Technology information security and risk management research paper sample

Business, Management

Information security signifies information protection from aspects that result in modification, usage, access, and perusal without permission. The main principles of information security are non-repudiation, availability, integrity, confidential and authenticity. Similarly, risk management relates to information security and is referred to as evaluation, mitigation and assessment of risks. Risk management ensures that ICT supervisors can evaluate the costs of using protection measures in information management while achieving gains in a manner that supports the business goals. The paper explains the issue of information security and the main principles that are concerned with it. The issue of risk management and the steps that should be followed so as to accomplish the risk management analysis is also described. In the risk management there are risk assessment process and the risk mitigation process. Therefore, through effective risk management, individuals and organizations can effectively manage occurrences of information insecurity.

Information security refers to the protection of information from agents that can disclose, disrupt, peruse, modify, inspect, use, or access it in an unauthorized manner. Since the current advancements started to take shape across the globe, there has been an increased need to ensure that data and information is protected in every possible way. In many institutions such as the government, banks, hospitals, military and private ventures, the issue of information security seems to have been given a great consideration whenever confidential and private data is being processed. There are many instances where information security can be compromised during collection, processing, storage, and transmission. In most cases, people take

information security as a legal, ethical and business requirement since any reckless disclosure of information may lead to numerous negative effects. This is why there is a need to understand the risk management strategies that are used to minimize the occurrence of instances that can lead to insecurity of information.

The following paper explains the issue of information security and the main principles that are concerned with it. It also describes the issue of risk management and the steps that are followed so as to accomplish the risk management analysis. In the risk management part, it explains the risk assessment process and the risk mitigation process. Through effective risk management, individuals and organizations can effectively manage occurrences of information insecurity.

Basic concepts and principles of information Security

Information security became an important issue during the early days of writing when presidents and military officials found it crucial to maintain confidentiality and privacy of sensitive correspondence. It was important for them to ensure that their secrets and all information regarding their operations were protected in all ways possible. This is because the consequences of tampering with sensitive information would negatively impact on a country’s security. This is the reason as to why Julius Caesar, a 50 B. C historian, invented a method of encoding his corresponding by the use of what is commonly known as Caesar cipher (Chen, 2010). The secret correspondence that came up during World War II became a basis for the current information security profession. Many advances were made as

countries and world powers tried to outdo each other in the war. Every country wanted to have a system that would ensure their success by protecting their military information and secrets from their enemies (Chen, 2010). Lastly, 20th century and 21st century saw the advancement and development of telecommunications, internet, and electronic data processing that would require advanced information protection. Terrorism and other threats increased the need for the whole world to be strict on information security, and academic and professional institutions emerged to ensure security of information systems.

Confidentiality

Confidentiality is a principle of information security that deals with how well information can be protected from unauthorized disclosure. Confidentiality of information is usually done by limiting of information access. To ensure that confidentiality of information is maintained, various authentication methods are used to deny access or limit access to individuals and systems that can be harmful. In most cases, information is usually protected by the use of passwords and identification numbers that are effectively used to identify the authorized persons (Goodman, 2008). Passwords are used in e mails and other authorized logins so as to limit and control access to various computerized systems and supports the objective of data confidentiality.

Integrity of information

Integrity of data or information refers to the assurance that individuals and systems get about the authenticity and completeness of information from the origin, through the transmission and reception. Integrity of data means

that the information contained in a system can be trusted and relied upon as totally accurate as it is supposed to be. Basically, integrity is one of the main indicators of how secure information is under any circumstances. Information resources and systems should always be trustworthy and reliable so that they can be used for the purpose that they had been created for (Goodman, 2008). In some instances of information insecurity, data may be changed inappropriately either accidentally or intentionally, and whichever the case, the integrity of such data will be considered as compromised. Integrity also refers to validity of data as either right or wrong, and information systems should be created in such a way that the data remains valid during processing and is not changed on transit.

Availability of Information

Individuals and organizations do agree that for information to serve its purpose, it must always be available when needed. Availability is a principle of information security that states that information storage systems, processing systems, security systems and transmission systems must be working property to ensure sufficient security of all information and data. There is no individual or organization that would like a system that is never available whenever they need it. In most cases, availability of information systems may be affected by problems such as natural disasters, hardware malfunction, intentional sabotage or accidental causes. Therefore, availability of information is a vital principle of information security since it ensures that data is processed, stored and delivered to the right people whenever it is needed (Chen, 2010).

Authenticity of Information

Authenticity is an information security principle that deals with how sure the receiver is about the origin of the data or document. Authenticity usually deals with such things as messages, e mails, transactions, documents and other forms of information exchange. Authenticity is usually verified by the use of passwords, key cards, finger prints and other types of biometric authentication methods. Sometimes it seems hard to ensure authenticity of information since nowadays there are systems and individuals that can crack some passwords especially if the password is weak. That is why there has been an emphasis on the use of strong passwords and a greater use of a larger number of proofs of identity. It is also crucial for one to note that sometimes passwords can be forgotten or even stolen, meaning that there is a need to be careful with passwords and other digital certificates (Vladimirov, 2010).

Non repudiation of information

Non repudiation is a principle of information security that assures all parties that the sender gets proof that the message is delivered, and the recipient obtains sender’s identity such that both parties cannot deny the transmission of data or information. The process takes place in such a way that a third party can validate and verify the origin of the said data and its integrity. Non repudiation ensures that individuals or organizations can not deny that a certain action took place if indeed it did, especially in issues dealing with sending of data, approving actions and receiving of information

(Spears, 2010). In this case, origin of data and its integrity can be traced by the use of public keys, digital signatures, and certificates.

Risk Management

In information security, risk management includes risk assessment, mitigation, and evaluation (assessment). The process of risk management ensures that ICT supervisors can evaluate the costs of using protection measures in information management while achieving gains in a manner that supports the business goals.

Risk Assessment

Risk assessment is usually the first process during the task of risk management. Risk assessment is usually used to determine the number of potential threats that can be traced in information systems and the corresponding risk associated with ICT systems (Spears, 2010). There are nine steps that are found in the risk assessment process.

System Characterization

System characterization refers to the definition of scope for the analysis, whereby all boundaries of the present ICT systems are determined together with all available information resources. This step provides vital information about all software, hardware, support persons, data flows, networks, system interfaces, system processes, data criticality, data sensitivity, physical security, operational controls and environmental security that is essential in defining the scope of the risk. All these details should be taken from all operational IT systems, and for those systems that are under development,

all security attributes planned for the future should be incorporated in the risk scope.

Threat Identification

Threat identification deals with the possibility of a threat to successfully utilize a given vulnerability. Any vulnerability found in an IT system can be referred to as a weak point that could be intentionally or accidentally triggered and exploited to cause a negative consequence (Antón, 2003). Threats can be categorized as natural, human, or environmental depending on the potential source. Natural threats include earthquakes, floods, storms, landslides, and tornadoes. Human threats refer to events that are triggered or caused by human activities. For example, support personnel may deliberately or accidentally do actions that may compromise information security such as access to unauthorized information or upload of malicious programs. Environmental threats may include those factors that include pollution, liquid leakage, power failure and such environmental issues. Human threats are the most common including hackers, terrorists, industrial espionage, insiders, and computer criminals.

Vulnerability identification

During risk assessment, it is important to examine all vulnerabilities that are associated with the IT systems. The vulnerable points in an IT system refer to the potential flaws and weaknesses that are likely to be exploited by the threats- agents. In a system, a weakness could be noticed in the process design, implementation, security procedures, and other system controls that can be used by a threat source, causing violation of information’s security

(Antón, 2003). For example, vulnerabilities could include terminated employees in an organization or an enabled guest ID on XYZ server.

Control analysis

At this point, all controls for the operational systems are analyzed in order to reduce the possibility of any breach of security in IT systems. In the systems that are still under development, the control systems that are planned for implemented are also analyzed for the same reason (Sumner, 2009). The control methods used can be utilized in dealing with either technical issues (hardware, software, and firmware) or non-technical issues (personnel, environmental). Also, the analysis can be used to do preventive controls (encryption, authentication) or detective controls (audit, checksums), aimed at preventing and detecting any threat, threat source or vulnerability.

Likelihood determination

According to Fenz , (2010), it is crucial to examine the likelihood that a given vulnerability may be exploited by a threat source. The main factors that should be considered during likelihood determination can be said to be the nature of vulnerability, capability of the threat source and effectiveness of the available controls. Once evaluated, the likelihood for each threat source is categorized as high, medium or low.

Impact Analysis

After rating the likelihood as ether high, low or medium, the next step should be the impact analysis, whereby an estimation of the impact of a successful exploitation of a threat is determined. In order to do an efficient impact

analysis, it would be important to consider three factors namely the system mission, system criticality and system sensitivity. Such data can be retrieved from existing documentations and assessment results based on qualitative and quantitative analysis of assets. In order to measure the impact of a threat exploitation, the issue must be considered in the terms of loss of data integrity, loss of availability, loss of confidentiality or loss of a combination of two or more of the given data degradations. Other quantitative measures can be measured in terms of lost profits, repair expenses or the level of efforts needed to correct the exploited state of IT systems.

Risk determination

Risk determination examines the level of the current risk in terms of the thereat likelihood, impact magnitude or adequacy of the current controls. A risk level matrix is usually used to analyze the risk by getting the product of threat-likelihood ratings and the corresponding impact. The risk level is then described in a matrix, whereby all the levels are denoted by high, low or medium. At this point the description is given a description of the risk scale and the necessary actions required to solve the problem such as taking up corrective measures (Bulgurcu, 2010).

Control Recommendations

At this point, controls are identified so that they can be used to mitigate or remove the risks that have been identified. The main objective of recommending control measures in the IT systems and information is to ensure that the level of the risk is significantly minimized to acceptable

levels. This can be achieved through legislation, regulation, policies, safety, reliability, operational impact and effectiveness of recommended options.

Results documentation

At this stage, the results are documented as an official report that can guide the management, budget allocators and others who are involved in policy making and implementing changes. This report does not state wrong doings, but it analyzes the assessment of risk so that senior managers can be in a position to allocate the appropriate funds to minimize or remove all potential problems associated with information security.

Risk Mitigation

Risk mitigation is another important process in risk management, involving prioritization, evaluation and implementation of the recommended controls from the risk assessment process. According to Spears, 2010, it is important for individuals and organizations to understand that it is practically impossible to remove all potential risks in IT systems. The only approach that people should use to minimize the impact is to select and implement the least expensive and most appropriate methods of controlling the risk to acceptable levels. The method should involve the least expensive method so as to ensure that the risk management process does not impact negatively on an organization’s finances and resources.

There are several mitigation-options that can be used by the management to mitigate the risks involved in security of IT systems. Risk assumption is the first mitigation option that seeks to accept the available risks and go ahead with the normal IT operations. Risk avoidance refers to practically avoiding

all risks through elimination of risks and their consequences. Risk limitation is the other option that can be used in risk mitigation so as to limit the risk through minimization of the negative impacts. The other option is called risk planning, and it is meant to manage risk through an effective prioritization, implementation and maintaining of the required controls. Also, research and acknowledgement can be used as an option to lower the risks and learn more about the controls. Risk transference is also important measure of transferring a risk by the use of other possible options like buying an insurance policy for the risk.

Assessment, evaluation and control

There is a basic approach that ensures very effective control implementation during the process of mitigation. The first step involves the prioritization of actions such that resources are first allocated to items with high risk levels. The next step is the evaluation of the recommended control options, so as to assess the most feasible and most appropriate options. The other step is to conduct a cost- benefit analysis so that the management can make the appropriate decisions regarding the cost effective measures to be taken. After a through cost- benefit analysis, a control method should then be selected by considering the technical, operational and management aspects of the risk mitigation. At this point, the personnel or staff for carrying out the tasks are chosen and assigned various tasks. After assigning of responsibilities, a safeguard implementation plan is created so as to give prioritization tasks and project scheduling dates. After all these steps are

successfully completed, the cost- effective and most appropriate control is implemented so as to minimize or eliminate risks and threats (Fenz, 2011).

Conclusion

The above paper has explained the issue of information security and the main principles that are concerned with it. It has also described the issue of risk management and the steps that should be followed so as to accomplish the risk management analysis. In the risk management part, it has explained the risk assessment process and the risk mitigation process. Through effective risk management, individuals and organizations can effectively manage occurrences of information insecurity. The main principles of information security are non-repudiation, availability, integrity, confidential and authenticity. In most of institutions across the world, with the current high rates of technological advancements, the issue of information security seems to have been given a great consideration especially in instances of confidential and private data is being processed.

There are many instances where information security can be compromised during collection, processing, storage and transmission. Risk assessment is usually used to determine the number of potential threats that can be traced in information systems and the corresponding risk associated with ICT systems. Risk assessment is usually used to determine the number of potential threats that can be traced in information systems and the corresponding risk associated with ICT systems. There is several mitigation options that can be used by the management to mitigate the risks involved in security of IT systems. These mitigation factors include risk avoidance, risk

assumption, risk limitation, risk planning, risk transference and research. This way, the management can choose the best control methods aimed at minimizing risks, threats and vulnerabilities.

References:

Antón, P. S. (2003). Finding and Fixing Vulnerabilities in Information Systems : The Vulnerability Assessment & Mitigation Methodology. Rand.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523-A7.

Chen, P., Kataria, G., & Krishnan, R. (2011). correlated failures, diversification, and information security risk management. MIS Quarterly, 35(2), 397-A3.

Fenz, S., Ekelhart, A., & Neubauer, T. (2011). Information Security Risk Management: In Which Security Solutions Is It Worth Investing?. Communications Of AIS, 2011(28), 329-356.

Goodman, S. E., Straub, D. W., & Baskerville, R. (2008). Information Security : Policy, Processes, and Practices. M. E. Sharpe.

Sumner, M. (2009). Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness. Information Systems Management, 26(1), 2-12.

Spears, J. L., & Barki, H. (2010). user participation in information systems security risk management. MIS Quarterly, 34(3), 503-A5.

Vladimirov, A. A., Michajlowski, A. A., & Gavrilenko, K. V. (2010). Assessing

Information Security : Strategies, Tactics, Logic and Framework. IT Governance Publishing.