International Research Journal of Computer Science (IRJCS)
Issue 2, Volume 2 (February 2015)
ISSN: 2393-9842
www.irjcs.com

A SYSTEMATIC APPROACH TO E-BUSINESS SECURITY

MUTHUSELVAM.R[1] , THANGARASU.N[2] MURUGADASS.M[3]
Assistant Professor [1,2,3]
Arignar Anna College (Arts & Science) – Krishnagiri.

ABSTRACT-- In the new economy, information is critical both as input and output. Hence information security management is of high priority. In contrast, 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. 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 systematic approach to e-business information security is presented. The key characteristic of this approach is that it is an insurance-based risk management process that encompasses the entire information infrastructure of an organization.

INTRODUCTION

The original purpose of the Internet was to move files among computers, to enable easy remote access to computers, and to build redundancy into the distributed system that it is, its use for commercial purposes has grown tremendously since the development of the World Wide Web. Simplicity and ease of use were the prime motivation for designing the Internet. Security, both for the Internet and the Web came as a later development, almost an afterthought. 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." In addition to the Internet being an open system, the rapid rate of development of new software and communication systems has led to a state in which software users are not fully knowledgeable about software and systems architecture. This makes users oblivious to a number of vulnerabilities that can lead to serious security breaches.

Organizations have always regarded information as an important resource. Organizations have always regarded information as an important resource. However, in today's knowledge-based economy, the significance of information both as strategic input and output has been accentuated. 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. Along with this opportunity comes the challenge of information security. Protecting online assets and network resources has become a mission critical concern for executives and managers.

It 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, integrity, availability, legitimate use, auditing and non-repudiation. An another concept of this paper, it is argued that the current system of focusing on software and hardware systems is inadequate. Instead, we advocate a risk management system coupled with a new type of certification authority.

E- WORLD AND E-BUSINESS

In today's Internet world, it is relatively easy to create, alter and transmit information. The advancement in computing capacity and interconnectivity has presented a situation where small efforts can cause potentially large losses. Both accidental and intentional breaches are easier and more likely. This is a major challenge to businesses that want to take advantage of the current information technology. Concern for information security is fairly widespread. 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 regarded as a key business driver.

COMMON SECURITY THREATS AND E-BUSINESS SECURITY OBJECTIVES

There is almost an uncountable number of ways that an e-business setup could be attacked by hackers, crackers and disgruntled insiders. Common threats include 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.

EFFECTIVE INFORMATION SECURITY POLICY - SIX OBJECTIVES

It concerned for 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.

CONFIDENTIALITY

Confidentiality involves making information accessible to only authorized parties, or restricting information access to unauthorized parties. Confidentiality 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.

Sixty-three percent(63%) of Internet 'health-seekers' and sixty percent(60%) 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-nine percent(89%) 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.

Similarly, information in transit has to be kept from the view of unauthorized parties and that it is retrieved only by a legitimate entity.

CURRENT PROCESSES AND TOOLS FOR IMPLEMENTING E-BUSINESS SECURITY

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. 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.

The current common e-business security practice translates into acquiring sophisticated servers, firewall software, intrusion detection systems, and obtaining digital certificates. We refer to this 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. We contend that regardless of how sophisticated the software and hardware devices might be, risk cannot be fully addressed without a systematic risk assessment and risk management process.

DESIGNING A COMPREHENSIVE AND SYSTEMATIC SECURITY POLICY

All security solutions need to begin with a policy. Some basic security policies framed are as follows:

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

The main theme 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.

Stage 1: *Develop a corporate risk consciousness and risk management orientation.*

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.*

Stage5: *Follow systematic risk assessment and risk management procedures to determine the level of risk after implementing the best practices on each component.*

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

DEVELOPING CORPORATE RISK CONSCIOUSNESS AND MANAGEMENT FOCUS

In order for any security policy to work, there has to be a strong organizational foundation. The goal is to create a systemic organization-wide risk consciousness and responsibility. 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 interests and the fortune of the organization depend very strongly on their ability to safeguard their information resources.

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 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.

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. Documented 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: confidentiality; integrity; availability; legitimate use, auditing, and non-repudiation.

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 cryptography, PKI and digital signature technology. 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	• Digital Certificate • Strong Authentication • Access Control • Audit And Tracing Software • Backup And Disaster Recovery • Biometric Software • Wireless Communications • Antivirus Software

In order to create a common set of standards (not necessarily identical implementation), we advocate the setting up and use of a “Security Certification Authority” that will certify that best practices procedures have been effectively deployed.

ANALYZING, ASSESSING AND INSURING RESIDUAL RISK

Once the best practices are in place and certified, 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 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. The organization needs to monitor the risk in those items without necessarily taking any immediate proactive measures.

They need to be watched in the background. 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 occurrence 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 avoiding 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. However, because of lack of information with regard to what constitutes best practices, we conjecture that this market is highly inefficient right now.

Probability	Low	High
High	III Insure and/or Have Backup Plan	Contain and Control Avoid/Prevent using Risk Management Strategies

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

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.

PRICING THE RISK OF E-BUSINESS INFORMATION SECURITY

Instituting a new type of Security 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. In particular, there is an urgent need for further research into issues such as the optimal investment in security mitigation technology and strategies; the appropriate pricing of information security risk for the purposes of making sound insurance management decision; and how to systematically incorporate the behavioral component into a systematic risk management strategy.

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. With the implementation of this approach, new financial security markets will emerge to handle the pricing and trading of this type of risk.

Two conditions are necessary for this new approach to become effective: 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 a 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. In the meantime, the onus is on business leaders to take the necessary initiative towards a comprehensive e-business security policy for their organizations because the current technical oriented ad hoc approach is fraught with high business risk.

REFERENCES

[1]. National systems and security maintenance centre for New Delhi, Bulletin Aug, 2013(Report on e-business and statistics vol-4)
[2]. Bellovin, S. M (1989), "Security Problems in the TCP/IP Protocol Suite," Computer Communication Review, (April), [April 20, 12].
[3]. Breidenbach, S. (n.d.), “How Secure Are You?” http://www.informationweek.com/800/prsecurity.htm
[4]. DTI Information Security Breaches Survey 2012 http://www.infosec.co.uk/page.cfm?Calling=/page.cfm/Link=35&HyperLink=http://www.infosec.co.uk/g/logos/dtiGREEN/ [May 9, 2001].
[5]. 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, 2011].
[6]. IBM (1998), “S/390 Security Advantage for e-business”, http://www-1.ibm.com/servers/eserver/zseries/ebusiness/security.html [April 19, 01].