stakeholders include:

- **Computer Scientists**
(This group concentrate on producing technological advances in order to enhance the security of computer-based systems. The field of cryptography is an obvious example of their contribution to protecting, for instance, E-commerce activities);
- **Law Enforcement Agencies**
(Mainly Government bodies, such as the FBI and local police, that are responsible for applying the law of the land - such as the UK Computer Misuse Act 1990 – in the context of computer security);



- Recipients
(Those for whom the computer security is intended to protect – primarily the business community);
- Abusers
(Those who deliberately attempt unauthorised activities, such as *hacking*, on computer-based information systems).

Another important and influential stakeholder, not mentioned above, but for whom the security of organisations is of concern, is the purveyor of security products. Their purpose is to sell products and services related to computer security. Therefore, they are important stakeholders in the computer security world. Furthermore, the products and services they sell, have a direct influence on the security of organisations.

At a simple level, the relationship between these stakeholders is straightforward: the recipients suffer security breaches, these breaches are perpetrated by computer abusers (although many breaches can be of an accidental nature), the law enforcement agencies attempt to deter/punish the abusers by applying the appropriate laws, and the scientists toil to develop ever-more secure products, financed by business, to plug gaps in the security cycle.

An example may help to illustrate the above relationship. In the 1980s, businesses (i.e. recipients) in the UK were reporting an increase of virus infections on their computer systems. There was also a fear, highlighted at every opportunity by the media (another stakeholder !), of outside agencies (i.e. abusers) gaining unauthorised access to sensitive government data. As a result of these security breaches, and particularly because of perceived public alarm, a new law was brought in to force: The Computer Misuse Act 1990. The purpose of this act was to deter unauthorised access (i.e. *hacking*) and the tampering of computer systems (e.g. insertion of viruses). Computer scientists, backed by industry, quickly developed tools (e.g. enhanced cryptographic algorithms, anti-virus software, etc.) to aid in the protection of computer systems.

However, the picture painted so far of information systems security is oversimplistic. The chain-reaction of events between the various stakeholders is often confused: sometimes it is the media that sets off events; sometimes it is the purveyors of security software/hardware; sometimes it is special interest groups. For instance, increasingly it is commerce and the media, not abusers, that are the driving force behind the chain reaction of events between stakeholders.

3 Why Our Computer Systems Remain Vulnerable

Traditional approaches to securing computer-based information systems are inconsistent and, for the most part, inadequate (Biggam and Hogarth [14]). A simple examination of the roles played by the main stakeholders may help clarify these issues.



Legal deterrents, such as the UK Computer Misuse Act 1990, have proved to be ineffective in the fight against computer crime. In the UK, the number of successful prosecutions remains relatively low. Consequently, given the work involved in bringing a prosecution, and the almost inevitable result, the police lack any incentive for tackling computer crime. Even in cases of successful prosecution, the penalties imposed are relatively light. Other issues such as the difficulty of gathering evidence: lack of specialist police training (and appropriate career structures); poor co-operation from businesses (who prefer to deal with the problem internally, rather in the full glare of the media or through Law Enforcement Agencies), all conspire to seriously hinder the job of Law Enforcement Agencies in their fight against computer crime. Indeed, in the UK there is no legal definition of a computer.

Recipients, e.g. businesses, have a special role in perpetuating the insecurity of computer systems. Computer security is often viewed as an expensive and time-consuming activity; something that adds little to the profits of an organisation. However, this is to misunderstand the value of security and the free advice that is available. Despite an abundance of security guidelines (e.g. "A Code of Practice for Information Security Management" by the dti) and available security-related software and hardware, including expertise, businesses regularly fail to implement sensible security policies. Importantly, other than for reasons of financial expediency, businesses may decline from implementing proper security systems because, on the whole, they can live with the consequences. Businesses constantly listen to security experts telling them that their business is doomed if they do not seek expert help immediately; but examples of businesses going out of business are rarely produced by the merchants of doom. Perhaps a case of "crying wolf" too often. Indeed, Jeon [15] takes the stance that much of the apprehension over Internet security is unfounded.

Computer Scientists concentrate on providing technical solutions to computer security breaches. Despite their efforts, computer security remains a major area of concern. Anti-virus software has not prevented virus infections; developments in cryptography have not made hackers redundant; the Internet, designed and developed by scientists (ironically, initially for reasons of security !) is the most open, and hence potentially least secure, computer environment !

4 The Internet, E-commerce and Security: Pertinent Issues

The Internet has taken on a life of its own. It was initially developed as a means of maintaining communication links between key military and political centres in the USA, in the event of a nuclear attack from the USSR (a misplaced defence mechanism, because one of the first things that become useless as a result of nuclear fall-out is electrically-based communication systems). The Internet is now used for many diverse purposes (Baresch and Schlechter [16]): pornography, games, gambling, business products, business services, banking, consumer tangibles/intangibles.



It is the last group – “consumer tangibles/intangibles” – that make up the vast bulk of activities on the Internet. These range from Dating Agencies to subversive groups motivated by political objectives. Of course, there are groups, wrongly labelled as the latter, whose interests lie in the sphere of human rights issues. The amount of actual business transactions that occur over the Internet is relatively small, compared to the other activities that swamp the Internet.

The main security issue pertinent to the Internet and E-Commerce is Transaction Security. If a message is sent over the Internet, and that message is in text and uncoded, then the sender and recipient need to appreciate that their data is unprotected and can be intercepted at any forwarding node.

How can a company protect transmissions ? There are two elements to consider: a) how to protect the data during its journey from sender to recipient; and b) how to authenticate the identity of the receiver. To protect data during actual transmission, conceal messages by sending non-text files (e.g. picture format) and making use of cryptographic software (Rose, Khoo and Straub [17]). To verify identity of recipient then use technologies such as Digital Signatures or SET (Secure Electronic Transaction).

If E-Commerce security is so simple then why are organisations not employing such techniques and why do we still have security breaches with Internet transactions (Harrison [4]) ? One problem is that companies are not using the technology that is available to them; another problem is that the security technology itself is not without difficulties: different standards prevail and can confuse the customer, leading to implementation difficulties (Piper [18]); government regulations can be restrictive; and, implications of technologies are causing trepidation (Baresch and Schlechter [16]), etc.

The use of Digital Signatures as a means of validating E-Commerce transactions, may help in understanding the difficulty of using new technologies to secure the Internet. A proposed Directive by the European Union (EU) on electronic signatures (EU Directive [19]) to be used to validate business transactions on the Internet, illustrates the seriousness of European Member States to treat the Internet as a business facility. This means that electronic signatures in relation to electronic data are legally recognised in the same manner as hand-written signatures in relation to hand-written data. What are the security implications for this proposal ?

There are serious security implications on the use of digital signatures. Firstly, if (when, really) a digital signature is fraudulently obtained, within the time it takes to send an e-mail message a business could have its capital removed and assets sold (over the Internet). Secondly, a digital signature can be copied many times, thereby increasing the fraudulent damage to a business (and it would be impossible to tell the difference between a copy and the original – in effect, there would be many “originals” in circulation). Thirdly, even if a criminal was



apprehended, it would prove immensely difficult to gather evidence and secure a prosecution (not only because of the usual problems, but also because of the difficulty in distinguishing the original from the copy).

In essence, the main barriers to e-commerce are that those sending data cannot easily be identified (allowing criminals can engage in credit card fraud), those receiving data cannot easily be identified (encouraging the existence of bogus companies), and the data in transmission is difficult to secure (facilitating the theft of passwords and credit card details).

The UK response to these barriers is contained in the development of a *Public Key Infrastructure* (PKI). This refers to the techniques, practices and procedures that support an encryption system. To allow identification of those sending data, PKI supports the use of an *electronic signature*; to allow authentication of the services offered by web sites, *digital certificates* will be issued (at a cost) to verify that the site is a bona fide company (called “trusted service providers”); and to secure transmissions, PKI supports the use of encryption software.

Does PKI solve the problem of insecurity on the Internet ? The use of electronic signatures is not a global response; nor is the issuing of digital certificates. Similarly, there is no agreed standard on encryption. The fragmented adoption of security standards together with national legal interpretations of what constitutes an enforceable e-business contract continues to hinder the growth of e-commerce. In effect, PKI will benefit the business community only if there is a global standard.

5 Conclusion

The EU member states are gearing up for regulating aspects of E-commerce, and the complexities of using Digital Signatures as a means of dealing with one aspect of security – user validation – encapsulates many of the fears and uncertainties surrounding new technologies. As shown earlier, there are major security problems related to doing business on the Internet, which in summary are:

- Business perception of Internet security (and business apathy)
- Confusion of technological security tools and Techniques
- Lack of coherent global approach
- Government restrictions (e.g. cryptography)

Too much time has been devoted to fine-tuning and developing the technology, and not enough energy has been directed towards helping business to exploit expert advice and services. This is of concern, particularly given that businesses themselves often highlight their security worries (Piper, 1998), i.e. that security is too time-consuming, too expensive, and is difficult to use.



These issues need to be addressed. Security procedures need to be packaged in such a way that their usability and user-friendliness are enhanced and that the cost is not prohibitive. Of course, responsibility for security implementation cannot be placed entirely at the feet of Governments, purveyors of security tools, scientists, etc. Businesses themselves must make efforts to contribute to the debate and to implement appropriate organisational changes to facilitate secure E-Commerce (e.g. development of security policy procedures).

Given the imminent implementation of the EU Directive on Data Protection, it is now timely to focus on the real issue of guiding the business community through the security maze.

References

- [1] Biggam, J. & Eadie, D. Securing the business I.T. environment: where are the solutions ? *Proc. Of the 6th Annual BIT Conference*, Manchester Metropolitan University, Manchester. 1996.
- [2] Joch, A., Safe Passage. *Information Technology Supplement*, (19)17, 1997.
- [3] Lucas, P. & Rolfe, R, Good news about card fraud, *Credit Card Management*, (11)6, pp. 38-45. 1998.
- [4] Harrison, A. Fraud doesn't faze e-customers", *Computerworld*, <http://www.computerworld.com/home/news.nsf/all/9905204fraud>, 1999.
- [5] Herald Newspaper. Teenage hacker cost BT £106,000. *Herald Newsgroup, Glasgow*, , pp 16, 9 October 1999.
- [6] CCTA, *CRAMM: An Overview of CRAMM*, CCTA publication, London, (on behalf of HMSO), 1992.
- [7] National Computer Centre (NCC). *The Information Security Breaches Survey*, NCC Consultancy Group, Manchester, on behalf of dti, 1996.
- [8] Gollman, D. *Computer Security*, John Wiley and Sons, Chichester, England, 1998.
- [9] International Computers Limited (ICL). *Business Security: Business Impact Assessment*, ICL IT Security Department Manual, London, 1998.
- [10] Audit Commission. *Opportunity Makes a Thief: An Analysis of Computer Abuse*, HMSO publication, London. 1994.
- [11] Lohr, S. Go ahead: be paranoid: hackers are out to get you, *New York Times Online*, March 17, 1997.
- [12] National Computer Centre (NCC). *The Information Security Breaches Survey*, NCC Consultancy Group, Manchester, on behalf of dti, 1998.
- [13] Checkland, P. B. *Systems Thinking: Systems Practice*, John Wiley and Sons, Chichester, England, 1981.
- [14] Biggam, J. & Hogarth, A. "The development of a 'computer security requirement specification': embedding and merging ICL's 'Business Impact Model' with Soft Systems Methodology (SSM)", *Proc. Of the*



4th BCS ISM Specialist Group, University College Cork, Cork, Ireland, 1996.

- [15] Jeon, I. The information dirt road: have you smoothed out the bumps in your site ? *LIMRA's MarketFacts*, **16(4)**, pp.18-21, 1997.
- [16] Baresch, D. & Schlechter, R. *Secure Electronic Communication – The European Community Approach*, InterMedia Special Report, International Institute of Communications, pp 6-11, 1998.
- [17] Rose, G., Khoo, H. & Straub, D. Current technological impediments to business-to-consumer electronic commerce, *Electronic Commerce* **(1)16**, 1999.
- [18] Piper, F. *Information Security and the Secrets of Encryption*, InterMedia Special Report, International Institute of Communications, pp 12-19, 1998.
- [19] EU Directive, *COM(98)197/2* of 13 May 1998, <http://www.ispo.cec.be/eif/policy/com98297.html>.