Information Security and e-Business/Commerce

Toshiyuki Sueyoshi*, Gopalakrishna Reddy Tadiparthi**
and Peter Anselmo***

Abstract

Information security is an increasingly important concern among many corporate leaders and system managers who are responsible for computer systems. A modern Information Technology (IT) system, drastically changing the current business/management, is structured by an open system where many different disturbances (e.g., corporate secret agents, hackers and terrorists) influence the IT-based decision making process and business performance/practice. This study is concerned about such a security issue, in particular focusing upon how the infrastructure of a corporate network is protected from hostile agents. The study is also interested in whether the security issue influences our corporate decision making in the e-business world.

Keywords: Information security; Information technology; Firewalls

1. Introduction

Information Security (IS) is a buzzword in the present-day world. The significance of IS has increased with inflated attacks on the information stored in computer systems. Internet evolved from the ARPANET (Advanced Research Projects Agency NETwork), which was created in 1969. Scientists and engineers wanted to share information with each other over the newly linked computers. This network was limited to a few computers and usually only those with knowledge of computers had access. During that time, security was not an issue, as the ARPANET was designed with openness in mind. (See Hayashi and Sueyoshi [28] for a detailed description on the historical perspective on Internet.) Today, the information available on Internet has increased, but the technology for security for this information has not increased on par. The requirements of IS within an organization have undergone major changes in the last several decades. Before a widespread use of data processing equipment, the security of valuable information was provided primarily by physical (filing cabinets with a combination lock) and

* Corresponding author: New Mexico Institute of mining and Technology, Department of Management, Socorro, New Mexico 87801-4796, USA, E-mail: toshi@nmt.edu
** New Mexico Institute of mining and Technology, Department of Computer Science, Socorro, New Mexico 87801, USA, E-mail: gopal@nmt.edu
*** New Mexico Institute of mining and Technology, Department of Management, Socorro, New Mexico 87801-4796, USA, E-mail: anslemo@nmt.edu
administrative (personnel screening procedures used during the hiring process) means. With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became apparent.

The current definition of “information” ranges from negative entropy (used in Information Theory) to any pattern that influences the formation and transformations of other patterns (Information [32]). In this study, information is defined as meaningful data stored in a computer. Security is defined as the state of being free from annoyance, harm, danger or loss (Security [67] and Security [68]). Information was coined during the 14th century and security during 15th century (Information [31]). This leads us to think why security was coined later than information. Venter and Eloff [74] have defined “information security” as the protection of information and minimize the risk of exposing information to unauthorized parties. Anderson [5] has emphasized on the definition for an enterprise, IS is a well-informed sense of assurance that information risks and controls are in balance. In this paper, we define IS as the concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use (McDaniel [48]).

It is easily imagined that we try to understand IS only when corporate secret agents, hackers or terrorists attack our computer systems and defense mechanism(s) is(are) employed to protect computer security. Unfortunately, many corporate managers are not familiar with current IT technologies related to IS. Conversely, IT engineers are not familiar with how to introduce IS into their organizations.

The purpose of this paper is to perform a comprehensive survey on different IS technologies, then document those into classifications from a perspective of IS enhancement and managerial applications. Based upon the classification on previous research efforts on IS, firewalls (a group of software) are examined as a defensive IS tool. After reviewing the firewalls, this study will discuss how to incorporate such an IS technology into corporate entities which are now facing serious business competitions. Thus, it is expected that this research makes a theoretical linkage between the new IS technology and e-business. Such a theoretical investigation has been never explored in literatures on both computer science and management.
This article is organized as follows: The next section (2) recapitulates previous research works on IS after presenting our conceptual framework for its classification. Section (3) describes the overview of e-Commerce/e-Business. Section (4) examines firewalls as a defensive IS technique. This section also discusses how to introduce the IS technology into a corporate climate where we need to make a close linkage between the IS technology and managerial decision making/corporate strategy. A concluding comment is summarized in section (5), along with future extensions of the proposed research framework.

2. Previous Research and Classification

Figure 1 depicts a conceptual framework on the classification on IS previous studies. As indicated in Figure 1, the e-business and e-commerce are a combined use of electronic communication technologies such as the Internet or EDI (Electronic Data Interchange) in order to exchange information and business transactions. After following previous research efforts on IS, the taxonomy, described visually in Figure 1, is proposed in this study. The broad classification is made in conjunction with previous research works, including Anderson [6], Bishop [15], Bishop and Bailey [16], Briney and Prince [17], Brinkley and Schell [18], Burstein [20], Howard [29], Howard and Longstaff [30], Linqvist and Jonsson [45], Rees et al [59], Richardson [61].

Figure 1 Proposed Taxonomy on IS
2.1 Internal

One of previous research efforts on IS is directed toward “internal aspects on IS.” These include the information protection technologies adopted within the inner perimeter of an organization. The internal perspective on IS can be separated into administration, network, hardware and software, all of which can be described as follows:

2.1.1 Administration

This category includes administrative measures taken by the organization management to safeguard information. As visually indicated in Figure 2, employee awareness can be created by giving training and educating non-computer workers to use only in-house developed software and not use any free downloadable unauthorized software in their system. A software agent system can also be produced and installed in each workstation to monitor the software installed in each employee computer. The computer security/usage policy should be available and easily accessible in hardcopy as well as on website. Each employee could also be provided with digital signatures to solve the problem of non-repudiation. Employees should be encouraged to report to the network administrator of any violations noticeable to them. (See, for instance, Bianco [13], Power [57], Richardson [60], Tzu [73] and Whitman [75].)

![Figure 2 Internal – Administration](image-url)
2.1.2 Network

This refers to the protection of the process by which data is transmitted from one network entity to another. Implementation of an Intrusion Detection system is very useful in detecting any potential attacks. The Intrusion Detection should be configured to escalate the concerned managers using pagers or other warning systems. Each employee should be given a username and password to access any resource in the internal network. Cryptographic keys can be employed to prevent sniffing within the network. Telnet should be discouraged and encrypted logins like SSH (Secure SHell) should be encouraged. Firewalls can be used to protect the internal network from external attacks. The policies of the firewalls can be enforced in a strict manner by not allowing any browsing traffic to flow through. The employees should not be allowed to make a data connection from the local telephone line to the Internet. This would bypass the firewalls and would create vulnerability in the Internal system. (See, for example, Bellovin [12], Cohen [22], Jayaram and Morse [33], Kent [36], Kumar [42], Kumar and Spafford [43], Richardson [60], Ristenbatt [62], Rosen [63], Stallings [70], Tzu [73], Whitman [75].) Figure 3 depicts such a structure of network components from the IS perspective.

2.1.3 Hardware

Media should be stored in a fire-proof safety vault with both physical lock and cryptographic lock. As depicted in Figure 4, authentication and access control to hardware resources can be provided with the use of biometrics (like scanning the retina of an eye or fingerprints) which cannot be duplicated or stolen easily. Data transfer between systems or to secure servers should be only through PCMCIA (Personal Computer Memory Card International Association) smart cards which accept only certain cards (See, for example, Ahuja [2], Amoroso [4], Landwehr et al. [44], and Richardson [60]).

2.1.4 Software

All the systems in the internal network should be configured for automatic updates from the software vendor and the system administrator should be updated with the current security attacks and be in a position to update the software when necessary. All proper anti-virus protection software should be installed in all systems. Anti-virus software uses stored virus definitions to detect and quarantine viruses. Virus definitions must be updated to defend against new viruses. Each workstation should be configured to automatically
download new definitions daily. Proper audit trials should be conducted and the audit logs should be monitored regularly for any kind of intrusions. All computer systems should not be left unattended. Hence, they should be set to automatic lock / log off when not in use. Each operating system should be capable of storing encrypted files when the security of the file is very important. Abbott et al [1] and Konigsford [39] described some of the operating system vulnerabilities. The in-house software development team should make use of the security SDKs (Software Development Kit) available while development. (See, for example, Aslam [8], Aslam et al. [9], Beizer [11], Bisbey and Hollingworth [14], Jayaram and Morse [33], Knight [38], Krsul [40], Krsul [41], McPhee [49], Tzu [73], Whitman [75].) Figure 5 visually describe such perspectives related to the software.
2.2 Actus Reus

This term is used mostly in courtrooms. In the proposed taxonomy, the term means a misuse of authority. This implies that a trusted authority misuses the trust vested in him. For example, a system administrator can steal the passwords of the users to avenge a personal fight.

2.2.1 Trust

All the employees trust either the software system analyst or the network administrator with their computers. All events in the operating system should be logged for watch of any remote logins or physical logins by any person. An appropriate warning mechanism would save a lot of data (Lynch and Rose [46]).

2.2.2 Cryptography

Various public key, Virtual Private Networks can be used to access the internal network from the external world. Logins should be only encrypted. (See, for example, Denning et al [23], Kahn [34], Schneier [64], Schneier [65].)

2.3 External

A lot of external factors can influence loss of data and insecurity of information.

2.3.1 Natural

In the event of a disaster, the initial recovery process takes roughly 1-2 days. During that time, systems are restored at a designated recovery site. The business continuity plan takes effectively the next step. Business units
need to know what they can expect from the disaster recovery effort. They also need to be able to work independent of IT systems for whatever time is agreed upon for the disaster recovery process. Each business unit must take an inventory of what they need to stay in business (identify dependencies). The business needs to identify critical suppliers and ensure that their contracts provide for disaster recovery (i.e. a manufacturing plant won't function without a steady flow of parts). Human resources and accounting need to be prepared, too. Paychecks need to flow. Bills need to be paid and emergency funds need to be available in such a case. Each business unit must create and maintain a business continuity operations guide (See, for example, Neumann [50], Neumann [51], Neumann and Parker [52].)

A disaster recovery manual should be prepared and be available with the operations engineers so that they can handle the situation when any natural calamity like earthquake, power loss, or floods occur. There should always be a backup power supply to take over for the important machines which host a large amount of important data. Data and media backups should be scheduled regularly and shifted to another off-shore location to restore if the calamity occurs in the first location (Marsh [47]).

2.3.2 Manmade

This mostly either can be intentional sabotage or unintentional accident. But, prevention is always better. Important documents should be shredded by a proper paper shredder. Access to external persons like janitor, repairman or maintenance personnel should be strict and sent in after through scanning. They should also be checked while exiting for any theft of important information. (See, for example, Parker [53], Parker [54], Parker [55], Perry and Wallich [56], Schwartau [66], Straub and Widom [72].)

3. An Overview on e-Business/e-Commerce

The e-Commerce or e-Business is an electronic transaction, performed over the Internet--usually via the World Wide Web (WWW)--in which the parties to the transaction agree, confirm and initiate both payment and goods transfer. There are two general types of e-Commerce activity; B2C (Business to Consumer) and B2B (Business to Business). B2C is usually, but not always, characterized by the purchase of goods or services, using the "shopping cart" and the acceptance of credit/debit cards in payment. Business to Business, on the other hand, is concerned with using the Internet to place and receive orders from other businesses; establishing legally binding contractual commitments and pooling the resources of companies across the
globe to tender for a project, with each party being authenticated and legally bound by their digital commitments. Transactions initiated using Web servers, usually rely upon Digital Certificates and the use of the SSL (Secure Sockets Layer) authentication and encrypted communication standard. In addition, to provide security for the secure transmission of documents, and other data, the use of the RSA (Rivest Shamir Adelman) standard is common, with PKI (Public Key Infrastructure) being used to create, issue and manage the use of public and private keys (or Digital Certificates). There have been many incidents lately of computer hackers breaking into e-commerce systems and stealing credit card information.

The customer's e-commerce site runs on the e-commerce vendor's Web Server. The Web Server must be put in what is called the DMZ (De-Militarized Zone) (See Stein [71]). This simply implies that the Web Server must be put directly on the Internet and made accessible to anyone on the Internet. All customer information (credit card information, name, address, etc.) is stored directly on the Web Server. The vendor will protect this information in a password, but the information is still out there accessible for the hacker (Gasser [26]). This architecture is shown in the typical e-commerce Architecture Diagram.

Figure 6 shows a customer doing an online transaction to buy books from a website. The customer connects to the Internet and then browses the portal or the homepage of a merchant. The business transaction on Web can be specified as follows:

(a) The customer browses the shopping cart of the merchant. A shopping cart is a piece of software that acts as an online store's catalog and ordering process. It is the interface between a company's Web site and its deeper infrastructure, allowing consumers to select merchandise; review what they have selected; make necessary modifications or additions; and purchase the merchandise. The server also hosts web software that runs some of the main functions of an online storefront such as product display, online ordering, and inventory management.

(b) The shopping cart software might access the books inventory which is a database and can be updated accordingly.

(c) Once the items have been decided, the customer is passed to another server for checkout. During the checkout process, the customer has to identify himself in the database and also provide a
shipping address and payment details for the product. All these details are collected by the authentication server.

(d) The username and password are validated and other details (shipping, billing etc.) are collected or updated in the customer database.

(e) Customer provides his credit card details to a payment gateway. A payment gateway is software that is hosted on a server that routes financial transactions between the merchant and the bankcard processing associations (Credit Card).

(f) The credit card details provided by the customer are verified and validated with the bank.

Figure 6 Typical e-Business Architecture for B2C
4. Firewalls – Defensive Information Security Technology

The concept of a collective description for a variety of methods, which restrict access to a network, is called firewall (Burgess [19]). It is a set of related programs, located at a network gateway server, which protects the resources of a private network from users of other networks (such as Internet). Firewalls may take different physical forms and provide different functions. A firewall typically consists of a PC (Personal Computer) or UNIX machine containing two NICs (Network Interface Card) and running a special program. One network card is connected to the company's private LAN (Local Area Network), and the other is connected to the Internet. The machine acts as a network security barrier through which all information passing between the two networks must travel. The firewall software analyses each packet of information passing between the two and rejects it if it does not conform to a pre-configured rule. A firewall combines hardware and software products to control the flow of data onto a network. The secure and protected network is said to be “inside” the firewall, the insecure unprotected network is said to be “outside” the firewall. A firewall on a network works in a similar way like a firewall in a building. A firewall in a building protects against a dangerous situation in one part of the building spreading to another part. In a computer network, a firewall protects a benign part of a network from dangers that might be present (even spreading

Figure 7 A Basic Firewall Schematic
out of control) in another part of the network. Their main purpose is to implement an organization’s security policy. The integrity of this protective barrier depends on the effective deployment, configuration and capabilities of individual firewall devices. (See, for example, Allen [3], Anonymous [7], Ford and Baum [24].) Figure 7 visually describes the basic scheme of the firewall.

4.1 Types of Firewalls

According to Cameron [21] and Ker [37], there are 4 types of firewalls based on their role in the different layers of TCP/IP (Transport Control Protocol / Internet Protocol), as depicted in Figure 8. Those four includes Network Level, Circuit Level, Application Level and Multi Layer Stateful.

4.1.1 Network Level Firewalls

They are also called as packet filtering firewalls. Traffic is filtered on a base of specific rules, involving source and destination IP address, packet type, port number etc. The administrator can use the router rules to permit a particular machine on the external network to FTP (File Transfer Protocol) to a specific machine on the internal network, but deny that same machine the ability to TELNET to the internal machine. Unknown traffic is allowed only up to the 3rd layer of the TCP/IP stack. See Figure 8. A packet filter looks at the header of packets as they pass through, and it might decide to DROP the packet (i.e., discard the packet as if it had never received it), ACCEPT the packet (i.e., let the packet go through), or something more complicated. Under Linux, packet filtering is built into the kernel. The tool inserts and deletes rules from the kernel's packet filtering table (Ker [37]). Figure 9 visually documents such a firewall at the network level.
Example

A chain is a checklist of rules. Each rule says “if the packet header looks like this, then here is what to do with the packet.” If the rule doesn’t match the packet, then the next rule in the chain is consulted. There are three default chains called “INPUT, OUTPUT and FORWARD.” User defined chains can also be created. When a packet comes in (say, through the Ethernet card) the kernel, it first looks at the destination address of the packet (routing). If it is destined for this box, the packet passes downwards in the diagram, to the INPUT chain. If it passes this, any processes waiting for that packet will receive it. Otherwise, if the kernel does not have forwarding enabled, or it doesn’t know how to forward the packet, the packet is dropped. If forwarding is enabled, and the packet is destined for another network interface (if you have another one), then the packet goes rightwards on our diagram to the FORWARD chain. If it is ACCEPTed, it will be sent out. Finally, a program running on the box can send network packets. These packets pass through the OUTPUT chain immediately: if it says ACCEPT, then the packet continues out to whatever interfaces it is destined for (Beale [10] and Harrison [27]). Such a chain process is listed in Figure 10.
The advantages and limitations of a packet filter can be summarized as follows:

Advantages

(a) fast (b) generally inexpensive as they can be easily incorporated in the routers. (c) very flexible, and (d) transparent.

Limitations

(a) Source, destination addresses and ports can be spoofed and one cannot be sure who is really making the request for access.

(b) Routers do not generally provide robust (if any) logging facilities, making it difficult to know when our network is under attack, or how to recover from a successful attack.

(c) They do not support the concept of strong user authentication, and access from un-trusted networks should not be granted without strong authentication.

(d) Both hardware and software of routers may contain exploitable weaknesses. Routers are generally designed for performance, not security.

4.1.2 Circuit Level Firewalls

A circuit level firewall, depicted in Figure 11, is a means of handling an outgoing connection request from a client on the internal network to a single machine acting as a firewall such that it will appear to the remote site that
the connection request actually came from the firewall. Traffic is filtered based on specified session rules, such as when a session is initiated by a recognized computer. Unknown traffic is only allowed up to level 4 of the TCP/IP stack (Ker [37]).

Example:

SOCKS includes two components, the SOCKS server and the SOCKS client. The SOCKS server is implemented at the application layer, while the SOCKS client is implemented between the application and transport layers. The basic purpose of the protocol is to enable hosts on one side of a SOCKS server to gain access to hosts on the other side of a SOCKS Server, without requiring direct IP-reachability (SOCKS [69]).

When an application client needs to connect to an application server, the client connects to a SOCKS proxy server. The proxy server connects to the application server on behalf of the client, and relays data between the client and the application server. For the application server, the proxy server is the client. The benefit of SOCKS is that it is a single communication protocol that authenticates users and establishes the communication channel. For each TCP or UDP (User Datagram Protocol) communication channel that the SOCKS protocol establishes, it transfers user information from the SOCKS client to the SOCKS server for user authentication, authenticates the user and the channel and guarantees the integrity of TCP and UDP channels. Finally, the advantages and limitations of this level of firewalls can be summarized as follows:

Figure 11 Circuit Level Firewalls
Advantages

(a) Prevents direct connection between internal and external machines.

(b) All incoming requests are blocked.

(c) If a user on an internal machine writes code that listens on some non-standard port, users on external hosts have no way to reach that port. This gives the Security Administrator a single point at which to control incoming connection requests.

(d) Stronger traffic authentication possible than packet filters.

(e) User level authorization also possible.

(f) Concealment of internal network structure due to proxy like functionality.

(g) Can provide useful statistical logs.

(h) Well suited for UDP applications. Decisions made on source and destination IP address and ports.

Limitations

(a) Configuration is more complex.

(b) Client software on the internal network will need to be modified to do the necessary “handshake” with the Socks software, and source code for the client software may be unavailable.

(c) Circuit level gateways do not interpret the application protocol themselves, and therefore does not control or monitor traffic at the application level. Circuit level gateways operate at the network layer, where only address and port number information is even available. Thus, the granularity of control is no better than that of a router. That is why most organizations permit only outgoing requests through a circuit level gateway.

4.1.3 Application Level Firewalls

Application Level Firewalls, also known as proxy servers or application gateways, are applications that intercept traffic flowing between a protected network and the Internet. They are the most secure firewalls. Like the circuit level firewall, an application level firewall is configured to be the only host address visible to the outside network, requiring all connections to the internal network to go through the firewall. An application level firewall is dis-
t nguished by the use of proxies (application gateways) for services such as FTP, TELNET, etc., which prevent direct access to services on the internal network. They are sophisticated devices and can also be used to implement protocol specific security such as passing and blocking incoming/outgoing FTP or blocking certain types of content such as file attachments or embedded Java applications. Application level firewalls provide a high level of intelligence. However, there is a trade-off for this high functionality, in that application or gateway firewalls operate slower than stateful inspection firewalls. They also present greater complexity when adding new applications.

For each desired application, special-purpose code is used to control traffic. It makes it easy to log and control all incoming and outgoing traffic. These features allow traffic analysis and content analysis (security issues). Figure 12 depicts such firewalls at the application level.

Example

The TIS (Trusted Information Systems) Firewall Toolkit provides proxies for telnet, rlogin, ftp, X etc. These provide configurable access control, authentication and logging mechanisms. The proxy, which runs on the firewall, passes requests through the firewall (at the application level), using rules that are supplied. One can configure the proxies to allow connections based on source IP address, source host name, destination IP address, and

Figure 12 Application Level Firewalls
destination host name. All packets and all application requests go to the firewall. On the firewall, the proxy software relays information from one side of the firewall to the other at the application level. The proxy prevents the applications on outside networks from talking directly with the applications on the inside network, and vice versa. No IP packets pass from one side of the firewall to the other. All data sets are passed at the application level. It also provides support for the authentication of users before they are allowed access to the Internet. Also, good auditing facility is provided.

Finally, the advantages and limitations of this level of firewalls can be summarized as follows:

**Advantages**

(a) Secures Addresses From Exposure

With application-level proxies, there is no direct connection between an application client and an application server. Proxy servers hide the address structure of the network and make it difficult for hackers to access confidential information.

(b) Supports Application-level Security

Application-level proxies communicate with client applications using application-level protocols. That indicates that the gateway has a complete understanding of the protocol and can therefore tightly control what data passes through.

(c) Allows Application-level Logging

Since client traffic passes through an application gateway, it's possible for network managers to log network traffic coming to and from an application proxy server.

(d) Can provide content filtering

**Limitations**

(a) Not Transparent

A user will be aware of the firewall. Typically, the user will first authenticate to the firewall which will only then open a second connection and relay the traffic.

(b) Requires Reauthentication By Each Application
Although application-level proxies provide a mechanism for user authentication, this authentication takes place on an application-level only. That implies each time a user starts a new application, they have to reauthenticate with a new application-level gateway.

(c) Offers Little Flexibility

As new Internet services become available, new software must be written for each application and service.

(d) 2 TCP connections in place of 1

The client server model is no longer true.

4.1.4 Stateful Multi Layer Inspection Firewalls

They are enhanced packet filters that use a process called stateful inspection or the “Stateful Multi-Layer Technique.” Rather than permitting or denying traffic based on just the packet header, these firewalls use data parsing software to look at the content of the packet, including its protocol, as depicted in Figure 13. If this packet fits the general mold for packets of its type, and passes all predefined rules, it is admitted. If the packet is aberrant, it is rejected. It maintains state, monitoring the progress of various connections.

4.2 Firewall Architectures

There are basically three architectures of a firewall (Rash [58]). The simplest approach is the Basic Border Firewall, as shown in Figure 14. The firewall includes a screening router and it performs certain packet filtering functions. The firewall host can be configured as a "Bastion Host," that is, a host that is minimally configured (containing only necessary software/services) and carefully managed to be as secure as possible.

The Basic with DMZ Network is a more secure architecture for both protecting hosts that offer public services such as WWW and protecting the internal network from external users accessing public services. The firewall examines all incoming traffic to determine if it should be passed to the DMZ network (where one or more hosts providing public services reside) or to the protected network. It examines all outgoing traffic to determine if it should be passed from the protected network to the DMZ network (requesting public services), to the protected network from the DMZ network (responding to public service requests), or to the external world. This firewall architecture may also be referred to as a Dual-Homed Gateway (due to having two...
network connections, one to the DMZ Network and one to the protected network) (See, for example, Zwicky et al. [77]).

One of the most secure firewall architectures is the Dual Firewalls with DMZ Network, sometimes referred to as a Sub-Network Firewall. See Figure 15. In this architecture, the protected network is further isolated from the hosts offering public services and the external world by adding a second firewall host. By protecting the public services network with one firewall host and the protected network with a second firewall host (creating an additional DMZ between the two firewalls), traffic between the protected network and the Internet must traverse two firewalls.

![Figure 13 Stateful MultiLayer Inspection Firewall](image)

![Figure 14 Basic with DMZ network](image)

842
In a single-layer architecture (Basic Border Firewall, Basic with DMZ Network), one network host is allocated with all firewall functions and is connected to each network for which it is to control access. This approach is usually chosen when cost is a primary factor or when there are only two networks to interconnect. It has the advantage that everything there is to know about the firewall resides on the firewall host. In cases where the policy to be implemented is simple and there are few networks being interconnected, this approach can also be very cost-effective to operate and maintain over time. The greatest disadvantage of the single layer approach is its susceptibility to implementation flaws or configuration errors; depending on the type, a single flaw or error might allow firewall penetration.

In a multiple-layer architecture (Dual Firewalls with DMZ Network), the firewall functions are distributed among a small number of hosts, typically connected in series, with DMZ networks between them. This approach is more difficult to design and operate, but can provide substantially greater security by diversifying the defenses being implemented. Although more costly, it is advisable to use different technology in each of these firewall hosts. This reduces the risk that the same implementation flaws or configuration errors will exist in every layer.

Wilner [76] described six key pitfalls in the deployment of popular commercial firewalls. Firewalls cannot protect against poor network administration. If users employ their own PCs to download information from the Internet, and later copy that information to a diskette, those diskettes may be brought to work and then may compromise the internal network. Similarly, if users deploy unauthorized dial-out software packages on their desktop PCs.
at work and download information into the corporate network, they may again introduce vulnerabilities or import hostile code. Also, firewalls implement authentication and encryption sloppily (Frantzen [25] and Kamara et al. [35]).

5. Conclusion and Future Extensions

Computer networks are increasingly being developed for information sharing and collaborative works in geographically dispersed organizations. Using the computer networks, many corporations attempt to develop new business transaction, so-called “e-Commerce or e-Business” that an electronic transaction, performed over the Internet—usually via WWW. It is true that such a new business trend enhances business activities not only between firms and consumers but also business and other business. Such is a positive business perspective due to the technological development of Internet business. Admitting the importance of e-Business/Commerce, we must acknowledge that there have been many incidents lately of computer hacker’s breaking into e-commerce systems and stealing credit card information and other important information related to business operations.

Information Security (IS) is a major concern in the present-day world. Today, the information available on Internet has increased, but the technology for security for this information has not increased as required by many corporations. The requirements of IS within an organization have undergone major changes in the last several decades. Before a widespread use of data processing equipment, the security of valuable information was provided primarily by physical and administrative means. With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident.

It is easily imagined that the introduction of IS is considered only when corporate secret agents, hackers and terrorists attack our computer systems and defense mechanism(s) is (are) employed to protect computer security. Unfortunately, many corporate managers are not familiar with current IT technologies related to IS. Conversely, IT engineers are not familiar with how to introduce IS into their organizations.

In this study, a comprehensive survey on different IS technologies is documented and such a classification is further separated from a perspective of IS enhancement and managerial applications. Based upon the classification on previous research efforts on IS, we examine Firewalls (a group of software) as our defensive IS tool. After reviewing the firewalls, this study
has discussed how to incorporate such a new IS technology into corporate entities which are now facing serious business competitions. Thus, it is expected that this research makes a theoretical linkage between the new IS technology and e-business strategy. Such a theoretical investigation has been never explored in previous studies on both computer science and management.

As a future extension of this study, we need to investigate how to make a linkage between IT strategy and corporate strategy. Such a combined use is essential for modern e-management. In this case, we need to develop not only a theoretical framework, but also an empirical study related to the conceptual development. Those are important future research tasks of this study.

Finally, it is hoped that this study makes a small contribution on IS. We look forward to seeing future developments of IS, as discussed in this article.

References


