Assessing and Managing Risks in Virtual Environments

ABSTRACT

The increase in popularity of electronic transactions has created a necessity to develop and adopt information security systems. As the popularity of e-services has grown, so has the need for effective information security. As such, information needs to be well defined, stored, integrated, transmitted and made available whenever needed in a safe and secure manner. The main goal of the information security process is to protect information confidentiality, integrity and availability. This paper highlights essential and common e-service architectures, who and what is involved in an online transaction, challenges related to online transactions and the role of both individuals and organizations towards successful and secure transactions. A general framework for establishing, assessing, and maintaining a reliable security management system for e-services is suggested. The proposed multilayer framework helps to determine how useful, comprehensive, and adaptive an information security management system actually is. It focuses on determining the critical processes of an information security system and how they can be identified and implemented in real-world situations in order to provide better and more secure protection.

Keywords: *electronic services, information security, risk assessment.*

1. INTRODUCTION

From a business perspective, e-services are a direct adaptation and implementation of the use of the Internet for business. With the rapid growth of the Internet, e-services activities have played a major role in expanding business activity and organizational services to much higher levels by allowing a larger number of potential customers, users, organizations, and companies to interact in a much shorter time frame, lower costs, and greatly enhanced convenience.

Online businesses and services may be located in various parts of any country. This can require a non-immediate exchange of information, goods, and money. As a result, often sensitive information is being exchanged online like, personal and financial information including names, addresses, phone numbers, and credit card details [7,8]. This has led a number of countries to develop robust tailored e-service architectures to suit their social and economic systems.

Information security is achieved by adopting and implementing the appropriate set of quality controls, whether they are policies, procedures, standards, practices, awareness programs or organizational structures and ethics [1,4,5,9,12]. Information security is an integral and essential element of business today.

Security may not be a company's core competence, but it is a core requirement and should be embedded into corporate business processes and culture. The main goal of the information security process is to protect information confidentiality, integrity and availability. A comprehensive security process encapsulates and consolidates the three main processes of prevention, detection and recovery (see Figure 1) [16]. A first step in this direction is the identification of critical data. Business information security contributes to the organization by improving and facilitating the interaction with trading partners, maintaining closer customer relationships, improving competitive advantage and protecting reputation. It can also provide a healthy foundation for implementation of known business frameworks, such as Enterprise Resource Planning (ERP) and Total Quality Management (TQM) [3].

The rest of the paper will go as follows. Security if electronic services will be covered first. This will address the different aspects of security including but not limited to: physical security, front and back end security, identity and access management, the proposed multi-layered model, and conclusion and future work.

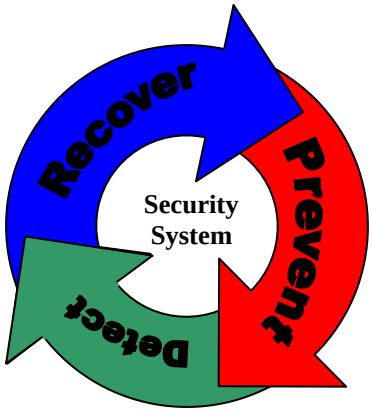

Figure 1: Main Processes of a Security System.

2. E-SERVICES SECURITY

E-service is a common term referring to any service provided online or through the Internet which may include commercial and noncommercial services. Among the widely accepted services are e-Commerce, e-Government, e-Health, and e-Education. By far, e-Commerce has the highest growth rate among these services.

Whether they are providing a service or offering a commodity, online businesses have some assets that need to be protected. The main focus of a secure e-service (like other distributed systems) depends mainly on protecting communications between the trading parties [20], and controlling the system access and any other resources involved in providing the service [2,19]. Using secured channels for communication protects the confidentiality, integrity, and authenticity of the information it carries. Access control verifies that only authorized parties have access to the resources and prevents any unauthorized users from accessing the system. In order to provide a secure transaction media, three levels of security are required: business environment and physical security, front-end security, and back-end security. Each will be elaborated on in the following sections.

2.1 Business Environment and Physical Security

The first and the most basic level is to control the physical access to the main computing facilities. This could be achieved through the use of locks, access logs, and surveillance cameras. The use of sophisticated alarm systems, swipe cards, CCTV, and 24 hour security increases the level of security at the physical level but bring more sophistication to the system. The emerging technologies represent a big challenge at this level. Portable media devices are becoming smaller, more powerful, and more common. Memory sticks, digital cameras, and portable hard disks pose a great security threat at this level. Such devices facilitate copying confidential information and removing it from the workplace.

To most businesses, the investment in security systems (in particular those related to prevention rather than detection and recovery) is invisible. Businesses need to balance the equation of expenditure. While investing some money in implementing and maintaining a good security system might be listed as over-expenditure, not doing so could be of greater cost to the business not only financially but also in loss of reputation etc. The main motive of most businesses is to protect their customer's interest and reputation in

the market. Implementing proper security systems opens more opportunity for businesses to grow and operate more efficiently.

While sharing the same goal (information security), different businesses have different priorities. While the main concern for the information technology sector is the protection of intellectual property; telecommunication companies are most concerned about reducing or possibly eliminating network downtime. On the other hand, protecting customer information, and maintaining data integrity are the main motives for government and financial businesses.

2.2 Front-end Security

The first step to achieving an effective front-end configuration is to determinate the safety needs of both the front and back ends. Software can be developed and customized to review and synchronize user IDs and passwords to prevent unauthorized access incidents [6,15,17,18].

2.2.1 Identity and Access Management

The majority of online businesses depend on user IDs and passwords as the main means of protection. Verifying user identity is front-line defense against unauthorized use. Access management covers all the system application functions and integrity requirements between the application itself and the end-user interface.

2.2.2 Human Errors and Misuse

It is often stated that people are the weakest link in any secure system chain. The foundation of a good security system is the definition of certain rules and precautions that users inside and outside the organization need to follow. The written procedures are effectively a security policy. When combined with a solid technical infrastructure and proper security awareness, written policies and procedures can be effective against human errors and intentional misuse. A first step in improving the security procedure is to conduct a periodic risk assessment. It is hard to control some threats without anticipating them first. It is important to educate users about the different risks and how critical the information that they are handling. Without questioning the honesty of users, proper precautions need to be implemented against any fraud or intentional misuse. When dealing with security systems, proper awareness and qualification of users is crucial for the survival of the business.

2.3 Back-end Security

All the hidden resources (hardware and software) behind the application level fall within this category. The underlying network infrastructure constitutes its major components. At this level, it is common to use firewalls, intrusion detection systems, encryption and decryption schemes, and access control lists. It is important to realize the difference between means of detection and means of prevention [6,15,17,18].

3. MULTILAYER MODEL

The proposed risk assessment multilayer model works in a hierarchal fashion (see Figure 2). It starts from the most basic security level and progresses to the optimal one. Going from bottom to top in this hierarchy, the ultimate security of the system is defined by its weakest link. Hence, an organization's system can't be considered secure on one level without fulfilling all requirements on the previous level. That is, by complying fully with the security requirements in one level, the organization can move up step-by-step to its optimal security level. This helps integrate the three main functions of the security system (prevention, detection, and recovery).

Increasing the security level brings more sophistication and complexity to the system which in turn requires more skills and technical knowledge to operate and maintain it. While it is desirable to achieve higher security levels, it is important to maintain a certain usability level (easy and user-friendly systems).

Depending on the needs of the business, it is not always the case that the highest levels of security are required to be put in place [10].

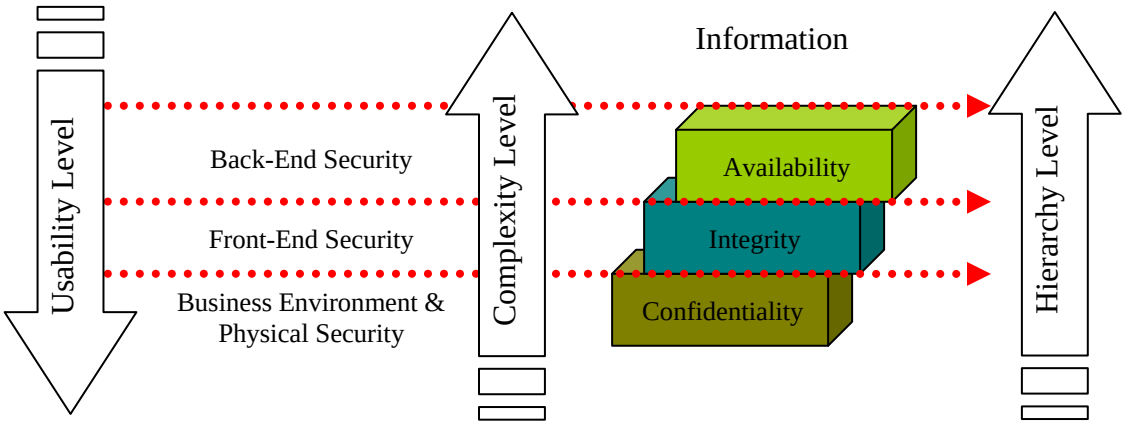

Figure 2: Multilayered Risk Assessment Model.

3.1 Business Environment and Physical Security

The main purpose of the security controls at this level is to secure the business physical assets and to prevent unauthorized access to the system. At this level, the authentication process and the physical security measures require little technical knowledge from the users. In other words, the system is user-friendly and not so complex. The main three processes of security (prevention, detection, and recovery) are achieved. The use of physical security prevents non-authorized users from having accessibility to the system. Using user IDs and passwords are simultaneous means of prevention and detection. They prevent unauthorized use of the system and at the same time detect when the system has been used and by whom. Backup systems and duplicate security precautions are mechanisms of recovery in case of one security process failure at this level.

3.2 Front-End Security

A security mechanism needs to be implemented to cover all the application functions and maintain integrity between the end user and the application itself through the use of authentication. As fewer people are involved with the technology at this level, it is normal that the increase in the level of system complexity results in a reduction in the usability level compared to the first physical layer. The processes of prevention, detection, and recovery are accomplished at this level by using access control, logging users access the application, and tracking any changes they may make, respectively [6,15,17,18].

3.3 Back-End Security

The security controls at the first two levels need to be supported by the proper infrastructure at the back-end. This will include any resources whether it is software or hardware that is beyond the application level. Firewalls, intrusion detection, and cryptographic schemes are good examples of the back-end security. High levels of technical knowledge and skills are consequently required. However, the main three processes apply here too. For example, encrypting messages, network intrusion detection, and providing

backup communication channels are clear examples of the three processes: prevention, detection, and recovery [6,15,17,18].

3.4 Risk Assessment

An effective and efficient security framework depends mainly on the organization's security policies and procedures. Those policies are not of any use until put in implementation. They could include network security, configuration management, disaster recovery, and change control. In order to understand what type of risks to anticipate and how to avoid them, one needs to:

- Identify business's valuable data and assets.
- List potential threats to those data and assets. This includes the type of the threat, where it could happen, from where it could come, and most importantly, the motives of the attacker.
- Evaluate the existing system's vulnerabilities and how the attacker can make use of them.
- Calculate the probability that those vulnerabilities could risk the business's data and assets.

Risks were and will always be an integral part of today's businesses regardless of the investments in the implementation of sophisticated security systems. When implementing a security system, it is of great importance to balance the cost, security, performance, and usability. There will be no such optimal security policy but one needs to reduce the risks to an acceptable level at an acceptable cost with an acceptable drop in performance, usability, and productivity.

In order to justify the spending on security mechanisms, one needs to calculate the Return on Investment (ROI) [13,14]. Calculating the ROI brings in an additional factor of complexity since:

- Business assets may not be quantifiable.
- Threats are known to happen to a certain degree (may happen but don't have to happen).
- Some vulnerability is known and others arise from time to time.

Recent reports have shown that losses due to computing vulnerabilities have increased from 17.8 million dollars in 2001 to over 264.59 millions in 2008 (see figure 3).

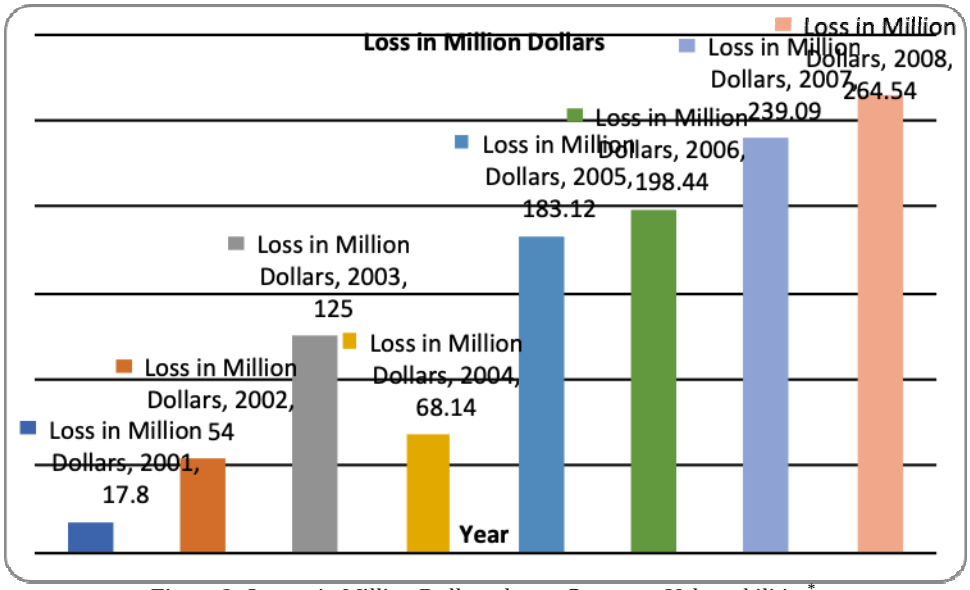

Figure 3: Losses in Million Dollars due to Computer Vulnerabilities[*].

The 2008 internet crime report [11] showed also an increase in the instances of reported computer related incidents over the past couple of years. Figure 4 shows some of the statistics of the years 2000 through

[*] Source: Internet Crime Report 2008.

2008. Those incidents ranged from credit/debit card fraud, identity theft, financial institution fraud, and computer fraud. Yet one should keep in mind that those figures represent only portion of the actual incidents (reported ones). According to some statistics, the reported incidents are only 30% of the actual figures. With some basic calculations, one can estimate the monetary loss per incident to be roughly one thousand American dollars in the year 2008.

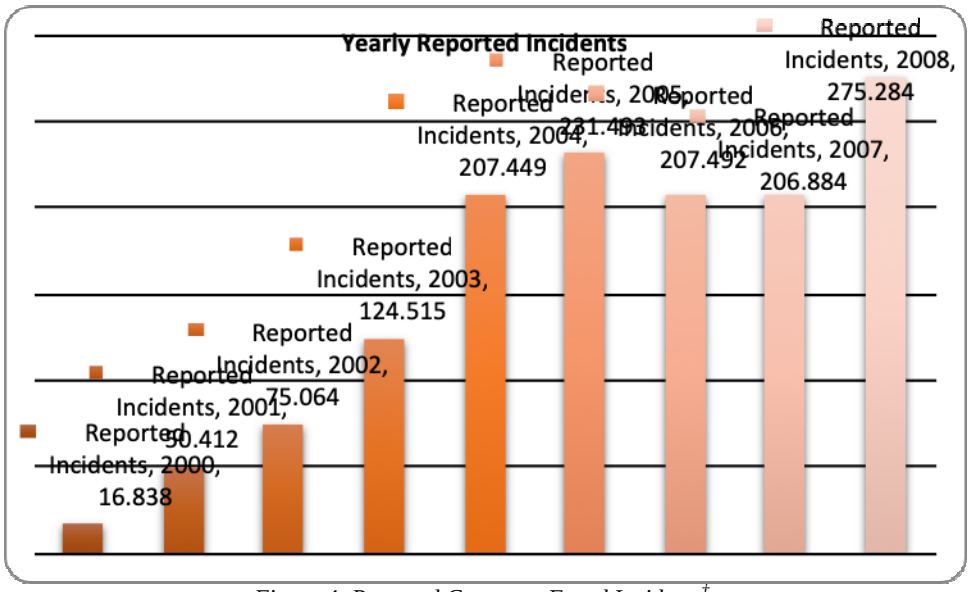

Figure 4: Reported Computer Fraud Incidents[†].

4. HOW THE MODEL FUNCTIONS

The proposed model is meant to help organizations evaluate their security systems in order to better protect their assets. The logical organization of the hierarchy suggests that businesses must first meet a certain requirement in one layer (starting at the bottom of the hierarchy) before moving to the next one. For instance, it will be of no use if the best application systems are put in place without a proper access controls. Moving up the hierarchy, the security system is measured by the highest level it achieves. Hence, fulfilling the requirements at the front-end implicitly means meeting the acceptable levels at the business environment and physical security requirements. Violating the security requirements at a lower level means that the entire system is effectively below that level until the violations can be remedied.

The violations could be categorized as either "Weakness" or "Concern". Both categories need to be addressed by the organization either immediately "weakness" or need to be investigated further "concern". Both categories indicate a non compliance with the security criterion, policies, guidelines, or procedures which could compromise the entire organization security system. Remedial actions are needed to strengthen the compliance with the security policies and guidelines.

Table 1 shows a sample security system evaluation sheet. An important step when implementing an integrated security system is to examine all the security related elements at the different levels of the organization (corporate level, department level, unit level, and personal level). The first step is to map all the security elements within the organization (shown here at the vertical axis). Then one assess those elements at the different hierarchy levels (physical security, front-end security, and back-end security) shown here at the horizontal axis. This will help identify any security gaps, concerns, or weaknesses that

[†] Source: Internet Crime Report 2008.

could cause potential security vulnerability. This will help identifying the responsibilities of both individuals and management of the organization within the context of the security process.

Table 1: Sample Security System Evaluation Sheet.

	Physical Security	Front-End Security	Back-End Security
Policies & Procedures	O	O	O
Standards & Guidelines	O	O	O
Training & Awareness	O	O	O
Physical Security	W	O	O
Investigations	O	O	O
Consultation	O	O	O
Crisis Management	O	O	C
Law Enforcement	O	N	N

O OK
C Concern
W Weakness
N Not Applicable

5. CONCLUSIONS

This paper has provided an overview of e-services and the requirements for secured online business transactions. A secure service is achieved by implementing and maintaining three levels of security policies and procedures. The front line is securing the physical assets and providing a secure business environment. The secured environment needs to be backed up with front and back end security systems along with proper infrastructure in order to develop, implement, and maintain each of the individual services.

Clearly, security must be of great concern to the provider of an e-service. It is the providers' assets, systems, and reputation that are ultimately at risk. As the entire security system is measured by its weakest point, we have shown how security issues exist across all of those three layers, with many issues common to all of them. A full set of security services along with the proper awareness must be offered at the three layers in order to secure the system as a whole. Implementing security measures at different levels can significantly reduce the system vulnerability to attacks.

The proposed risk assessment model is a practical tool for businesses to evaluate the quality, scope, required investment, efficiency, and effectiveness of their security systems. This allows them to tighten, replace, or improve their security policies accordingly. To tackle the security issue with more depth, the proposed framework analyzes the security systems at three different layers. The interrelationship between the three layers allows the businesses balance the amounts of sophistication and usability since humans are considered the weakest link in this chain.

This research contributes to the existing literature by introducing the multilayer risk assessment model which coincides with the information industry demands of an in-depth security system. This model also

allows security system designers and developers to pay particular attention to some areas that could cause vulnerability when implemented in the final system.

REFERENCES

[1] Ashri, R., Payne, T., Marvin, D., Surridge, M. and Taylor S. (2004). Towards a Semantic Web Security Infrastructure, Proceedings of Semantic Web Services Symposium.

[2] Bonatti, P. and Samarati, P. (2002). A unified framework for regulating access and information release on the web, Journal of Computer Security, 10(3), 241-272.

[3] Fogg, B. J., Marshall, J., Laraki, O., Osipovich, A., Varma, C., Fang, N., Paul, J., Rangnekar, A., Shon, J., Swani, P. and Treinen, M. (2001). What Makes Web Sites Credible? a Report on a Large Quantitative Study, Conference on Human Factors and Computing Systems, Seattle, USA, 3(1), 61-68.

[4] Gandon, F. and Sadeh, N. (2003). A semantic e-wallet to reconcile privacy and context awareness, Proceedings of the Second International Semantic Web Conference (ISWC03).

[5] Gandon, F., and Sadeh, N. (2004). Semantic Web Technologies to Reconcile Privacy and Context Awareness, Proceedings of the 1st French-Speaking Conference on Mobility and Ubiquity Computing, CD-Format, New York, USA.

[6] Han, S., Dillon, T. and Chang, E. (2007). Anonymous Mutual Authentication Protocol for RFID Tag without Back-End Database, Lecture Notes in Computer Science, 4864, 623-632.

[7] Hart, P. and Saunders C. (1997). Power and Trust: Critical Factors in the Adoption and Use of Electronic Data Interchange, Organizational Science, 8(1), 23-42.

[8] Hart, P. and Dinev T. (2006). Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended e-Services Use, e-Service Journal, 4(3), 25-59.

[9] Head, M. and Yuan, Y. (2001). Privacy Protection in Electronic Commerce – a Theoretical Framework, Human Systems Management 20, 149-160.

[10] Henning, R. R. (2000). Security Service Level Agreements: Quantifiable Security for the Enterprise, ACM 1999 New Security Paradigm Workshop, Ontario, Canada.

[11] Internet Crime Compliant Centre (2008). 2008 Internet Crime Report, http://www.ic3.gov/media/annualreport/2008_ic3report.pdf. (Accessed April 25, 2010).

[12] Ives, B. and Learmonth, G.P. (1984). The Information System as a Competitive Weapon, Communications of the ACM, 27(12), 1193-1201.

[13] NDI Executive Exchange (2016). Maximizing ROI in Your Cybersecurity Program, Foley and Lardner, LA, USA.

[14] Marks, Norman (2018). Is There an ROI in Investing in Cyber or Information Security, Norman Marks on Governance, Risk Management and Audit, USA.

[15] Reiter, M. and Stubblebine, S. (1997). Toward Acceptable Metrics of Authentication, Proceedings of the 1997 IEEE Symposium on Research in Security and Privacy, Oakland, USA, 10-20.

[16] Smith, M. D., Bailey, J. and Brynjolfsson, E. (2000). Understanding Digital Markets: Review and Assessment, in Understanding the Digital Economy, E. Brynjolfsson and B. Kahin (eds.), Cambridge, MA, MIT Press.

[17] Tan, C., Sheng, B. and Qun L. (2007). Serverless Search and Authentication Protocols for RFID, Pervasive Computing and Communications, 3-12.

[18] Tan, C., Sheng, B. and Qun L. (2008). Secure and Serverless RFID Authentication and Search Protocols, IEEE Transactions on Wireless Communications, 7(4), 1400-1407.

[19] Tanenbaum, A. S. and Van Steen, M. (2002). Distributed Systems: Principles and Paradigms, Upper Saddle River, N.J., Prentice-Hall.

[20] Voydock, V. L. and Kent, S. T. (1983). Security Mechanisms in High-level Network protocols, ACM Computer Survey, 15(2), 35-71.