ISSN:0975-9646

Approaches for Information Security Modeling

Harshitaa.B [1], G.Praveen Babu[2]

[1]*M.Tech.(Comp.Networks & Info.Security) student, School of IT, JNTUH, India,*
[2] *Associate Professor of CSE, School of IT, JNTUH, India*

Introduction: In this era of globalisation, organizations heavily depend on IT to facilitate their business operations. IT provides with numerous opportunities and improved efficiency for many modern day organizations. It also comes with its own set of security risks. The ever changing risk context of an organization, collaboration with other organizations, ecommerce clearly insists upon an effective Information Security system.

In this knowledge driven economy information is a critical asset to an organization. Considering the fact that information has been a critical asset for any organization or a business enterprise, Information Security has been less about being a technical aspect for the business and more important for the sustainability of the business.

The exact role of Information Security is still not clearly defined in many organizations, while some still view Information Security as a cost centre, it has been shown that effectively managed Information Security organizations can be instrumental in helping an enterprise meet its business goals by improving efficiency. This paper is a survey of few recent security models to provide for Information Security modelling. The first section describes the security model requirements and the issues related with the concept. It is followed by the section describing the process of risk assessment and the key factors associated with it. The last section answers for the complete management of the risk.

I. INFORMATION SECURITY MODEL:

Information Security is protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability. The other properties to be included would be authenticity, reliability, accountability.

Many modern day large enterprises understand that Information Security is critical for their healthy functioning as they rely on public networks. Knowledge about the Information Security has never been more important. The security staff of an organization has a huge responsibility to understand the risk context of the organization and develop a novel security system that helps to meet the business goals. However, Information Security has struggled as a function. It has been always viewed in isolation and never been included as an equally important asset in order to meet for the overall business objectives. It is considered to be a sole responsibility of the security department. Technology has been evolving and with it many security tools, systems and frameworks. There are direct solutions to fix a certain security glitch in a certain system and left at it. However, these solutions never really wait to analyse the interdependencies between that system to others and how it might have affected the overall organization making it a drawback in reaching the desired goals.

Security officers have always struggled to develop a security model in order to align it with business goals of the organization. This is due to the fact that security is viewed differently by different departments in that particular enterprise. The security officers strive to develop a model that integrates with the business goals and objectives. It involves the study of tools, risk, assets and threats. The senior management views it in terms of cost, productivity and immediate results. It is viewed by them as a process of protecting intellectual property of the organization. A marketing department views it as a function that should provide it with unhindered business to reach its day to day targets. The financial department views it as a function that minimizes the loss and risk of the financial assets. So, security officers are just expected to react with immediate technical fixes to any of these department security breaches. This way the security mechanisms are often static and simple while the risk context of the organization keeps changing from time to time. This lack of comprehensive knowledge will lead to unnecessary expenditures over security and controls.

Enterprises need to establish Information Security policies supported by standards, procedures and guidelines. This guidance establishes the direction for the Information Security program and expectations as to how information is to be used, transmitted, destroyed and shared within and outside the business environment. Hence an Information Security Model, which accumulates operational data and security experience, should be formulated to assist the data collection process for risk analysis studies. It aims to collect all currently available Information Security data, and to evolve over time by incorporating new data.

II. RISK ASSESSMENT

Risk assessment is a process of studying key factors affecting the proper working of an organization and the impact it has on the healthy working of an organization. In this modern era, business world is constantly changing. It is unpredictable and more complex every day. Its huge dependence on IT is fraught with risk. Businesses have viewed risk as a necessary evil that should be minimized, managed and mitigated whenever possible. In recent years, increased regulatory requirements have forced businesses to expend significant resources to address risk. For the current global economic environment, identifying, managing, and exploiting risk across an organization has

become increasingly important to the success and longevity of any business. Security risk can be regarded as the effect and probability that intruder exploits the weakness in asset and destroys security attributes. A risk assessment gives organizations a clear view of vulnerabilities to which they may be exposed, whether internal or external. A good assessment provides a basis for determining efficient risk control or mitigation responses. An efficient risk assessment process, applied consistently throughout the organization, allows the management to better identify, evaluate, and risks for their business and decide whether they are required to be taken based on the impact. This is all done while maintaining the appropriate controls to ensure effective and efficient operations and regulatory compliance.

III. KEY FACTORS FOR RISK ASSESSMENT

Risk assessment is a powerful means for assuring safety of information system. The effective way to provide security is the process called risk assessment. It involves collecting information about the assets and threats associated with them. The data collection efficiency is based on the previous security experiences about threat and countermeasures in different areas. The important factors to be considered for any risk assessment are threats, assets and vulnerabilities. **Threats** are the potential events that are likely to happen that may lead to an unwanted incident. **Asset** is a valuable data, process and system that is likely to be target of attackers. **Vulnerability** is a weakness in the system or an error in implementation that can cause an unexpected event compromising the security of the system.

A security model for risk analysis has been proposed which involves recording and studying of organizational security data [1]. It follows the method of RDR combined with a model for entity representation giving an easy way for security documentation. RDR method concentrates on a simple analysis of large data rather than a complex analysis of complex data. A probability risk assessment model [2] based on the factors effecting the working of a system is also an effective way of security modelling. It considers factors like vulnerability, system failures and attacks. The vulnerability factor leaves a system open to threats and attacks. A risk analysis is done based on the impact this attack has on the system. A factor like probability of failure internally or externally due to such attacks is assessed. So a more risk a system faces, the more loss it causes. In the case of an attack or failure the risk factor is increased causing loss again. Four key links are considered (eliminating risks, reducing these risks to an acceptable level, living with these risks given they are at acceptable levels, transferring them to other organizations).

However, all the approaches make use of vulnerability tools and few other good mechanisms to evaluate the damaged caused by a threat based on the vulnerabilities etc., such mechanisms give remedial cures for a single system within an organization. They hardly consider some problems that should not be neglected, such as relevance between vulnerabilities attacks based on the previous system compromising and negligence of safety measures leading to vulnerability. In recent years, many researchers begin to turn to explore attack paths produced by exploiting and relating multiple vulnerabilities. One such approach [3] takes into account the interdependency of the assets and the link between different vulnerabilities. It develops an assessment model for information system security by deeply identifying weakness in the system and analyzing relevance between them. The whole invading process is obtained, in which the attacker exploits system vulnerabilities to promote its privileges and finally control its attack goal. The method combines the probabilities with destructibility that vulnerabilities are exploited, and presents an algorithm to quantitatively assess potential security risk in the system. This approach considers a series of network nodes each consisting of three elements namely the assets, rights and vulnerabilities. It concentrates on finding all possible intruder paths targeting a particular asset through their vulnerabilities. To fully assess potential risk of the entire system, not only the direct consequence that vulnerabilities bring about should be considered, but also all the information about the system and the opening services in every node has to be integrated and analyzed. The proper approach is to identify all of the paths along which attacker possibly exploits vulnerabilities to invade the system, and then estimate success probability of each path, in the end calculate risk values of each asset or the entire system. The first step is assessing the algorithm for attacker paths. The algorithm is developed by identifying asset and its rights to access using its vulnerability. It is further followed with identifying the vulnerabilities of another asset and thereby capturing its rights to access and so on. Next step is weighing the attack paths. This step helps to really understand the impact of that certain attack and how it can eventually affect the whole system. The third step would be to set up an algorithm to assess risk. This part involves assessing the risk factor of the vulnerabilities, assets, system. Thus risk assessment is accomplished. Using the above observations and variables the risk context of an organization is deduced.

IV. RISK MANAGEMENT

Risk management is an approach to deal with risks by anticipating possible losses and design and implement procedures that minimize the occurrence of loss or the financial impact of the losses that do occur. (*Fundamentals of Risk and Insurance*, Vaughan and Vaughan). It is a rigorous approach to assessing and addressing the risks from all sources that threaten the achievement of an organization's strategic objectives. A process, affected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. (COSO)

The losses are caused due to malicious attacks on IT infrastructures (e.g., virus attacks, malware), unintentional or intentional damage caused by employees and failures of critical processes, applications, or infrastructure components (e.g., computing servers, data centers). Such events can lead to significant financial and productivity

losses. In recent times, there has been substantial growth in the field of IT security risk management. However, most of these often overlook the complicated interdependencies between different parts of an organization, even though these interdependencies can have a large impact on the organization's overall risk. Therefore an IT security risk management which accounts for these complex interdependencies is to be modelled. By using mathematical modeling and analysis, this type of approach can provide valuable decision support to risk managers.

One such risk management approach involves three phases [4]: data collection, risk assessment, and risk mitigation to provide a unified approach to the whole process. It incorporates available risk data, which depends on the domain knowledge of security experts.

It requires a huge data collection process. This model informs the risk assessment phase of the framework, which is based on the methodology of cascades of failures. The overall goal of our framework is to enable an organization to use the risk data it collects to analyze its overall risk state and then to deploy resources to reduce its risk exposure over time. The management framework involves assessing different variables such as risk caused from an asset to another asset, risk caused by a threat to an asset, threat caused through compromising an asset and a threat caused to an asset due to the existing of another threat. Next the impact of each of these scenarios is calculated and mitigation of risk is taken upon. It is important to note that this is a process that has no finish line.

CONCLUSION

Information Security has never been more critical than now. This paper insists that the Information Security should just not be an isolated function or department in the organization. It should be modelled in such a way that it integrates the business goals and objectives. While a risk assessment is the process of identifying and quantifying risks which takes places seldom. The risk management process is an ongoing process of mitigating the risks and minimizing or removing that risk. It should be ingrained into the institution's culture to be most effective.

REFERENCES

[1] Kwok LF and Longley D. Security Modelling for Risk Analysis. Proc. 18th IFIP World Computer Congress,IFIP 2004, 2227August 2004, Toulouse, France, pp2945.

[2] Kbar, G., "Security risk analysis based on probability of system failure, attacks and vulnerabilities," *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference* ,May 2009

[3] Mounzer, J.; Alpcan, Tansu; Bambos, N., "Integrated security risk management for IT-intensive organizations," *Information Assurance and Security (IAS), 2010 Sixth International Conference on* , vol., no., pp.329,334, 23-25 Aug. 2010

[4] Huiying Lv, "A novel security risk assessment model for information system," *Advanced Computer Control (ICACC), 2010 2nd International Conference on* , vol.4, no., pp.282,287, 27-29 March 2010

[5] A Business model for Information Security