An Effective Design of Model for Information Security Requirement Assessment

Shailaja Salagrama
Scholar, Doctor of Philosophy, Computer Information System, University of the Cumberland's, Williamsburg, Kentucky, USA

***Abstract*—Information security is a major domain of analysis for enhancing the security of sensitive detained business organizations. These days, attackers are advancing themselves by applying highly advanced technological solutions such as artificially intelligent malicious codes, advanced phishing methods and many others to acquire sensitive and critical data from businesses. This paper presents a novel model framework to analyze the requirements of information security for a more robust information system and its assets in organizations. The framework of this model is designed in such a fashion that both new and legacy organizations can adopt it to define the requirement of security that will ensure confidentiality, integrity and availability of information systems and their components - including sensitive domain business and private data that is critical to the organization. There are two different model frameworks which are proposed here. The first one provides specifications of the security requirements and the second provides for the audit of the access logs to capture any unethical practices and violations by internal users. The proposed model for security requirements provides the roadmap to analyze and build proper security requirements to secure business sensitive data. Stepwise processes which are needed to analyze and define security requirements are the key factors of this security model, as they help in clear definitions of security frameworks and infrastructure for an organization. The Audit Model provides the framework for defining information auditing requirements, thus enabling the capture of unethical and unauthorized access to the information system components of the organization.**

Keywords*—*Information security; network security; web security; confidentiality; integrity; availability; communication technology; information system; internet security; security framework introduction

I. Introduction

Recent developments and advancements in information technology have shifted various systems onto the online platform. This new paradigm of processes and activities on the information and communication technology platform enables stakeholders to execute the required applications over the Internet so that the required services can be secured digitally without necessitating any physical movement to the service provider. Therefore, information security becomes one of the potent concerns of service providers and users. Protection of vital information such as business-related sensitive data, users' personal data, users' transaction data etc. is vital In recent times, cybercriminals have become highly sophisticated with new-generation hacking methods and tools, making security and protection of vital information a significant challenge to business entities and users. Information security provides safeguards to systems which are typically used to process, store, and communicate data. There are various sources of information, and these include the operating environment, management, databases, network infrastructure and the Internet. Securing all these artifacts associated with the information technology and systems is highly challenging - both directly and indirectly as they are heterogeneous in nature and in their functions. While some studies show that cryptography can provide the security to information and its related agents which are used to process, store, and transmit data, it may not be so. This is because the existing cryptographic algorithms may fail to secure the vital information once the decryption key is discovered [1]. Further, by using message analysis, the attackers can analyze the key and therefore decipher the messages that are encrypted. The numerous attacks on various cryptographic systems and their results have demonstrated that these algorithms have been breached by the attackers.

Information security has both technical and non-technical perspectives to it. Purely technical security measures are inadequate for securing information. Therefore, non-technical measures, such as social security measures should also be in place to enhance the overall security effectiveness, so that the information and information system assets can be completely secured. It is simple to design a social tool that can effectively launch a social engineering attack and secure vital information such as access identities and passwords from victims. This indicates that a purely technical security framework is not adequate for securing vital information [2][3].

Today, what we need is an adaptive security framework for securing information systems and assets. Adaptive security is considered to fall under active security measures that could secure the loopholes and vulnerabilities of the information systems and assets. The level of information security required is heavily dependent on the functional profile of the organization and the equipment and hardware used in the processing of sensitive information. Risk analysis and Vulnerability analysis are the primary processes through which security requirements are analyzed. This helps to identify, manage, and create countermeasures for securing critical information, information system assets and the components vulnerable to security threats. Adequate protection of data is very critical if the information system must generate trust among the stakeholders. A security breach may cause huge financial, trust and image losses [4]. This research article proposes the use of an Analytical Framework for Security Effectiveness that can be applied to critical business data associated with information systems.

II. Effective Secuirity Framework

The analysis of various risks and vulnerabilities is performed on the information system to model the gaps in the security and privacy of sensitive and critical data. Any effective security framework should have the three basic components proposed in the Fig. 1.

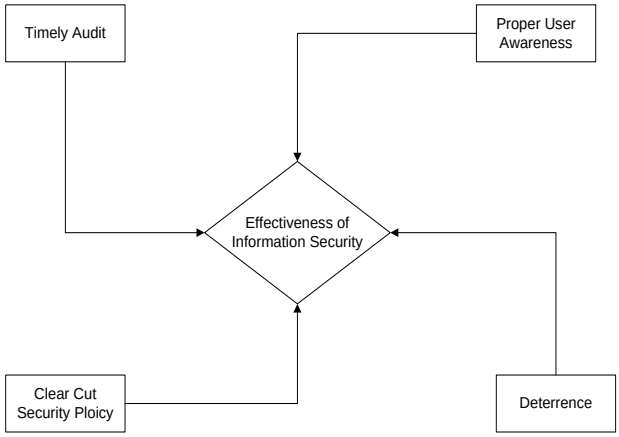

Fig. 1. Effectiveness of Information Security for any Firm, making the Information Security Effective.

To secure the vital information from misuse must be the main consideration. As shown in Fig. 1, four different aspects are mandatory for effective information security, where each one is related to the other to provide security to information [5][6].

To an individual information system firm or organization, the security policy must be very clear in concept and deployment [7]. A clear-cut security policy excludes not only the third party in practice but also direct deployment with respect to the information system assets. Deterrence always prompts the regulatory and legal aspects for the internal users not to go beyond the defined scope or violate the system to disclose sensitive information. This must be in place within the users of firm to assure robust security to the information system assets and critical information. User awareness to different categories of threats associated with social engineering attacks is mandatory and a regular process must be in place to make users aware of the latest trends and procedures of such types of attacks. Audit ensures establishing the violation parameters and depth along with the identity, so that a regular audit must be executed by using the right tools and technology to determine the violators and if necessary, to take legal actions. These four base frameworks provide effective information security to an information system.

III. Internet and Security

Almost all online web application requires Internet services to be made available to the users. Internet is open to all as it is a public network in nature. Due to this fact the risks to confidentiality, integrity and availability of information are very high, with hackers constantly trying to acquire the sensitive information to gain potential benefits by disclosing and abusing the same.

A. Security Analysis Framework

Security analysis is one of the most important processes to scope out the security requirements. Four parameters are considered to analyze the security for Internet based systems. The analysis parameters are detailed under Table I.

TABLE I. Secuirty Analysis Framework

Sl. No.	Analysis Factors & Security Breaches		
	Security Domain	**Dependency Factor**	**Security Breaches**
1	Physical Security	Medium	Theft, Loss of Data, Natural and Man-made Disasters
2	Data Security	High	Eavesdropping, Hacking, Impersonating, Malicious Activities
3	Network Security	High	Denial of Service Attack, Replay Attack, MAC Spoofing, Router Poisoning
4	Web Applications	High	Cross Site Scripting, Hijacking, Database Hacking, SQL Injection, Session High Jacking

These four security domains are mutually associated with the Internet world and analysis of security is performed with respect to the dependency factor the corresponding security breaches. The profiles of the information systems firms and organizations which deal with the business processes on Internet-based applications are detailed in Table II.

TABLE II. Security Domain

Sr. No	Web Applications and Security Risk Factor Level		
	Organization Type	**Dependency on Web Application**	**Security and Risk Factor**
1	Non-IT Domain	Nil	Nil
2	Mixed IT Domain	Moderate	Medium
3	Complete IT Domain	High	High
4	Third Party IT Support Domain	High	High
5	IT Cloud Support Domain	High	High

Firms are selected on the basis of the five different domains mentioned in Table I. The analysis parameters such as ‘not required’, ‘moderate’ and ‘high’ are defined with the security and risk factors. An equation is created to assess the risks and vulnerabilities to different domains of firms as defined below.

Ri = Risk Factor Variable where i= 1,2,3,4
Vi = Vulnerability Variable where I = 1,2,3,4,…,n.
Si = Severity Variable where I = 1,2,3.
Ri ←→ Vi where value of R = Value V

$$\text{If } \sum_{i=1}^{4} R \times \sum_{i=1}^{n} S \times \sum_{i=1}^{3} \geq 100 \quad (1)$$

- Analysis : All Four Domains of Security
- Include All Security Risks and Breaches
- Develop the Security Model for Each Risk and Breach
- Define Security Policy by Developed Security Model

$$\text{if } \sum_{i=1}^{4} R \times \sum_{i=1}^{n} S \times \sum_{i=1}^{3} = 50 \text{ and } < 100 \quad (2)$$

- Analysis : Analyze only three domains of Security
- Include All Security Risks and Breaches
- Develop the Security Model for Each Risk and Breach
- Define Security Policy by Developed Security Model

If $\sum_{i=1}^{4} \mathrm{R} \times \sum_{i=1}^{n} \mathrm{S} \times \sum_{i=1}^{3} = 25$ and < 50 (3)

- Analysis : Analyze only two domains of Security
- Include All Security Risks and Breaches
- Develop the Security Model for Each Risk and Breach
- Define Security Policy by Developed Security Model

If $\sum_{i=1}^{4} \mathrm{R} \times \sum_{i=1}^{n} \mathrm{S} \times \sum_{i=1}^{3} = 1$ and < 25 (4)

- Analysis : Analyze only one domains of Security
- Include All Security Risks and Breaches
- Develop the Security Model for Each Risk and Breach
- Define Security Policy by Developed Security Model

B. Analysis Functional Flow

Analysis is the first critical process to advance the security to the information system and its Internet based applications to protect it from adversaries and security breaches. Functional Flow of Analysis is presented in Fig. 2.

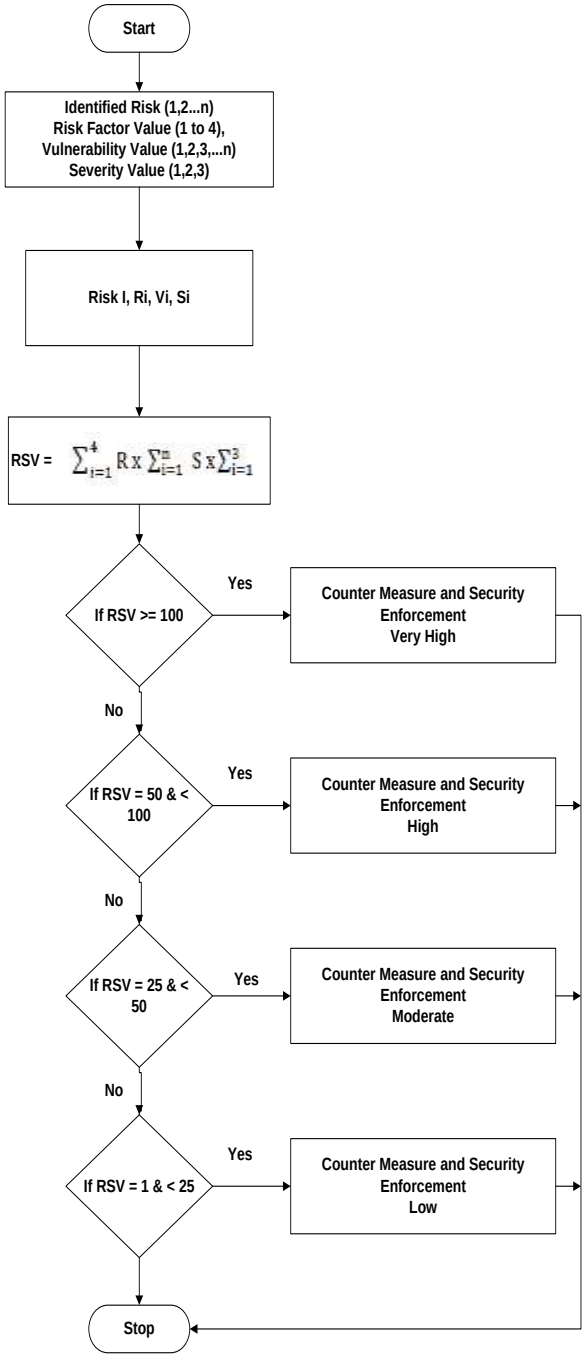

Fig. 2. Functional Flow Definition and Security Counter Measure.

IV. Counter Measure and Security Enforcement

Counter Measures are steps taken to secure the information system and data by preventing them from unauthorized access and disclosure, maintaining the integrity and providing the availability [8][9]. In accordance with Fig. 2 the requirement of countermeasures to secure the information system and its assets - specifically the Internet based applications and their data from security breaches - is identified by the following Table III.

In Table III, the defined equation-based countermeasure requirement specification is assessed as per the corresponding security domain. In Table IV, the security domains and counter measure tools and techniques are presented to enforce the security control.

According to Table IV, for security domain countermeasure tools and techniques that secure the information system and its assets, security from the network side can also be considered [10]. Advanced tools and technologies can also be employed to enhance the security of sensitive and vital data.

TABLE III. Counter Measure Details for Security Breaches

Sl.No.	Security Standard and Counter Measure		
	Security Standard	**Equation Map**	**Security Domain Counter Measure**
1	Very High	1	Physical Security
			Data Security
			Network Security
			Web Application Security
2	High	2	Data Security
			Network Security
			Web Application Security
3	Moderate	3	Network Security
			Web Application Security
4	Low	4	Web Application Security

TABLE IV. Security Domain Counter Measure Tools and Techniques

Security Domains	Tools/Technology and Techniques	
	Tools/Technologies	**Techniques**
Physical Security	Biometric Access, CCTV, Device Lock	Continuous Surveillance, Proper Locking Door and System Cabinets
Data Security	Storage Encryption, Storage Lock, Data Encryption	Sensitive Data backup, Backup Data Encryption, Strong Key for Encryption
Network Security	VPN, SSL, SSH, Firewall, DMZ	Proper Device Hardening, Proper Firewall Configuration
Web Application Security	Parameterized API, Input Validation, Secured Authentication, Prevent Directory Browsing, Hash and Salt Password, Role based Authentication and authorization, SSL, Proper Session Management	Validate the input of users to allow access, apply strong and robust authentication and authorization on role-based identity, use secured socket layer for all sensitive web pages, and do time out for inactive session.

V. Security Audit Framework

A parameterized security audit is important to assess all events that are being recorded with database logs and user account logs [11] [12] [13]. The parameters are defined with respect to priority. The audit parameters are derived by the given Pseudocode.

Input Security Parameter i = 1 to n

Priority = p

Scope = s

Interval = g

Audit Process = a

If p = high then scope = i x 5, g = 7 and a = Manual

If p = medium then scope = i x 3, g = 30, a = automated

If p = low then scope = i x 1, g = 90, and a = Automated

The priority parameters with formulated Pseudocode are derived and the tentative benchmark to audit the logs related to the information system and its assets. They are presented in Table V.

TABLE V. Defined Parametrized Security Auditt

Role Name	Audit Parameters			
	Priority	**Scope**	**Interval**	**Automated/ Manual**
Administrator	High	Identify all violations within the defined role	Weekly	Manual
Internal User	High	Identify all violations	Monthly	Manual
External User	Medium	Identity all accessed areas	Monthly	Automated
Others	Low	Identity as per role	Tri-Monthly	Automated

VI. Conclusion

Proposing a framework of information security is an extremely complex process. In this research, we have attempted to propose a model framework that would help analyze the security framework for a given information system and its assets; thus, enabling recommendations related to information security tools and technologies that would help in securing critical and vital data. The model framework includes two different models that provide the specifications of security such as information security requirements, tools, and technologies to apply security and security audit to capture any deviation from ethical practices by the users through access logs. The proposed models are effective in specifying the requirements and selecting the security technologies, tools and techniques that can be deployed and also for enhancing the features of security to critical system and sensitive data. The mathematical procedures ascertain the verification and assurance of the correct parameters being adopted, while analyzing the requirements of security with different security domains to secure the system and its critical assets.

VII. Future Scope

The proposed Effective Design Model for Security Requirement Analysis and auditing information systems of

organizations provides an effective framework for specifying and defining the information security framework. The scope of this research can be furthered with the proposed research work to enhance the given model by adding the hazards analysis and recommendations by integrating the disaster recovery option and its various techniques. The assurance of business continuity with respect to disaster recovery requirements including all natural and other disasters related with information system can be studied along with the framework to ease the requirements-scoping and to enhance the overall security to business organizations.

REFERENCES

[1] S. Kowalski, Lectures in Security management at the department of computer Sciences and Systems, University of Stockholm, 2011.

[2] R. E. Turner, C. Edgely, & G. Olmstead, Informational control in conversations: Honesty is not always the best policy. Kansas Journal of Sociology, 11 (1975), pp. 69-89.

[3] OASIS, Assertions and Protocols for the OASIS Security assertion Markup Language, 1(1).

[4] NIST (2008). Performance measurement guide for information security. National Institute of Standards and Technology special publication 800-55.

[5] ISO/IEC 9796-3 (2006). Information technology -- Security techniques -- Digital signature schemes giving message recovery. International Organization of Standards and International Electrical Commission.

[6] Common Criteria. (2009). Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model Retrieved June 2009, from: www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R3.pdf.

[7] SOA. (2009). Service-Oriented Architecture. Retrieved September 2010, from: http://www.soa.com/products/standards_support/.

[8] Zuccato, A. (2007). Holistic security management framework applied in electronic commerce. Computers & Security, 26(3), 256-265.

[9] Anderson, R. (2001). Why Information Security is Hard, An Economic Perspective. Proceedings of the 17th Annual Computer Security Applications conference, IEEE computer society. Washington DC, USA.

[10] N. Bar-Josef, The Structure of Cybercrime Organization- hackers has Supply Chains Too! Security Week, www.securityweek.com, 2010.

[11] D. Dasgupta, J. Gomez, F. Gonzales, M. Kaniganti, K. Yallapu, and R. Yarramsettii, ―MMDS: Multilevel Monitoring and Detection System‖, Intelligent Security Systems Research Laboratory, Division of Computer Science, University of Memphis, USA.

[12] Von Solms, S.H. (2010). The 5 waves of information security – From Kristian Beckman to the Present, Security Privacy, Silver living in the Cloud, Proceedings of the 25th IFIP TC 11 International Information Security Conference, SEC 2010, Held as Part of WCC 2010, Brisbane, Australia.

[13] Mwakalinga, J., & Kowalski, S. (2011c). Architecture for adaptive information security systems as applied to social networks. The IEEE International conference on computer communications and networks, July 31 - August 4, 2011, Maui, Hawaii, USA.