An Intangible Information Security Frame Work Against Attacks in Business Environment

Vinod. D, Sivanesh kumar. A, Parthipan.V, Rajesh. M

Abstract: ***The objective of the research work is to propose a strategic reasoning for information security Frame work against various attacks in business organization. The earlier information security research works and incidents include the activation of appropriate safeguards; the prevention and reduction of risks and recovery from impacts were considered for various security needs. The information security requirements that are well aligned with the business needs are essential for a secured design that may enhance product viability and return on investment (RoI) factor. Hence the strategic reasoning for information security models are implemented to unravel the issues of information security requirements based on the environments and development of business applications. The sensitive information in any business organization could be leaked by a poor planning system with various vulnerable policies to ensure that planned actions occur. A Systematic information approaches are implemented with evidences of the security breaches of an organization to enhance the overall security.***

I. INTRODUCTION

Information Security techniques have been implemented and maintained in every organization and the techniques are utilized in critical situations. One of the legitimate challenges in business organization today is the information loss that is due to vulnerable security policies. While the loss occurs in the business environment, the potential security guards tend to prevent the various attacks in the business processes. Risk levels have to be identified before attacks occurred and then it is easy to defend the known attack, and unknown attack [4]. This chapter discusses the review of an extensive range of attacks in business organization with different information security policies that are to be adopted to prevent future attacks. A recent security environment like smart grid often collects consumers' fine-grained power usage data through smart meters to facilitate various applications such as billing, load monitoring, regional statistics, and demand response. However, the smart meter reading streams may also pose severe privacy threats to the consumers by leaking the ON/OFF status of their appliances [3]. A formal approach is proposed based on the logical problem of false data injection through compromised cyber links to a physical control system is modelled by linear quadratic Gaussian dynamics being studied to overcome the situation.

The control input stream is compromised by an attacker to modify the cyber control signals transmitted with the objective of increasing the quadratic cost by the physical organizer. At the same time maintaining a degree of acceptable distance between legal and un-trusted state is characterized systematically [1] .(Many researches work to-words information security focus on preventing confidential information loss; they are carried out in product development centre with many business processes where reliability and security aspects are highly critical. The safety is dependent on the belief of the differentiable capability aligned with chosen plaintext attacks. This results in an undisclosed subspace that genuine users are using to perform decoding, in contrast to an eavesdropper that deploys the mother code [2].

II. INFORMATION SECURITY IN BUSINESS PROCESS AND DEMANDS

The world of modern information has begun with digitally coded messages travelling from an array of micro sensors to a revolving communication satellite and down linked then routed through a cascade of access points either wired or wireless networked data. The assets in the entire life cycle of business processes are information in their raw form and filtered styles. Generally, any information is a tuple with a set of data values, and their data types connected by corresponding association vectors in that specified context. The value of the data is to be preserved and the type has to be maintained along with the correct association vector in the in-plant context during transmission of information as packets. Such information can be very well classified as structured, semi- structured and unstructured information [5].

Irrespective of the categories of the information type, these entities are to be secured against a wide variety of attacks originated from outside as planned activities and inside threat. There are many instances where the confidentiality and the integrity aspects of the critical business information may be lost due to various attacks. Information security is needed to protect data within information systems which is valuable and critical to the business of the organization. It relies on information

Revised Manuscript Received on September 22, 2019.

Vinod. D Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, raosusipooji@Gmail.com

Sivanesh kumar. A, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences

Parthipan.V, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences

Rajesh. M, KRS College of Engineering, Vandavasi, India, Raga Academic Solutions, India

technology tools and utilities to store and to process information, so as to maintain information security as shown in Figure 1.

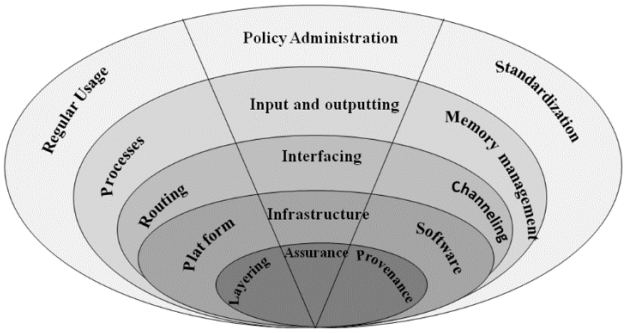

Figure 1 Conceptual Frame Work for Business Processes

The investigation of anomalous or unsatisfactory security defects ideally ends with identification of the common cause in policy administration across various levels of assurance. The systematic approaches for the usage of information security are followed in order to obtain a maximum of security performance within an organization like the product development center. Information securities are planned and executed that is essential to the organization that depends on information systems. In most of the vulnerability cases information is exposed to the risk of cyber-attacks with the resulting damages. It is needed to know of the scope of the attack and the possibility of incidence which can determine the need to prevent the attacks by selecting appropriate safeguards or repairing damages [6].

III. INFORMATION SECURITY ATTACK CLASSIFICATIONS

Information security environment for business processes has to focus on computational security layer that has defended most of the attacks in the recent days. But computers are handling increasingly complex organizational tasks with most of the complicated preconditions and post conditions in business process. It is useful to plan and schedule the security actions in advance in order to ensure that desired actions will be carried out without violating security policies. The typical information security issues that are qualitative will either prohibit any flow of information within a high security level or allow any information flow in secured environment. Information leakage usually occurs when there is any lack of confidence about the confidential data that can also be reduced. Models were developed that described how attacker believe based on the execution of a probabilistic or deterministic program in the said application [7]. Generally, security models will have two goals: one for preventing accidental or malicious destruction of information, and the other controlling the release and propagation of that information. The information flow control is vital for large or extensible systems where there are number of collaborating processes. The security provided for various nodes that are running in different platforms have to be enhanced for the successful collaboration towards the privacy policy [8]. The privacy and the non-repudiation policy are to be adopted in a dynamic run time environment to achieve the required level of information assurance under various attacks are shown in Figure 2. Information systems are complex and have a variety of substantial and insubstantial components. The security system components can be classified at the chosen level of generalization according to their structural and transactional information texture.

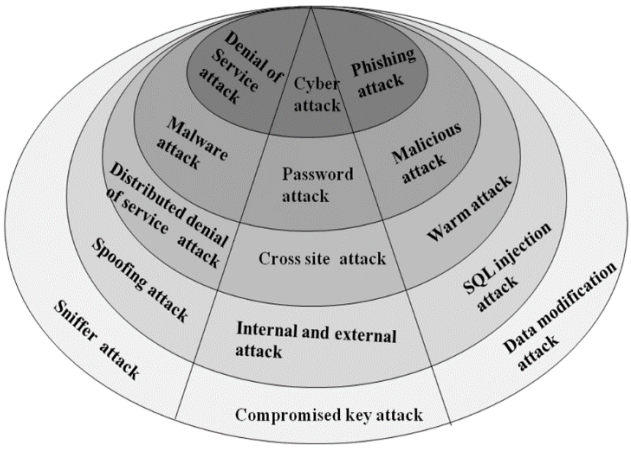

Figure 2 Security Attack in Business Processes

The organization may cause random attack with classified environment in business organizations that are more dependent on reliable operations of their information systems. Generally, attacks like denial of service, distributed DOS, spoofing, sniffers, warm and SQL injection will occur in business surrounding that may bypass the security safeguards and target the organization assets that lead to threat. When any organization globally faces increasing security threats, it can undermine the operation of these systems. Taking into account of today's high threat cyber environment, organizations need security assurance models to protect their expensive information [9].

IV. CHALLENGES IN INFORMATION SECURITY

Information security is needed to protect data which are held on IT systems are more expensive and information loss may cause un- acceptable risk to the business organization. The challenge in information security is to store and process information, so it is essential to maintain secure information flow asset in business organization. The purpose of information security policies is to preserve confidentiality, integrity and availability to make the asset most popular to access, retrieve and precede information flow. The existing methods are typically investigational in nature being highly dependent on the assessor practice, and the security metrics are usually qualitative to address the dual problems of investigational analysis and qualitative metrics by developing two complementary approaches for security assessment analytical modeling, and metrics-based assessment [10]. It is to avoid experimental evaluation; a formal model that permits the accurate and scientific analysis of different security attributes and security flaws is put forward. In order to avoid qualitative metrics leading to ambiguous conclusions, quantitative metrics can be derived based on the set of statistical formulas.

The vulnerability analysis model responses are needed for a theoretical foundation for modeling information security, and

security metrics are the cornerstone of risk analysis and security management. In addition to the security analysis approach, security testing methods are discussed as well. A Relative Complete Coverage (RCC) principle is proposed along with an example of applying the RCC principle. The Personal information is reachable to authorized users and it is no longer required for internal users in their multiple login. Information security management is focused on challenges for conceding the use of information services, interfaces and access to mitigate the evolution of information policies as shown in Figure 3.

Innovative ideas are proposed to overcome the challenges on information security with a multi-level modeling approach for vulnerability using model composition and refinement techniques, a data-centric, quantitative metrics mechanism, and multidimensional assessment capturing both process and product elements in a formalized framework. The information based on its accessibility can be categorized into structured, unstructured and semi- structured information categories. The structured information is highly defined and intended to be processed by a computer program and by some users held in relational databases and the unstructured information that does not have a fully defined structure, and most likely will be read and used by humans. Information is produced by common office applications (a letter or an email).

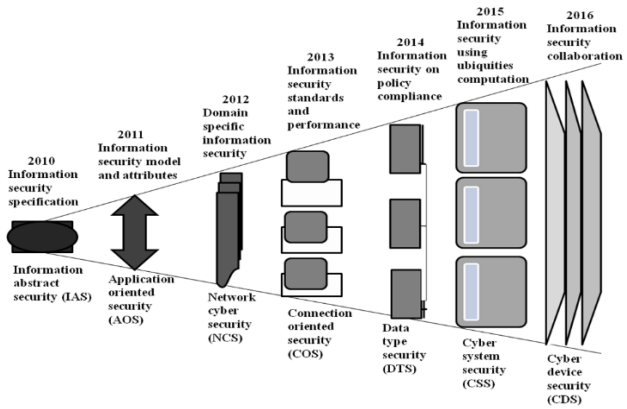

Figure 3. Evolution of information security requirement space

But at the same time, the semi structured information that lies somewhere in between, like invoices, purchase orders, and receipts, which containing data to be computer-processed but coming in formats and layouts that first need to be identified and classified task that often is handled by humans but increasingly is being automated as the tools improve. Information security controls a production which introduces and maintains an organization policy adopted on its goals and objectives that force its operations. In addition to its information technology (IT) dependent operations it uses its risk measurement which results in formulating an IT security policy that chains and can be applied to its organization policy to protect its assets and guarantee its operations being in a secure environment where protection is required. The Security management is to support the collection, protection, and largely security policy for the information security controls in a business enterprise. Progressively more connected information in a strong business environment to collaborate with other organizations, suppliers, clients, and outsider is necessary to co-ordinate security planning for sharing information and its applications. Other aspects of security management include assessment and classification, and narrow compliance. Generally every security manager faces challenges in mitigating their security decisions to prevent attack from confidential business asset. If there are no security incidents in the present investigation, the internal and the external user may feel that there is speculation in security [11]. The root of this challenge is a lack of transparency and concurrence over what security means in practice. Open information security management maturity model (OISM3) addresses this by using security aspects in a business sector.

Models, Methods, Metrics and Logics (M3L)

The possible models for prevention, analysis and mitigation of various attacks on multiple processes are many in the existing literature. The backbone models for any IS techniques identified within the scope of this proposed research are shown below [12]

- **Trust Model:** The predictable trust model for achieving organization information security in the presence of proper visualization in suspicious entries is necessary. The metric and measurement of the trust level is calculated based on the degree and context of information exchange being done. It is a key for analyzing trustworthy understanding of the relationship to evaluate the various levels of information exchange during the suspicious entry. The trust significance for each and every unique identity is concerned in direct or indirect message by evaluating its distrust value throughout the condition based on the situation.

- **Attack model**: The process of information security targets to defend the attack in various possibilities for detailed model in business and security objectives. The attack models are designed to build the safeguards for assorted business, agreement, personnel, access control, precedence, and stability and information management to assure the secure environment. It is to improve the secure surroundings for business and confidential information exchange which is guided through the information security management standards (ISMS) like ISO/IEC 27004:2009. It provides the guidance to measure the risk level of understandability for a secure business organization environment.

- **Assurance model:** Business Information Assurance is part of community authority in which the top level management provides accurate and correct information to the external investors on the efficiency and effectiveness of their security policy and operations. The number of security operations performed on the asset over a session is also a factor to determine the business continuity. Business continuity planning (BCP) is an

important issue and it has to be covered carefully.

- **Provenance model:** Information security provenance model is a kind of information being frequently referred for data provenance or data extraction. The provenance of a data item has been includedfor any internal user in a business organization and if any threat in the original data then the evaluation report for formal data verification can be made available by means of this model. If an internal user modifies any information the security centre helps to determine the derivation history of information starting from its original sources. The original information cannot be modified; instead, a new report will be created and stored in a database; now the security administrator can trace the internal user with the help of report created by information monitor centre. The variety of data illustration models and request domains has lead to less recognized definitions of provenance so as to improvise the outcome.

- **Security generic processes (SGP):** Generic processes present the necessary communications for the execution, evaluation, and development of ISBP processes. The information management is to meet the security across business audit to authenticate the agreement with internal policies and regulatory requirements in security methodology.

- **Security strategic processes (SSP):** Strategic processes management is dependable for choosing and designing security services to present value within the cost and risk parameters of the organization. Strategic management is responsible to external investors for the use of assets through governance planning. The clients of strategic management are consequently external and possibly internal investors.

- **Security tactical processes:** Strategic management is the client of tactical management with respect to the standards of ISM processes. Tactical management is responsible for strategic management in various security performances and activities of the ISMS in organization assets.

- **Security operational processes:** Operational management is responsible for providing feedback to tactical management about the incident in the security environment. The suspects are identified and the assets are secured through the information system.

- **Deontic trust logic:** The trust can be organized in each context with a set of system or scheme to identify a member can be trusted. These intention can specify the reliability for a member 'a' in a meticulous context with a system based on the suspicion values in that context that can be specified using typical deontic logic having the following statuses (i) Permissible (PE), (ii) Impermissible (IM)(iii) Obligatory (OB). A member 'a' is acceptable if it is defined (df) necessarily to have a low suspicion value (L), then it is obligatory that it has to be assigned trust for business environment.

V.Strategic information reasoning in BYOD

The strategic information security models and verification procedure for BYOD (Bring your own device) is to meet the expected qualities in the latest information security model being developed. The information asset in any business organizations like a product development sector, the confidentiality, integrity and availability metrics are to be maintained for secure information flow. Information Quality assurance is also related to integrity which includes the accuracy of information transaction significance and unity, and reliability of repositories. An information quality objective is typically upon quality assurance and control techniques. The information quality assurance can be measured with security objectives and incorporate with business policies as shown in Figure 4.

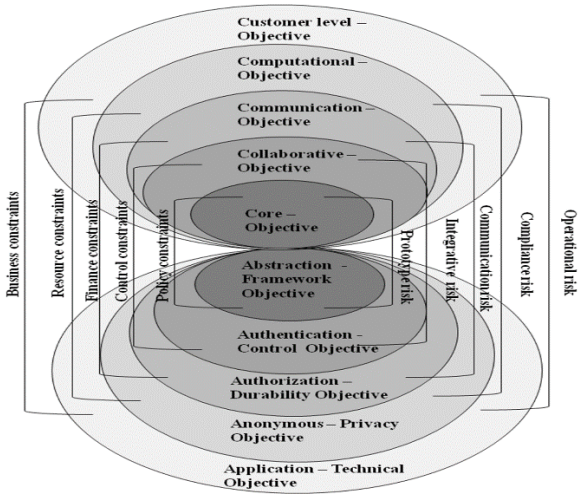

Figure 4. Information Security objectives and reasoning

An information security management model using strategic reasoning principles is to comply with existing methodologies towards bring your own device (BYOD) approach in information and communication technology (ICT). An informative mathematical approach has been derives as followed and derived in equation1,

M = < O P T I O N S>

O_N= the set of network connectivity options

P_O= the set of propositions

T_S= temporary rules at that session

I_C=input connectivity device

O_I=initial default options

N_P=network permission

S_A=status of accepted services

$$\sum_M = \prod (O_N + P_O + T_S + I_C + O_I + N_P + S_A) \quad \text{Eq 1.}$$

ISM $_{BYOD}$= Computing System Security (Service (Application (Network + Hardware + Information))))

ISM $_{BYOD}$ = Computing System Security (Service (Application (Connectivity +Devices+ Data+ Association))))

ISM $_{BYOD}$ = Computing System Security (Service [(Options in Connectivity + Propositions)][(Temp. Rules+ Incoming Devices + Outgoing Data + Network Permissions+ Sessions Control)))

ISM $_{BYOD}$ = Information Security Service [O + P + T+ I + O + N + S]

1. Both internal and external usages of information in the information business management (ISM) and the safeguards have to be established to protect from theft, misuse and damage.
2. Forecasting the security policy to defend any kind of attacks in different business environment .Each and every business organization exists for a particular profit that requires for setting goals and meeting certain target.
3. A business objective in information security environment is to regulate goals and other fulfilment to protect information asset or else it may be forced externally by the government.

The business environment also needs technical reasoning and security objectives to cover the fundamental architecture of information security systems and to create direct impact on organization as shown table 1 and graphical view in figure 6 with its flow analysis with respect to business strategic needs and demands.

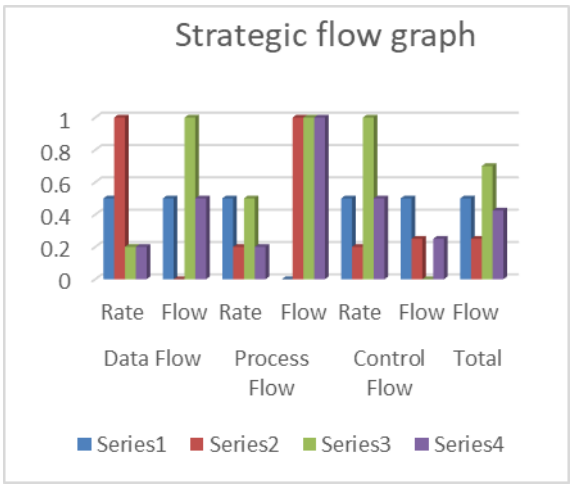

Figure 6. Strategic Information Flow Analysis

VI. CONCLUSION

A security framework for interacting a strategic information security needs and demands are integrating the various policies for an effective security management in BYOD was proposed. The outside attacks on the network and inside threats are also considered. A combination of information security management technique has been used through which the significance, criticality and determination of the various information are accomplished. The actual execution and the reliable associations within the business security organisation and the risk evaluator modules has been improved not only information availability but also confidentiality of various business entities. The model has been implemented with conceptual frame work for business environment with respect to its demand through the combination of existing and upcoming standards of information altercation by the compliance box module. The pre and post M3L deployment of information inside the business association can be made protected through the attack classification model for various information flow analysis.

REFERENCE

1. Syed Mubashir Ali, Tariq Rahim Soomro (2017), "Integration of Information Security Essential Controls into Information Technology Infrastructure Library: A Proposed Framework", International Journal of Applied Science andTechnology,Vol. No. 4,pp. 95-105.
2. Shebaro, B, Sultana, S, Gopavaram, SR and Bertino, E (2018), "Demonstrating a lightweight data provenance for sensor net-works", in Proceedings ACM Conference Computer Communication Security, pp. 1022-1024.
3. Ruochi Zhang andParvVenkitasubramaniam(2017), "Stealthy Control Signal Attacks in Linear Quadratic Gaussian Control Systems: delectability Reward Tradeoff", Vol.14, No.19, pp. 201-214.
4. Open Group Standard Open Information Security Management Maturity Model (O-ISM3) (September 2017), Version 2.0, ISBN: 1-937218-98-0, Document Number: C17.
5. Nicholas Kolokotronis, AlexandrosKatsiotis and Nicholas Kalouptsidis (2016), "Secretly Pruned Convolution Codes: Security Analysis and Performance Results", IEEE Transactions on Information Forensics Security, Vol. 8, No.11, pp. 201-214
6. Mikko T.Siponen and HarriOinas-Kukkonem (2007), "A Review of Information Security Issues and Respective Research Contribution", ACM digital library, Vol. No.38, pp. 256-262.
7. MikolasJonata and Joseph Kiniry(2009), "Reasoning about Feature Models in Higher- Order Logic", International conference Ireland Issue No.11.
8. Lewis, Riyana, Louvieris, Panos (2014),"Cyber security Information Sharing: A Framework For Information Security Management In UkSme Supply Chains", Vol. No.2, pp. 210-220.
9. Ivan Tirado (2008), "Business Oriented Information Security Requirements Development", ACM Digital Library, Vol. 2, No.978-1-60558, pp. 89-91.
10. https://core.ac.uk/display/22625883.
11. https://betanews.com/2017/01/10/biggest-security-threats-2017
12. https://betanews.com/2017/01/10/biggest-security-threats-2017.
13. Sivanesh kumar, A and Khanna V, "Adaptive energy-efficient Clustering for multichannel MAC protocol" International journal of Control Theory and applications, Volume 09, Issue 36, January, 2016
14. Technique for associative learning information transclusion by Wiki-style mashups Tosic, M. Manic, M. e-Learning in Industrial Electronics (ICELIE), 2011 5th IEEE International Conference on DOI: 10.1109/ICELIE.2011.6130022 Publication Year: 2011 , Page(s): 38 – 43
15. An image-map system with spatio temporal color process functions Mori, M. ; Sasaki, S. ; Kiyoki, Y. DOI: 10.1109/ICTKE.2012.6408537 Publication Year: 2012 , Page(s): 104 – 111