SECURITY ASSURANCE FRAMEWORK

Nagini Madhuranthakam

Qualifications: BE (IT); PGDBAM; ADEIM; ADTQM; ADIBM; ADIR&PM; (M. Tech - Cyber Security).

Guided by Dr. Ravi. K. Seth, Professor at Raksha Shakthi University, Department of Information Technology & Telecommunications. Lavad, Dahegam, Ahmedabad, Gujarat, India.

Abstract: Information is crucial for all Organizations for their smooth functioning of their all Operations in the Local and Global Market Place. For an organization, information is a valuable asset and that should be appropriately protected. Organizational Processes for the Information Security is to give utmost importance for the combined Protection of the Systems, Operations and Internal Controls to ensure the Confidentiality, Validity, Verifiability, Integrity, Availability, Usability, Authenticity, Anonymity and Non-Repudiation of Data or Information.

Key Words: Security Assurance Framework;

I. INTRODUCTION

Information is very important for all practical purposes for any Organization. Information is one the life line and key Asset of the Organization. Currently the Process and Procedures for Security of Information is Crucial to all organizations to protect their information and conducts their Business in the Local and Global Markets.

The Major stages of Data Management are Identification of Data Collection of Data, Enumeration of Data, Segregation of Data, Analysis Data, Design of Data, Authorization of Data, Storage of Data, Retrieval of Data, Manipulations of Data, Transfers of Data, Authentication of Data, Assessment of Data, Reporting of Data, Sharing of Data and Destroying of Data. This Processed Data is called Information and this Information need to be protected in its all stages and in it full life Cycle

Information Security is defined as the 1) Protection of Information, 2) The System of Handling the Information, 3) Software that is used to Collects, Creates, Validates, Verifies, Stores, Retrieves and Reports the Information 4) Hardware that is used to Handle, Manage, Maintain, Use, Store and Transmit that information, 5) Network that is used to Transmit the Information and 6) World Wide Web that is Used to Store, Transmit and Retain.

There should be a mechanism to Assure the Security of the Information in all its Levels for an Organization.

II. BODY

Information Security performs four Roles for an organization which is to protect the ability of the organization's to function smoothly, enable the applications to perform safe operations, that are intended to implement on the organization's Information Technology Systems, secure the data of the organization to collect and use, and lastly is to preserves the Assets of the technology that are in use at the organization. There are many challenges and risks that are involved in implementing information security in organization.

The main reasons for Information Security are to assess, assert, validate, verify, confirm, maintain and manage the Confidentiality, Integrity, Availability, Assurance, Authenticity, Anonymity, Usability and Non-Repudiation. To maintain the same it is needed to have a definite Framework that Assures the Information Security for an Organization. Levels of Security that needs to be built in this Information Security Assurance Framework are Physical Security Level, Operating Systems Security Level, Software Security Level, Network Security Level, Web Security Level and Environmental Security Level.

There are few Security Principals in the context of Information Security as per books that are written for Information Security by several Authors. They are Minimum steps to Operate, Fault Tolerant System, Full Intervention for safe operations, Transparent Design, Segregation of Authority based Privileges, Minimum Privileges for safe access, User Friendly Mechanism, Common Users Acceptability, Work Factor and Compromise Recording. This newly defined Security Assurance Framework will take care of the Security Principals as well in all the Levels of Security.

While Designing the Information Systems for any Business, Organization, Agency, Government, Industry and Person, the Primary Importance will be given to the Functional Requirements and those Functional Requirements only will be addressed. Quality and Security are the Non-Functional Requirements for any Business, Organization, Agency, Government, Industry and Person, so will be given Less Importance while initiating the Designing Process.

In general, in the Life Cycle for Software Development, after completely designing the Functional Requirements, in the Process of Software or Applications Development, then Non-Functional Requirements will be added, as a patch work. The reason behind this sort of methodology or approach may be because of the possibility that while providing these crucial Non-Functional Requirements there is a chance of the missing the main Functional Requirements. To make sure that all the Functional Requirements are addressed in the Designing of any Systems, Non-Functional Requirements are taken care as an Add-on to the Designs.

In this way of approach there is a chance of breaches and vulnerabilities in the System that sacrifices the Security and Quality in the Designed Systems. For this Reason, It is Important to give utmost importance to both Functional and Non-Functional Requirements from the Initiation stage of the Project Design and both should be Integral Part of the Designing Process.

The process of Requirement Analysis that is adopted for Analysis and Design of any Systems, should be Assuring the Robust Systems with Security, Quality and the Required Functionality. The Requirement Analysis should address the need of Physical Security, Operating Systems Security, Software Security, Network Security, World Wide Web Security and Environmental Security from Initiation Stage of the Systems Analysis and Design Life Cycle.

Security Assurance Framework is fully discusses and warrants all these Levels of Security. The Systems that needs to be built are to be Initiated, Designed, Developed, Tested, Deployed and Used as defined by the Information Security Framework. This Framework guides Analysts to give importance to Security at all Stages.

The Manufacturers of Physical Devises follows the Standards that are defined by International Organization for Standards (ISO) for them to produce Devices for Local & International Markets.

The Providers of the Operating Systems as well follows the Standards that are defined by ISO for them to release their Operating Systems for International and Local Markets.

Designers and Developers of Software Products, Applications or Packages for Various Industries follows the Standards that are defined by ISO for them to release their Software in the Local and International Markets and as per the Market Requirements.

Manufacturers of Network Devices & Providers of Network Services, as well follows the Standards that are defined by ISO, to float their Network Devices & Network Services in their Local and International Markets.

Web Services Providers & Mobile Services Providers are also follows the Standards that are defined by ISO for their Services in the Local and International Markets.

There are Certain ISO Standards for Environments that are to be Maintained and Managed by the Business, Organization, Agency, Industry, Person and Government for their Operations in the Local and International Market Area.

There are Certain ISO Standards for various Industries like Banking, Financial Services, Retail, Insurance, Logistics, Telecommunications, Service, Process, Manufacturing, Government, Healthcare, Medical, Pharmaceuticals, Media and Entertainment.

There are Certain ISO Standards for an Information Technology, Information Processing, Information Analysis, Information Systems, Information Sciences, Image Processing and Information Management for Various Industries.

Software Engineering Institute (SEI) Introduced a methodology called Capability Maturity Model (CMM) broadly refers to a "process improvement approach that is based on a process model". This assures the Quality of Services Delivered in the Process of Life Cycle for Software Development.

Industry wise Secured Information Systems Management in Private & Public Networks is clearly discussed by ISO.

These are the Guidelines for Information Systems, Information Science, Information Technology, Information Audits, Information Analysis, Information Processing, Image Processing and Information Management for Various Industries.

Securities Requirements are discussed in ISO List are in the Interest of Businesses, Organizations, Persons, Governments, Industries and Agencies for their Quality of Services and Reliability of Products in the Local and Global Market Area.

Most of the Companies that are there in the International Markets are having their ISO Certification for their Quality of Services and Products.

Quality Assurance Certificate may not assure the Security in the Products or Services. Companies that are focusing only Local Markets may or may not follow the Local or Global Standards for their Presence in the Market.

There is no Regulatory Mechanism to check the Authenticity of these Providers of Services or Products in the Market Area. So addressing the needs of Security cannot be expected or assured from the Regulators, as there are no Guidelines for these Providers of Services and Products. There are no Guidelines or Checklists Launching Applications or Software for General Public in the World Wide Web (WWW) or Mobile Communications Domains.

There is no specific ISO Standard that Emphasises the Requirement for Security in an integrated way in Physical Level, Operation Systems Level, Software Level, Hardware Level, Netware Level, World Wide Web (WWW) Level and Environment Level.

Physical Security can be provided by providing Locks and Safes, by using Authentication Techniques like Barcodes / QR Codes, Smart Cards / Magnetic Strip Cards, Biometrics & RFIDs, by installing Physical Intrusion Detection Systems and Identifying and Preventing Direct Attacks by People or Environment. There should be a Mandatory Mechanism to Track and Trace the Physical Security Access Controls.

Operating Systems Security can be provided by understanding clearly Concepts of Operating Systems like Memory, Information, Process, Data, Control, Peripherals, Network, Wireless Systems and Web Management. Operating Systems Security will take care of Process Security like Process Monitoring, Management and Logging. Operating Systems Security will also take care of Memory & File Systems Security by having Virtual Memory Management, Access Control Mechanism, Password Based Authentication, File Descriptors, Symbolic Links and Shortcuts. Operating Systems Security will also provide Application Program Security by Compiling & Linking, by checking Simple Buffer Overflow, Stack Based Buffer Overflow, Heap Based Buffer Overflow, Format Strings, Race Conditions and Boundary Conditions.

Software Security is provided through Securing the Software from Malware Attacks, Countermeasures to stop Malware Attacks, by providing Diversity, by Building Robustness, by creating Auto-Execution, by assigning Privileges by following the Suitable Practices to Avoid Malware Attacks and the Software or Applications should be designed to protect from Malware Attacks.

Hardware Security can be provided by having the best Control Systems for managing Memory Devices, Internal & External Peripherals (Printer, Plotters, Display Units, Storage Drives, various Input / Output Devices) and Robust Cabinets to hold them. There should be mechanism to record the Hardware Accesses for future reference.

Network Security can be established by having good Network Topology, by having less Network Security Issues, by using strong Network Protocols, by keeping Fire Walls – IDS & IPS, by using powerful techniques like Tunneling – VPN, SSH, IPSec, SOCKS and by strongly designing Wireless Networks. Network Security should have a strong ISO-OSI Model Protocols which will take care of Security in all levels of the Model like Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer and Application Layer.

Web Security can be provided by designing or architecting the Need based World Wide Web with HTTP, HTML, HTTPS, Dynamic Content, Sessions and Cookies Management in their Web Applications or Websites. Web Security Applications are to give importance to address the Attacks on Client Systems like Session Hijacking, Phishing, Click-Jacking, Vulnerabilities in Media Content, Privacy Attacks, Cross-site Scripting, Cross-site Request Forgery and Defense against All. Web Security also should address the issues of Attacks on Servers like Server Side Scripting & Its Vulnerabilities, Data Bases & SQL Injection Attacks, Web Server Privileges and Defense from Server Side Attacks.

Environmental Security can be provided by having proper process and plan for Digital Rights Management, Digital Media Rights Management, Software Licensing Schemes, Legal Issues, Privacy Management, Disaster Recovery Plans & Business Continuity Plans.

Integrated Approach for providing Security in all the Levels is only can assure the Foolproof, Robust, Reliable, Dependable, Legitimate and Secured Systems.

There is need for finding the single Platform that Assures the Information Security. There is need for designing such Security Assurance Framework that should address the need of Physical Security, Operating Systems Security, Software Security, Network Security, Web Security and Environmental Security. Our Research and Analysis is aiming to give Single Integrated Security Assurance Framework that helps the Organizations to have the Assurance of Security for their Information.

Systems with Security Alerts, User Prompts, Awakening Messages, Caution Notifications, Preventive Suggestions, Control Systems, Audit Trails and Directive Reports can assure the Completeness of the System in its Operational Area in any Market.

This is Possible only when we have a Security Assurance Framework in place, where the Stakeholders like Businesses, Organizations, Persons, Governments, Industries, Agencies, Regulators (like Reserve Bank of India. Company Law Board, Securities and Exchange Board of India, Telecommunications Regulatory Authority of India, Insurance Regulatory Development Authority, etc...), Law & Order Protecting Agencies (like Army, Navy, Air force, Boarder Security Forces, Police, etc...) are having specific Roles and Responsibilities that are clearly will be defined in this Framework.

Issues to Address for Secure Software is to have Privacy & Security, Reliability, Fault Tolerance in Software Development Life Cycle Models, Proprietary Software Development Methods – Capability & Maturity Model Integration, Team Software Process, Personal Software Process, DevOps, Agile Development Methods, Common Criteria (ISO IEC 15408, ISO IEC 27000, etc..) in place to achieve that.

Security Development Life Cycle Management will have to provide Education & Awareness to User of the Systems, providing the same from Project Inception stage, Design & Follow the Best Practices for Security, By doing Product Risk Assessment & Analysis and Creating Security Documents, Tools & Best Practices and having Secure Coding Policies.

Security Development Life Cycle Management will also have Secure Testing Policies, The Security Push, The Final Security Push, Security Response Planning, Security Requirement Analysis, Secured Product Releases, Security Response Execution and different Security Audits.

Security Development Life Cycle Management will also have Integrating Security Development Life Cycle (SDL) with Agile Methods, SDL Minimum Cryptographic Standards, SDL Banned Function Calls, SDL Required Tools & Compiler Option, Threat Tree Patterns like Tampering with Process, Data Flow & Data Storage, Repudiation, Information Disclosure of Process, Data Flow and Data Storage in place.

III. CONCLUSION

To build the strong Security Assurance Framework that will give Guidelines and Checklists for all Stakeholders about their Responsibility in all the Levels wherever it is required or warranted. So that there will be definite mechanism that supports the Cyber Forensics.

ACKNOWLEDGEMENT

International Organization for Standards(ISO), Institute of Electrical and Electronics Engineers(IEEE), Software Engineering Institute(SEI) Capability Maturity Model(CMM) or Capability Maturity Model Integration(CMMI), Open Web Application Security Project(OWASP) and Agile Development Framework.

REFERENCES

- Embedded Systems Security-- David Kleidermacher, Mike Kleidermacher [Elsevier]
- Security in Embedded Devices – C. H. Gebotys [Springer]
- Practical Embedded Security – T. Stapko [Newnes]
- Network Security -- Kaufman, Perlman, and Speciner [PHI] Some additional materials needed
- Computer Security – M. Bishop [Addison-Wesley]
- Introduction to Computer Security – Goodrich and Tamassia (Addison-Wesley)
- Digital Watermarking and Steganography -- Cox, Miller, Bloom, Fridrich, Kalker [Morgan Kaufmann]
- Multimedia Security Handbook -- Borko Furht and Darko Kirovski [CRC Press]
- Security Engineering -- Ross J. Anderson [Wiley]
- Wireless Security – R. K. Nichols and P. C. Lekkas [McGraw-Hill]
- Defense-in-Depth: Foundations for Secure and Resilient Enterprises – Christopher May, Josh Hammerstein, Kristopher Rush, Jeff Mattson [Software Engineering Institute, Free from CMU]
- First Responders Guide to Computer Forensics – Richard Nolan, Colin O'Sullivan, Jake Branson, Cal Waits [Software Engineering Institute, Free from CMU]
- Information Security Management Principles-- David Alexander, Amanda Finch, David Sutton, Andy Taylor [BCS Learning]
- IT Security and Risk Management -- J. Slay and A. Koronios[Wiley]
- Information Security Management Handbook-- Harold F. Tipton and Micki Krause [Auerbach Publications]
- Analyzing Computer Security -- Pfleeger and Pfleeger [Prentice Hall]
- Security in Computing – Pfleeger, Pfleeger, Shah {Pearson]
- Introduction to Computer Security -- Matt Bishop [Addison-Wesley]
- Database Security – A. Basta andM. Zgola [Cengage Learning]
- Database Security -- Castano, Fugini, Martella [Pearson]
- Database Security and Auditing-- Hassan Afyouni [Cengage Learning]
- Effective Oracle Database 10g Security by Design -- David C. Knox [McGraw-Hill]
- Addison Wesley_ Computer Security_ Art and Science - By Matt Bishop
- https://www.owasp.org/images/7/76/Jim_Manico_(Hamburg)_-_Securiing_the_SDLC.pdf
- https://www.synopsys.com/blogs/software-security/category/secure-coding-guidelines/
- https://software-security.sans.org/resources/paper/cissp/defining-understanding-security-software-development-life-cycle

AUTHOR PROFILE

- Information Technologist with 26 Years of Diversed Industry Experience in automating the End to End Systems with High Level of Security in both Public & Private Networks.
- Providing Consultancy Services to various Organizations in the field of Cyber Security.
- Information Systems Audit for Security Issues is the Prime Role.
- Designing the Security Assurance Framework for Netizens.
- Providing Consultancy Services to several Organizations for Strategic Planning, Policy Making, Architecting Information Technology Solutions, Quality Assurance, Business Systems, Security Assurance and Cyber Forensics.
- Giving Support for Multiple Verticals of Business and Designing the Solutions, Processes & Road Maps for various Business Units for Cyber Security.
- Expert in **Cyber Forensics and Cyber Security Area.**
- Well Versed with **Cyber Laws & IT Laws for National & International Court of Laws.**
- Having proven Skills in Designing, Developing, Deploying and Delivering Very Smart & Innovative Software Products and defining Policies & Strategies for various Industries.
- Architected Software Products for the Banking, Financial Services, Insurance, Retail, Telecommunications, Logistics, Airline, Cargo, Travel, Media & Entertainment, Healthcare and Travel Industries, Ecommerce Products for various Industries as an Individual Contributor.
- Having Powerful Leadership, Excellent Client Engagement & Client Management skills
- Holding Excellent Technical Service Delivery and Product Management skills like Software Testing, Software Quality Assurance, Software Release Engineering, Software Configuration Management and Software Version Control by using the Trace-ability Matrix in the Software Product Management.
- Expert in Business Process Reengineering, Enterprise Resource Planning and Data Warehousing & Data Mining.
- Adept in Designing Storage Area Network, Network Operating Centres, Network Attached Storage, Disaster Recovery & Business Continuity, IT Security, Proof of Concept Centres, Centre of Excellence, Call Centres, Service Delivery Centres, Microsoft Solutions Framework(MSF), Conducting User Acceptance Testing, etc…
- Performing the Roles of Head of Product Management, Head of Project Management, Head of Information Technology Management, Head of the Network Administration Management and Head of Program & Account Management.
- Establishing Working and Business Relationships with the Clients of Banking Industry, Financial Services, Insurance, Telecom, Retail, Healthcare, Media & Entertainment, etc. in India, Sri Lanka, Bangladesh, Nepal, Middle East, United Kingdom, United States of American, Asia Pacific and African Regions.
- Always believed to dedicate for the Best of the Organization
- Ultimate Commitment and Involvement in Performing Jobs
- Fabulous Communication and Convincing Skills
- Dedicated Research and Development Expertise