Framework for E-Business Information Security Management

Eben Otuteye

Associate Professor, Finance and E-Business
Faculty of Administration
University of New Brunswick
Fredericton
NB E3B 5A3
Canada

Email: otuteye@unb.ca
Phone: (506) 458-7354
Fax: (506) 453-3561

Framework for E-Business Information Security Management

Abstract

In today's economy, information is one of the most important assets of an organization, probably second only to human resources. Information has become important both as input and output. Hence information security is of great concern to companies that want to implement e-business. The Internet, which is the primary medium for conducting e-business is by design an open non-secure medium. Since the original purpose of the Internet was not for commercial purposes, it is not designed to handle secure transactions. Surveys show that lack of transaction security is one of the key reasons why consumers are hesitant about shopping online. This paper first presents an outline and analysis of the security needs of online businesses. This is followed by an evaluation of the current tools and practices for ensuring e-business security. The shortcomings of the present practices are noted. A framework for e-business information security is presented. The key characteristic of this framework is that it is an insurance-based risk management process that encompasses the entire information infrastructure of an organization.

Key words and phrases: E-Business security, network security, system security, transaction security, risk assessment, risk management, best practices, insurance.

1. Introduction

In 1991 the NSF lifted the restriction of commercial use of the Internet and that marked the beginning of the age of electronic commerce. The incipient growth was turbo charged with the development of the World Wide Web and GUI-based browsers shortly after.[1] Since then e-commerce has been growing at a phenomenal rate. Despite this extraordinary growth, surveys show that consumers are reluctant to make their purchases online because of security concerns. For the same reason a number of businesses are hesitant to move their operations online. These security concerns stem from a number of factors. The principal cause of security concern has to do with the key innate characteristic of the Internet as an open system.

The original purpose of the Internet was to move files among computers and to enable easy remote access to computers. More than anything else, simplicity and ease of use were among the main motivation for designing the Internet. This has "led to a simple and scalable network design that offers a *best-effort* service, in which the network does not guarantee anything, not even delivery of the data."[2] Security, both for the Internet and the Web is essentially an afterthought. In addition to the Internet being an open system, the rapid proliferation of new software and communication systems has led to a state in which software users are not fully knowledgeable about software and systems architectures. This makes users oblivious to a number of vulnerabilities that can lead to inadvertent security breaches or those that can be maliciously exploited.

In contrast to the simple open design of the Internet, the present economy has evolved into what is primarily a knowledge-based economy in which information security is of paramount importance. In today's economy, information is the second most important asset apart from human resources. In the knowledge-based economy information is key both as input and output. At first glance, it appears we have a situation that presents tremendous opportunity for global commerce: a global communication infrastructure that is very conducive for low cost transmission of information and a global economy that is tending to be highly information-based. However, the potential global electronic commerce scenario cannot be realized without a reliable supporting information security framework. Protecting online assets and network resources is extremely important; it ought to be a mission critical concern of any e-business.

This paper is in two parts. The first part presents an outline of the significance and impact of information security for e-business with emphasis on the security threats and potential losses that could arise from those vulnerabilities. E-business security is analyzed as consisting of six dimensions: confidentiality and privacy, integrity, availability, legitimate use, auditing and non-repudiation. The consequence of each type of security breach is discussed and various technological solutions are presented. It is noted in this section that the present approach is inadequate primarily because the solutions tend to be threat-specific, technology centered and rather *ad hoc*. Furthermore, it is argued, those solutions are subject to a basic flaw, namely, that they are geared primarily toward

[1] See PBS (n.d.) "Life on the Internet", http://www.pbs.org/internet/timeline/ .
[2] Mathy, Edwards, and Hutchison (2000), http://www.comsoc.org/pubs/surveys/.

creating assurance rather than managing risk. The rationale for the framework is rooted in two publications based on studies conducted by the US General Accounting Office in an attempt to identify commendable security practices that could be emulated by federal agencies[3]. While the GAO approach implicitly recommends the practices of the leading organizations, this paper advocates best practices that could be conceivably significantly different from what is done by those leading organizations. Thus what is presented here is a more general approach.

Building trust is critical to e-business success.[4] However, the main thesis of this paper is that the current system of professing trust by alluding to the level of sophistication in software and hardware systems is inadequate. Instead we advocate a risk management system coupled with a new type of certification authority. True e-business trust requires a double coincidence of confidence for both the organization and the customer: the organization has to be confident about its ability to handle risks associated with various threats and vulnerabilities, and customers need to be confident that the organization or system they are interacting with is trustworthy with regard to their security concerns. A patchy trust building system, in our view, does not have long-term viability. This paper addresses the process for organizations to gain confidence in their security mechanism. Organizational confidence must precede customer confidence. In fact, in this framework, customer confidence is based on certified organizational confidence.

We posit that effective e-business security decisions have to be part of an overall corporate information security and risk management policy. A comprehensive systematic security policy needs to be established and technologies can then be applied in the context of the overall policy. It is shown that the problem of e-business security risk lends itself quite naturally to well-established risk assessment, risk analysis, and risk management methodologies and strategies. The paper concludes that the risk management approach makes the problem amenable to market pricing of the risk and enables risk transfer, hedging and/or insurance to be applied in managing information security. The problem of e-business security is then presented as a six-step sequential decision making process. It is hoped that the result of such a process will create the requisite double confidence in both organizations and customers.

2.0 Significance of corporate information security

The present reality is that we live in a global interconnected world. Every facet of society, including businesses, is organized within this paradigm. It does not mean every aspect of life is online but rather that even if one is not a direct participant in this cyberlife it is impossible to escape the impact of cyber activity on one's life. This paper is about e-business security and thus the focus will be from a business perspective. From the point of view of businesses, information has become a very highly priced asset. The main issue with e-business security is that the very nature of information together with the principal media for its creation, storage and transmission – computers,

[3] See US GAO (1999a,b).
[4] Tan and Thoen (2000), http://www.electronicmarkets.org/netacademy/publications.nsf/all_pk/1812.

communication networks, and especially the Internet – make it extremely difficult to control. In today's Internet world, it is easier to create, alter and transmit information.

The advancement in computing capacity and interconnectivity leads to a situation where small efforts can create potentially large losses. Accidental and intentional breaches are easier and more likely. It is getting more and more difficult to secure information. In short, total information security is just impossible. This situation is both an opportunity and a challenge. It is an opportunity because there is value that can be created and claimed by providing viable solutions to this pervasive problem. It is a challenge because without a realistic and feasible solution that will provide businesses the necessary assurance to proceed to transform into online businesses, significant economic value will go unrealized.

In practice, how big is the concern for information security? According to *InformationWeek* Research's Global Information Security Survey conducted in June, 2000, nearly three-quarters of information security professionals regard security as a top priority, up from 56% two years ago. Those in banking, health care, finance, and telecommunications rate information security as the highest business priority, with retailers a little less concerned. In every sector, security is increasingly being viewed as a key business driver.[5] It is estimated that the explosion of computer viruses and denial of service attacks will cost businesses around the globe more than $1.5 trillion this year (2001). The results from Information Week Research's *2000 Global Information Security Survey*, fielded by PricewaterhouseCoopers LLP, also shows that in the U.S. alone, damages in the form of lost revenue spurred by viruses and computer hacking will amount to $266 billion, or more than 2.5% of the nation's Gross Domestic Product (GDP).

2.1 Objectives of e-business security

There is almost an uncountable number of ways that an e-business setup could be attacked by hackers, crackers and disgruntled insiders. The intent is not to produce an exhaustive list here but some of the common threats are: hacking, cracking, masquerading, eavesdropping, spoofing, sniffing, Trojan horses, viruses, bombs, wiretaps, etc. While the list of actual manifestation is long, conceptually, they break down to a few categories. These are spoofing, unauthorized disclosure, unauthorized action, and data alteration. From a business perspective Denial of Service (DoS) attacks appear to be the most serious threat. DoS attacks consist of malicious acts that prevent access to resources that would otherwise be available. Even though data may not be lost, the financial losses that could be incurred from not being able to supply a service to customers could be of much higher value. A well-planned security strategy will address all these areas. A well-planned strategy, in turn, depends on the security goals.

[5] See http://www.informationweek.com/800/prsecurity.htm; http://www.informationweek.com/800/prsecurity.htm. The *2000 Global Information Security Survey* was completed by 4,900 security professionals spanning 42 countries and six languages.

What are the goals of information security and what is the nature of the e-business security problem? E-business security concerns fall into four main categories: loss of data integrity; loss of data privacy; loss of service; and loss of control. Responding to these concerns requires an integrated and effective information security policy. In conducting e-business, every organization ought to be able to:

- positively identify or confirm the identity of the party they are dealing with on the other end of the transaction;
- determine that the activities being engaged in by an individual or machine is commensurate with the level of authorization assigned to the individual or machine;
- confirm the action taken by the individual or machine and be able to prove to a third party that the entity (person or machine) did in fact perform the action;
- to protect information from being altered either in storage or in transit;
- be certain that only authorized entities have access to information;
- ensure that every component of the e-business infrastructure is available when needed;
- be capable of generating an audit trail for verification of transactions.

Effective information security policy must have the following six objectives[6]: privacy and confidentiality; integrity; availability; legitimate use (identification, authentication, and authorization); auditing or traceability; and non-repudiation. If these objectives could be achieved, it would alleviate most of the information security concerns. Each information security objective is discussed below with emphasis on the specific challenges it poses to Internet mediated businesses.

2.1.1 Privacy and Confidentiality

One of the goals of e-business security is privacy and confidentiality. Privacy or confidentiality involves making information accessible to only authorized parties, or restricting information access to unauthorized parties. Privacy concerns did not originate with the Internet. However, conducting business over the Internet has exacerbated the situation. As an example, one context in which this issue has been addressed extensively is the area of confidentiality of electronic health data. There have always been concerns about confidentiality in health care. Online intermediation has complicated the problem and heightened the misgivings that already exist. For example, recent surveys reported by the Georgetown University Institute for Health Care Research and Policy contain some rather revealing statistics about people's concern for privacy:

> "Sixty-three percent of Internet 'health-seekers' and sixty percent of all Internet users oppose the idea of keeping medical records online, even at a secure, password-protected site, because they fear other people will see those records. … An overwhelming majority of Internet users are worried about others finding out about their online activities: eighty-

[6] See a similar but slightly different view by Greg Shanton, http://www.amsinc.com/Amscat/Security%20Story/SecurityStory.htm.

> nine percent of Internet users are worried that Internet companies might sell or give away information and eighty-five percent fear that insurance companies might change their coverage after finding out what online information they accessed."[7]

Obviously, these are rather significant numbers that anyone with interest in providing any type of online services (not just health) will be concerned about. To maintain the confidentiality and privacy of Web users, organizations have to find ways to keep information secret from unauthorized view. From an operational point of view, that means information that is stored has to be secured in a way that it can only by accessed by authorized parties. Similarly, information in transit has to be kept from the view of unauthorized parties. Furthermore, once information is transmitted from one entity (either individual or machine) to another, there has to be a way of ensuring that it arrives intact at the appropriate destination and that it is retrieved only by a legitimate entity.

Web technology makes it easy for a user's information to be tracked, collected and disseminated. As Web functionality increases, greater convenience is creating greater privacy losses. Users leave trails of information that can be used to determine which sites they visit, what they read or purchase, whom the correspond with, etc. Data on browsers' habits can be easily collected and sold to advertising companies. Databases can be linked to enrich information content. Information that is relatively benign when collected separately may reveal more than a user will like to reveal when the information is spliced from different sources.

2.1.2 Integrity

The need for accuracy of information in an information-driven society cannot be over stated. Typically, information is either stored at a given location or being passed from one point to another. Either way, the primary concern for information integrity is that it remain intact so that nothing is added nor taken from it that is not intended or authorized. The extreme cases of lack of information integrity are when a whole database is lost or replaced with something else. Between these extreme cases are situations where data is corrupted either minimally or significantly such that major repairs have to be done to make it useable again. Data reliability can be compromised by a deliberate or unintentional modification.

Transmitting information over the Internet (or any other network) is similar to sending a package by mail. The package may travel across numerous trusted and untrusted networks before reaching its final destination. It is possible for the data to be intercepted and modified while in transit. This modification could be the work of a hacker, network administrator, disgruntled employee, government agents or corporate business intelligence gatherer.

2.1.3 Availability

[7] http://www.healthprivacy.org/usr_doc/41774.pdf

System availability is one of the fundamental requirements of e-business security. Availability means that systems, data, and other resources are usable when needed despite subsystem outages and environmental disruptions.[8] Lack of availability is essentially loss of use. The most commonly known cause of availability problems is Denial of Service (DoS) attacks even though there are other common causes such as outages, network issues, or host problems. The goal is to ensure that system components provide continuous service by preventing failures that could result from accidents or attacks. From a security point of view, availability is enhanced through measures to prevent malicious denials of service.

Closely related to availability are reliability and responsiveness. Reliability implies that a system performs functionally as expected. Responsiveness is a measure of how quickly service could be restored after a system failure. In other words, it is a measure of system survivability. This does not necessarily mean that the failed system is revived, just that service is restored or not lost at all despite the failure. One advantage for e-businesses is that the Internet, being a distributed system, affords a greater opportunity for building redundancy into systems so as to mitigate denial of service problems. In fact, system survivability is at the heart of the design of the Internet and appropriate use of it should result in minimal availability problems. Nevertheless, there are still real threats to availability because DoS attacks are not limited to the Internet component.

2.1.4 *Legitimate use*

One of the key issues in e-business security (and also generally with any computer security) is legitimate use. Legitimate use has three components: identification, authentication and authorization.

Identification involves a process of a user positively identifying itself (human or machine) to the host (server) that it wishes to conduct a transaction with. The most common method for establishing identity is by means of username and password. The response to identification is authentication. Without authentication, it is possible for the system to be accessed by an impersonator. Authentication needs to work both ways: for users to authenticate the server they are contacting, and for servers to identify their clients. Authentication usually requires the entity that presents its identity to confirm it either with something the client knows (e.g. password or PIN), something the client has (e.g. a smart card, identity card) or something the client is (biometrics: finger print or retinal scan). Biometric authentication has been proven to be the most precise way of authenticating a user's identity. However, biometric processes such as scanning retina or matching fingerprints to one stored in a database are often considered intrusive, and there always exists some measure of fear that this information will be misused.[9]

---

[8] Neumann (1995), p. 97.
[9] Sieglein, (2000), http://www.planetit.com/techcenters/docs/security-defensive_tools/expert/PIT20001220S0006 .

Another approach to authentication is by the use of digital certificates. A digital certificate contains unique information about the user including encryption key values. These public/private encryption key pairs can be used to create hash codes and digitally sign data. The authenticity of the digital certificate is attested to by a trusted third party known as a "Certificate Authority." This whole process constitutes Public Key Infrastructure.

Once an entity is certified as correctly identified, the next step in establishing legitimate use is to ensure that the entity's activities within the system are limited to what it has the right to do. This may include access to files, manipulation of data, changing system settings, etc. A secured system will establish very well defined authorization policy together with a means of detecting unauthorized activity.

2.1.5 Auditing or Traceability

From an accounting perspective, auditing is the process of officially examining accounts. Similarly, in an e-business security context, auditing is the process of examining transactions. Trust is enhanced if users can be assured that transactions can be traced from origin to completion. If there is a discrepancy or dispute, it will be possible to work back through each step in the process to determine where the problem occurred and, probably, who is responsible. Order confirmation, receipts, sales slips, etc. are examples of documents that enable traceability. In a well-secured system, it should be possible to trace and recreate transactions including every subcomponent after they are done. An effective auditing system should be able to produce records of users, activities, applications used, system settings that have been varied, etc., together with time stamps so that complete transactions can be reconstructed. The ability of an e-business infrastructure to produce audit trails, however, is not sufficient for assigning responsibility. An effective non-repudiation system needs to go with traceability in order to determine exact points of responsibility.

2.1.6 Non-repudiation

Non-repudiation is the ability of an originator or recipient of a transaction to prove to a third party that their counterpart did in fact take the action in question. Thus the sender of a message should be able to prove to a third party that the intended recipient got the message and the recipient should be able to prove to a third party that the originator did actually send the message. This requirement proves useful to verify claims by the parties concerned and to apportion responsibility is cases of liability. In the absence of proper security, an originator of a message cannot ascertain that the recipient (and the right one for that matter) did receive the message and neither can the recipient hold the originator responsible for sending the message. Obviously, this is a crucial requirement in any business transaction when orders are placed and both buyers and sellers need to be confident that not only are they dealing with the appropriate parties but also that they have proof to support the claims of any action taken in the process. Non-repudiation

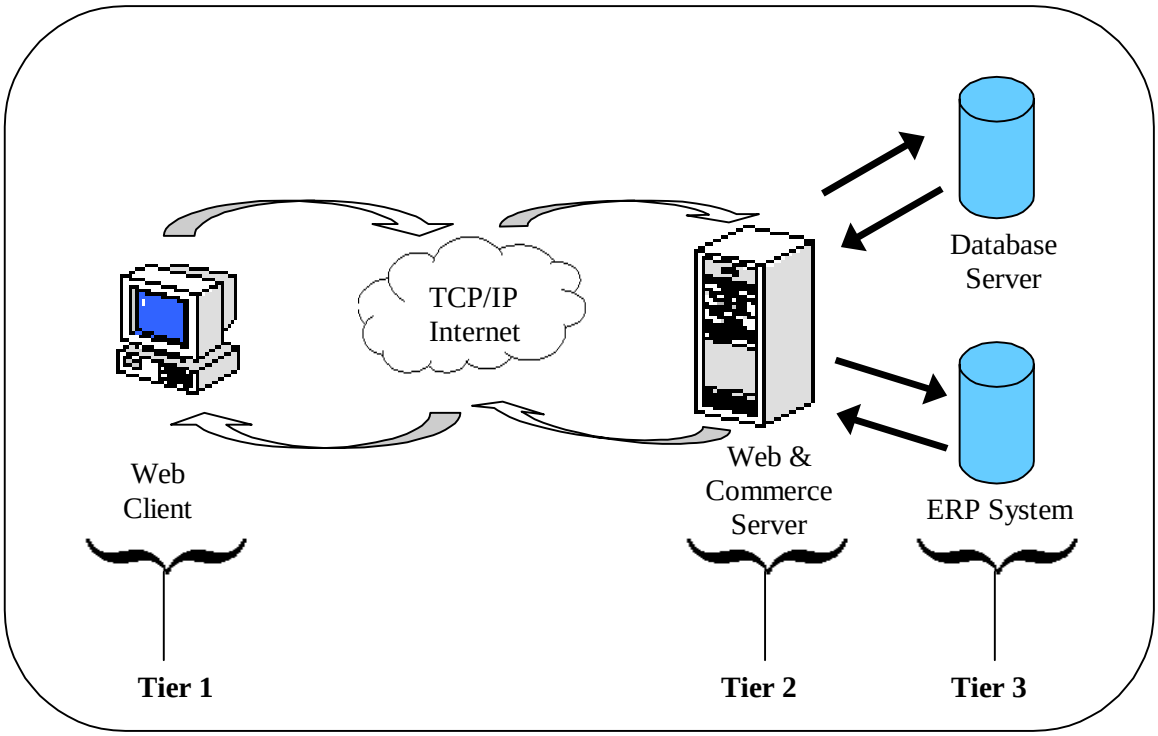
protocol is also useful in forensic computing where the goal is to collect, analyze and present data to a court of law.[10]

3.0 Current Processes and Tools for Implementing E-Business Security

Even though the previous section identified six separate e-business security objectives, it is worth noting that these objectives are very much interrelated and no part is fully useful nor even fully achievable on its own. One of the problems of the current e-business security implementation is that components of e-business infrastructure tend to be looked at individually and separately for security purposes. Hence security solutions are generally *ad hoc* and have a tendency to be component driven. Essentially, the current common "security policy" implemented by most e-businesses runs like this: assemble a catalogue of threats and vulnerabilities and then shop for technology tools that alleviate those concerns. Security solutions are targeted at counteracting specific groups of threats and vulnerabilities, such as vulnerabilities in applications, services, databases, network devices and operating systems. However, what is needed are comprehensive solutions that will produce peace of mind to the business and trust and confidence in customers and partners. While the current practice is essentially *ad hoc*, it is generally applied in a somewhat systematic fashion by ensuring security of various components from the desktop to local network to Internet channels and through authentication to other servers. A typical three-tier e-business architecture is shown in figure 1 below.

Figure 1: 3-tier architecture

[10] "What is Forensic Computing?", http://www.computer-forensics.com/forensics/welcome.html.



Each component – client, web and commerce servers, database server, and ERP systems - is subject to potential attacks. The first line of defense is to protect network assets. We will use the IBM model as a point of reference for purposes of this discussion.[11] The IBM framework is based on three key security elements:

- Network security
- System level security, and
- Transaction level security.

The idea is that this process will help ensure that an organization's resources as well as customer's and business partners' privacy are protected when conducting e-business transactions.

3.1 Network Level Security

Network level security provides protection against attackers who attempt to deny service to legitimate users by gaining control of machines or resources within a private network. The most common way to protect private networks that are connected to the Internet from these kinds of attacks is with firewall technology. A firewall is a set of related programs,

[11] IBM (1998), http://www-1.ibm.com/servers/eserver/zseries/ebusiness/security.html [April 19, 01].

located at a network gateway server that protects the resources of a private network from users from other networks. It is a combination of hardware and software used to implement a security policy governing the network traffic between two or more networks. The network firewall is the primary line of defense against external threats to an organization's computer systems, networks, and critical information. Firewalls can also be used to partition an organization's internal networks, reducing the risk of insider attacks.[12] The most common of these technologies include:

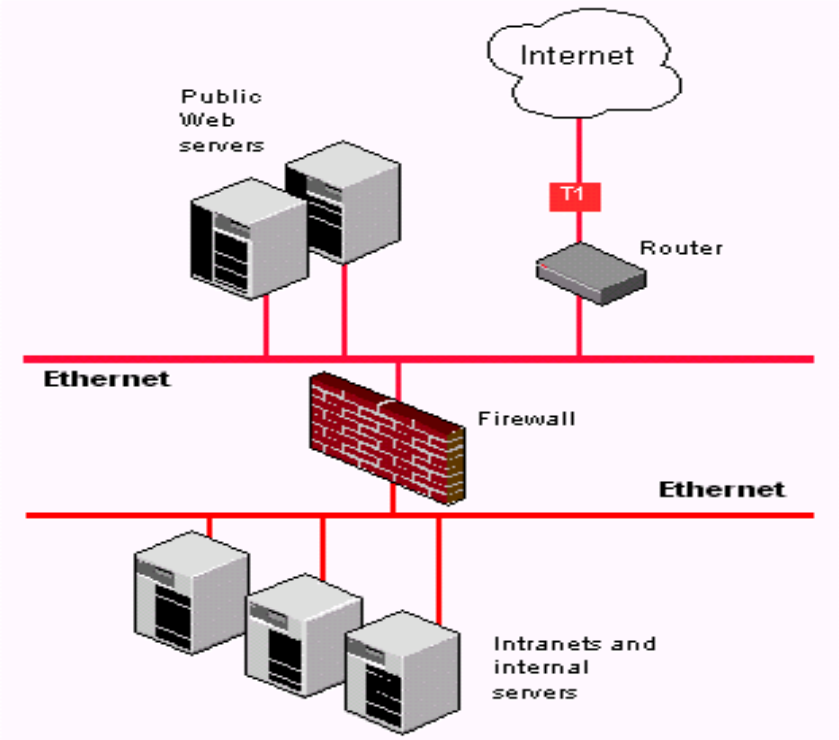
- Packet filters to limit traffic
- Application gateways
- Proxy servers to mediate TCP/IP connections
- Domain name services to hide network information
- Encrypted IP tunnels (or virtual private networks (VPN)) that allow private communications to occur over public networks

Even though firewalls are deployed to keep unwanted requests for service out of the networks they are supposed to protect, it is prudent to still be concerned about the security of the server. In case an attacker successfully penetrates the firewall, it will be useful to minimize the risk that any damage can be done to the servers. It is also important to keep potential insider attackers in check. Attackers from inside the firewall should not be able to breach defenses and create unwanted connections to the outside world. For this, system level security is required.

Figure 2: Firewall setup

[12] Carnegie Mellon University (CERT) (1999), "Deploying Firewalls", http://www.cert.org/security-improvement/modules/m08.html.

From Computer Desktop Encyclopedia
© 1999 The Computer Language Co. Inc.



Source: http://www.techweb.com/encyclopedia/defineterm.cgi?sstring=firewall

3.2 System Level Security

System level security is the ability to utilize operating system functions and applications in combination with hardware architecture to help protect against corruption of service and control user access to system resources (files, programs, databases and so on).[13] "The biggest cause of security problems is bad management. In distributed systems, the first place management affects security is in the system's configuration. A bad system configuration can mean disaster. If configuration is not controlled, it is difficult to express management policy in the system's operational characteristics. As system complexity increases, the problem becomes acute."[14]

3.3 Transaction Level Security

The actual act of completing transactions on the internet depends on transaction level security. Transaction level security refers to the ability of two entities on the Internet to conduct a transaction privately and with authentication. In assessing e-business security,

[13] IBM (1998).
[14] Rubin and Daniel E Geer Jr. (1998), p.34

all the components of a transaction have to be considered: the client, transport, server, operating system, applications and database components. Both service and user authentication are crucial. To have a complete picture of the security of a transaction, one must consider the hardware of the user, the operating system of the user, the client software of the user, the hardware of the host, the operating system of the host, the server software of the host, the base transport protocol, the higher level (generally HTTP: the HyperText Transport Protocol) protocol, the general structure of the network itself, and the various forms of content.[15] This level of security provides a basis to enable the payment for goods and services to occur in privacy. Currently, the leading technologies for implementing transaction security are Secure Socket Layer (SSL) and Secure Electronic Transaction (SET).

4.0 Security Policy

All security solutions need to begin with a policy. Sensitive information cannot be fully protected unless the identity of what is to be protected is established and the means of protection determined. One way is to visualize the architecture as depicted in figure 1 and to map out a protection structure plan for each component. Basically, that is how e-business security is practised today. In order to achieve this goal of providing end-to-end security, an organization must address all hosts, systems, applications, and networking devices. The concern for infrastructure protection needs to be balanced with user convenience. When creating a security policy, there is a requirement to balance easy accessibility of information with adequate mechanisms to identify authorized users and ensure data integrity and confidentiality. Some basic security policy questions that must be answered are:

- What components are most critical but vulnerable?
- What information is confidential and needs to be protected?
- How will confidentiality be ensured?
- Will the confidential information be encrypted?
- Who is authorized to access or modify information?
- What authentication system should be used?
- What intrusion detection systems should be installed?
- Who has authority and responsibility for installing and configuring critical e-business infrastructure?
- What incident handling measures should be in place?
- What plans need to be in place to ensure continuity or minimum disruption of service?

It is expected that the outcome of answering the above questions will be a security policy with, at least, the following characteristics:

- The policy is clear and concise

- The policy has built in incentives to motivate compliance
- Compliance is verifiable and enforceable
- Systems have good control for legitimate use: access, authentication, and authorization
- There is regular backup of all critical data
- There is a disaster recovery and business continuity plan

4.1 Current Practice

To a large extent, current e-business security practice is rightly based on answering the types of questions listed above. The problem, however, is that this kind of approach is *ad hoc* in the sense that it usually entails providing only technical (software and hardware) answers. This usually translates into acquiring sophisticated servers, firewall software, intrusion detection systems, obtaining digital certificates, etc, what we refer to as the "latest gizmo" driven approach. While there is nothing wrong with installing these devices, the implicit false assumption is that security risk problems can be minimized by that approach. Small and medium sized businesses are the ones especially at risk. We contend that regardless of how sophisticated the software and hardware devices might be, risk is not fully addressed without a systematic risk assessment and risk management process. The weakness of this *ad hoc* approach stems from the fact that many traditional security paradigms are ineffective against Web threats.

4.2 Proposed Framework

The main thesis of this paper is that e-business security can only be effective if it is regarded as part of an overall corporate information security risk management policy. For that purpose a six-stage security management strategy is proposed:[16]

Stage 1: Develop a corporate risk consciousness and risk management culture. Develop management focus.

Stage 2: Perform a thorough risk assessment of the whole business. Identify and rank risks based on threats, vulnerabilities, cost and countermeasures.

Stage 3: Devise a systematic risk-management based e-business security policy.

Stage 4: Put risk control mechanisms in place. Implement technological best practices with regard to e-business infrastructure components: clients, servers, networks, systems and applications, and transport mechanism.

[16] While this is based on GAO (1999a,b), the practices of the organizations surveyed by the GAO lack the key component advocated here, namely, the implementation of best practices.

Stage 5: Follow systematic risk assessment and risk management procedures to determine the level of risk after implementing the best practices on each component. Insure residual risk of low probability but high cost events and manage the rest.

Stage 6: Monitor and audit diffusion of risk management culture, policy implementation and enforcement, and revise as needed.

4.2.1 Developing corporate risk consciousness and management focus

In order for any security policy to work, there has to be a strong organizational foundation. This organizational foundation is made up of a risk conscious culture and strong management focus. The goal is to create a systemic organization-wide risk consciousness and responsibility. There needs to be a managerial champion in the capacity of Vice-President for Information Security, for example. Both top-down and bottom-up strategies need to deployed so as to generate a collective sense of mission. Both management and employees must have a keen sense of how their fortunes and the fortune of the organization depend very strongly on their ability to safeguard their information resources and to protect customers' and partners' privacy.

4.2.2 Performing Risk Assessment

Risk Assessment is based on identifying threats, vulnerabilities and cost. A simple equation can be used to represent this process:

Risk = (Threat x Vulnerability x Cost of business disruption)/ (Cost of Countermeasure)

Threat is simply the probability of an attack (or possibly, inadvertent misuse). Vulnerability is 1 minus system effectiveness (which is a number less than 1). That means 100% system effectiveness will produce zero risk. Cost of disruption is a measure of what it costs to restore the system back to full function plus any loss of revenue that may occur during the disruption period. One way to mitigate this cost is to build in redundancies. For the sake of simplicity, this model assumes that the effectiveness of a countermeasure is directly proportional to the cost of the measure.

4.2.3 Devising a systematic risk-management based e-business security policy

The focal point for any viable e-business security strategy is a sound well-articulated security policy. Even with a strong management focus and a security conscious organizational culture, the security policy is the first tangible evidence of a credible and operational security system. Every organization that is serious about security must have a comprehensive and coherent security policy. The policy must address each system component, internal and external threats, human and machine factors, managerial and non-managerial responsibility. The security policy has to have as its foundation, the six

objectives of e-business security: privacy and confidentiality; integrity; availability; legitimate use (identification, authentication, and authorization); auditing, and non-repudiation.

4.2.4 Implementing Best Practices in Securing E-Business Infrastructure

This aspect of security policy is where vulnerabilities are handled. Vulnerability is often the first thing to address, since that is where the organization and the system administrator tend to have the most control. This is the area of security risk management that is principally a technology issue. Each component has to be addressed with a view to implementing a complete e-business secure infrastructure. Notable elements in that strategy will include PKI cryptography and digital signature technology, applied via Secure Sockets Layer (SSL) digital certificates to provide the authentication, data integrity, privacy and availability necessary for e-business. This is where the system information security officer can go over a checklist of what is necessary and what the organization has. A typical checklist will include:

- physical protection for computers
- network systems management
- email control security
- networks security
- firewalls
- Encryption
- PKI
- incident handling
- antivirus software
- digital certificate
- strong authentication
- access control
- audit and tracing software
- backup and disaster recovery
- biometric software
- wireless communications security

At the moment, businesses are using various (sometimes very poor) proxies for best practices as substitute for overall security strategy. There is no systematic industry standard for doing it and there are no known best practices for organizations to model their strategies. So far the closest one comes to best practices are the practices of so - called “leading organizations”. These are organizations that are significantly ahead of the rest in terms of implementing robust security systems[17]. While those practices may be exemplary, they may not necessarily earn the title of best practices when subjected to an objective rigorous analysis. The type of best practices that is advocated here is one that is not only impressive in its design and implementation but one that can be analytically proven to be optimal, similar to the process of analytically proving optimal coding in software development.

4.2.5 Analyzing, Assessing and Insuring Residual Risk

Once the best practices are in place, any risk that is not covered must be addressed by means of an insurance mechanism. Those risks need to be further assessed in terms of the probability of the events and the subsequent financial impact on the organization. A

[17] US GAO (1999a,b).

simple matrix commonly used for insurance decisions can be developed to classify the sources of risk as in Table 1 below. The events in Quadrant I are risks and vulnerabilities that have low probability and low impact if they occur. The traditional way for dealing with those items is to handle them on event-by-event basis. Quadrant II contains events with high probability but low impact. These are events whose management will be incorporated into the daily routine of the organization to ensure that actions are in place to curb the probability of such events. By definition, there will not be insurance market for events in Quadrant IV. Events that fall in Quadrant IV are dealt with by preventing their occurrence much like those in Quadrant II except the organization should be willing to devote more resources to controlling Quadrant IV events. Events in Quadrant III are those that will normally be handled by insurance – either one that is explicitly traded in the financial market or an equivalent intra-organization device. Already, the market for this is beginning to develop.[18] However, because of lack of information with regard to what constitutes best practices, we conjecture that this market is highly inefficient right now.

Table 1: Probability vs. Impact Matrix.

Probability / **Impact ($$)**	**Low**	**High**
Low	**I** **Ignore**	**II** **Contain and Control**
High	**III** **Insure and/or Have Backup Plan**	**IV** **Avoid/Prevent**

4.2.6 Monitoring and revising the system

Implementing effective e-business security is a dynamic process. The technology is changing very fast and so are the threats and vulnerabilities. Creating a security and risk management culture is a slow process. It is necessary to create an effective monitoring

[18] For example, Counterpane, http://www.counterpane.com/pr-lloydsqa.html; InsureTrust.com, http://www.insuretrust.com/ [April 1, 01].

and feedback system in order to determine the efficacy of each of these aspects of the security policy.

5.0 Challenges and Opportunities

This proposed framework for information security immediately brings into focus some challenges together with some corresponding opportunities. The main challenge is that at this present time we do not have all the building blocks in place yet for an organization that wants to implement this framework to do so. In particular, the following issues have to be dealt with:

- Devising efficient and effective technology for monitoring vulnerabilities and identifying threats in a preventive proactive manner. This could be achieved by developing component-specific or threat-specific software.
- Developing software for information security risk management, similar to those developed for, for example, nuclear risk management, environmental risk management, commodity price risk management, etc.;
- Identifying and implementing best practices in information security risk management – identifying the processes and corresponding metrics;
- Adapting traditional risk assessment and risk management strategies to e-business information security context;
- Pricing the risk of e-business information security;
- Instituting a new type of Certification Authority to certify and rank insurability based on the parameters of the pricing model above.

The present challenge is that none of these components is currently in place. The converse of that situation is that it provides an opportunity to initiate a process that will help put the relevant tools in place in a systematic well-planned manner.

6.0 Summary and Conclusion

The problem of information security in today's networked world is presented together with current common solutions applied to solve it. It is argued that the purely technological approach is not sufficient to produce trust or minimize risk so as to cause companies and their clients to conduct e-business with confidence. A risk management approach is presented. There is already evidence that the market will welcome this approach. It is therefore not surprising that industry forecast groups are beginning to

predict that “new security markets will emerge, existing markets will evolve, and legacy security environments will mature and take on new life”[19].

Two prerequisites are necessary in for this new approach to become effective: an industry standard needs to be set for what constitutes best practices in e-business security, and a new type of “Certification Authority” will have to be instituted to certify that an organization conforms to the set of best practices. These best practices and their certification will then become the standard upon which market prices for e-business insurance will be set.

References

Arbaugh, W.A., Fithen, W.L., McHugh, J. (2000), Windows of Vulnerability: A Case Study Analysis, *Computer*, (December), 52-58.

Bellovin, S. M (1989), "Security Problems in the TCP/IP Protocol Suite," *Computer Communication Review*, (April), http://www.ja.net/CERT/Bellovin/TCP-IP_Security_Problems.html. [April 20, 01].

Breidenbach, S. (n.d.), “How Secure Are You?” http://www.informationweek.com/800/prsecurity.htm

Carnegie Mellon University (CERT) (1999), “Deploying Firewalls”, http://www.cert.org/security-improvement/modules/m08.html, [April 19, 2001].

Chambers, C., Dolske, J., and Iyer, J. (n.d.), "TCP/IP Security," http://www.linuxsecurity.com/resource_files/documentation/tcpip- security.html [April 19, 01].

DTI Information Security Breaches Survey 2000 http://www.infosec.co.uk/page.cfm?Calling=/page.cfm/Link=35&HyperLink=http://www.infosec.co.uk/g/logos/dtiGREEN/ [May 9, 2001].

Felten, E. W., Balfanz, D., Dean, D., Wallach, D. S. (1997), “Web Spoofing: An Internet Con Game”, *20th National Information Systems Security Conference* (Baltimore, Maryland), (October), http://www.cs.princeton.edu/sip/pub/spoofing.html [April 23, 2001].

IBM (1998), “S/390 Security Advantage for e-business”, http://www-1.ibm.com/servers/eserver/zseries/ebusiness/security.html [April 19, 01].

Longstaff, T.A., Chittister, C., Pethia, R. and Haimes, Y.Y. (2000), “Are We Forgetting the Risk of Information Technology?”, *Computer*, (December), 43-51.

[19] Yankee Group (2001), http://www.advisor.com/Articles.nsf/aid/SMITT184. [April 1, 01].

Mathy, L., Edwards, C. and Hutchison, D. (2000), “The Internet: A Global Telecommunications Solution?”, *IEEE Network Magazine*, (July/August), http://www.comsoc.org/pubs/surveys/ [April 21, 2001].

Microsoft Corporation (2000), “Security Management for ASPs”, Microsoft Enterprise Services White Paper, http://www.microsoft.com/technet/ecommerce/aspsec.asp#e, [April 21, 2001].

Morris, R. T. (n.d.), "A Weakness in the 4.2BSD Unix[+]TCP/IP Software,": http://www.ja.net/CERT/Morris/r.t.morris-TCP.html [April 19, 01].

Neumann, P. G. (1995), *Computer Related Risks*, (Addison-Wesley).

PBS (n.d.) “Life on the Internet”, http://www.pbs.org/internet/timeline/ [April 21, 2001].

Rubin, A. D. and Geer Jr., D. E. (1998), “A Survey of Web Security”, *Computer*, Vol. 31, No. 9, (September) pp. 34-41.

Shumway, R. M. (1998), "Common-Sense: An Alternative Approach to Web Security", Proceedings of the 21st National Information Systems Security Conference, 142-153.

Sieglein, W. (2000), “Authentication: What You Have vs. Who You Are”, http://www.planetit.com/techcenters/docs/security-defensive_tools/expert/PIT20001220S0006 [April 19, 2001].

Slade, R.M. (1998), “REVIEW: ‘Web Security Sourcebook’”, *The Risk Digest*, Volume 19, Issue 97, (Fri. Sept. 18), http://catless.ncl.ac.uk/Risks. [April, 23, 01].

Tan, Yao-Hua; Thoen, Walter (2000), “A Logical Model of Trust in Electronic Commerce”, in Schmid, Beat F.; Lechner, Ulrike; Stanoevska-Slabeva, Katarina; Tan, Yao-Hua; Buchet, Brigette: *EM - Communities & Platforms. EM - Electronic Markets*, Vol. 10, No. 4, 10/2000, http://www.electronicmarkets.org/netacademy/publications.nsf/all_pk/1812. [April 23, 2001].

US GAO (1999a), “Information Security Management: Learning From Leading Organizations”, GAO/AIMD-98-68 (May), http://www.gao.gov/special.pubs/ai9868.pdf [April 1, 2001].

US GAO (1999b), “Information Security Risk Assessment: Practices of Leading Organizations,” GAO/AIMD-00-33 (November), http://www.gao.gov/special.pubs/ai00033.pdf, [April 1, 2001].

Verisign (2000), “Securing Your Web Site For Business”, http://www.verisign.com/server/rsc/gd/secure-bus/ [April 21, 2001].

Yankee Group (2001), "Where the Investment Dollars Will Go in 2001: The Top Seven Wonders of the Internet Security World", *The Yankee Report*, Vol.1 No.6 - March 2001, reported by *Security Advisor* at http://www.advisor.com/Articles.nsf/aid/SMITT184 [April 20, 2001].

Zakon, R.H. (2001), “Hobbes’ Internet Timeline”, http://www.zakon.org/robert/internet/timeline/ [April 21, 2001].