Preventive vs Detective vs Corrective Security Controls

Prakash Choudhary[1], Rajeshwari Gundla[2], Siddharth Nanda[3]
[1]U.G. Student, [2]Faculty, [3]Senior Faculty
SOE, ADYPU, Lohegaon, Pune, Maharashtra, India[1]
IT, iNurture, Bengaluru, India[2,3]

Abstract **-** This paper involve Security controls type. Security controls help reducing risk in an organization and also exam expects . To understand security controls there are two perspective their goals and how they are implemented. Based on that there are three-part post which focuses the initial two post consists the goals of security controls and implementation method is the last post. As security controls alluded to countermeasure or safegaurds to reduce vulnerabilities. In particular, security controls endeavor to avoid or confine the effect of a security episode.Security controls depends on their objectives in relationship to security episodes. Some basic grouping are Preventive, Detective, Corrective.

Keywords **-** Security controls, goals, implemented, countermeasure, safegaurds, Preventive, Detective, Corrective

I. INTRODUCTION

These type of controls is used for protect the information of an organization, people, and other assets. It is important that sensitive data should be protected in view of potential effect of lost secrecy, trustworthiness. Security controls will in general fall into two classification. To start with security shortcoming in the framework should be settled.[2] For instance if a framework has a known powerlessness that assailants could misuse, the framework to be fixed with the goal that the weaknessis removed. Second, the framework should offers just the expected usefulness to each approved client, with the goal that nobody can utilize capacities that are redundant. In today's time security controls are not insufficient. Many technologies are use to secure information but still some facilities is not enough. For example mechanical locks are having vulnerabilities due to that it has an risk to an data ,it is more effective and more cheaper to exploit them. Where attackers utilize distinctive methods to decode and practice to find vulnerable from any location using the technologies. This paper will conclude preventive, Detective, Corrective.[2]

II. SECURITY CONTROLS TYPES

1. Preventive Controls: These are the controls which prevent loss from occurring. So when we plan to use a preventive countermeasure we has to be secure from malicious action from occurring by blocking or stopping something from causing our data. Some example of preventive controls are: Security gaurds, Strong authentication, Intrusion prevention system IPS.[1]

2. Detective Controls: These controls are especially for the monitoring activity to discover the case where correct practices where not followed. Detective countermeasure are executed to distinguish any pernicious exercises. Some example of detective controls are: Alarms, Video surveillance, Motion detectors.[1]

3. Corrective Controls: Corrective controls are designed to re-establish the framework back to state preceding a destructive event. Example of corrective controls are: Restoring operating system or data from a recent back up, Installing fix.[1]

Advance persistent threats usually target victims at user's end using social designing method attack that are usually more effective because they are targeted with knowledge gathered from long range interpersonal communication destinations. It is possible that hacker will search for information readily available on the internet to find individual victims and organisational roles to target. They do this in order to gain knowledge of organisational arrangement, internal working and eventually to target people they trust will potential approach to a own the most delicate. For example If a gathering of individual want to target victim who is handling sensitive credit report information within an organization , they may watch your organization on business websites such as LinkedIn or to discover the finance manager's name. Once the hacker knows the name of a potential victim, they will add the victim name to the rundown of targeted individuals when they decide to launch the social engineering attack

III. IMPORTANCE OF PREVENTIVE, DETECTIVE, CORRECTIVE SECURITY CONTROLS

This paper highlight the importance of effective security controls that can be avoid, detect, limit security hazard to physical property, data, PC framework or other assets. Where in the field of information security such control protect confidentiality, integrity and availability (CIA) of information. As these 3 control i.e. preventive, detective, corrective are against security controls. It is very important but it is usually overloaded by most organization. It is necessary an event that you don't need anyone to snatch away your information or destroy it, in case of physical access. The reason could by anything, the attacker doing it for personal gain, financial gain, for seeking revenge or you were the vulnerable target available. If these security isn't

kept up appropriately, all the well being estimates will be pointless once the assailant gets past by increasing physical access. These controls ensure that security incidents does occure that it is to be settled as quickly as possible.

IV. LITERATURE SURVEY

All these security controls survey involves that risk is unavoidable in organisation and other assets. Due to flexibility in the internet connection. However security professional need too ensure that the risk are kept to a minimum. [4] The aim of risk management is to reduce the potential of any internal or external risk. Where risk management gives a framework for an organisation to deal with and to react to uncertainties. Where an organization management identifies any risk from threats, the management allows the information technology and information security team to work on such risk. [5] Once the information security development team creates the ranked vulnerability worksheet, the team chooses one of the risk control strategies to control the risk. Information system controls also play a vital role to ensure secure operations of an information system. Where information system controls are established to ensure that the business applicationsachieve their objectives in an effective manner. An organisation also needs to form a set of policies, procedure and technological measures.

V. COMPARISON TABLE

Preventive	**Detective**	**Corrective**
Prevent problems from occurring	Alert manager where preventive controls fails	Solve or correct a problem
It occure before an attack	It occure during an attack	It occure after an attack
Example is security awareness training for all users	Example is installing motion detection sensors	Example is a virus is cleaned from an infected server

VI. DISCUSSION AND FUTURE WORK

In this paper it has been understand the implication arising from privacy and security controls help design a more secure and useable information system. [2] By adopting the three security control measure of preventive, detective, corrective control as a guide in proposing privacy and security control solution a more hosted solution can be achieved.

1] Preventive control is designed to prevent organization before it can happen. The most common thing in preventive control is password andconfirmation measures. The main aim of confirmation measures is to access to information and data to authorized person only and traditionally authentication measures require users to key in their username and password in secured login form.[3]

2] Detective control is respond during the occurrence of an event. When an organization is dected, so detective control identify and classify the incident progress. Mostly it should use antivirus software. Where antivirus software may not be as effective as the following system. Which work best in detecting and preventing intrusions of an organization.[3]

3] In corrective control where an organization is discovered after a event has ended then corrective control measures has been limit the user of any harm brought about by any incident. This type of control is recovered to ordinary working state. Which will be more efficiently and be more secured. [3]

VII. CONCLUSION

In this paper the primary target depends on security problem that has been discussed for an organization behave like their opponent and understand that it is any loophole that can be used against their organization and that a decided assailantwill stop at not to find a technical vulnerability to exploit or determine where loopholes exist in an organization.

VIII. REFERENCES

[1]. Osop, H. and Sahama, T., 2016, September. Quality evidence, quality decisions: Ways to improve security and privacy of EHR systems. In *2016 18th International Conference on e-Health Networking, Applications and Services (Healthcom)* (pp. 1-6). IEEE.

[2]. Bordel, B., Alcarria, R., Morales, A. and Castillo, I., 2018. A framework for enhancing mobile workflow execution through injection of flexible security controls. *Analog Integrated Circuits and Signal Processing*, *96*(2), pp.303-316.

[3]. Moses, S. and Rowe, D.C., 2016. Physical Security and Cybersecurity: Reducing Risk by Enhancing Physical Security Posture through Multi-Factor Authentication and other Techniques.

[4]. Ficco, M. and Rak, M., 2017. Security SLAs for Cloud Services: Hadoop Case Study. In *Reshaping Accounting and Management Control Systems*(pp. 103-114). Springer, Cham.

[5]. Marquardson, J. and Gomillion, D., 2018. Cyber Security Curriculum Development: Protecting Students and Institutions While Providing Hands-On Experience. *Information Systems Education Journal*, *16*(5), p.12.

[6]. Albadrany, A.O. and Saif, M.Y., 2018. Review on security challenge faced organization based on-cloud computing. *International Journal*, *7*(6).