Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

Holistic Approach to Information Security Risk Management

Pratik Sawant
IT Advisory Risk Consulting
KPMG
Pune, India.

***Abstract*– Risk management is a very important area in information security. Risk management comprises of risk identification, risk assessment and risk treatment. Risk identification on current security infrastructure helps organizations to reveal vulnerabilities, threats and identify the risks that these two factors pose to their security infrastructure. Risk assessment helps in analyzing the identified risks using aspects like probability and impact and risk treatment helps in reducing the impact of the risks to an acceptable level [1]. Risk management is mandatory requirement of ISO 27001:2013 and ISO 22301:2012 standards and the organization going for these certifications must comply with it. The eventual goal of a risk management activity is to define appropriate safeguards tailored to your company's risk profile and priorities. Risk management activity usually precedes and help define audit plans and facilitate the development of a corporate security plan. Qualified team members from information security department of an organization perform risk assessment at predefined period or after any change to provide reasonable assurance to the top management about the organization's risk profile. Risk management allows organizations to adopt security strategies that are tailored to their unique operating environment, threat landscape and business objectives. Risk-based security strategies deliver value to an organization by allowing it to understand the impact of risk and the efforts required to mitigate the risks. These security strategies help organizations in complying with regulations, thwart security attacks etc. Risk-based security strategies may differ markedly from the approaches currently adopted by many organizations.**

Keywords*– *Threats, Vulnerabilities, Risk Assessment, Security Strategies.

I. RISK IDENTIFICATION.

Risk identification is the process of identifying information security risks. Risk is a possibility of something bad happening which may have negative consequences on the organization. Risk identification has two important components which are identification of vulnerabilities and threats. Vulnerabilities are weakness or gaps in the security infrastructure [2].

Vulnerabilities can be technical or gaps in security procedures. Examples of technical vulnerabilities can be absence of antivirus software, unrestricted access to users, absence of security guards etc. Examples of vulnerabilities in organizational process are criminal check not carried out in background verification process, change management process not in place for managing changes to the critical IT infrastructure etc.

Threats are the factors that exploit the vulnerabilities. Threat can also be any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations. Examples of threats are disgruntled employees, hackers, fire, natural disasters etc.

Risk is the negative consequence or impact that arises when threat exploits vulnerability.

Risk Statement - There is a risk of fire at the company premises if additional fire extinguishers are not deployed which may result into damage to the infrastructure and injuries to the employees. In the above risk statement, fire is the threat which exploits the vulnerability of lack of fire extinguishers and imposes negative impact/consequences of damage to the infrastructure and injuries to the employees on the organization. It is recommended to carry out risk management on an annual basis or if there is any change in the security posture of the organization.

II. RISK ASSESSMENT.

Risk assessment is the process of analyzing the risks. Probability or likelihood and impact or severity is the critical factors that need to be considered while analyzing the risk. The total amount of risk exposure is the probability of an unfortunate event occurring, multiplied by the potential impact or damage incurred by the event.

$$Risk = Probability \times Impact \qquad (1)$$

Probability is the likelihood of threat exploiting a vulnerability in given time period. More the probability of threat exploiting a vulnerability greater the risk value. Similarly, impact is the severity of the consequences that the organization will have to face if the risk materializes. If the severity of consequences is more then it also increases the risk value. Below tables give the quantitative view of the impact (severity), probability (likelihood) and risk.

Likelihood/Probability Rating	
Almost Certain - 4	Chances of threat exploiting this vulnerability are common and are expected to occur in most circumstances.
Likely – 3	Chances of threat exploiting this vulnerability are high.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

Moderate - 2	Chances of threat exploiting this vulnerability are low to moderate. There is a reasonable probability that this threat shall manifest.
Unlikely - 1	Chances of threat exploiting this vulnerability are low.

Table 1.0 - Likelihood/Probability Rating

Impact/ Severity Rating	
Severe - 4	A risk event that, if occurs will have a severe impact on achieving desired results, to the extent that one or more critical outcome objectives of an organization will not be achieved.
Very High - 3	A risk event that, if occurs will have a significant impact on achieving desired results.
High – 2	A risk event that, if occurs will have a moderate impact on achieving desired results.
Low – 1	A risk event that, if occurs will have a minor impact on achieving desired results.

Table 2.0 – Impact/Severity Rating

The impact can further be specified in a context that is relevant to the business objectives of the organization such as financial impact, customer/client impact, reputational impact and regulatory impact.

Impact/Severity	**Risk Rating**			
Severe (4)	4	8	12	16
Very High (3)	3	6	9	12
High (2)	2	4	6	8
Low (1)	1	2	3	4
Probability/Likelihood	Unlikely (1)	Moderate (2)	Likely (3)	Almost Certain (4)

Table 3.0 – Risk Rating

Severe Risk (12-15)	Discontinue operation and /or immediate corrective action required.
Significant Risk (8-11)	Corrective action needed. Action to be taken in short term as appropriate.
Moderate Risk (4-7)	Attention required.
Minor Risk (1-3)	Implement practicable short-medium term control measures.

Table 4.0 – Risk Description

It is recommended that information security team to draft the identified information security risks in the risk assessment report/template.

III. RISK TREATMENT

Controls must be identified and implemented to mitigate the identified risks. Identification and implementation of controls will involve cost benefit analysis. Cost benefit analysis will ensure that cost of implementing the controls do not overshoot cost incurred after risk materializing. Different types of controls are **Detective controls Preventive controls and Corrective controls** [3].

Detective controls (e.g. – Intrusion Detection System) will detect the threat in advance and alert the administrator so that threat can be eliminated before exploiting the vulnerability. Preventive controls (e.g. – CCTV cameras, Access controls) will prevent the threat from entering the system with their presence. Corrective controls (e.g. – Audit Trails) are used to conduct root cause analysis so that the threat doesn't exploit the vulnerability again.

The different types of risks involved in a risk assessment activity are **Inherent risk, Gross risk, Net risk and Residual risk.**

Inherent risk is the risk that is raw or untreated. Inherent risk value is derived by assessing the risk without taking any efforts to reduce the likelihood or impact of the risk. **Gross risk** is the risk value derived by assessing the risk after taking into consideration the existing controls that are in place to mitigate the risk. **Net risk** is the risk value derived by assessing the risk after implementing new controls to further mitigate the risk. **Residual risk** is the risk that remains after treating the risk since in an ideal condition risk cannot be eliminated.

To treat the risks, organizations must identify an acceptable value of risk. The acceptable value can be derived by assessing the information security posture of the organization, client/customer requirements, Regulatory requirements and top management thought process. Risks having net risk value lower than the acceptable value can be accepted. Organizations must ensure that the residual risk value is lower than the acceptable value. Risk treatment involves risk treatment plan. Risk treatment plan consists of options to treat the risk like risk acceptance, risk avoidance, risk mitigation and risk transfer.

Risk acceptance is admission or approval on the risk by the management. If the risk is accepted, then it does not require further treatment or mitigation. Such risks can only be monitored on a periodic basis. **Risk avoidance** is rejecting the activity, project etc. that comes with significant risk value. Organizations reject/avoid certain activities, processes and projects that have significant risk associated with them that can posses' threat to the objectives of the organization. **Risk Mitigation** is treating the risks by implementing new controls so that likelihood and impact are reduced to an acceptable level. **Risk transfer** is transferring the risk to a third party so that cost/impact incurred after the risk materializing can be recovered. Insurance is an example of risk transfer. CISO and head of the departments shall be consulted before proceeding with the risk treatment plan.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

IV. CONCLUSION

In this paper we have presented the overview of risk management activity which includes risk identification, risk assessment and risk treatment. Elements used in risk identification were threats and vulnerabilities. Factors used for risk assessment were likelihood and impact. We have presented a quantitative view of these factors. Impact has been specified in a context that is relevant to the business objectives of the organization. Different types of information security controls, and information security risks are discussed in detail. The paper also provides a holistic approach for treating the risks with multiple treatment options. The observations and strategy discussed in this paper can be extended to many other fields or can be customized as per the requirements of the organization.

V. REFERENCES

[1] eSecurity Solutions, "SECURITY RISK ASSESSMENTS WHITE PAPER", August 2019.
[2] CDW, "MOVE TO A RISK BASED SECURITY STRATEGY", June 2017.
[3] NIST, "Risk Management Framework for Information Systems and Organizations", December 2018.