International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.3, No.9, September 2014 DOI:10.15693/ijaist/2014.v3i9.9-13

Information and Data Security Concepts, Integrations, Limitations and Future

Sandeep Dhawan
Director of Technology
OTTE New York USA

***Abstract*—When we talk about the Information Security (IS) it deals with usually cyber security and countermeasures, wearable technology and information security, cyber warfare, information security, network security, mobile security and World Wide Web security. Furthermore, information and data security compact with the risks and threats that can be encountered to an individual, corporate or Government, types of threats and defensive measures that can be taken.**

This paper talks about the concepts of information and data security on the whole; it's integration and implementation methodologies with our online and offline information systems along with its limitations and future. It's technological overview and how information and data security can be implemented and ensured in an organizational culture. How the privacy and individual rights can be affected if standards are not met.

Applications of the information and data security were discussed that along with evidences, examples to strengthen the application and implementation needs.

Index terms – Information Security (IS), Parkerian hexad, CIA Triad, Foundation of Information Assurance & Security (IAS) Octave, Reference Model of Information Assurance & Security (RMIAS), Certified Information Systems Auditor (CISA), Payment Card Industry (PCI), Optical Head mounted Display (OHMD)

I. INTRODUCTION

In the context of individual and corporate online presence and ecommerce advancement, its importance, safety and security of information and data is the most influential concept that came into focus. This concept further provides opportunities and ways this information and data can be protected not only in physical form but as well as virtual and online form. This paper proceeds as follows: Definition of Information security, its elements, model of data security, wearable technology and information security issue, and IS attributes. Second part discusses about the information security threats and risk management, integration and implementation of IS and types of controls that can be applied to maximize and achieve the information security. Third part of the paper provides with limitations and classification of IS, its future and conclusion.

A. Information security (IS)

Information security (IS) is a phenomenon that protects the information from being unauthorized access and use in anyway such as for the purpose of misuse, disrupt, disclosure, modification etc and it is a general term that is usually used for physical and electronic form of information. Data security means protecting your pool of data such as databases from vulnerability, mishandling and unauthorized access and use.

B. Effect of Data Security Models against Threats

Figure 1 shows a generic in-depth view of onion model of defense where data is layered inside along with the application adopted, its host and network .It shows powerful encrypted network, reliable host and application control can ensure the security and safety of your data from being unauthorized access and misuse.

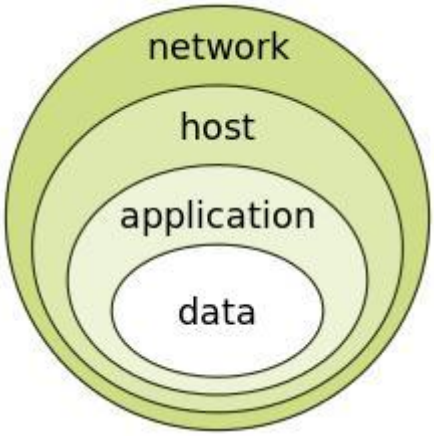

Figure 1 In Depth, onion model of defense Courtesy K. Bolino

II. RELATED WORK

US code defines the Information security mainly in terms of protecting the information and information system from unauthorized access and use. It focuses on three basic aspects of IS. i.e. Confidentiality, Integrity and Availability.[1].

Donn.B.Parker defines the six main elements of the Information Security known as Parkerian hexad. And the elements of Parkerian hexad are:

1. Confidentiality
2. Control (Possession)
3. Integrity
4. Authenticity
5. Availability
6. Utility

Parkerian hexad added three new attributes to classic IS attributes of CIA Triad [2] (Confidentiality, Integrity and Availability). All these attributes are atomic and breach of information Security can be described in terms of anyone of these fundamental and indispensable attributes of the IS. In the definition provided by Donn.B.Parker the concept is based on the fact that an individual, corporate or government will encounter to a loss if the Parkerian hexad elements will compromise at any stage of the information security.

Anderson provides the definition of information Security as being able to have a well informed sense that assures the controls and information risks are at balance.[3]

Foundation of Information Assurance & Security (IAS) Octave is the series of analytical and extensive literature analysis to come to the point of developing an extension of the CIA triad and deals with one of the four dimensions of Reference Model of Information Assurance & Security (RMIAS).[4].

The attributes of CIA triad are refer to as security goals and fundamental aspects of the IS literature. While there's a continuous debate about other attributes and their addition to the classic trio. From rest of the other attributes "Accountability" has been proposed many times for addition and it has been pointed out that "non repudiation" is not a well fitted attribute for addition to the classic CIA triad. [5].

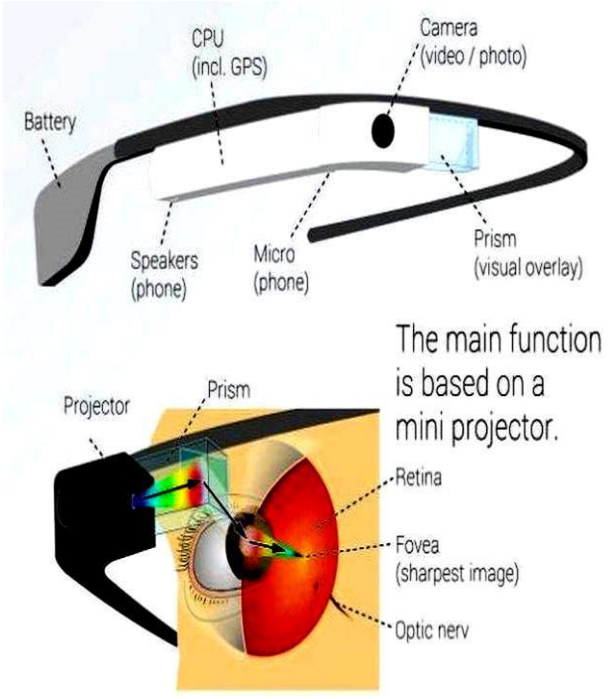

Figure 2a. Google Glass, A Wearable Technology by Google Inc.

kind of
by

providing a body contact so consumer be able to wear it and gain the benefit of those electronic technologies that are incorporated in that device or gadget.[6]

Google Glass **(Figure 2a)** is one of the latest wearable technologies based on optical head-mounted display (OHMD).User of this technology be able to get information in hands-free style that can be wearable on eyes. You can say it is a next stage of mobile computing and this concept of wearing a tech gadget that even captures the personal information from unencrypted wireless networks, although unintentionally, when Google captures the data for street view. [7].

Figure 2b. Wearable Technology and IS Issue

This means no doubt, technological advancement and development of such computing urges and initiate the information technology industry for setting up advanced attributes for the individual's personal and corporate information and data security **(Figure 2b).**

III. Objectives & Overview Of The Proposed Mechanism

A. Objective & IS Attributes

This paper mainly focus the techniques, due diligence and adoptability of these techniques in the light of IS attributes.

If accuracy and consistency of the data during its entire life-cycle is ensured this means that information meets its integrity criteria. [8].This means there's no way of change and amendment of that information in an undetected or unauthorized way. Usually information systems provide message integrity in order to keep the confidentiality of the information.

Availability means the information systems used to store the confidential information must be up and information should be accessible when needed. These systems are used to control the computed information and must be able to retrieve the

information and be functioning accurately all the times. High availability systems usually remain up and provide uninterrupted and smooth flow of access preventing all the denial-of service-attacks through prevention measures. Authenticity means, ensuring the digital signatures and other security system incorporation in ecommerce. It's necessary to validate the data and genuine authenticity of the both parties making transactions at both ends of a business.

When one party of a transaction cannot denies a receiving and other cannot deny having sent a transaction. This also implies to one's intention of fulfilling the contractual obligations, and known as non repudiation. Electronic commerce deals with authenticity and non repudiation through digital signatures and public key encryptions.

B. Overview of the Information Security Threats and Risk Management

It's not uncommon to say that your online presence, confidential information and information systems are at continuous security threats by those black hat hackers who are always in search of backdoors and loopholes.

CISA [9] provides the definition of risk management, according to it the risk management is a process of identifying the threats and vulnerabilities to information resources and decision of taking countermeasures if any, to an acceptable level analyzing the value of that information resource for the organization which is under observation.

IV. Integration and Implementation of IS

Now, the question is how this risk management to information security threats can be implemented.

A. Controls

Controls are ways of protecting the IS attributes that are: confidentiality, integrity and availability. 133 controls have been listed under ISO/IEC 27001:2005, which are cut down to 113 in ISO/IEC 27001:2013

Administrative or procedural controls: This type of controls can be implemented through approved procedures, policies, written guidelines. These procedures help in implementation of controls and define the framework for the people performing a certain business. Similarly some industries have their well defined data security standards which must be followed.

Best example of administrative and procedural control is MasterCard **(Figure 3b)** and Visa **(Figure 3a)** with their Payment Card Industry (PCI) data security standards.

Figure 3a. Visa logo used 2006-2014 Courtesy Visa Inc.

Figure 3b. MasterCard logo used since 16 December 1995 Courtesy MasterCard Inc.

It is obvious to say that when selection and implementation of the logical and physical control is required, administrative and procedural controls comes at the first step in the implementation of IS.

Logical controls: Logical controls are a step-ahead implementation level of IS. It is achieved through principal of least privilege where a user of any system is only provided with a logical of access of as to what is required to perform his tasks.

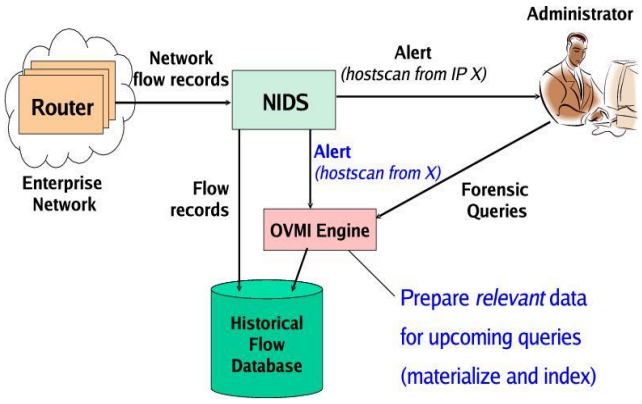

Figure 4. Network Intrusion Detection System

No other programs or procedures are provided with an extended access. For example network intrusion systems **(Figure 4),** data encryption, network firewalls and passwords are logical controls for the implementation of IS.

Physical controls: Information security is compromised when person putting an application for reimbursement is also able to authorize the payment and print a check, or when a programmer can access the system of a DBA. Physical controls allow the segregation, monitoring and control of the environment where an IS implementation is needed.

V. Limitations

Information security is a broad spectrum phenomenon, for each kind of organization classification for security information might be different.

Such as for business information may be (1) Public (2) Sensitive (3) Private (4) Confidential. For government sector it might be (1) Unclassified (2) Sensitive but unclassified (3) Restricted (4) Confidential (5) Secret (6) Top Secret. For other sectors it may be like Traffic Light Protocol [10] (TLP): (1) White (2) Green (3) Amber (4) Red etc.

Lim & Joo S. defines the information security culture as totality of patterns of behavior that an organization possesses and contributes towards the protection of all kind of information. [11].

Schlienger, Thomas, and Stephanie Teufel also urge that organizational information and security culture can be managed in five steps (1) Pre-evaluation (2) Strategic- Planning (3)Operative-Planning(4)Implementation(5)Post-Evaluation.[12].

Effective implementation will need appropriate understanding and training of this classification and handling procedures, policies and guidelines may be required for each kind of organization dealing with a different set of information security classification.

VI. FUTURE

Here we will talk about the ways and methodologies and defensive measure can be taken to deal with information and security threats.

Protected information must be restricted. Access control framework can be an effective defensive measure and must be implemented through a three step procedure i.e. identification, authentication and authorization.

Identification: It will assert the verification process with a claim i.e. providing a username on a website and claiming a member area.

Authentication: This process ensures the verification of the claim that is made in the identification assertion. Verification process adopted by webmaster will verify the PIN, password, mother-maiden-name or anything that was supplied during registration process to validate your request. Driving license, magnetic swipe cards, finger prints, palm prints, retina scans and voice prints are all different kinds of information used for authentication and verification processes. When strong endorsement is required, a process of two-factor authentication or multi-factor authentication might be adopted.

Authorization: Once a person program or computer is identified and authenticated next step is authorization of Run, View, Create, Change and Delete. This starts with administrative policies and procedures that who is authorized to access what kind of information under what circumstances and to what extent. This is known as authorization. This access control mechanism can work under any of the below approaches or can be a combination of three.

Non- discretionary, discretionary approach and Mandatory access control approach.

Other examples of the access control mechanism are role based access controls, file permissions, group policy objects, TACACS,RADIUS, Kerberos and other simple access lists used in routers and firewalls.

Other defensive approaches: Other approaches that can be adopted to deal with the Information and Data security are application security such as Antivirus software, secure coding, security by design and use of secure operating systems, installation of firewalls[13], intrusion detection and intrusion prevention systems.[14]

VII. LAWS ON INFORMATION & DATA SECURITY

It's a matter of fact that "Privacy Policy" and Laws on information and data security should be on continuous change along with the advancements in technology.

Below is a partial listing of US, Canadian, UK and EU laws and regulations that have significant impact on information and data security.

Data Protection Act 1998(UK), Data retention laws (EU), Computer Misuse Act 1990(UK), FERPA (US Federal Law), HIPPA 1996, FFIEC, Sarbanes-Oxley Act of 2002 (SOX), GLBA1999, PCI DSS, PIPEDA, etc.

VIII. CYBER SECURITY STANDARDS

ISO standards for information security professionals to be considered are:

ISO 15443, ISO/IEC 27002, ISO-20000, ISO/IEC 27001.Others: NIST, FIPS, IETF, IAB, IISP, BSI [15], and ISG.

Figure 1 show the results of detection efficiency for the Misbehaving nodes (malicious) 20, 30….100 scenarios. Clearly our MOTS scheme achieves more detection rate than the CONFIDANT and Improved CONFIDANT model.

Figure 2 shows the results of delay constraint for the malicious nodes 20, 30….100. From the results, we can see that MOTS scheme has higher detection of malicious nodes than the CONFIDANT and Improved CONFIDANT schemes.

IX. CONCLUSION

In this research work, we have concluded that Information and Data Security is an on the go due diligence effort and must be adopted through a set of pre-defined written policies, procedures and guidelines to avoid the unseen security threats.

User Privacy Policies, Laws and Standards are subject to be continuously updated along with the advancement in technology and computing. Organizations can ensure their information and data security by adopting the industry wide standards, that can protect their information from being misused, mislead, interrupted, disclosed, disrupted or compromised. Furthermore, organizations should classify the codes of their secure information and employees should be involved, trained, assessed, monitored and reviewed continuously to become able to face any undetected security threat to their information and data security.

REFERENCES

[1]. 44 U.S.C. 3542
[2]. Perrin, Chad. "The CIA Triad" Retrieved 20 August 2014
[3]. Anderson, J. M. (2003), "Why We Need a New Definition of Information Security," Computers & Security, 22(4), 308–313. doi:10.1016/S0167-4048(03)00407-3
[4]. Cherdantseva Y. and Hilton J. " Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals. In: Organizational, Legal, and Technological Dimensions of Information System Administrator. Almeida F., Portela, I. (eds.). IGI Global Publishing. (2013)
[5]. "Engineering Principles for Information Technology Security"
[6]. Vangie Beal, Definition of term Wearable Technology, webpedia.com, Retrieved 21 August 2014
[7]. B Jemima Kiss, Google Glass: privacy fears continue(2013), theguardian.com, Retrieved 21 August 2014
[8]. Boritz, J. Efrim. "IS Practitioners' Views on Core Concepts of Information Integrity". International Journal of Accounting Information Systems. Elsevier. Retrieved 20 August 2014.
[9]. ISACA (2006). CISA Review Manual 2006. Information Systems Audit and Control Association. p. 85. ISBN 1-933284-15-3.
[10]. "OECD: Development of Policies for Protection of Critical Information Infrastructures". Oecd.org. Retrieved 23 August 2014
[11]. Lim, Joo S., et al. "Exploring the Relationship between Organizational Culture and Information Security Culture." Australian Information Security Management Conference.
[12]. Schlienger, Thomas, and Stephanie Teufel. "Information security culture-from analysis to change." South African Computer Journal 31 (2003): 46-52.
[13]. A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco
[14].Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington.
[15]. "BSI-Standards". https://www.bsi.bund.de. BSI.

Author Profile

Sandeep Dhawan received the **B.Tech.** degree in electronics and communication engineering from the National Institute of Technology, Kurukshetra, India, in 2003 and Master of Information System degree University of Ballarat, Australia in 2006. Currently working as a Director of Technology in OTTE New York, USA.