Implementing Information Security Risk Method (ISRM) To Ensure The Business Continuity

Posted on October 16, 2018

Abstract

The information security risk method (ISRM) is the main method 9f for controlling information security risk. This paper reviews the methods used for this purpose and suggests the use of the information security risk method (ISRM). It is essential that every organization implements this in order to ensure business continuity.

Introduction:

This is an “Information Society” as a result of the swift expansion of global IT infrastructures during the past few years. Due to these global IT infrastructures, it is now possible to have an easy flow of information even across national borders. Now, IT is being used to support operational processes in business instead of its use at the strategic level.IT infrastructures are enabling organizations to face the challenges of quickly altering the economy (Gupta & Saini, 2013). These have also changed the way information is managed today, as every organization is now making use of more and more information technology. With this, new dependencies and risks have emerged globally. Risk is basically defined as the consequence of uncertainty on objectives, and this, in the context of information security, is linked with the uncertainty of the destruction of an information asset, leading to harm to the organization(Webb, Ahmad, Maynard, & Shanks, 2014). Information assets are critical possessions that executives depend on to perform the business.

Although information assets represent sensitive information, information security environments are becoming more and more complex and have numerous issues, such as open systems and the strategic misuse of electronic integration (Kotulic & Clark, 2004). Information security includes many comprehensive areas that also mainly cover the technical aspects. Also, when a business opens its internal networks to customers along with its business associates and dealers, then there is a need to ensure that there is no external intrusion and that data is always protected. For business continuity and trustworthy information, technology is a criterion(Fenz, Ekelhart, & Neubauer, 2009). For this purpose, information security risk management (ISRM) is being used in organizations with other measures. Information security risk management is a risk management procedure that is connected with the use of information technology. It includes recognizing, evaluating, and considering risks to the confidentiality, integrity, as well as availability of an organization’s possessions(Abbass, Baina, &

Bellafkih, 2016)

ISRM has many characteristics that are in common with other security methods. However, it has a main feature in that it doesn't reflect regional and cultural issues and undertakes that all organizations function as huge systems that need refined formation security procedures. This process also matches risks in agreement with an organization's general risk tolerance. It is not possible to remove all risks. However, with information security risk management, the organization can only identify and attain a suitable risk level. Modern organizations are facing the issue of protecting information resources from multifaceted security threats. The main concerns related to security are seepage and amendment of sensitive information. In this category, there is also included the threat to intellectual property and as well as trade secrets(Webb et al., 2014). One reason for having more information seepage today is the use of social networking as well as cloud computing(Webb et al., 2014). The paybacks of cloud computing are strong. Thus, there is a need to develop the appropriate security for cloud applications. There is a problem with this that it offers a higher level of risk as vital services are often subcontracted to a third party. In order to safeguard information resources, ISO27000 can be used as an information security standard (Webb et al., 2014). ISO27000 offers a wide assortment of managerial and technical controls for the purpose of protecting information resources. Here, organization selection controls are linked with the level of security risk exposure. Thus, the far better approach in this regard is to make use of a risk management approach to secure the organization's information (Webb et al., 2014). This paper will discuss Information security risk management (ISRM) as a model for effectively addressing security risk management in different organizations operating in different industries.

Research Questions:

- What are the essential features of information security?
- What types of risks are associated with information security?
- What are the advantages of using ISRM?
- How will risk be assessed under ISRM practice?

The paper will include different situations that were facing issues with information security and how different risk assessment methods were used there for the purpose of removing the security risks. The literature review will provide all the deficiencies inherent in different models and will propose ISRM as best practice in order to address all the issues.

Literature Review:

In today's environment, where organizations possess a number of informational assets, organizations get exposed to a wide range of internal and external security threats. There can be the manipulation of information assets along with the robbery of critical evidence (Ayatollahi and Shagerdi, 2017).

There are also some natural risks associated with the destruction of data, such as accidental mistakes by computer operators. For example, in 2013, mobile malware targeted 99% of Android devices, as reported by Cisco (Ayatollahi and Shagerdi, 2017). There can be unauthorized usage of software and computers for the purpose of illegal activities. Furthermore, hackers and Trojan horses are other threats to data security.

Today, different types of risk management methodologies are used by different organizations to manage and control all these risks. These are being used at national and international levels. All these are developed to address the specific needs, and these have different objectives, along with structure and level of use. There is a common purpose behind these methods: to rank and estimate the risk value while suggesting the most appropriate mitigation plan. There are different drawbacks linked to all the methods, and these include the absence of awareness, extraordinary cost, and prerequisite for expertise as well as lengthy process. Also, these do not consider the context of information security communication inside the organisational construction. These methodologies also possess frameworks with a horizontal plane assessment of risks that can be carried out either at the operational level or at tactical or strategic levels. These thus result in the form of lengthy reports grounded on technical evaluation of the information security risks. Moreover, there is no use for these lengthy reports as these do not get communicated to the required business units. These also lack the complete details of the business case. These reports are also not used for making strategic decisions.

Some countries make use of computerized physician order entry (CPOE) systems that enable clinicians to enter medication along with other orders into a central electronic system(Aarts & Koppel, 2009). There are fewer hospitals that are implementing this system so far, although the Institute of Medicine (IOM) and governmental and business groups in the U.S. are recommending this to be used. First, such a system was used in the early 1970s for the purpose of cost savings. CPOE can be used to reduce medical errors(Aarts & Koppel, 2009). Other advantages of CPOE systems include direct reach to pharmacies, reduction of committed errors of drug names, and the simple assimilation of information into medical histories. This system can also be connected with decision-support systems that have the function of providing reminders related to dosages as well as different drug allergies(Aarts & Koppel, 2009). Thus, this technology can be used to refine patient security. Research has found cost savings and patient protection, in addition to local or national health IT strategies, as motivators for the adoption of CPOE systems.

Risk management can be implemented in an organization with the use of both proactive and reactive approaches. Companies use a reactive approach to retort to the safety risks that have previously happened in the organization. Due to different security incidents, an effective response is generated using a reactive approach. The examination of the reasons for creating security incidents assists in avoiding them in future. While applying the reactive approach, there is a need to follow the six steps (Stroie & Rusu, 2011). There must be laws in organizations that can protect human life and prevent work accidents. If there is any damage, it must be stopped and not allowed to spread after the damage is also required to have an assessment of the damage. For instance, in case of a cyber-attack, there is a requirement to assess the cyber damage. This will consist of conducting detailed

investigations related to the incident and immediate actions for restoring or replacing the hardware. Then, there is a need to define the damage causes. After this assessment, repairs should be made to the damages. Moreover, policies and responses must be reviewed using a reactive approach. The other approach is the proactive approach, and it has many advantages over the reactive approach (Stroie & Rusu, 2011). It is economical to lessen the likelihood of the risk as compared to reacting towards the incident after it happens. Organizations must have plans for the protection of their assets and for the implementation of controls in order to lessen the risk of mistreatment of an organization's susceptibilities by malicious software. Also, if an organization is using effective security strategies, this will result in reputational benefits along with cost savings and a reduction in incident response times. However, if an organization fails to implement adequate security measures, then the organization's competitive position will no longer be in the industry. This is because, in today's technological world, businesses have huge amounts of customer data. Customers, in return, expect business to protect their sensitive data. Thus, breach prevention, along with information security management, is significant to organizational success.

Usually, data breaches are narrated into one of three comprehensive categories: confidentiality breaches, integrity breaches, and availability breaches. Confidentiality breaches are attempts to obtain admittance to delicate data, while integrity breaches are more linked with modification. There are availability breaches that result in system outages. Organizations are now able to lessen the number of breaches, but their rate is still very high in some industries, such as healthcare. Moreover, with the change of conditions, risk management methodologies also evolve. One of the proactive approaches to risk management that has evolved with time is to use the information security risk management (ISRM) model. Information security risk management (ISRM) provides organizations with the most effective and cost-effective methods that enable them to regulate their information assets. It delivers an organization with a road map for the purpose of protection of information infrastructure.

The principal action of ISRM is risk assessment, which begins with the recognition of risks, their prioritized ranking, defining suitable control strategies, and checking their status. It has three main functions in an organization. It classifies the organizations IT setting and assesses business capabilities. Identification of all potential security risks is also one of its functions, along with mitigation. Finally, it also enhances the organization's security risk position. Thus, it is a constant process that allows an organization not only to identify and analyse the risk but also to use the controls to lessen the risks to information assets.

Furthermore, it has four objectives. These include risk identification, risk assessment, risk treatment, and risk review. This process focuses on the second stage, risk assessment. It is the first step in risk management methodology. During this stage, a substantial amount of information related to the organization's information resources is collected (Webb et al., 2014).

Risk assessment is a multifaceted process, and risk cannot be correctly coped with unless it is carefully assumed(Naseer, Shanks, Ahmad, & Maynard, 2016). If there are more information assets, then risk assessment complexity increases so that organizations can protect these assets that can be

spread over different targets(Naseer et al., 2016). Risk assessment capability and security control monitoring are its two capabilities. Effective ISRM is essential to the success of any organisation, and it is also a source of competitive advantage when an organization has better ISRM procedure effectiveness than its competitors. It is a strategic procedure that proposes to support the protection of the confidentiality, integrity, and availability (CIA) of an organization.

There are a number of industries that are making use of the information security risk management (ISRM) model. It also has numerous applications in the healthcare industry, where it is used as an effective tool for the management and control of risk. Healthcare workers are stimulated to use and share electronic health information. For this reason, they are particularly susceptible targets for data breaches. Now, protecting health information is more puzzling than it was in the past due to the change in the nature of data usage. Information security risk management (ISRM), being the strategic model, drives to support shelter patients' data confidentiality and safeguard data integrity, in addition to assuring data availability. If any of these aspects are not fully addressed, then there can be issues such as legal and financial losses to healthcare centres. However, if the data is secured, then patients' and clinicians' confidence will be enhanced, and this will lead to better usage of health data. Moreover, the United Kingdom and the Netherlands have also efficaciously prompted the acceptance of health information technology. There are still a few countries that have yet to make considerable developments in inpatient situations(Jha et al., 2009).

ISRAM is based on this formula that equals the level of risk with two factors: the likelihood of incidence of security breach along with the results of incidence of security breach. Based on this formula, this process is carried out in the form of a survey by organizations in an attempt to minimize the risk for their information assets.

Discussion:

Today, healthcare organizations are using computerized health information systems (CHISs) as a basic requirement for the purpose of dropping healthcare costs along with enhancing healthcare quality and safeguarding patient safety. This also has the advantage of decreasing medical mistakes due to the use of efficient systems. Therefore, the clinical, fiscal, and managerial actions of hospitals are progressively reliant on the enactment of CHIS compared to the past. There are huge advantages of computerized health information systems. However, a drawback of its use is the lack of information security. In the healthcare sector, most of the information is patients' personal information. It's very risky to use a system that is not secured with reference to the personal information of patients. Therefore, it must be secured and saved with reference to confidentiality and availability. During the past year, hospitals in different countries have faced greater challenges.

During the survey of acute care hospitals that had the American Hospital Association membership, electronic-record functionalities were examined in detail (Jha et al., 2009). During this survey, it was found that some hospitals had electronic health records in their clinical areas, and these account for

only 1.5% of U.S. hospitals. Also, 7.6% of U.S. hospitals have the use of basic systems in their operations(Jha et al., 2009). There was thus an association between the adoption of electronic health records and specific hospital characteristics. VHA has been efficaciously using electronic records systems for more than a decade with intense enhancements in clinical excellence. It was found that there were more chances for bigger hospitals situated in urban areas to use the computerized provider order entry for the purpose of medications(Jha et al., 2009). Primary barriers to the implementation of technology funds during the survey include huge capital requirements along with high upkeep costs. There is a need for policymakers to pay attention to financial funding, interoperability, and the teaching of information technology to support staff(Jha et al., 2009).

In 2014, a case study was conducted in the healthcare industry in the northwest of Iran. The sample in this case study consisted of managers from the information technology sections. Data was collected from these managers by the use of a questionnaire that had three parts: personal information, systems characteristics, and risk identification. Natural disasters, human threats, and environmental threats were used as information security threats in hospitals. Data was then analyzed using both quantitative and qualitative methods. The results of the study showed that fire, lack of smoke alarm systems, and lack of access to a strong and up-to-date antivirus system are some threats that are under consideration in healthcare organizations. Inappropriate structure of the networks and careless computer users come under physical/environmental threats in this case study. There was more use of technical safeguards than administrative and physical safeguards. The most prevalent security control methods comprised precautionary control actions, such as admission control and user certification. Thus, in order to control the fire, early warning fires along with smoke detection systems must be used in diverse extents of the hospitals. The access level of people in any healthcare organization must be restricted or defined earlier. There must also be a proper training of the computer users. Physical safeguards must also be used to protect the IT infrastructure.

To promote the use of electronic health records, the new government in 2014 in Iran implemented a health reform plan(Zarei & Sadoughi, 2016). According to this plan, it was required to connect hospital information system programs via the Internet to the Iranian system of electronic health records (SEPAS system) (Zarei & Sadoughi, 2016). A problem that emerged with this system was that having the connection through the public Internet network resulted in significant upsurges in the risks of illegal admittance to facts and figures related to patients. Thus, there were no stated rules on the privacy of patient information, which caused problems with the system's effectiveness. Also, there were more cases of cyber-attacks in Iran due to the disputed nuclear programme started by the country.

To overcome all the above difficulties, it is necessary to use a system that addresses all the issues and is more trustworthy. In spite of having a number of models in the industries, the shield of information assets from the multifaceted and quickly developing security hazard landscape is a noteworthy trial for contemporary organizations (Webb et al., 2014). The best model to use in this regard is information security risk management (ISRM). Its successful implementation needs all individuals to be part of the identification and assessment of risk along with its mitigation. Individuals

who will be part of the risk assessment must be authorized to interconnect willingly and fairly throughout the process. In addition to this, this process must be similar to the audit procedure (Bornman & Labuschagne, 2005). Rather, it must be used as a procedure for the protection of assets in order to achieve the goals related to information security. During the risk assessment process, assets first need to be identified. It is essential to have a complete and up-to-date collection of all information assets. These assets can be hardware, software, and data, along with the facilities. Then, these assets must be valued by the organization based on the CIA's effectiveness. Threats also need to be identified in order to effectively address the problems. The threat can be any activity that can harm the system. Threats can be in the form of hardware or software letdowns along with personnel changes. There can also be the accidental annihilation of data due to unauthorized access or due to some other reason. There can be environmental reasons that can cause harm to the data, such as power failure and natural disasters. Computer viruses and hackers are also the main threats that are faced by information security in today's environment.

Security is considered a strategic business matter due to the rise in the number of data breach occurrences. There are also new policies and laws in different industries as a result of data breaches and data protection failures. These laws have the ability to impose fines associated with breach incidents and accidental data loss. This serves as the process of ensuring the safety of the procures along with the strategy of risk minimization. Organizations feel apprehensive about data security in order to escape from the high cost of patient lawsuits and fines imposed by the government for failing to protect data.

The findings of this study contribute towards the current body of literature connecting to data privacy needs. Information controlled in this study could benefit healthcare physicians to comprehend the influences linked with data security risks and consistent prevention policies desired to diminish data privacy gaps. Thus, business leaders can make use of this study to manage information security risks. This study can also be used to devise new methods to manage strategic significance linked with information security more successfully. Healthcare practitioners need to act before an incident happens. There is a need for widespread preplanning, the creation of main operational procedures, and lengthily scrutinising organizational strategies and trials.

Conclusion

Today, in almost every industry, there is a use of more and more technology, and organisations are operating their systems based on the technology. For this purpose, the main data that organizations use serves as their main assets. The protection of this data is required for the existence and growth of the business. Organizations suffer vital monetary losses as a result of data breaches. Keeping these losses in view, organizational managers are now required to use methods that can save them from these losses. There are web-based solutions and remote and mobile technologies that can increase the information security risks for organizations. It is not possible to avoid the use of such technologies as these are essential in today's business environment for the purpose of making progress

competitively. The use of technology in today's business environment is serving as a source of competitive advantage. Organizations' use of computers and computer networks leads to a reduction in costs. This also helps in the achievement of suitable and effective facilities.

Therefore, organizations need such measures that ensure the security of the data along with the security of other assets of the organization. For this purpose, a number of methods can be used. Most of the methods have several drawbacks that do not make them effective (Gupta & Saini, 2013). Thus, there must be the use of such a method that focuses on the effectiveness of the methods in the form of improving the security of the system as well as its reliability. The policymaker must focus on financial support in this regard, along with addressing the issues of staff training.

Organizations can make use of ISO 27001 to manage risk. These can also adopt ISMS standards to service security authorities in the body of inventiveness. One of the most effective methods is the practice of information security risk management (ISRM). Its main goals are to ensure confidentiality along with integrity and availability in the form of a CIA triad related to IT assets. Here, confidentiality refers to the safeguarding of systems' confidentiality. This system ensures that only authorized users have access to the data and no other outside person has access towards the data. Here, integrity refers to the procedures and controls that are in a position to safeguard variations in systems. Moreover, availability ensures that data is available to authorized users on a continuous basis. All these components are achieved successfully if all the organization's employees have active participation in this process. However, the ultimate responsibility for the effective use of ISRM practice is still towards the board of directors and executive management. Organizations cannot use traditional methods to control the risks associated with information security. The factors responsible for the risk in the information assets are linked to each other and are not addressed with the use of traditional methods. The best approach in this regard is to use the above-proposed model.

When an organization applies technology to information, it results in information security risks. This information can be distorted and inappropriately disclosed. It can also be modified by the unauthorized user for some other purpose that is not suitable for the organization. This results in dollar losses to the organization (Blakley et al.,2001). From the literature, the most common information security risk is fire, as well as technical and environmental threats. The high-impact risk factor requires more consideration in mitigating risk. There is always a need to identify the underlying causes of risks, and these must be addressed beforehand. So that organizations do not face any adverse consequences. In this regard, it is also important to address the causes more effectively when the operating industry is healthcare. In this industry, these must be addressed at the macro level to ensure patient safety.

Most of the time, organizations lack the required resources in the form of financial sources and other material sources, which leads towards the failure of the program. Thus, top management must be responsible for ensuring the success of the program, at least in terms of financial requirements. This also shows the management's commitment towards information security. With an effective ISRM program, the board of directors found an adequate level of risk and made well-knowledgeable risk

management choices. They also determine the potential influence of these risks on the association. There is also the identification of information security risks to achieve the organization's respective missions. This also allows the fulfilment of regulatory requirements in an economical way.

While using the ISRM strategy, the risk profile and appetite of the organization must be used. If there is no risk profile, then risks cannot be minimized in the organizations through the use of this method. ISRM strategy must have an aim to achieve business goals and maintain the security of the organization. ISRM is used as one constituent of a complete enterprise risk management (ERM) competence, and it must be consistent with the goals and policies of the organization. Also, while developing the ISRM strategy, it is required to comprehend the organization's present business circumstances. These circumstances show the capability of organizations to execute the strategy. For example, if an organization is functioning at a loss and has no budget for any model to be implemented, then it is not possible to devise any such strategy. This will only waste the organizations time, thus, it is required to have the necessary sources for the purpose of effective implementation of the model to ensure the safety of the organization assets. With regard to financial resources, there are several other factors that need to be considered.

The use of ISRM is essential in every industry. But it is more important in the health industry. This industry is facing huge pressure to reduce costs and improve healthcare quality. There is also a need to ensure patient safety by reducing the mistakes that are committed by healthcare providers. These mistakes can be in the form of delivering the wrong services and not following the correct prescriptions. Thus, to achieve the above objectives, the use of ISRM is essential in every industry. It is a structured and continuous process that removes the risks and achieves the objectives effectually. As it is a continuous process, it effectively addresses all the issues that come in the form of information security, as information security risks are not constant over time. This is because the conditions of the organizations continuously change, and thus, the information assets of the organizations, as well as associated risks and solutions, also change. This also provides the opportunity to focus more on high-risk areas. ISRM is such a practice that lessens the overall risks adhered to in the organisation's structure of the information assets. This is also effective in terms of the cost-benefit analysis of the implementation.

Reliable ISRM signifies a major trial for organizations, as effective data is needed to enter the system for the purpose of generating effective decisions. This is because the structure and type of information technologies have altered extremely over the last period. The simple separate batch requests changed into dispersed computing surroundings. These changes are responsible for the nature of security risk analysis and its control.

References

Aarts, J., & Koppel, R. (2009). Implementation of computerized physician order entry in seven countries. *Health Affairs*, *28*(2), 404-414.

Abbass, W., Baina, A., & Bellafkih, M. (2016, October). Improvement of information system security risk management. In *Information Science and Technology (CiSt), 2016 4th IEEE International Colloquium on* (pp. 182-187). IEEE.

Ayatollahi, H., & Shagerdi, G. (2017). Information Security Risk Assessment in Hospitals. *The Open Medical Informatics Journal*, *11*, 37.

Blakley, B., McDermott, E., & Geer, D. (2001, September). Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 97-104). ACM.

Bornman, W., & Labuschagne, L. (2005). A Framework for Information Security Risk Management Communication. In *ISSA* (pp. 1-11).

Fenz, S., Ekelhart, A., & Neubauer, T. (2009, September). Business process-based resource importance determination. In *International Conference on Business Process Management* (pp. 113-127). Springer, Berlin, Heidelberg.

Gupta, S., & Saini, A. K. (2013). Information System Security and Risk Management: Issues and Impact on Organizations. *Global Journal of Enterprise Information System*, *5*(1), 31-35.

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *information security technical report*, *13*(4), 247-255.

Jha, A. K., DesRoches, C. M., Campbell, E. G., Donelan, K., Rao, S. R., Ferris, T. G., ... & Blumenthal, D. (2009). Use of electronic health records in US hospitals. *New England Journal of Medicine*, *360*(16), 1628-1638.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management*, *41*(5), 597-607.

Naseer, H., Shanks, G., Ahmad, A., & Maynard, S. (2016). Enhancing Information Security Risk Management with Security Analytics: A Dynamic Capabilities Perspective.

Shedden, P., Smith, W., & Ahmad, A. (2010). Information security risk assessment: towards a business practice perspective.

Stroie, E. R., & Rusu, A. C. (2011). Security Risk Management-Approaches and Methodology. *Informatica Economica*, *15*(1), 228.

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security*, *44*, 1-15.