E-Business Information Systems & Security

Bijender Singh Yadav[1] Sandeep Garg[2] Dr. Ruchira Bhargav[3] Dr. Pardeep Goel[4]

[1]Research Scholar, J.J.T.University, Chudela, Jhunjhunu (Rajasthan)

[2]Asst. Prof. of Mathematics M. M. (PG) College, Fatehabad Haryana – 125050

[3]HOD, Computer & IT J.J.T.University, Chudela, Jhunjhunu (Rajasthan)

[4]Dean of Sc Faculty & HOD Mathematics Deptt. M.M.(PG) College, Fatehabad, Haryana - 125050

Abstract - ***Dependability on technology and risk involved. Defence against the risk always lag behind.***

The relationship between various concepts of security frameworks are presented in this paper. Presentation of main elements and their organization for information system security is described. Organizational dealing with concepts, technological, functional and personnel framework defined. Main cause of risk, attack , vulnerability, attack and other weaknesses in a security procedure and their solution attempted.

Keywords - Information security; information system; social-technical; communication technology; security perception; digital forensics; vulnerability; deception; disruption; threat modelling; diligence.

--♦------------------------------------

1. INTRODUCTION

What the new technologies have brought, then, there are more options and opportunities for conducting information warfare. There is greater dependence on technology throughout society and with it potentially greater losses from technology security attacks. There are new, automated tools for defence as well, but defences are rarely perfect and inevitably lag behind.

This paper takes a tour to provide a review of Information Systems Security relevant to e-business. For the purposes of this thesis, the state of the art is defined as the highest level of development of a device, technique, or scientific field, achieved at a particular time. The identification of the main features of the state of the art enables us to describe problems that need a solution, and, subsequently, to suggest a possible solution to these problems. The main goal of the chapter is to describe a major problem arising in information system security management, addressing which forms the focus of the work described in this thesis. One of the characteristics of information system security is the lack of generally agreed definitions for commonly used terms. A wide variety of interpretations of information system security terminology is used both in industry including commonly used buzzwords and in academic. Although the collection of security-related concepts in practice is the same, the terminology itself is frequently used in different contexts. For this reason, and in order to be able to present the state of the art in a systematic way, a methodological tool is needed to describe both the practical and conceptual aspects of the field.

Basic information system security concept's framework is the tool used here, within which the relationships between the various concepts are established. The state of the art is described using this framework. A conceptual framework makes it possible to organise and present the main elements of information system security. The framework and the logic behind its development, the framework components in a more detailed way followed by security threats discussion, further followed by explanation of perceptions of security. Next, commonly accepted security goals and requirements are discussed. There after various approaches to information security design and management, including the evolution of these approaches and a detailed discussion of the perimeter security approach. Methods for information security and information system security development are presented, discussion of techniques for information security management. Information security policies are discussed, information security standards, personnel and human factor-related security, forensics is described, current security methods, including application security, cryptography, and security mechanisms and tools are discussed. Security models are presented followed by the major e-business security challenges are considered, and prior research on e-business security is presented. The material discussed is summarised and conclusions drawn. The paper concludes with the proposals for filling in the gaps in the current state in the art of information security.

2. FRAMEWORK

Security is an essential requirement since the age of existence of living things. As different systems of human being developed the requirement has taken its own course. Security for information technology and information system is a complex and ever evolving subject. Not only is the term e-business security used in various contexts and with respect to a broad range of information technology issues, the information security discipline is also very broad. It includes a wide range of subjects, such as computing, management/business, and human-related issues. Being the interdisciplinary nature of information system covers topics as disparate as computer science and psychology. A number of information system frameworks have been defined, covering a variety of aspects of the subject, such as frameworks for information system development, frameworks based on sociological models, and frameworks for information system research methods. Information security, as one part of information system, is also complex and broad, and can be approached from a range of perspectives. Siponen considers research methods and objectives, and proposes the use of organisational role as a framework for analysing approaches to information system security. In particular, the organisational roles for information system security include –

- Technical,
- Socio-technical,
- Social views.

Here we present information system security in terms of the conceptual framework shown diagrammatically in Figure 1. This framework is used here as a tool to discuss the discipline in a consistent and systematic way. The logic behind this framework is as follows. The business environment is constantly changing along with advances in technology. At any given point in time, the state of the art in information technology, as indicated in the topmost box, affects the operational and management capabilities and constraints applying to the business environment. Information technology involves the followings:

- Computer hardware,
- Software,
- Data storage, and
- Communication technologies.

Although a business environment benefits from advances in information technology by expanding and/or modifying its business activities, these advances in information technology produce a new range of threats. The next box down, i.e. information system threats, represents threats derived from the use of information technology. The various threats to information and information system also constantly change different business environments at different times are characterised by differing uses and sophistication of information technology, and, as a result, different threats apply. Note that, for Figure 1: Information Systems Security Framework our purposes, a threat can be defined as any circumstance or event that has the potential to harm a system.

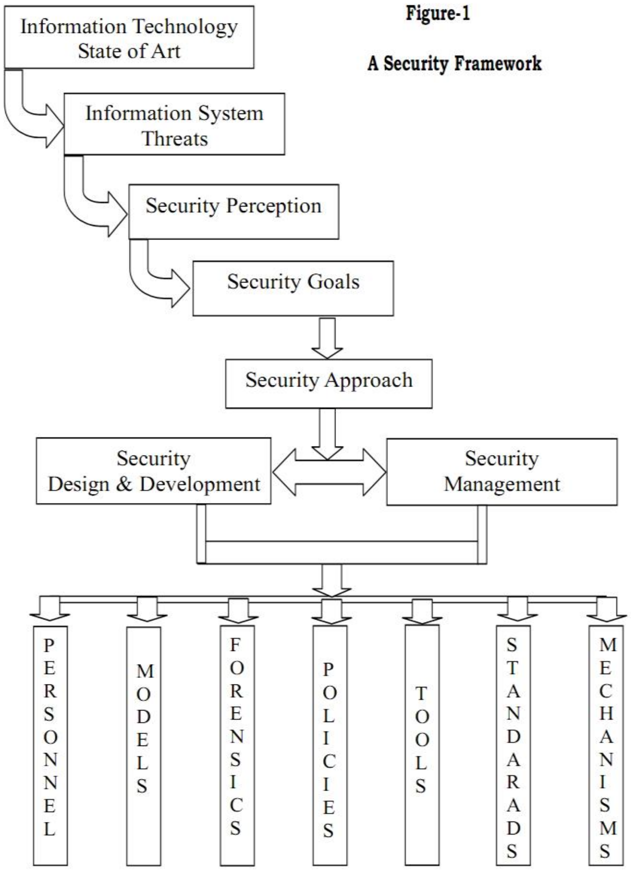
Figure-1

A Security Framework

The perception of, and exposure to, threats define the way in which security is defined, i.e. they determine the interpretation of the term security. This is represented in the framework by the Security perception box. The perception of security has changed over time. For example, before the widespread use of networks, and the Internet in particular, the main perceived threats to information technology were those applying to isolated computer systems. That is, security was considered to be an issue of protecting a computer against what might/could happen to it. Subsequently the perceived threats have changed in line with changes in the use of information system. Changes in the nature of the perceived threats have resulted in changes in perceptions of security. There is no commonly accepted definition of both information security and information system security either in academia or in practice. We provide a definition of these terms for the purposes of this thesis in section to come. The perception of security leads to the identification of security goals as represented by the Security goals box in the framework. We thus argue here that the perceived threats, and the exposure to a specific set of threats, establish the perception of security and, hence, the fundamental goals and objectives of security.

Confidentiality, Integrity, and Availability are commonly considered to be the fundamental goals of information technology security; they are sometimes also referred to as objectives, requirements, or properties The specific perception of security, the definition of the security goals, leads to the establishment of the security approach, or model, as represented by the Security approach box as shown in Figure 1. A model represents a philosophical and theoretical framework of a scientific school or discipline within which theories, laws, and generalisations, and the experiments performed in support of them are formulated. Along with the changes in security perceptions, the approaches to security also change, and different security models have been dominant at different periods. A detailed discussion of security model evolution is provided below in coming sections. Currently, the perimeter security model is the dominant approach for securing corporate information system. This model implies the existence of an organisational security perimeter, i.e. a boundary at which security controls are in effect to protect corporate assets.

Following the chosen security approach, security safeguards are designed and developed the Security design and development box, and security management the Security management box in Figure 1 is implemented in order to optimise the effectiveness of these safeguards. A security safeguard is a protective measure or control that is intended to meet the security requirements for a specific system.

Security safeguards include a wide range of tools, operating and personnel procedures, mechanisms and policies, models, management techniques, physical devices, legal measures, and standards. Security design and development activities relate to the safeguards listed above, while security management is concerned with achieving information system security goals by selecting appropriate security safeguards and managing their operation. Security management is another term lacking a universally accepted definition. We provide a definition of information system security management. For our purposes, security management includes the following topics:

- Organisational, dealing with concepts such as organisational structure distributed, or centralised, hierarchy, business goals, and business environment.

- Technological, covering the information technology issues relevant to the business;

- Operational, covering how an organisation operates its processes business logic and physical environment.

- Functional, dealing with specific functions and processes, including security management functions and responsibilities.

- Personnel, covering the users that interact with the system and its processes, including security awareness, rules, policies, and controls governing user activities.

The safeguards are represented by the boxes in the bottom row of the framework diagram, and are defined as follows:

- Personnel - Users that interact with the system and its processes, including security awareness.

- Security models - Models that represent a particular policy or a set of policies.

- Security tools - Artefacts used in the systems development process.

- Security mechanisms - Methods or procedures used to help enforce a security policy.

- Security policies - Sets of laws, rules, and practices that regulate how an organisation manages, protects, and distributes sensitive information, a statement of what is, and what is not, allowed.

- Security standards - Statements regarding hardware or software, configuration, or level of performance that are to be adhered to in operations.

- Digital forensics - The umbrella term for all forms of research and analysis of computers and computer use directed at obtaining evidence of intrusion, attack, or wrongdoing.

This framework appears to encompass all the elements, both conceptual and practical that comprises the information and information system security domain today. In the remainder of this paper, the main characteristics of the various elements of the framework developed above are described. In doing so, we characterise the state of the art in information system security, and provide the basis for identifying both issues with current approaches to information system security and gaps in the current understanding of information system security.

We argue here that the chosen approach to designing and managing security the security model defines the way in which information system security safeguards are designed, developed, deployed and managed. The framework above suggests that the approach to security should be derived from the security goals, which are they derived from a perception of security that is based on identified threats. Hence, we start our more detailed description of the elements of the framework with a discussion of security threats, since we claim that threats depend on the specific operating environment, and threats are a fundamental component of many existing security model. This is followed by a discussion of the notions of ‘security perception’ and ‘security goal’. Finally, security models are discussed in relation to ongoing advances in information technology, and with respect to changing security perceptions and goals.

3. SECURITY THREATS

Innovation in the field of technology has increased the dependence of organisations on information technology, and the increasing complexity of information technology and information system, makes organisations increasingly vulnerable to any malfunctions in these systems. With rapid advances in information technology and changes in the business environment, threats to information system are constantly changing and proliferating. Whitman argues that there are changes in the identification of threats in the roll-out of new technologies. According to the author, these changes may have shifted the organisational security focus. As information technology advances, more powerful tools are provided to developers and users, and the greater is the computer/technology literacy of the ‘average’ user. Information security is usually considered as being concerned with identifying possible threats based on what is already known, and providing methods within the organisation to address the prioritised threats it faces. Threat is a very broad term. Threats become more specific when discussed in the context of vulnerabilities and attacks.

Definitions of the terms -

- Risk
- Threat
- Vulnerability
- Attack [55], and no universally accepted definitions exist for these terms.

A vulnerability is a weakness in system security procedures, design, implementation, controls, etc., that can be exploited to violate system security policy. Threats are generic, while vulnerabilities are environment-specific, since they depend on the protective measures used in the system. Threats are changing and constantly increasing in number as information technology develops. For example, threats related to computer-based networking only arose once networks became common. These factors together imply that the number, variety, types and power of information system threats are constantly growing. For this reason it is not possible to present a complete list, but instead we give a list of broad categories of threats. A number of threat classification schemes have been proposed, including by authors from both academic and industry. We use here the Shirey threat classification scheme described by Bishop, that divides threats into the following four broad groups:

Disclosure	Unauthorised access to information
Deception	Acceptance of false data
Disruption	Interruption or prevention of correct operation
Usurpation	Unauthorised control of some part of a system

Table 1 : Threat classification by Bishop

Thief does not harm anybody until unless he commits a theft. Similarly a threat itself does not harm a system, but a successful attack does. An attack is a realisation of a threat. An attack is an act that tries to bypass security controls. Threats can also arise from accidental or environmental incidents. For the purposes of our discussion we consider these types of security violation as an attack too. With the advancement in information technology, new types of attack are constantly being invented, and hence we again define general categories of attacks, attack methods and vulnerabilities, rather than attempting to list specific examples. It is important to note that attacks are typically not associated with just one threat category, but may implement multiple threats. We give below a list of attack categories, including some of the more widely discussed classes of attack.

❖ **Malware**- A collective term for many varieties of deliberately malicious software-

- **Viruses** - Self-replicating and propagating programs, usually operating with some form of input from the user, although generally the user is unaware of the intent of the virus.

- **Worms** - Replicating programs that can spread between systems autonomously, without the need to infect a carrier in the manner that a virus does.

- **Trojans** - Programs that pretend to be something else in order to enter a system and encourage people to use them, typically resulting in unexpected and unwanted effects.

- **Spyware** - A program that reports on the contents, status, or operation of a computer to a remote system or user.

❖ **Denial of service** - A form of attack in which legitimate access is prevented or impeded as a direct result of activities originating from unauthorised parties.

❖ **Social engineering** - The use of fraud, spoofing, or other social or psychological measures to get legitimate users to break security policy.

❖ **Insider attacks** - Attacks involving an employee or other trusted individual, generally one with a higher than normal access.

❖ **Impersonation attacks** - An attempt to gain access to a system by posing as an authorised user.

❖ **Hacking** - Breaking security systems by either skilled or unskilled persons.

❖ **Exploitation of implementation errors** - An attack taking advantage of weaknesses that exist as a result of errors in development, yielding a system which is not consistent with security policy requirements.

Basic motive and purpose of attack can also be the base to categorise the attack. Attack categories of this type are as follows.

❖ **Harassment** - Sending unwanted threatening or injurious messages to an opponent directly, either in person or through a medium such as email.

❖ **Cyber terrorism** - The use of information technology by terrorist groups and individuals to further their agenda.

❖ **Political or industrial net espionage** - Network-enabled espionage.

Different factors are responsible for the impact of attack and the seriousness of the attack. Some of the factors are as follows-

❖ Technical capabilities

❖ Attacker competence

❖ Technological advances

❖ Vulnerability & exploitation opportunities

The aforesaid techniques also include:

❖ **Abuse of cookies** - Using the information contained in cookies for illegitimate purposes.

❖ **Buffer overflow** – This is possible as a result of a common programming error in which excessive input exceeds the memory space allocated to it, potentially causing the program to execute arbitrary code or switch operational control to an arbitrary memory location.

❖ **Domain Name System hacking** - An attack on the DNS infrastructure that has the potential to affect a large portion of the Internet.

❖ **Packet sniffing** - Traffic monitoring used by an attacker within a network to gather information about the network.

❖ **Phishing**- Posting of a fraudulent message to a large number of people via spam or other general posting, asking them to submit personal and financial information.

❖ **Routing table poisoning** - Malicious alteration of routing tables by modifying routing information update packets sent by the routing protocol.

❖ **SQL injection** - An attack that manipulates parameters that are used in SQL statements.

❖ **Spamming** - Indiscriminately sending unsolicited, unwanted, irrelevant, or inappropriate messages, especially commercial advertising, in mass quantities.

- **Spoofing/masquerade** - An attempt to gain access to a system by posing as an authorised user.
- **SMiShing** - A compound of phishing and SMS, where mobile phone users receive text messages containing a Web site hyperlink, which, if clicked, downloads a Trojan horse to the mobile phone.
- **Vishing** - The telephone equivalent of phishing.

Vulnerabilities can be technological – Under this category some examples are as follows-

- Uniform Resource Locator parsing errors,
- Flawed password schemes,
- Faulty implementation of Request for Comments specifications,
- Poorly configured default permissions,
- Flawed security models, etc.

Vulnerabilities can be Management oriented - Under this category some examples are as follows-

- Inadequate or lack of security policies
- Lack of user awareness
- Improper firewall configuration
- Organisational culture shortcomings etc.

To be more clear about the concept the email communication can potentially be manipulated and abused in a number of ways, including by spam, address harvesting by gathering of email addresses for the purposes of spamming, or harassment by sending unwanted threatening or injuring messages via email. Valid email addresses are needed by spammers, and various techniques are used to procure them including legal purchase, theft and brute force and dictionary attack.

The example of Denial of service is preventing a server from providing a service, can result from direct attacks or from non-security-related problems. The denial of service may occur at the attack source by withholding from the server the resources needed to perform its functions, at the attack destination by blocking communications with the server, along the intermediate path by discarding messages from either the client or the server, or at some combination of locations.

Possible consequences of attacks for an organisation include:

- Software corruption/modification
- Hardware malfunction
- Data corruption/modification/exposure/theft
- Identity theft
- Intellectual property theft
- Financial loss
- Damage to reputation
- National-level infrastructure disaster.

4. SECURITY AWARENESS

Awareness of security has its own role in everyone's life. Similarly the definition of information system security varies widely, as is true of almost all other information system related terms. There is no formal commonly accepted definition of Information Systems Security. According to Smith et al., Information system Security is the effective implementation of policies to ensure that the confidentiality, availability, and integrity of information and assets are protected from theft, tampering, manipulation or corruption. The National Security Telecommunications and Information Systems Security Committee defines it as the protection of information systems against unauthorised access to or modification of information whether in storage, processing, or transit, and against denial of service to authorised users, including those measures necessary to detect, document, and counter such threats. According to Slade , System security includes the totality of security safeguards to provide an acceptable protection level for a system and for data handled by a system.

In the literature, a formal definition of information system security is often not provided at all, but instead security is discussed with respect to its role. Since information is an asset of an organisation, management is expected to ensure that appropriate levels of control are in place to protect this resource. Information security is concerned with protecting information resources that are owned or managed, while its goal is to deny unauthorised access. Information security says Denning, is intended to support the mission of an entity, which depends on timely access to its information resources.

From this discussion, it appears that information security is commonly deemed to deal with the protection of information resources by denying access to unauthorised users. That is the common perception of security focuses on controlling access by preventing unauthorised access.

This perception is reflected in the widely discussed generic security goals, or security requirements of Confidentiality, Integrity and Availability. This set of security requirements are based on the principle of authorisation, namely who is allowed to access what and in what manner. These security requirements are discussed in the next section.

5. SECURITY GOALS

It is commonly accepted by the security community that there are three main security requirements or properties as they are called by Tettero and Landwehr are used with the following meanings:

- Confidentiality
- Integrity
- Availability

Although there are some slight differences in definition and interpretation, in general the three basic security requirements are used with the following meanings:

Confidentiality – This requirement ensures the necessary level of secrecy at each data processing entity, and prevents unauthorised disclosure; it ensures that information is not made available to unauthorised parties.

Integrity – The integrity involves maintaining the accuracy and reliability of information and processing methods, and preventing unauthorised modification of data, thereby ensuring that data is correct, as defined by the process designer.

Availability - Involves ensuring timely access to data and resources to authorised users, so that data, information and other elements of information systems are accessible and useable by an authorised user.

The above three definitions are based on those given in.

Aforesaid three security requirements have been in use by the security community for many years. With involvement of information technology in the business and change in the business environment, the question arises whether these still represent the complete set of security goals that a modern business or e-business information system should achieve? Are all these requirements always needed? For example, in an e-commerce system assuring the confidentiality of the information delivered may not be important at all if the system is simply acting as an online catalogue of merchandise, though of course if it is used to accept credit card numbers, they will require protection. How is privacy maintained in the world where information/data harvesting techniques are improving constantly?

Some authors introduce additional requirements such as accountability and non-repudiation, depending on the circumstance.

Accountability ensures that actions affecting an information system can be uniquely traced back to the responsible entity.

Non-repudiation is one of the five main classes of security services defined in the Open Systems Interconnection Security Architecture. Here we use the definition given by Dent and Mitchell, according to which non-repudiation is a service that enables the participant in a communications session to prevent another party in the session from denying having taken a particular action e.g., having sent or received a message. The Open Systems Interconnection security architecture defines two main types of non-repudiation:

- **Non-repudiation of origin**, in which the recipient of a message is provided with the means to prevent the originator of the message from denying having sent it.
- **Non-repudiation of delivery**, in which the sender of the message is provided with the means to prevent the recipient of the message from denying having received it and having recognised its content.

While discussing the use of non-repudiation in an e-commerce framework, covering issues relating to the transfer of a document, such as proving the identity of the person that sends a document, the time the document was sent, and acceptance of the document. Non-repudiation can be provided in a range of ways, and typically involves an exchange of cryptographically protected messages such as those specified in ISO/IEC 13888. However, while a non-repudiation mechanism can provide evidence that might potentially be useful in resolving disputes, such evidence is of little value in the absence of a non-repudiation policy specifying how evidence should be generated and managed, and how it might be used in the event of a dispute.

Healey argue that security requirements can be met in many different ways, some of them completely outside the scope of system software, while security requirements have to be applied in the context within which the entire system operates. Bishop argued that the interpretation of a security requirement in a given environment is dictated by the needs of the individuals, customs, and laws of the particular organisation. As a result of technological changes, organisations experience not only operational changes, but also conceptual and behavioural changes. The security requirements should reflect these changes and adapt to the modern reality, and so they should be updated in line with the specific business situation.

6. SECURITY MODEL

A security model is an essential aspect of any process of life. This model must take account of the state of the art in information technology. The security models in use are thus likely to vary over time, as technology and its use develop. In this section, examples of such changes are presented, focussing on those relevant to the current dominant security model.

6.1 DEVELOPMENT OF SECURITY MODEL

With binging of the information era security evolved as important aspect of business. Definitions of the terms as well as perceptions of the subjects have changed in line with technological advances. Until the 1980s, the term security was mainly used in relation to isolated computers, which is reflected in the literature of that time. At that time, the notion of computer security was only related to the processes inside the computer. The main security issues related to secure operating systems and secure access to computer and computer resources. Earlier the need for computer security was primarily associated with government and military rather than commercial applications. Key work at that time addressed issues such as information flow controls in the operating system, although problems often remained in the form of unauthorised information flows via covert channels.

Early work on computer security was sponsored by the US Department of Defence. This pioneering work only addressed data confidentiality issues and not the integrity. The security models developed by the department of defence reflected the perceptions of computer security and the concept of government security. The department of defence model involves classifying resources and users into sensitivity levels, such as unclassified, confidential, secret, and top secret, forming the notion of multi-level security. The Orange Book of the department of defence Trusted Computer System Evaluation Criteria built on the department of defence model, and defined a set of criteria for the development and evaluation of secure computer systems. More general awareness of security issues amongst non-government information technology users was slower to develop. However, during the 1980s a range of products became available to protect data for commercial users, e.g. in the form of database security features. Of course, certain industry sectors (notably banking) deployed security functionality very early, but typically using bespoke systems.

Probably the most important development in information technology during the 1980s as far as security is concerned, was the growth of networking, which provided organisations with the means to interconnect their computers both locally and, using WANs, to some extent globally. The concept of computer networking was introduced in 1962 in an MIT series of memos written by Licklider, discussing the Galactic Network concept of a globally interconnected set of computers, somewhat like the Internet of today. With the arrival of ARPANET in 1969, the critical ground rules that were formulated for its successful operation did not include security issues, but instead focussed on reliability and connectivity.

The networked infrastructure developments during the 1980s changed dramatically the role of computers in industry and the related terminology. The concept of an information system was introduced, and the difference between computer and information system and their respective contributions to organisations, along with the differences between the terms data and information, became evident. Differences also emerged in related terms. The introduction of the notion of a system made it clear that there are many functional aspects that need to be made secure whether it is a computer system or a more general entity such as an information system. Global connectivity has massively increased through use of the Internet both by industry and domestically. The widespread development of LANs, PCs and work-stations in the 1980s provided inter organisational connectivity, and also allowed the Internet to flourish. This was accompanied by a major shift in technical and management issues, such as the invention of Domain Name System (DNS), a distributed, hierarchical global directory that translates machine/domain names to numeric IP addresses.

Connectivity between various parts of an organisation implies resource sharing, and brings with it a range of serious security vulnerabilities. During the 1990s, it became widely recognised that security is everyone's problem. Organisations found themselves facing a conflict that arose from the desire to be both connected to the outside environment for usability reasons, and disconnected because of the associated threats to their information. With the growth in connectivity, the increasing awareness of security issues across industry, and the emergence of firewalls as a security enabler, the security perimeter model emerged, and rapidly became dominant. The security perimeter, a collection of tools, mechanisms and techniques, is built to protect an organisation's internal resources from external access. The security perimeter is applicable at an organisation's boundaries, so that it can protect the resources within. With the arrival of e-commerce and e-business in the late 1990s, and their subsequent growth in importance, security issues have become even more serious. In particular, these new modes of doing business are only made possible by the adoption of the relevant information technology and by giving very large numbers of people access to organisation networks. Network-level security is widely practiced in order to protect the internal resources of an organisation, and the perimeter security management approach has become dominant.

6.2 THE CURRENT MODEL

The perimeter security model is commonly used for managing corporate information system security. It implies the existence of a logical barrier around a specified set of corporate resources. In practice, the security perimeter is constructed using a collection of security products, notably including network firewalls. The goal is to prevent malicious/non-authorised users and applications from accessing corporate resources, include its business functions. Information system security is thus based on a trust hierarchy, in which the company's employees automatically get maximal trust at least as far as the security perimeter measures are concerned, while external users get minimal, if any, trust. This approach does not distinguish between different applications with different levels of sensitivity running in the business. Mobile devices operating outside the physical corporate domain, and connecting via public networks, which are increasingly used in e-business activities, are not given a high trust level, even if the users of the devices are trusted employees. The modern business environment in which e-business systems operate is also changing with respect to the extent to which businesses control their own information technology. Organisations are no longer likely to have total control over the systems and networks upon which their e-business applications depend. Jones et al. argue that, as a result, it is becoming more important to understand, and regulate, perhaps by contractually binding statements of requirements, the relationships between the stakeholders responsible for different parts of a system. In addition, there is a real and growing problem with interoperability between different e-business solutions.

One of the characteristics of a modern organisation and especially of an e-business organisation is the distribution of resources and assets. Resources and assets are physically and/or logically located at different sites. Management of the resources is also distributed between various hierarchical functions. In addition, in an e-business, the number of users such as employees, customers, partners, suppliers are likely to be large, and many of these users both from inside the organisation and from other organisations need access to corporate information. In order to provide a deeper understanding of perimeter security we next briefly describe the security safeguards used to enforce the perimeter.

6.3 THE SECURITY PERIMETER ARCHITECTURE

The tools necessary to enforce the security perimeter include such things as firewalls, Intrusion Detection Systems (IDSs), Intrusion Prevention Systems (IPSs), De-Militarised Zones (DMZs), and network security features using cryptography. A firewall is a system that enforces a boundary between two or more networks, with the ability to permit or deny the passage of data according to a predefined security policy. Such tools appear to be the most popular form of web security measure. A firewall is a hardware- and/or software-based device, whose basic task is to control traffic between computer networks in different zones of trust, e.g. between an internal trusted network and an external un-trusted network such as the Internet, in order to detect, prevent, or mitigate certain types of network attack. An IDS is an automated system for alerting operators to a penetration or other contravention of a security policy. IDSs are designed to detect malicious activity, and can often manage to do so quite impressively. However, their performance is greatly dependent on the following factors:

- The skills of the person that is managing and configuring the tool;
- The availability of the means to interpret the huge amounts of data captured by these systems.

Intrusion Prevention System is a second-generation Intrusion Detection System that either stops an attack or interacts with an external system to address the threat. A DMZ is a way of separating sensitive information from that intended to be publicly available. It is also known as a perimeter network, and its purpose is to isolate and limit the damage an attacker can do by gaining access to a server. In particular, it can be implemented using firewalls in situations where organisation internal networks are separated from publicly accessible servers, such as Web servers, which themselves are separated from the public Internet by another firewall. The use of a DMZ increases network overhead and there is usually a performance dip at the server level when a DMZ is activated. There is also no clear consensus on the best way to implement a DMZ or how many DMZs are the most efficient design.

Tools used in implementing perimeter security are designed to prevent malicious content from entering the organisation. However, in practice they may give a false sense of security, in particular since they cannot prevent attacks that originate inside the firewalls. Also, firewalls, IDSs, and IPSs require a lot of maintenance to ensure that they function as intended. Although widely used, these safeguards have limited effectiveness when applied in a highly interconnected environment. Most network-level security mechanisms used as part of a perimeter defence fail to identify all web-based attacks, and thus let malicious traffic pass through the organisational perimeter. As a result, attacks may occur.

The boundary approach quickly becomes inappropriate as security requirements become more refined and functional requirements expand. Since the logical extension of the boundary security model results in identifying ever more zones that must have their boundaries protected, eventually there will be overlapping zones and it will be necessary to implement security access controls at each boundary. 'No matter how complex these zones become, the policy implementation is simple: separate insiders from outsiders'.

Boundary protection models do not allow for the implementation of robust security rules, since, by firewalling each zone, the security analyst tries to define security as a large access control problem. Also, it is impossible to interpret access control criteria for each information technology device, because the model is not consistent across different types of network component, and each of these components has a different function.

The feasibility of the perimeter security model in the modern technological and business environments is increasingly criticised both by academics and practitioners. The modern business operation is based on global interconnectivity and information sharing. The hard-shell perimeter model has changed with the advent of the Internet. If you step back and look at your corporate Intranet, with its hardened perimeter, says Simmonds, you will probably be in for a nasty shock. That once simple, secure boundary resembles a piece of Swiss cheese.

The notion of de-perimeterisation has recently been introduced, and describes possible alternative approaches to corporate information security management. De-perimeterisation means that the opening up the networks through the achieving acceptable levels of risk. The need for open networks is driven by several business needs, including remote employees, mobile connections, collaboration with other organisations, and integration with other organisations' processes. According to Palmer, de-parameterisation as it is called refers to the erosion of the hard-shell model used to describe the structure of traditional information security implementations while capturing the growing requirement for perimeters to be breached in order to facilitate commerce and collaboration. Nowadays, a new model is needed and this will be de-perimeterisation. De-perimeterisation advocates, the need for a distributed security model. This can already be seen to be taking place, where anti-virus, intrusion detection and firewalls are embedded on individual devices, supplementing current centralised security solutions for more detailed discussion of de-perimeterisation

7. SECURITY DEVELOPMENT METHODOLOGIES

As the information system developed with the pace of time security development methodologies and methods have evolved in a similar way, and they share common features such as objectives, means, challenges, and primary concepts. Baskerville [39] identifies three generations of security design methods, i.e. the checklist methods used in the 1970s, mechanistic engineering methods used in the 1980s, and logical and transformational methods used since the late 1980s. The third generation methods, i.e. the currently used systems development methods, include logical and transformational methods. The logical methods include the techniques of Yourdon, Constantine, and Checkland's Soft Systems Methodology, a detailed discussion of these approaches can be found. The transformational methods are represented by the Systems Development Life Cycle and its more recent UK variant Structured Systems Analysis and Design Methods.

The third generation methodologies have both strengths and weaknesses. Flexibility is a major strength of these methodologies. Weaknesses include problems with migrating from the abstract models into a real working system, integration of both physical and logical security components, a separate cost-benefit evaluation of security, and, because of the reliance on abstract models, the methods are oriented toward adding security to a new system. Typically, information systems are developed in accordance with a systems development life cycle, which is a general approach to the development of an information system. A systems development life cycle provides a well-defined process for considering an organisation's business requirements, translating them into an information systems context, and then developing an information system that supports those requirements. A systems development life cycle provides a model of a system. However, security is not one of the issues that is addressed in this methodology. Also, when modelling a system or any part of it, only the specific state of a system at some static point of time is described. Changes that take place at any other time are not covered by the model.

According to Avis and Fitzgerald the systems development life cycle approach has a number of weaknesses, including:

- Failure to meet the needs of management
- Instability
- User dissatisfaction
- Problems with documentation
- Incomplete systems
- Application backlog
- Maintenance workload.

In direct contradiction to Baskerville, Avis and Fitzgerald claim that the systems development life cycle approach is inflexible, because, in this methodology, the outputs that the system is meant to produce are usually decided very early in the systems development process. As a result, the design is output driven, which leads to inflexibility with regard to the changing requirements of a system. Although it is widely accepted that information system security design and implementation require a comprehensive approach, and that they should cover a variety of topics, information systems security issues are often only considered after a system has been developed, and rarely during its design, coding, testing or deployment. Security is a requirement which has to be considered at all stages of development, and security-relevant issues are often considered only at a technical level i.e. covering such things as encryption techniques, security protocols, logging, etc.

Another approach to the development of secure systems is based on the Capability Maturity Model. The model identifies five different levels of the maturity of software development in order to address security engineering goals, but it does not cover the configuration and operation of systems, but their development only and also suffers many of the limitations of the other approaches. Although security is an important issue for e-business, traditionally, as for any information system, security is considered only after the definition of the system. This can give rise to a range of possible problems. For example, if security is only considered at certain stages of the system development process, then the necessary security safeguards could conflict with the functional requirements of the system. Hence, there is a need to develop a discipline for secure information system development. If the security of network architecture is not properly designed from the beginning, the security goals are difficult to achieve during practical operation of the network. The advisability of considering security from the very beginning of the system development has recently begun to be appreciated, and in particular in the system requirements specification phase.

8. INFORMATION AND INFORMATION SYSTEM SECURITY MANAGEMENT

Information system security management is concerned with both the organisation and with people. There is no commonly accepted formal definition of information and information system security management. In a more general management context, security management deals with the identification of an organisation's information assets, and the development, documentation and implementation of policies, standards, procedures and guidelines, and the allocation of resources to make these tasks possible. The security management subject area is the subject of increasing interest, arising from the growing recognition of its importance in the effective deployment and use of security measures. The current approaches to security management can be divided into three groups, namely:

- Approaches based on security management standards
- Approaches based on best practice
- More formal approaches

Security management approaches currently existing have a number of shortcomings some of the as follows:

- Only security issues within a narrow scope are addressed, although many dimensions ought to be considered following a holistic approach;
- Only cover parts of the commonly used System Development Life Cycle for modern systems development;
- The implications on security management of e-commerce are not addressed sufficiently.

Management tools, such as information classification, risk assessment and risk analysis, are used to identify threats, classify assets and to rate system vulnerabilities so that effective controls can be implemented. The various currently available security management techniques and tools are next briefly described, and their main characteristics are emphasised.

8.1 CHECKLISTS

The idea of checklists is to identify possible countermeasures and turn them into a list. As the name implies, in this approach, information system security techniques and procedures are presented as a list, from which practitioners can choose specific solutions that meet their needs. The early information security checklists, such as that provided by American Federation of Information Processing Societies and the Security Audit and Field Evaluation list, support secure systems design by enabling the selection of appropriate security controls. Another widely known checklist is the standard ISO/IEC 27002 (ISO/IEC 17799) (which is discussed in section 10 below). Peltier et al. argue that checklists, if used inappropriately, can impact the free flow of ideas and information and, hence, may be most suitable for use at the end of the security design management process. However, they have also been widely criticised, since they have a very narrow scope and address observable issues only, without considering the social aspects of the security problem.

8.2 RISK ANALYSIS

The existing perimeter security approach has an impact on the security methods currently used in organisations. In conjunction with this, the security measures deployed by on organisation are typically selected as a result of an activity which has several names, including risk analysis, risk assessment, and risk management. Security risk is an inescapable fact of e-business. They go on to describe four possible approaches to risk :

- Accept
- Ignore
- Assign it to someone else
- Mitigate

Risk analysis involves identifying and ranking risks, while risk management is a continuous process, covering a variety of risk analysis and risk mitigation activities. Wang and Zeng [42] argue that risk analysis is one of the most important phases of risk management. According to Tregear [41] risk assessment following a formally defined method is critical to establishing effective information system security management. Academic research argues about the real value of risk management. Goel and Chen identify a number of problems in using risk analysis techniques, including:

- The lack of standardised metrics and processes for the valuation of assets.
- The lack of the means to measure the impact of threats, and to estimate the benefit of controls.
- An acute shortage of data that would enable a reasonable statistical analysis to estimate risks.
- The poor quality of data on threats and vulnerabilities.
- Reliance on checklists and guidelines makes risk analysis ineffective or expensive because of the need for internal data collection, e.g. using penetration testing and/or honey pots.
- Organisations do not have the ability to determine the quality of assessments, and have to rely on the verdicts of consultants.

Although risk management and risk analysis techniques are widely discussed, these tasks are not trivial, and are sometimes very difficult to perform effectively. Risk analysis is an appropriate approach for helping to select safeguards for tangible information technology assets i.e. computer assets, which are mostly physical in nature, even though it is still problematic. Risk analysis involves identifying risks by estimating threats and vulnerabilities. In order to perform a risk analysis in practice, a quantified analysis of risks has to be carried out, which implies using estimates for probabilities. Quantifying asset value could prove to be a difficult task, especially for intangible assets such as information.

The evolution of the information technology environment, says Gerber and von Solms has brought the following changes in the business environment:

- Business processes are no longer conducted in isolation.
- Information is the core of all business processes.
- Organisations are interdependent, and operate as a whole.
- Each organisation must deploy appropriate information security management.
- Information security should be approached in a holistic way.

Risk evaluation based on information technology, building on an isolated, closed world, assumption is no longer appropriate, and a holistic view of assessing risks should be adopted, rather than the traditional approach to risk assessment. Zukato argue further that risk analysis alone is not sufficient to develop security requirements for e-commerce. Traditional risk analysis is related to the natural science model3, which is already represented in the current ways of managing risk. However, issues such as law, politics, economics, etc. should also be part of the overall management of risk. Finally, e-business development is relatively new to many companies, and therefore there is limited knowledge about the relevant risks.

8.3 THREAT MODELLING

A threat model is used to characterise an organisation's environment both internal and external in terms of possible attacks and their levels of severity. Organisations need to identify information security threats in order to establish a list of possible security-violating scenarios. Threat identification provides organisations with information regarding the types and extent of possible security violations. Threat models are a widely used tool in the development and design of an information security model and they can be used to provide inputs for the security model, and can be used as a basis for selecting the types of defences to be used to protect against information security attacks. There are number of methods for threat gathering, including:

- Checklists
- Examination of historical data
- Brainstorming

A threat vector technique involves three variables to define i.e. source of threat, threat, target, for each possible attack path. Two problems with this approach are as follows:

- The defined threat vectors for a specific company will be based on the perceptions of the security designer;
- Two of the variables threat and target are likely to be constantly increasing in number and variety.

‘Security experts tend to focus on the threats they know how to model and prevent. The attackers focus on what they know how to exploit, and the two are rarely exactly the same’, argues Blaze.

8.4 DUE CARE AND DUE DILIGENCE

Information security comes down to technical measures only. One of the consequences of not operating an effective information system security programme is that an organisation may be liable for misuse of its information systems argues Anderson. That is, every organisation must perform due care i.e. actions undertaken to provide proper, just, required and sufficient care, so far as the circumstances demand of information system security. The management of every organisation is legally responsible for any security violations of information system under laws such as the US Federal Sentencing Guidelines. Control Objectives for Information and related Technologies, and for health care and medical organisations. Due diligence refers to proof usually documented that due care has been exercised. Management is charged with showing that due diligence has been performed during the decision-making processes for any organisation. If an organisation's management fails to appreciate that information security governance is an essential and integral part of corporate governance, then they fail to perform due care and, as a result, will fail to perform due diligence.

In order to try to protect themselves against possible any future claims, managers often buy products and services from major suppliers, without any prior security assessment, although these products and services may have limited effectiveness. Ironically, such decisions are considered by some organisations as due diligence. Because of the complexity of a modern networked organisation, it is difficult to obtain an enterprise-wide view of security management and, hence, those responsible for security often lack knowledge of the real security requirements of their organisation. The result is that due care and due diligence cannot properly be performed.

9. INFORMATION SECURITY POLICIES

The term information security policy refers to a set of organisational-level rules that govern the acceptable use of computing resources, security practices, and the development of operational procedures. An information security policy is one of the two most important documents for ensuring the effective deployment of information system and information technology within a modern business enterprise the other being the Strategic Information Systems Plan. Information security policy is the starting point and reference framework on which all other information security sub-policies and standards must be based, and it must show the commitment of the executive management towards information security in the organisation. In the information system security framework presented above, information security policies are developed through information system security design and development. Managing the development of security policies as a project involves the application of a variety of skills, tools, experiences, and techniques. Information security policies are implemented through information system security management, which also deploys additional safeguards, as presented in Figure 1.

An Information security policy argues Solms and Solms is a method by which a well-defined process is put into place, so that all information security issues are considered in a foolproof manner. The authors argue that the SDLC is an appropriate tool for such a task. Information security policies are essential to support the efficient and secure running of an organization. However, modern organisational information security policies appear to be increasingly unable to handle security breaches. The most prevalent model for handling breaches appears to be an ad hoc one, where the latest breach becomes the model for future occurrences. The problem with current approaches, argue Rees et al. , is that they do not address the problem of keeping up with the increasing rate of change in e-commerce technology and applications, and they also do not provide means for keeping such policies consistent and aligned with organisational objectives. The application of information system security countermeasures is generally limited to addressing specific vulnerabilities i.e. hardening operating systems for publicly available servers, applying and monitoring IDSs, and installing and configuring firewalls. To conclude, although information security policies should be derived from the corporate strategy, supported by the executive management, and relate the entire organization by covering all the relevant aspects of business activities, these policies are usually written by technical information system security professionals and relate usually the information access problem only.

10. STANDARDS OF INFORMATION SECURITY

Information security management standards are among the most widely used methods for security management. Standards in the information security domain aim to capture industry best practice, and to provide generic and authoritative instructions to be applied at an international level. Compliance requirements for organisations are usually driven by the industry in which they operate. Some organisations might need to meet the compliance requirements in more than one standard. Information security management standards are typically expressed in terms of goals. The baselines are typically created by academic groups, and the guidelines are then developed by Information Security practitioners [40]. The most commonly used standard for information security management is ISO/IEC 1779910. ISO/IEC 17799 is just one of the 27000 series of international standards for the management of information security. ISO/IEC 17799 has frequently been criticised for just providing a checklist instead of detailed guidance on how to conduct security management. The 27000 series aims to address this issue by providing detailed guidance on a range of information security topics. Also, argues Zuccato, the standard is appropriate for a traditional organisation but not for an e-commerce organisation. The importance of insider threats for information system security management is widely recognised, and is also addressed by ISO/IEC 17799. However, argue Theoharidou et al., ISO/IEC 17799 is ineffective in addressing insider threats. A lack of proper theoretical background on human behaviour, caused by the failure to adopt a holistic approach, is suggested as one of the reasons for this.

SOX (the Sarbanes-Oxley Act) require that companies establish a financial accounting framework to generate financial reports. The reports must include verifiable and traceable source data. The source data must remain intact, and shall not undergo undocumented revisions. In addition, any revisions to financial or accounting software must be fully documented, describing what was changed, why, by whom, and when. Web services security has been the subject of major recent development effort, resulting in a number of web services security standards. These standards are mostly concerned with protocol definitions, and there is a lack of a global vision addressing management issues.

Many organisations are not aware of the contents and contribution of all the available standards, and hence many organisations do not comply with them. For example, organisations securely managing electronic forms of information often ignore critical data that is still kept in other forms. Security for this other data is thus not addressed by the safeguards implemented to protect electronic data, although ISO/IEC 17799 explicitly addresses this situation.

The perceptions of information systems security standards held by managers in government agencies, revealed that just a few of the agencies succeeded in achieving compliance. `Low management involvement' was the recurring theme in responses given in interviews carried out during the study. The information security management standards focus on ensuring that certain security processes exist, but the standards fail to advise on the practical implementation of these security processes. Siponen emphasises that `it is not important that something is done, but . . . how well it is done'. Also the author argues that the processes, guidelines, and principles of information security management standards are abstract and over-simplified.

11. HUMAN FACTOR IN SECURITY BREACHES

Any organization even fully automated systems require human intervention. One of the most common ways in which information can be lost by an organisation is through its personnel. Therefore, security requirements cannot be addressed by technical and technological means alone, the customers and the employees involved significantly influence the success of security measures says Whitman. The reason for security breaches is more often human failure than weaknesses in technology. The human factors should be given proper attention, both in ensuring user knowledge, understanding and use of security features, and also the obligation and willingness of users to follow the relevant security procedures and policies. Security incidents are usually a function of security policy, ethics training, and proper execution of the access policy. Also, according to the author, a failure by individuals to follow policy can arise from a failure in, or absence of, a control mechanism to regulate user access. Internet users are often not informed about the threats arising from the use of Internet services, and hence are likely to be vulnerable to the risks.

Users, whether they are employees, customers or any Internet user can also cause harm intentionally, possibly with criminal intent by infecting the organisation with a virus, sabotaging systems, or to perform fraud or money laundering. Hence, an awareness of cybercrime and the associated issues is increasingly essential. One of the best ways to instil a security culture is to educate and train staff about what they should be doing. Security awareness and training programmes can serve to inform employees about information security policy, to sensitise them to social engineering tactics and potential losses, and to train them in the use of security practices and technologies. Various surveys show that only a low percentage of organisations have established information security training programmes for their staff.

To conclude the section, information security is commonly viewed as a technological problem, although it can be violated significantly by an organisation's personnel. Personnel are not trained enough with respect to information systems security in organisations. Security safeguards with respect to personnel and human factor-related security are under-treated in organisations, and usually ignored both during the information system security development process and by the organisational information system security management. This type of safeguards should be addressed by other safeguards listed in the information system security framework; related information explained in section 2. and similarly graphically displayed in Figure 1, in particular by a set of appropriate information security policies.

12. SECURITY MODELS

A security model provides a template for security policy enforcement in a system. While most security models cover the same topics, the approaches may vary. The security model is a philosophy that guides the way an organisation approaches security. Security models are fundamentally important security design and analysis tools. There are number of general categories of security models, where some models can be classified under more than one category. Some models relate to confidentiality and integrity and some apply to environments where policies are static and others address dynamic changes of access rights. We next review some of the more widely discussed such models. We divide the models we discuss into four main categories relevant to the security-

- Confidentiality
- Integrity
- Access rights
- Business rights

12.1 CONFIDENTIALITY-RELATED MODELS

a. **The Bell-LaPadula model** - This abstract security model was developed during the period of the ‘computer security’ perception. It defines users and any other active elements such as computer programs as subjects, and passive elements usually meaning data as objects. Four different access modes are defined, covering the reading and writing of data referred to in the model as observation and alteration. The Bell-LaPadula model was the first mathematically specified information flow security model. It has been formally proven that, if its conditions of four security levels and three main rules are properly implemented, then information can only flow in a secure way between subjects. The underlying mathematical model is state machine based (where the security of a system is defined in terms of sets of permissions for subjects accessing objects). The scheme is designed to model the protection of secret information, i.e. to provide data confidentiality.

b. **Chinese Wall model -** Separation of data of two different users is the aim of this model. This model ensures that the data of two different users stay separated, regardless of the levels of sensitivity of the data themselves. This model is able to represent a security policy that deals equally with confidentiality and integrity, and is hence useful for the business environment. Indeed, it even complies partly with British law, which requires use of policies similar to that instantiated by the Chinese Wall model.

c. **Non-interference model -** The non-interference property can be used to ensure that any actions taking place at a higher security level do not interfere with those taking place at a lower security level. This ensures that users at a lower security level cannot discover which commands are being executed by users at a higher security level. This model is concerned with the knowledge that a subject has about the state of the system, rather than directly with the flow of data.

12.2 Integrity-related models - We give here three examples of models addressing data integrity, namely the Chinese Wall, Biba and Clark-Wilson models.

a. Chinese Wall model - This model was introduced in section 12.1.

b. Biba model - The Biba model is another state machine based model; it has two fundamental rules, namely the 'no-write up' rule i.e. a user cannot write to a higher level and the 'no-read down' rule i.e. a user cannot read from a lower level. The Biba model addresses data integrity, using an information flow approach. The integrity property is represented as a set of ordered integrity levels; the higher the level, the more confidence users can have that:

∗ The program will execute correctly.

∗ The data are accurate and/or reliable.

Neither the Bell-LaPadula nor the Biba model provide a way to define security and integrity ratings, and to make modifications to such ratings. They also do not deal with delegating or transferring access rights.

c. Clark-Wilson model - Like Biba, the Clark-Wilson model is concerned with data integrity, but it operates very differently from the Biba model. While government and military users are typically primarily concerned with confidentiality issues, the commercial sector is often more concerned with protecting the integrity of data. This model is thus more relevant to the commercial sector then most other models. Data integrity is achieved by preventing its unauthorised modification; authorisation is required to apply a program to data that may be accessed through that program. External information is tracked by auditing, which is required by this model. The principle of Separation of Duties is enforced by dividing an operation into a number of parts, and requiring different users (or different rules) to perform each part of the operation. As a result, critical tasks cannot be performed by just one entity.

12.3 Access rights-related models - A large number of models fall into this category, including the following.

a. Graham-Denning model - This model addresses two issues that are not covered by either the Bell-LaPadula or the Biba models; that is it provides a way to delegate access rights, and to define and modify security and integrity ratings. The Graham-Denning model provides a set of basic defined rights in terms of commands that can be executed by a subject on an object.

b. Harrison-Ruzzo-Ullman model - This model extends the Bell-LaPadula model by providing means for changing access rights and for creating and deleting subjects and objects.

c. Lollipop model - The Lollipop security model, otherwise known as the Eggshell model, models the perimeter security approach. According to this model, an organisation's security architecture is designed to surround the organisational assets with a wall of safeguards (e.g. firewalls), to control access to the assets, while the inside is left `soft', giving access to anybody who is allowed to pass through the wall (the perimeter). This model has two major limitations that are inherent in the perimeter security approach:

∗ Once an attacker has penetrated the perimeter safeguards, he/she has access to all the internal information systems resources;

∗ There is only one level of security (outside the perimeter versus inside the perimeter), while almost all business functions require a range of different security levels.

Also, as discussed above, this security model does not fit the e-business mode of operation, where access must be given to a variety of participants such as customers, suppliers from the external environment.

d. Onion model - A firewall provides a single layer of defence against threats arising from Internet, i.e. external threats. In order to provide protection against internal threats, layered security architecture can be applied. In this model, security measures, such as authentication and access control, are applied at various layers of the system, such as at physical, segmentation, monitoring, or auditing layers. Such a security architecture is also referred as the `defence in depth' approach. These layers of security measures are intended to make life more difficult for an attacker. However, for an e-business organisation, these multiple security levels are likely to interfere with the performance of critical business processes, because of the need for e-business processes to interact with other entities both inside and outside the organisational perimeter.

e. Non-interference model - See the discussion in section 12.1.

12.4 BUSINESS ENVIRONMENT-RELATED MODELS

As discussed above, some models have been developed to address business needs. This group includes the following models.

a. Chinese Wall model

See the discussion in section 12.1.b

b. Lollipop model

See the discussion in section 12.3.c

c. Onion model

See the discussion in section 12..3.d

d. Orange Book

The Orange Book, i.e. the Department of defence Trusted Computing Security Evaluation criteria (see section 6.1), can be regarded as defining a security model. The Orange Book has limitations. The criteria defined in the Orange Book were designed to be applied to monolithic computer systems with centralised processing functions. As a result, it is very difficult to apply these criteria to internetworked systems, where data storage and processing take place at multiple locations in the information systems infrastructure. Subsequent developments in security evaluation criteria that gave rise to the European ITSEC12 and the harmonised Common Evaluation Criteria address these issues.

To conclude the section, information security models usually address two of the security requirements triad, namely the confidentiality and integrity properties, and there is no availability property-related model. Also, most of the information security models can be classified as access rights-related models.

13. E-BUSINESS SECURITY STATE OF THE ART

In order to make the discussion of the security domain comprehensive and within the context of this thesis, we now provide a separate discussion of e-business security issues and a review of the prior research on the security challenges in this area. Realisation of the e-business mode of doing business is made possible using the open standards of the Internet. The use and implementation of these technologies gives rise to a wide range of security vulnerabilities and threats, which are discussed below.

13.1 E-BUSINESS SECURITY ISSUES

E-business is based on the information flow on a open network such as internet. Therefore security is widely accepted as one of the main barriers to the successful deployment of e-business. Security issues are classified here into two groups, a broader group covers Internet related security problems in general, and a more specific group includes Web application vulnerabilities.

a. **Internet-related security problems -** Data communication between the participants of e-business through the network is one of the main characteristic which widens the scope of potential attacks. Security breaches and unreliable e-services can result in a range of types of business losses, including e-business productivity losses, asset losses, and reputation damage. New threats and problems arise when using Internet technology, and especially when a company adopts the e-business mode. A particular danger in running an e-business arises from its `openness' to the environment, and the various connections and communication channels it shares with the external world. E-business involves performing business interactions (transmitting documents represented by information flows) between organisation portals using Internet technology. Use of a web browser brings with it various threats and vulnerabilities for the end user (business or private customer). The range of threats includes issues such as:

- Violation of user privacy by abusing information held about a user (such as login name or computer name);
- Cookies, stored on the client machine and exchanged between the Web client and the Web server to maintain connection information, can be used for the purpose of gathering potentially sensitive user information;
- Executable downloads, such as Java applets and ActiveX controls, can be a source of vulnerability at the client;
- Push technology, used by many sites to deliver web content to customers, give rise to serious security vulnerabilities (the content provider could, for example, send malicious code or cause Denial of Service attacks);
- Attacks on network servers - Web servers, application servers, mail servers, etc.

Poorly configured networks are subject to confidentiality, integrity and/or availability threats. Traditional authentication methods such as passwords, when used for access control in an online environment, are subject to a range of vulnerabilities i.e. arising from keystroke loggers, which record the keys struck by a user. Because of the global access it provides, the Internet is very vulnerable to malicious actions, while worms, viruses and other types of malware continue to evolve both with respect to the mechanisms they use and their infection speed. Existing server and network infrastructures include large numbers of tools and mechanisms designed to mitigate known threats. Finally, ‘day zero’ vulnerabilities that reveal them only when they are first exploited, need different approaches and solutions.

Jungck and Shim use the January 2003 SQL slammer worm as an example of an attack that took advantage of vulnerabilities in firewalls and IDSs (Intrusion Detection Systems). In order to allow service provision, many firewalls left open the port that Slammer attacked, and most IDSs left that port unmonitored. It is very difficult to update every system to address every known threat; it is difficult for administrators to manage such a process, and for organisations to afford the necessary updating activities. The authors also emphasise that increasing Internet bandwidth is another obstacle to information security, because the growth in bandwidth has exceeded the ability of processors to filter the traffic. Closing the gap between bandwidth and processor capabilities is only made possible by either slowing traffic to a speed at which security applications can be performed, or by abandoning security monitoring to meet network performance goals. It is thus clear that information security problems span a wide range of issues, including lost flexibility for high-speed operation, changing protocol threats, and problems related to traditional designs. The problem is beyond silicon, systems, and applications, however. It's in the standards we write, without security in mind, the complexities we introduce by not adhering to standards, and the network topologies we continue to paste together without a holistic view. Internet businesses often face major operational uncertainties arising from system complexity, rapid development, interconnectivity, and a lack of familiarity with the new technology based economy.

Many e-business organisations suffer from problems with the information systems that facilitate e-business. Such problems include poor security, flawed controls, inadequate management controls, and poorly designed and unreliable back-end systems. In general, management lacks reasonable assurance whether or not their digital operations are effective and efficient, information generated by e-processes is reliable for decision making, or e-operations are compliant with the applicable laws and regulations. This lack of confidence is depicted in highly publicised security breaches and e-service failure'. Effective design of e-business processes is essential to avoid security defects. Because of the critical reliance of e-business on correct execution of its e-processes, tools to verify e-process design and implementation need to be developed.

We also observe that digital copyright has become a major concern for businesses that engage in online content distribution using approaches such as pay-per-view, subscription, trading, etc. Advances in Internet technology have enabled digital service providers to sell their digital content via computer networks. Digital content can be easily copied, altered, and distributed to a large number of recipients, which could cause significant revenue loss to media companies. Intellectual property protection is a growing concern for content owners. Privacy issues and identity of the customers are considered to be an important aspect of e-business, as well as communications- and transaction-related issues.

Attacks on e-business information system can occur at various levels of the system. Examples of such attacks are as follows -

- Denial-of-service attacks.
- Damage caused by malware.
- Attacks arising from exploits of the Web Services application interface.
- Script-based injections causing damage to an application and/or its data.
- Network interception arising from protocol weaknesses.
- Defeat of encryption arising from faulty cryptographic key management or poor selection of encryption methods.
- Database administrators stealing sensitive database content or configuration parameters.
- Application programmers insert undetected malicious code in application software, causing problems, such as widespread security failures or subversion of critical business transactions.

b. **Web application vulnerabilities and challenges -** Today the web has become the back bone of every aspect of life. The potential of the web services for both application developers and users has increased exponentially. However, certain features of web services make them particularly vulnerable to a number of possible attacks. Gehling and Stankard observed that the attacks on web applications and web services are the fastest growing new category of attack, and describe the following vulnerabilities particular to web services:

- The web services format was designed to bypass existing security measures, to be platform independent, and to support any application call structure; hence, additional security measures are needed.
- Although the flexibility of Simple Object Access Protocol and other technologies makes communication among applications easy, it also simplifies interception and manipulation of messages.
- Simple Object Access Protocol messages are transparent to firewalls, which means that perimeter security controls are likely to be bypassed.

Today's online activity such as online shopping, online banking, and online business make use of web servers, which are also frequently attacked. One class of weaknesses that makes such attacks possible are the well known and commonly occurring SQL (Structured Query Language) command injection vulnerabilities. Such attacks are made possible by inadequate checking of un-trusted user inputs (substrings) during communication between the application layer and the back-end database in the web-application architecture. These attacks typically involve manipulation of SQL statement parameters in input fields, such as customer number, address, or search phrase. Attacks taking advantage of such vulnerabilities can result in loss of confidentiality, integrity and authenticity for important business data.

Many security flaws in e-business applications arise from design-related flaws. According to the reports of a survey conducted, security design flaws were found in 70% of all analysed defects. Although, part of the flaws were of low business impact, or were not easily exploitable. 47% of the remaining serious defects could have been caught and fixed, inexpensively during the design stage. There are several reasons for the presence of such flaws few of them as follows:

- Many designers and developers are not trained in general security principles.
- Designers and developers do not consider security as an explicit application requirement.
- Security issues are addressed only after vulnerability is discovered.
- Marketing pressures lead to shortcuts in application design and development, resulting in less robust software that may include security flaws.
- There are many different e-commerce applications written in a variety of languages running on a range of different systems.
- Generic e-commerce applications have specific security requirements, which some existing security architectures are not able to meet.
- E-business operation is very complex, and so are the e-business applications that implement these operations.

It is very difficult and expensive to significantly improve its security once operational use of an application has commenced. The new approaches are needed to support dynamic business processes and their management. Such measures should provide the following:

- The ability to prescribe how Web services are used to implement activities within a business process.
- A way of deciding how business processes are represented as Web services.
- The ability to decide which business partners perform what parts of the business process.

13.2 E-BUSINESS SECURITY RESEARCH

Ngai and Wat conducted a literature review of two hundred seventy five research articles on e-commerce published in nine leading journals over the period 1993 - 1999. This section contains a review of prior research on security for e-business and e-commerce, although the distinction between these two modes of business is often not clearly made. This review was used to devise a classification scheme for e-commerce research. They classify articles under three main headings, namely by year of publication, by the percentage of the total number of articles in selected journals, and by topic. According to the findings of this review, among the technology-related articles, security was the most popular topic-about 33% of the technology-oriented articles were on e-commerce security.

In recent years research in e-commerce security has focussed on two broad areas, namely research on improving e-business security through policy measures, and research on technical security measures for e-commerce. Wareham et al.came to this conclusion based on an analysis of 582 articles on e-commerce research published over the period 1997 - 2003 in both academic and professional journals. Following Ngai and Wat, the authors give the distribution of primary topics identified in their sample. The topics were grouped into four major domains –

- Information technology and infrastructure,
- Applications and industry themes,
- Business issues, and
- Other social issues.

The findings of the study performed by Wareham et al.have significant differences to those of the Ngai and Wat review of the period 1993 - 1999. Security was found to be one of the most underserved research areas, represented by only 2.4% of the articles. The authors point out the surprisingly low percentage (16.6%) of research on information technology and infrastructure, and argue that it would appear to be necessary for information technology researchers to understand the technical underpinnings of the central issues before proceeding with enlightened social, business, and application research'. Prior research on improving e-business security is presented here using the classification provided in i.e. we divide our discussion into technical and organisation-related issues.

a. **Technical security research -** Security for e-business is often regarded as purely a communications security problem, with the use of cryptography as a suggested solution. Gollmann argues that cryptography protects the information transmitted between two points, i.e. it protects the communications media. Digital watermarking is one technique that can be used to protect on-line content. A watermark can serve various purposes, including content protection, fingerprinting, ownership assertion, authentication and integrity verification, and usage control. Various watermarking techniques have been suggested. Proposed applications include using digital watermarking for intellectual property protection in electronic commerce transactions for identity authentication in e-business activities, and for automatically protecting e-business data. The specific requirements on the watermarking technique vary with the application.

Although Memon and Wong argue that watermarking is undoubtedly important for protecting various forms of digital content, there are difficulties that still need to be solved. Watermarking techniques can be classified as either fragile or robust. While fragile watermarks are easily corrupted by image-processing procedures, robust watermarks resist common image-manipulation procedures, and are useful for ownership assertion purposes. However, devising robust digital watermarking schemes is a very difficult problem because of the numerous image manipulation techniques that a robust watermark must be able to survive. Two classes of security service, namely access control services and communications security services, are usually considered to be the most crucial for an e-business organisation. Access control prevents unauthorised use of resources, and communications security ensures the confidentiality and integrity of transmitted data. Joshi et al.argue that new access control mechanisms for Web-based applications are needed, because the existing access models are insufficient. The authors present a comparative assessment of security models used for Web-based applications and workflow systems, and claim that existing access models do not support dynamic changes in the content and context of information, or allow monitoring of the system state or transactional activities. Such features should be present in access models.

b. **Organisation-related security research -** Chua et al.conducted a survey designed to test whether or not existing e-commerce research focuses primarily on certain specific stakeholders. The survey was based on publications in seven out of the top nine e-commerce journals. The results demonstrate that academic e-commerce researchers concentrate their attentions on two stakeholder groups, specifically customers and the internal organisation i.e., managers and employees of a Net-Enhanced Organisation (NEO). Other stakeholders, such as suppliers, indirect stakeholders, investors, and regulators, receive disproportionately less research interest. The authors argue that at least four stakeholder groups, namely investors, suppliers, regulators, and indirect stakeholders, will increasingly demand the attention of NEOs, and therefore information system and e-commerce research needs to reposition itself.

Privacy is a security-related issue relevant to e-business. The findings of a study conducted by Sinclaire reveal that there has been limited research in the area of information security and privacy, particularly at the organisational level. Sinclaire based his findings on a review of a range of MIS research literature published over the period 2002 - 2004 in four highly ranked journals for information system research publications. Sinclaire makes a distinction between information security and information privacy. Based on the definitions of information privacy as `the ability of the individual to control personal information about one's self', and the Panko definition of information technology security as providing confidentiality, integrity, and availability, Sinclaire presents the following statistics regarding research on security. A total of 24 articles were reviewed, of which 74% addressed information security and 26% addressed information privacy; 29% of the information security research articles address planning, and 71% address protection. Analysis of research within the protection category reveals that 50% pertain to authentication/verification, 25% are about types of threats, 17% address standards, and eight percent pertain to firewalls. Analysis of information privacy research reveals that 67% address user perceptions and the remaining 33% pertain to surveillance issues.

Detailed requirements definition and analysis, as the first step in e-business systems design, has been proposed to support collaboration between the parties in e-business activities. Androutsellis-Theotokis et al.discuss various requirements with respect to their importance for e-business collaboration, such as workflow and collaboration orchestration, authentication and access control, logging and non-repudiation, data storage security, availability, integrity, and anonymity. Herrmann and Pernul argue that security and integrity are two security requirements that are relevant for e-business. Jones et al. consider e-business requirements in terms of the trust and dependability of business partners.

E-business security management research covers a wide range of issues. As elsewhere, some authors use the terms e-commerce and e-business interchangeably, without making a distinction between these two concepts. Koskosas and Paul suggest a socio-organisational approach to information system security management in terms of a framework of security goal setting. The framework illustrates three important issues in the process of security goal setting, namely trust, culture, and risk communication. Using three case studies, the authors present evidence that there is a chain reaction among these three issues, with a subsequent effect on the level of security goal setting . Wang and Chen discuss the issue of e-business management in terms of three types of flow. The authors present an approach in which the object of e-business management is the set of e-business activities. According to Wang and Chen, generally speaking, e-business management is a dynamic object formed by the circulation of three flows, namely information flow, fund flow and material flow (or logistics). Hence, e-business management should focus on guiding the co-ordination of these three flows. That is, e-business management must be concerned with combining and coordinating each procedure and resource, and the main goal must be to achieve collaboration and harmony between these three flows. This collaboration is dominated by information flow during e-business activities.

Bodin et al. propose a method for optimally allocating a budget for maintaining and enhancing the security of an organisation's information systems. The method is based on computing ratings according to confidentiality, data integrity, and availability criteria. The availability criterion itself is broken down into three sub-criteria: authentication (of the correct users), non-repudiation (a user cannot deny using the system, if in fact he or she used it), and accessibility or non-denial of service.

Rees et al. propose a framework for creating security strategy and policy for applications. This framework, known as PFIRES (Policy Framework for Interpreting Risk in E-business Security), was initially developed for e-commerce activities, but has been generalised to handle security policy for all types of organisations engaged in computing and Internet operations. The authors argue that PFIRES offers a possible starting point for understanding the impact of a security policy on an organisation, and is intended to guide organisations in developing, implementing, and maintaining security policies.

13.3 CONCLUSIONS

Global representation by business environment and more specifically the Internet-based technologies used by e-business provide a wide range of services, each with its own capabilities and security vulnerabilities. Even if we assume perfect protection from firewalls, strong defence from unbreakable cryptographic algorithms, and installation of all available software patches, if e-business processes are not designed or implemented properly then the e-business will still be exposed to losses. Also, generic e-business applications are created using a variety of technologies, which may not work in all environments. Prior research on e-business and e-commerce security has focussed mainly on technical security measures, and on improving security through policies. Unfortunately, relying solely on technology solutions for e-business security is not enough.

14. SUMMARY

This paper discussed the context of a conceptual framework for Information Systems Security. This framework provides a context within which we have described the elements making up the Information Systems Security domain. The approach to security is derived from the perception of security, which encompasses both the definition of security and its goals. The current dominant perception of information security is as a means of prevention, limitation and blockade. Given the modern information technology environment, and building on the current security countermeasures (such as, antivirus protection, IDSs, IPSs, firewalls, access control mechanisms, and other tools and methods) widely used by organisations today, it can be concluded that organisations typically identify the main dangers to their information and information systems as arising from the external environment. This environment is perceived as the source of threats that could harm the business, arriving via the networks that connect the business to the external environment. In line with this perception of security, the main security goals of CIA (confidentiality, integrity, availability) are commonly accepted. The currently widely adopted security model builds on this understanding of security and its goals. The current commonly adopted approach to information security design and development is the Perimeter Security model, which first emerged in the 1980s with advances in networking. This use of networking arose first in academic and government environments, and only somewhat later in business environments. Although technological advances have dramatically changed the modern business arena (including operationally, conceptually and behaviourally), the perception of security, the development of security requirements, and security design and development are still the same as they were at the beginning of the networking era. This model has an impact on the entire security framework, and practical security designs derive from it. In general, the design, development and management of Information Security including e-business information security models, techniques, mechanisms, tools, and policies are based on the prevailing conceptual model for Information Security. Some of the most significant security issues, policies and tools, and how they are affected by the perimeter security model, are given below.

Security goals - Security goals are much the same as those defined decades ago for a closed organisation, and hence are unlikely to be appropriate for the modern open business.

Threats - Threats are constantly changing and increasing in number and variety; as a result threat assessments may rapidly become unrepresentative.

Models - Models of security underlie the design and development of operating systems, and are typically concerned with access control, defined in terms of roles and access limitations.

Risk analysis - It involves estimating the risks resulting from known potential threats and/or vulnerabilities. Such an analysis may not capture the risks arising from `future' attacks, and is also problematic in terms of both practical execution and the subjective perception of risks and their measurement/estimation. As a result, risk assessments may not provide good estimations of the true risk.

Policies - Policies support the ruling perimeter security approach by providing access control rules. Such policies are typically written at a technical level, and serve as the basis for developing security tools, products, and techniques, building on the security models and access control rules. That is, they are primarily aimed at preventing access by unauthorised users, user-oriented policies are usually ignored and/or are not considered to be important.

Tools - Tools typically support the dominant security perimeter approach (e.g., firewalls, IDSs, IPSs, antivirus systems, etc.). Such tools primarily address known threats and/or attacks, and implement the idea of `blockade'. Moreover, such tools are not effective when configured or applied wrongly.

Standards - These provide guidelines on what information systems security issues need to be addressed in a specific industry. Such standards exist for various business environments, although they are not always implemented in the same way in different organisations and different countries, if they are implemented at all.

Security design and development methodology - The prevailing approach to information security design is `to protect against future attacks'. These future attacks are typically defined based on the current state of the art, whether published or discussed in organisational or professional communities.

Personnel - Personnel’s are often not trained for information system security awareness. Due diligence procedures appear to be rarely implemented, even when the individuals concerned are working with very sensitive information and processes of critical importance.

Forensics - These are problematic because of the complexity of e-business information system, and the common lack of complete documentation. This latter problem typically arises because security is added as a patch after a security incident has taken place. E-business realisation is made possible by using and implementing the open standards of Internet and Information technology, which gives rise to security vulnerabilities. E-business security challenges are addressed by the security measures that are included in the framework presented in section 2, and discussed in details in sections 3 - 13. That is, the e-business mode of doing business is subject to the same perception and model of security that apply to the components of the framework.

3.16 CONCLUSIONS

Information system and e-business security reveals a number of conceptual and practical issues, including the following.

- There is no formal definition of the term ‘security’ with regard to information and information system.
- The information system security discipline is built on a perception of information and information system `security' rather than on definitions.
- The perception of `security' is based on addressing threats, although threats change constantly.
- Information system security development is undertaken using methodologies that do not address modern business security requirements; in particular, current development methodologies do not take into account the dynamics and complexity of organisational information system.
- There is no broadly accepted formal definition of information system security management.
- The e-business information system security is designed and managed according to the perimeter security model.
- The commonly practiced perimeter security model does not fit the modern business environment.

The modern organisation faces a business environment which is very different from that of the 1980s. The possibility of interacting with suppliers, customers, competitors, partners, and financial and government institutions via the Internet changes the way operations are performed, the business and financial relationships, and the ways of dealing with money. As a result, there are new security vulnerabilities and threats, and so this new environment requires a different set of security goals. The currently used security models, mechanisms and techniques support the perimeter model by meeting the `pre-e-business reality' security objectives. The models reviewed above are designed to support security policies that control access to data.

This leads to the conclusion that the perimeter security approach is not appropriate for the e-business mode of doing business. The use of the perimeter security approach is thus a major problem for the information system security discipline today. The goal of the research described in this thesis is to suggest a solution to this problem. In terms of the security framework presented in this paper, a new security model is needed, based on a different perception of security and different security goals. The main conclusion of this paper is that a new process-based approach has the potential to provide a more rational, and hence, more effective, security designs for an e-business organisation.

REFERENCES

[1] A. Andreu, Professional Pen Testing for Web Applications, Wiley Publishing, Inc., 2006.

[2] A. Dent and C. Mitchell, User's guide to cryptography and standards, Artech House, 2005.

[3] A. Jaquith, The security of applications: Not all are created equal, Research report, at Stake, 2002, can be found at: www.netsourceasia.net.

[4] A. Liska, The Practice of Network Security|Deployment Strategies for Production Environment, Prentice Hall PTR, Pearson Education Inc., 2003.

[5] A. Moser, C. Kruegel, and E. Kirda, Exploring multiple execution paths for malware analysis, IEEE Symposium on IEEE Symposium on Security and Privacy (SP '07) (2007), 231 - 245.

[6] A. Pons and H. Aljifri, An active watermarking system, IACIS, Issues in Information Systems (2002).

[7] B. Schneier, Applied Cryptography, John Wiley & Sons, 1996.

[8] B. von Solms and R. von Solms, The 10 deadly sins of information security management, Computers & Security 23 (2004), 371 - 376.

[9] C. Chua, D. Straub, H. Khoo, S. Kadiyala, and D. Kuechler, The evolution of e-commerce research: A stakeholder perspective,Journal of Electronic Commerce Research 6(2005), no. 4.

[10] C. Gutierrez, E. Fernandez-Medina, and M. Piattini, Towards a process for web services security, Journal of Research and Practicein Information Technology 38 (2006), no.1, 57 - 67.

[11] C.Landwehr, Formal methods for computer security, Computing Surveys 13(1981),no.3.

[12] D. Avison and G. Fitzgerald, Information Systems Development Methodologies, Techniques and Tools, 3rd ed., McGraw-Hill Education (UK).

[13] D. Denning, Information Warfare and Security, 12th printing ed., Addison-Wesley, February 2006.

[14] D. Dzung, M. Naedele, T. von Hoff, and M. Crevatin, Security for industrial communication systems, Proceedings of the IEEE, vol. 93, June 2005, pp. 1152 - 1177.

[15] D. Gollman, E-commerce security, Computing & Control Engineering Journal (2000).

[16] E. Ngai and F. Wat, A literature review and classification of electronic commerce research, Information & Management 39 (2002), 415 - 429.

[17] G. Chakrabarti, A. Manimaran, Internet infrastructure security: A taxonomy, Network, IEEE 16 (2002), no. 6, 13 - 21.

[18] G. Palmer, De-perimeterisation: Benefits and limitations, Information Security Technical Report 10 (2005), 189 - 203.

[19] G. Schryen, The impact that placing email addresses on the Internet has on the receipt of spam: An empirical analysis, Computers & Security 26 (2007), 361 - 372.

[20] J. Dhillon and G. Torkzadeh, Value-focused assessment of information system security in organizations, Information Systems Journal 16 (2006), no. 3, 293 - 314.

[21] J. Joshi, W. Aref, A. Ghafoor, and E. Spafford, Security models for web-based applications, Communications of the ACM 44 (2001), no. 2, 38 - 44.

[22] J. McCumber, Assessing and Managing Security Risk in IT Systems, Auerbach Publications, 2005.

[23] J. Rees, S. Bandyopadhyay, and E. Spafford, PFIRES: A Policy Framework for Information Security, Communications of the ACM 46 (2003), no. 7, 101 - 106.

[24] J. Rust, Corporate management of computer forensic evidence, InfoSecCD '06: Proceedings of the 3rd annual conference on Information security curriculum development, 22 - 23 September 2006, pp. 175 - 178.

[25] J. Sherwood, A. Clark, and D. Lynas, Enterprise Security Architecture: A Business-Driven Approach, CMP Books, 2005.

[26] J. Wareham, J Zheng, and D. Straub, Critical themes in electronic commerce research: a meta-analysis, Journal of Information Technology 20 (2005), 1 - 19.

[27] John Wiley & Sons, 2003, Computer Security.

[28] M. Bishop, Introduction to Computer Security, Addison-Wesley, 2005.

[29] M. Gerber and R. von Solms, Management of risk in the information age, Computers & Security 24 (2005), 16 - 30.

[30] M. Osborne, How to cheat at Managing Information Security, Syngress Publishing, Inc., 2006.

[31] M. Whitman, Enemy at the gate: threats to information security, Communications of the ACM 46 (2003), no. 8, 91 - 95.

[32] Model checking-a rigorous and efficient tool for e-commerce internal control and assurance, Knowledge Emory, Goizueta Business Library, GBS-DIA-2001-007 (2001).

[33] N. Memon and P. Wong, Protecting digital media content, Communications of the ACM 41 (1998), no. 7, 35 - 43.

[34] N. Williams, E-business security issues for SMEs in a virtual hosting environment, ISICT '03: Proceedings of the 1st international symposium on Information and communication technologies, Trinity College Dublin, 2003, pp. 357 - 364.

[35] O. Tettero, Intrinsic Information Security. Embedding Security Issues in the Design Process of Telematics Systems, Telematics Institute Fundamental Research Series, No. 006(TI/FRS/006), 2000.

[36] R. Anderson, Why cryptosystems fail?, Proceedings of the 1st ACM conference on Computer and Communications Security, ACM, 1993.

[37] R. Baskerville, Information systems security design methods: implications for information systems development, ACM Computing Surveys 25 (1993), no. 4, 375 - 414.

[38] R. Bragg, M. Phodes-Ousley, and K. Strassberg, Network Security: The Complete Reference, McGraw-Hill/Osborne, 2004.

[39] R. Baskerville, Information systems security design methods: implications for information systems development, ACM Computing Surveys 25 (1993), no. 4, 375 - 414.

[40] Siponen, An analysis of the traditional IS security approaches: implications for research and practice, European Journal of Information Systems 14 (2005), 303 - 315.

[41] Tregear, Risk assessment, Information Security Technical Report 6(2001),no.3,19-27.

[42] Wang and Y. Zeng, The risk identi¯cation and assessment in e-buisness, FSKD 2005, LNAI 3614 (L. Wang and Y. Jin, eds.), Springer-Verlag Berlin Heidelberg, 2005, pp. 1142 - 1149.