richardfrancis.info

Web | Data | Process

Digital Design and Management Services

*

E-Business Analysis

3 LITERARY REVIEW

3.1 What is e-business?

There are numerous definitions of e-business, however, put simply, e-business is a business process over a digital network. These business processes could be ordering products from a supplier, business-to-business (b2b). Selling products via an auction site like ebay.com, either business-to-consumer (b2c) or consumer-to-consumer (c2c). Indeed, when an employee reads information published on his organisations website, its business-to-employee (b2e).

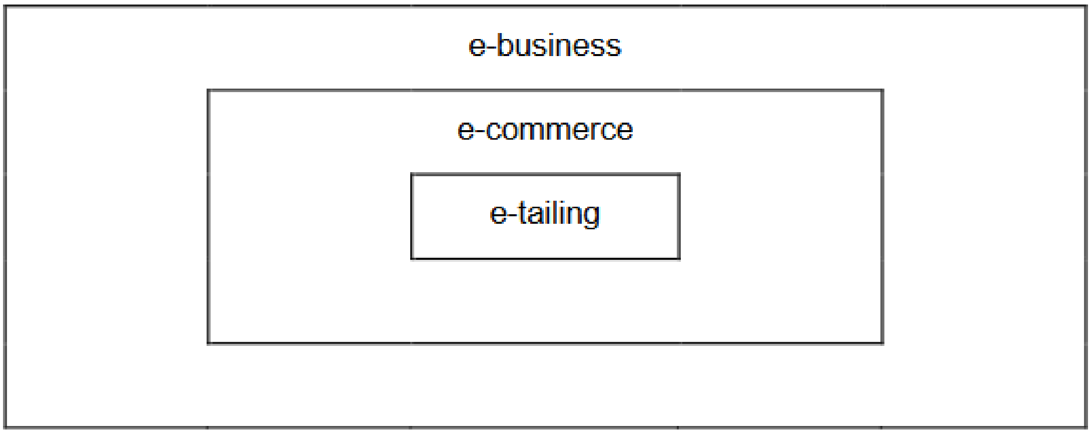

Fig 3.1 Source: electronic commerce handbook 2006

Shoniregun (2006) highlights two specialist fields within the e-business environment, illustrated above, they are e-tailing and e-commerce. E-tailing is essentially retailing online. While e-commerce (eC), encompasses a broader scope. Singh et al (cited in Groucutt and Griseri 2004, p.19), defines eC as, "the online exchange of value, without geographical or time restrictions, between companies and their partners, employees or customers".

Groucutt and Griseri (2004) argue that the term e-business has wider influences than eC, that include political, economical, social, technological, legal and environmental. Indeed, it is the social influences that are central to the topic of this paper. The cyber crime that has evolved in the shadow of e-business, threatens social acceptance (Shoniregun et al, no date; Bandyo-padhyay, N. (2002). The legal framework, in which e-business is conducted varies, according to geographical region.

3.2 Security issues in e-business

Ask oxford (2006) define security as, “the safety of an organisation against terrorism or espionage”. Indeed the activities of cyber criminals are such that this definition holds true for e-business. However, information security does have additional considerations. Therefore a more detailed definition is required. In 2002 Awad highlighted four security basics, “confidentiality, authentication, integrity, access control and non-repudiation”. Additionally, in 2002 Bandyo-Padhyay discussed “trust”; how it affects e-business, consumers and what can be done to improve it. Unfortunately these issues do not comprehensively explain information security goals.

In 2003 Whitmann and Mattord added the term “availability”, and explained that data must be made available to those who are authorised to view or modify it. The most detailed and accurate description of information security discovered by this research, was made by Vorster and Labuschagne (2005) where they noted that, “an organisations approach to maintaining confidentiality, availability, integrity, non-repudiation, accountability, authenticity and reliability”. The term accountability does not regularly appear in security definitions. However, the research suggests that this term is crucial to the success of any security model. Unless cyber criminals are prosecuted to the full extent of the law then there is no deterrent.

Although the description of information security made by Vorster and Labuschagne is accurate and detailed, one vital ingredient is still missing. Privacy is freedom from intrusion, being left alone, control about oneself and freedom from surveillance (Jahankhani, 2005). This issue of freedom is central to many debates in e-business. The use of cookies, which are discussed in more detail in section 3.3.7, is a major concern for many online shoppers. Indeed browsers are now equipped with cookie blocking technology.

3.3 What are the threats to E - Business?

In 2003, Whitman and Mattord defined a threat as, “an object person or other entity that represents a constant danger to an asset”. The threats to an e-business are numerous and many are conceived, everyday. The threats may be managerial incompetence, technical failure, intentional, unintentional or even an act of God (Whitman and Mattord, 2003). However this section focuses on intentional attacks, defined by Oppliger in 2002 as, “active attacks”. These active attacks include denial of service, degradation of service, spoofing and session hijacking. Moreover, in 2006 Shoniregun, added social engineering and highlighted cookies as the most worrying threats to an e-business. At this point it is important to note that this list is not exhaustive, however the list does categorise and highlight the main threats to e-business at present. The following sections outline some of the more worrying and well-known threats.

3.3.1 Virus

A virus is a small program that multiplies itself (Dr Solomon, 1996), Oppliger may describes them as causing a degradation of service. On the other hand, viruses are also responsible for causing a complete denial of service. In 2005, the computer crime and security survey (CSI) identified viruses as the computer crime that causes the highest financial loss. Indeed the survey revealed that $42,787,767 was lost to American industry due to viruses alone. There are thousands of viruses, many of which are completely harmless.

However there are a few viruses that do cause harm, these were written by unscrupulous programmers, who write virus programmes for many reasons, including “just having fun”. Viruses may be spread on floppy disks, USB keys, or even in e-mails. For example, the I Love you, Melissa and Love Bug viruses have between them caused the closure of Ford’s, the British Parliament and the American Pentagon’ e-mail systems (Jahankhani, 2005). Furthermore, these viruses have undermined the confidence and trust of many Internet users.

3.3.2 Trojan horse

Often mistaken for a virus a Trojan horse does not multiply itself, instead, it is a program that does what you do not expect it to do. For example, the aids information disk which was sent out in 20,000 e-mails under the guise of teaching users about aids. When instead, the Trojan, once activated, encrypted and hid all the files on the victims PC (Dr Solomon, 1996).

3.3.3 Worms

In 2005, Shoniregun defined the worm as, “a self replicating program that propagates over a network”. Furthermore, Shoniregun identified two categories of worms, mass-mailing and network-aware, he goes on to note, “the network-aware worm has been known to degrade the Internet operation”.

3.3.4 Social Engineering

Fraud is also a very common type of threat to an e-business. Indeed, identity theft is a growing crime in the UK and beyond. Social engineering is where information is either stolen or coheres from an unsuspecting victim. The information is then used to assume the victims’ identity and profit from the scam. In 2005 the CSI noted that, “the average loss for unauthorised access went up to $303,234”, and that, “the theft of proprietary info went up to $355,552”. While in the UK, phishing attacks have increased 1,471 percent (Young, 2006). Unfortunately, the evidence suggests that while all other forms of Internet crimes are falling, the identity theft is on the increase.

3.3.5 IP Spoofing

The term IP Spoofing is used to refer to an attack where an intruder places the wrong IP address in the source of the IP address field of the packets being sent out (Opplinger, 2003; p.62). Spoofing is made possible by the discovery of a security weakness in the TCP known as sequence prediction. Indeed, there are variations of spoofing, including non-blind, blind, man in the middle attack and denial of service. The latter is possibly the most difficult to defend against. The reason for this is that the crackers/hackers are only interested in consuming resources. They simply wish to flood the victim with as many packets as possible. (Tanase, 2003)

3.3.6 Session Hijacking

A form of spoofing, session hijacking is the act of taking control of a user session after successfully obtaining or generating an authentication session ID (Imperva, 2006). When a TCP connection is made between a client and server all information that is relevant for the connection is made in the clear. This allows the attacker to learn the initial sequence numbers chosen by the client and server, then misuse the data and hijack the already established connection (Opplinger, 2003; p.66).

3.3.7 Cookies

Cookies are small text files that are placed on your computer hard drive, while visiting a website. On the whole cookies are not malicious, however they are being used for malicious purposes. Indeed, during an electronic commerce lecture at University of East London on 5th October 2006, Dr Shoniregun identified cookies as the most dangerous threat to e-business at present. The reason for this is that cookies are locked to the system clock. This means the user may not be aware of the cookies existence, while valuable data is being sent to an unauthorised third party. Furthermore, the ease in which cookies can be placed on a PC is a matter for concern.

3.3.8 Hackers and Crackers

Hackers are programmers that normally are very experienced Internet users. Although the term hacker used to have a lot of respect within the programming community, it is now more often used to categorise a criminal. In 2005 Jahankani defined hackers as, “people who do not have bad intentions but want to learn every thing about computer systems”. Therefore a hacker will enter a system without authorisation, breaching data protection laws and privacy requirements. A detailed anatomy of a hacker is illustrated in appendix 1. Crackers, on the other hand are commonly responsible for unauthorised access, website defacement, sabotage, fraud, session hijacking, IP spoofing and viruses. The research revealed that crackers do not have the skill level of hackers, instead they rely on code written by others to conduct their criminal activities (Jahankani, 2005). For the purpose of this paper both term are used to mean cyber criminal.

3.4 What are the defences?

As mentioned earlier in this paper, there are numerous methods, whether software, hardware or security personnel, that can be used to defend data and information. This section outlines some of the most popular.

3.4.1 Cryptography

The study of encryption and decryption is cryptography. The history of cryptography can be traced back to 1900 B.C, when Egyptian scribes used non-standard hieroglyphs to inscribe clay tablets. Furthermore, between 1939-1942 the allies broke the secret German enigma code using decryption techniques (Whitman and Mattord, 2003; p.325). Cryptography is based on mathematical procedures that allow users to scramble data, so that only the sender and receiver may read the contents of a message.

There are three basic cryptography methods; symmetric key, all users have the same secret key to encrypt and decrypt messages. An asymmetric key is where there are public key and private keys that enable users to encrypt with the private key and decrypt using the public key. Finally, one-way hash functions which change a message into a fixed string of digits (Shoniregun, 2005; p.15).

Although cryptography is responsible for improved security, there are issues that should be addressed. For example, the algorithms that are the basis for cryptography can be deciphered. Moreover, when an encrypted message is received by an organisation the hacker may be able to access the message in plain text format. Indeed, the determined hacker could access the decryption software and modify it so that authorised users cannot see their own data.

3.4.2 Digital certificates

In 2005 Shoniregun explained that, "..digital certificates are electronic identification cards that establish an individuals credentials when doing business over the Internet". A digital certificate is software that is installed in your browser. Using cryptographic technology the software identifies you to websites that are equipped to check your identity automatically.

Digital certificates may be obtained from trusted third parties, such as Verisign (www.verisign.com) or Cybertrust (www.cybertrust.com). Also a digital certificate may be classified, according to the level of security required (Awad, 2002; p.449). The data stored in a digital certificate is illustrated below and the class of certification is highlighted.

Contents of a digital certificate

User's basic information (name, address, SSN, etc)
Digital signature and ID information of issuing authority
User's public key
Dates of validity and expiration of the digital ID
Class of certification (1-4)
Certificate number of digital ID

3.4.4 IPSec (IP layer)

In 2003 Roland and Newcomb (cited in Shoniregun, 2005) defined Internet protocol security (IPsec) as, "a collection of open standards that work together to establish data confidentiality, data integrity, and data authentication between peer devices". The diagram below illustrates the high level architecture used in IPSec. The IPSec module is a module that implements the IPSec protocols, its main aim is to secure traffic sent or received from another IPSec module (Oppliger, 2002; p.228).

Figure 3.2 Source: (Opplinger, 2002; p.228)

With hundreds of IPSec modules trying to establish virtual private network (VPN) networks with each other, the main drawback is that they all need to be configured individually. This takes considerable resources, while not all the configurations may be correct. RFC 3715 has identified known incompatibilities between network address translation (NAT) and IPsec. IPsec does not interoperate with most firewalls and gateways that implement NAT (Shoniregun, 2005; p.20).

3.4.5 Intrusion detection systems (IDS)

The IDS works like burglar alarm, which uses sound and visual technologies to notify system administrators of an attack on their data. There are two main types of IDS the first, host based, sits on a server and monitors the system for changes.

The second, network based, is more complex to maintain and configure. The network based IDS looks for patterns in network traffic that may indicate a denial of service attack (Whitman and Mattord, 2003; p.286).

The research indicates that this technology does contribute to overall improved e-business security. However, the technology could be improved by adopting a proactive methodology, rather than a reactive one.

3.4.6 Firewalls

The term firewall has been used for some time in relation to buildings. The term is used to describe the protection of spreading fire from one room to another. In computer terms, the same could be said for a firewall. The firewall software / hardware is used to protect one part of a network from another. Indeed, the purpose of a firewall is to protect a company' intranet from the unauthorised communication into or out of the network (Opplinger, 2003; p.130).

Firewalls are an important tool in the fight against cyber crime, unfortunately they are not the cure. Goodwin 2000 (cited in Bandyo-padhyay, 2002) highlighted the statistic that "80% of security breaches are caused by a company' own staff". A Firewall will not protect from insider threats, furthermore, according to CSI, 2005 viruses are responsible for losses totalling $42, 787, 767.

3.4.7 Biometrics

Biometrics is science and technology of quantifying and statistically scrutinizing biological data. Biometrics is an old technology that is being applied in a new way. Fingerprints are a well-established means of identification. Voice recognition is more recent, however this technology may be found cars and homes. Iris scans, are already being tested in Heathrow airport, are another application for this technology. Indeed, biometric technology has the potential to drastically reduce cyber crime in the near future (Awad, 2002; p.459). Although biometrics is well placed to reduce cyber crime, there are issues that insure it will not eradicate the problems of e-Security. Firstly, the price of biometric technology places it outside the reach of the average computer user. Secondly, the time it will take to comprehensively introduce affordable biometric technology is unacceptable. Thirdly, existing network security issues are not resolved with biometrics. Finally, kidnapping is a real option for the determined criminal. Indeed, removing a finger or an eye from a potential victim may even become the norm.

3.4.8 Anti-virus software

Norton (www.Norton.com) and MaCafee (www.MaCafee.com) are two of the most well-known anti-virus software manufacturers. Their software is designed to scan a system for viruses then quarantine the code. The problem with anti-virus software is that, during the time it takes to manufacture the software, cyber criminals are developing new and advanced viruses. This means when the updated anti-virus software is available to the market, it’s out-of –date.

3.4.9 Honeypots

There is an old saying, “attack is the best form of defence”. The research suggests that honeypots are one of the few security techniques in which proactive pursuit of cyber criminals is central. A honeypot is system designed to catch attackers. Any attacks against a honeypot are made to seem successful, giving administrators time to log, track and apprehend the attacker (Awad, 2002; p.403).

3.5. Risk assessment models

3.5.1 BS7799

The British standard 7799 (BS7799), is a code of practice for all technologically enabled businesses. Each section is concerned with security for specific issues that are affecting technologically enabled businesses around the world and in the UK (Business link, 2006). A detailed explanation of each section is included in appendix 2.

In 2005, Shoniregun described the BS 7799 as, “a code of practice for information security management , which looks like developing into a truly international standard”. However, Dr Shonireguns’ research also identified statistics that show, the vast majority of computer security experts in the UK were still unaware of its existence two years after its introduction.

3.5.2 Shoniregun risk assessment model

The Shoniregun model is a hybrid risk assessment methodology. The model is based on the strengths and weaknesses of previous risk assessment models. The model has two phases and two levels to each phase. Phase 1, level 1 deals with business and technological conception. Phase 1, level 2 highlights risk; staffing, planning, monitoring and control. In phase 2, level 1, the focus is placed on risk; directing, evaluation, identification and estimation.

The final stage is phase 2, level 2, which details simulation, risk occurrence, trend production and a profile of vulnerability (Shoniregun, 2006; p.99). A detailed illustration of the model is included in appendix 3.

The research indicates that the Shoniregun risk assessment model is the most comprehensive risk assessment model available to date. Indeed, only two minor flaws have been identified with this model. The first is that, there are more than identified risks associated with e-business. This is to say that while experts monitor, assess and evaluate, criminals are finding new methods of attack. Secondly, the adoption rate for such a complex methodology is likely to remain low. Human nature dictates that the easiest way to do something is normally the most popular. The model need to be automated, in order to increase adoption rates.

3.6.1 Clark Wilson model

The Clark Wilson model is predominately about preventing unauthorised modification of data, fraud and errors. The security issues that are addressed include internal and external consistency, and access rights to data. Indeed, users have to collaborate in order to manipulate data (Gollmann. 2000; p.56).

However, this model was not designed for Internet technologies. Therefore there are numerous methods of cyber crime that the model does not consider. For example, phishing websites would be the same threat using the Clark Wilson model as a form of e-Security.

3.6.2 Harrison-Ruzzo Ulman model

Harrison-Ruzzo Ulman model specifies access rights of subjects for accessing objects in the system. In addition, Joshi et al (2001) describe this model as a discretionary access model (DAC), which "allows copying of data from one object to another". Indeed, Joshi also points out that this could cause serious violations of security goals.

3.6.3 Lattice based access model

The lattice-based model requires two subjects to access secure data. Wikipedia (2006a) describe the model as "a subject is allowed to access an object only if the security level of the subject is greater than or equal to that of the object.." Although useful; for centralized systems, the lattice-based model does not adequately support the heterogeneous web environment.

3.6.4 Mandatory-based access model (MAC)

According to Joshi (2001) an important goal of MAC is "to control information flow in order to ensure confidentiality and integrity of information, which is not addressed by the DAC". In this model the rules are designed to ensure that information does not flow from a higher security level to a lower one.

3.6.5 Multi-level security model (MLS)

Wikipedia (2006b) define MLS as a security model which, "permit simultaneous access by users with different security clearance and needs-to-know, and prevent users from obtaining access to information for which they lack authorization". However, the idea of sharing sensitive information, all be it with trusted personnel does minimize security. In an environment where data can be shared worldwide, surely the fewer people who have access the better.

3.6.6 Role based access model (RBAC)

Joshi et al (2001) describes RBAC as “a highly desirable goal for addressing the key security requirements of web based applications..”. The advantages of this model include simplification of security administration and separation of duties. Joshi et al goes on to state that RBAC model is ideal for the web however, Joshi makes no mention of cyber crime activities. For example, how would this model protect users against e-mail viruses or Phishing activities.

3.7 Legislation

Within the EU there are numerous laws and governing authorities. For example, in the UK the secretary of state for trade and industry has overall responsibility for the eAgenda (Shoniregun, 2006; p.62). France, Germany, Italy and the rest of European union has its own laws. Moreover, from a worldwide viewpoint China, the US and Korea are all prolific Internet using nations with individual laws and law enforcement policies. The lack of any global law enforcement is possibly the main reason for the growth in cyber crime. Furthermore, cyber criminals have less to fear if they are caught. Many receive sentences or fines that are simply not a deterrent, indeed the computer misuse act, 1990 recommends a sentence of no more than five years.

3.7.1 US cyber security enhancement act

As previously discussed, cyber security laws are varied. In 2002 The US introduced the cyber security enhancement act, which has increased penalties for cyber crime activities. Indeed Hales (2002) noted that, “life in prison, is now a punishment for malicious computer hackers”. Hales goes on to state that the freedom that the Us is renowned for is disappearing with legislation that allows the police too much power.