Table of contents

Executive Summary

This report emphasizes on exploring the activities of monitoring and controlling of risk in the organizations regarding of the information security. It is very crucial for those companies which are handling clients' sensitive information and bearing a risk on their head from multiple threats. In this report the study will be focused on the "Ernest & Young "company which is one of the top most audit form providing services like Assurance, Tax advisory, consulting, financial advisory and legal advisory to many client companies throughout the world. In this process the report also addresses the risk control activities followed by the respective company, special policies or laws been implemented in order to gain the integrity of the customers or client companies. Thus, this report will be a guideline for many other audit firms and also the reader to know what is the monitory mechanism followed by the company to have protected information system.

As the company E& Y is having enough confidence in providing the secured information system. At present it has acquired the worldwide customers above 5000 client companies and employees more than 2, 00,000 people in this 10,000 of them are tax and advisory practitioners. Hence in depth analysis will be made on the information security system of the company E&Y (Ey.com, 2015). This assignment will be lesson to the reader to know the secrets behind the success of the company in maintaining the high grade security system and integrity among the people.

Introduction

It is well known facts that information system is a life blood for every organization specially the audit firms. No matter how large or small the company is but the information security is must and should to ensure the security of the information assets inside the company. Due to the raising demands and competition the audit firms are surrounded by multiple threats and risk. It is very essential to have special programs for providing security, handling risk, monitoring security mechanism etc. In this process the technology plays a key role in handling all those activities and resulting in the confidentiality, integrity and availability of the data to the customer's perception.

As in previous two assignments we have gone through the risk and threats identification regarding of the information security system in E& Y Company and somewhat strategies followed by the company to handle different types of security issues. But this part of the assignment helps in providing in-depth knowledge of the security programs handled by the E&Y in which controlling risk, protection mechanism done by using advance technology like software and internets will be considered. It also focuses on the E&Y Company's law and ethics, personnel involved in the process in order to give clear image of the information security system of the company.

Aim & objective of the research

The research aims to conduct in-depth analysis on the information security system in the E&Y Company. In regards of this aim the following are objectives set by me.

- To critically evaluate the risk controlling strategies and functions involved in the E& Y Company.
- To explain the risk control activity and mechanism of the protection through some conceptual framework and analysis.
- To identify different issues in company and suggesting the usefulness of the PRT monitoring in information security management.

Literature Review

Security Program of E&Y

A security program is the framework designed by the company to keep the desired security levels by controlling the risk, doing various mechanisms for providing protection to the information assets. Finally this program ensures to update the security practices and ethical practices involved in the organization in order to provide integrated information security system.

Risk Management in regards of Information Security System

Risk assessing, controlling and monitoring are the important activities done in the risk management process. The main aim of the risk management is to identify the vulnerabilities of the organization's information systems and taking proper actions to assure the confidentiality, integrity and availability of all components internally and externally to the organization (Enisa.europa.eu, 2015).

Before moving in to the topic of the risk controlling it is essential to know the issues arise in the company during the handling of the information. This will enables us to know the whistling elements which alert more towards the controlling of risk through various strategies. This is perhaps the important stage in the risk management because it might make you think and enables to take decision regarding the risk controlling measures to be taken so that the issues of threat will be minimized. The risks related to the information E& Y Company are basically been categorized as follows:

As E&Y Company is providing the services to many client companies in respective to the taxation and auditing, advisory services, and financial services so it has to engaged with maintaining multiple information of the company. There are various types of threats can be occurred in the organization. This includes the physical loss of the data due to the electric power, disk failure, and some other natural disasters (Ey.com, 2015). The information can be threatened due to the unauthorized access to the own data and client or customer's data. As the company possesses different company's confidential data so the possibilities of the threats are also high. There are also some type of risk occurs while transferring the data through internets, intranets, physical transferring to other locations etc. About the information in the electronic system it might be corrupted by intentionally but he external parties who get benefited. They might be using the key stroke loggers or Trojan horses software's on PC's to acquire the rival party's data and take advantage of those data. There are some more mistakes held as a part of the security issues like employees in the organization has loose lips that sinks ships. This means the spreading of the passwords of useful information to the outsiders (Appliedtrust.com, 2015) so in order to avoid all those security mistakes that occur in the organization, E&Y has adopted the following risk controlling strategies.

4 BASIC STRATEGIES OF RISK CONTROLLING

The company E& Y has faced information security threats inside the organization then it found the competitive disadvantages can be occurred in the organization. In order to control of the risk the company takes helps of the information security communities and information technology through the usage of various software and hardware to control and protect the risk. Here are some basic strategies applied by the company E& Y:

- ✓ Apply strategy
- ✓ Transfer the risk
- ✓ Reduce the impact
- ✓ Accept the risk without control or mitigation.

Apply strategy for Avoidance of risk:

Based on the Apply strategy of the risk control; it enables to avoid the risk through the exploitation of the vulnerabilities. It is one of the preferred approaches followed by the company E& Y because prevention of risk is better than that of the eradication of the risk. It accomplishes in taking counteracts to the threats involved in the information system inside the company. Ex: It identifies the employee’s behavior to find out the threats causing persons, providing trainings and motivational program to make employees feel satisfied and work with loyal. This strategy also enables to remove the vulnerabilities inside the organization; it means the threat causing elements or person should be removed from the organization. Ex: Some viruses attacked systems should not use for maintaining the information which is confidential and sensitive (Google Books, 2015). For this special policies will be applied by the company like providing training and development, ethical strategies application, using of advance technology to avoid disrupt data.

Transference of risk:

It is of the risk controlling approach followed by most of the audit and finance companies in order to shift the risk to other assets, other process or other organizations. This process enables the organization to provide the security to those organizations which has threat to their information system, does not have the good security management inside the organization. For those companies this approach will be suitable in handling the issues regarding the security. Based on this concept the companies will hire the external personnel or companies to take the responsibilities of providing expertise security for the information which is in electronically or physically (Ey.com, 2015). Basically, E&Y Company is very good in handling the information securely so many of the companies are having trust to transfer their risk in form of information. But it does not tie up with any companies to transfer their risk.

Reduce the impact through Mitigation

Mitigation strategy applied by the organization tends to reduce the impact of the exploitation through planning and preparing. According to this strategy there are three types of plans can be undertaken by the company i.e. Disaster recovery planning (DRP), Business continuity planning (BCP) and incident response planning (IRP). For long term risk handling the BCP will be suitable to the company. This action will be taken by the company while the incidence of threat is in progress. In order to use the control of the DRP it crucial to determine the level risk involved in the company, assess the probability of the risk, estimating the potential damage that could occur from attacks and taking the account of feasibility of other controls.

The DRP plan enables to recovery of the lost data, reestablishments of lost services etc. Ex: The corruption of the data can be back up by some software. The disruption of the physical data found can be mitigated by appointing trusted employees and security personnel on each level of the organization. The IRP strategy enables to analyze the information, gathering of the intellectual data in order identify the threats and take proper action accordingly. The advantage of outsourcing the company enables the company to concentrate on the own business strategy. The disadvantages of the strategy are the expensive services and need to have legal contracts to greater services and recovery (Google Books, 2015). The following of these strategies enables to protect the currently available data or assets by appointing extra personnel for providing information security personnel.

Different categories of risk control in E&Y Company

There are different types of risk control functions adopted by the company, based on the different levels of risk these are follows:

- **Control Function:** The controls and safe guards which re designed based on the vulnerability level of the risk involved in the information security system. The prevention or detection are been done on the basis of the adoption of the technology, enforcement of the policies.
- **Architectural layer:** The risk of information security applied to more than one layer of the system of the organization. Ex: Using firewalls in the network structure.
- **Strategic control:** The risk which can be controlled by adoption of the policies, strategies and ethical practices inside the organization (Ey.com, 2015).

As per the analysis the company E&Y are presently implementing all the above categories of risk controls in the organization.

Personnel & Security at E&Y

The company E& Y has a good framework for the efficient security system for confidential information. It leverages the security system by taking the help of the technology and also the human personnel. There are some special personnel employed for the organization to monitor and control the risk of handling information, it also engaged with using some PRT monitor software to assure the security of the information which is the form of the electron.

In the process of enabling the mechanism of the protecting the information the special committee was being appointed namely the security committee. This committee has been headed by the chief security officer. Under this authority there are two branches involved in it , i.e. information security manager and local security committees are present. The main role of the information security managers involves in making policies and providing some security against the threats of the rival parties. In this process he maintains the security technology to assess the security system in the organization by much software includes the PRTG software of monetary control of the information system (Ey.com, 2015).

Beyond that there are many security personnel involved in the security committee of the organization which includes security analyst who assures the policies and requirements of the organization in order to meet the functions of the organizations. He also enables to apply new process and technology to the organization. He is also responsible for designing and implementing new security technology in the organization.

The local security committees present in the organization responsible for directing the employees. The committee engages with handling the local security issues and provides the full fledged information system in the organization (Ey.com, 2015).

PRT Network monitoring

PRTG Software Used by Security administrators of the E&Y security committee. This software really works as a tool for implementing a protection mechanism to the electronically information present in the organization. There are many benefits of using this tool by the E&Y. Company; this will be discussed in the next section:

- **Trust Worthy to many security administrators**

The PRTG software enables to protect the key information about the organization through network monitoring system providing 24/7 services to the clients. It is being used by 1, 50,000 administrators world widely every day. This software is available in nearly 10 languages globally (Paessler.com, 2015). It monitors various network devices which include bandwidth, servers, application, virtual environment and remote systems LoT and much more. This software monitors LANs, WANs, different servers, website, appliances, URL's etc. It avoids the problems relating to the network when business is in emergencies. The clears the problem of network goes down, employees can't able to read emails, customers facing troubles to get the information about the parent companies etc. The network monitoring helps in avoiding expensive outage, address the bottlenecks the problem has caused. It helps in reducing the cost of the hardware that needs to be implemented for controlling the risk of the information.

- **Band Width Monitoring**

This feature tends to monitor the firewall traffic and collects various information regarding to the usage of the machines, software and devices. It simply maps out the network usage of the current company. So it will be evidence of many issues incurred in the business and shows the past performance and helps in taking actions and decision based on it. It also finds out who is using the data so it will be easy to find out the information which was hacked by the external personnel. Hence, proper action can be taken in the process of the organization. It supports multiple protocols for collecting the data ex: Packet sniffing, Netflow, Jflow, Sflow etc.

- **PRTG as a sensor alarm**

PRTG software not only monitors but also helps in giving warnings for various issues related to the systems and networks. It is connected with more than 200 sensor types for all types of common network services including HTTP, SMPT/ POP3, FTP etc. It monitors and detects the problems regarding of the URL, the traffic of the network connection, a port of the switch and load of the CPU on the machine. This software also helps in monitoring the services provided by the outsourcing personnel in the company and also enables to print the report on the performance. Hence this software used by the audit company enables to monitor the performance of the information holders and decreases the burden of the security personnel inside the organization (Paessler.com, 2015).

- **Fair price based on the package**

The use of this software will enable to provide fair price and also offers many other services which includes customer services and take necessary guidelines about the suitable services for a specific company. Based on the package of the sensor offered by the company the price will differentiates. The sensor packages start from the 500 to 2500 sensors. The customer service provides the information related to the next up gradation of software and enables to have an extension of the services based on the demand of the users.

Laws & Ethics

As we know the security plays a big role in any audit or financial firms which is running with various E-commerce and internet. As the technology grows the evils in business also increasing in a drastic manner so the following discussion will be made various issues faced by the legal system in maintaining the updated technology and few laws will be discussed in regards of the computer crimes in the UK. There are various laws followed by the E&Y Company in regards to the information security system. The employees appointed for the security purpose must have the global information assurance certificate or any other certificate has the ISO standard of 27001:2005. Based on this law the employees must fight for the information security principles toward accessing and controlling the risk of the information security system in an organization (SearchSecurity, 2015). Beyond that there are many other laws related to the data accountability and Trust and cyber security information sharing act are there which helps in protecting the confidentiality of the information.

An ethic is policies or standards that guide the human behavior in respective to the activities and decides what is wrong and what is written in an organization. Every company should follow the ISSA code of ethics in order to protect the information in the organization. Laws and ethics are correlated to each other without ethics the laws cannot be forced on any individual in the organization. As the internet began the started the issues and crimes related to that also began. So the growing technology is advantageous to the society, business, but at the same time it has the risk of that level. If the user forgets to follow the ethics and cause harm to many organizations in the way of causing theft of the useful information, blackmailing the people for gaining money in illegal ways etc (Sans.org, 2015). Such situation the laws of the information security will be helping the individuals.

Draw backs & Suggestions

From the analysis of the issue regarding to the information security and risk, protecting and monitoring it is clear that the decision of adopting new PRGT software is benefited to the organization. As every object has two sides advantages and disadvantages. So it is essential to take the pros and omit the disadvantages of the object. In this process the following are the disadvantages which have to be considered while adopting the PRTG software.

- The purchasing of the software is cost effective and needs continuous repayment in order to activate the sensors timely.

- As the company is providing services globally so it is suggestible that the number sensors used by the company should be above 1000 sensors. It will help in monitoring the whole network of the E&Y Company.
- The main drawback is that it is very complicated to obtain the license from the government on each monitoring sensors.
- The software download process is easy, but the real complaint here is that the configuration. PRTG boasts more than 80sensors. In this it is difficult for a company or an individual to determine which sensor applies to a specific device is difficult task. So in such case the PRTG auto discovery services provided by the company will be suggested to use.
- As manually adding device is pain full so auto discovery work is much better than the adding device manually (Aaron Leskiw, 2015).
- It is suggested to have a trial version of PRTG for 30days before purchasing the real one for the company.

Conclusion

As far from this analysis, it has been addressed that the information security system is essential for any organization which are maintaining the sensitive data. Maintaining the information security system , it requires a specific security committee to be appointed and policies and procedures, law and ethics to be concerned as the part of the risk control in the information system. It is suggested to use the PRTG software for the company which is engaged with many sensitive information in order to monitor and control the risk incurred in the process.

References

Aaron Leskiw, A. (2015). *Review: Paessler PRTG 8 Network Monitor*. *Network Management Software - Reviews & Network Monitoring Tools*. Retrieved 14 October 2015, from http://www.networkmanagementsoftware.com/paessler-prtg-8-review

Appliedtrust.com,. (2015). *Every Company Needs to Have an Information Security Program*. Retrieved 14 October 2015, from http://www.appliedtrust.com/resources/security/every-company-needs-to-have-a-security-program

Enisa.europa.eu,. (2015). *Risk Management & Information Security Management Systems â€" ENISA*. Retrieved 14 October 2015, from https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms

Ey.com,. (2015). *EY cited as a leader with â€œexceptional strategy" in information security consulting services*. Retrieved 14 October 2015, from http://www.ey.com/GL/en/Newsroom/News-releases/News_EY-cited-as-a-leader-with-exceptional-strategy-in-information-security-consulting-services

Ey.com,. (2015). *EY Cybersecurity*. Retrieved 14 October 2015, from http://www.ey.com/GL/en/Services/Advisory/EY-cybersecurity

Ey.com,. (2015). *Global Information Security Survey 2014 - Adapt: take a dynamic approach*. Retrieved 14 October 2015, from http://www.ey.com/GL/en/Services/Advisory/EY-global-information-security-survey-2014-adapt

Ey.com,. (2015). *Home*. Retrieved 14 October 2015, from http://www.ey.com/UK/en/Home

Ey.com,. (2015). *Risk appetite: the strategic balancing act*. Retrieved 14 October 2015, from http://www.ey.com/GL/en/Services/Advisory/Risk-appetite--the-strategic-balancing-act

Ey.com,. (2015). *2012 Global Information Security Survey - Fighting to close the gap - Unbalanced alignment*. Retrieved 14 October 2015, from http://www.ey.com/GL/en/Services/Advisory/2012-GISS---Fighting-to-close-the-gap---Unbalanced-alignment

Google Books,. (2015). *Information Security*. Retrieved 14 October 2015, from https://books.google.co.in/books?id=lpEsu3_sejwC&pg=PA111&lpg=PA111&dq=4+BASIC+STRATEGIES+OF+information+security+RISK+CONTROLLING+of+E%26Y&source=bl&ots=NH_ZDN897Z&sig=F-wYxz3RZOKqcxEpk9syJXysj1M&hl=en&sa=X&ved=0CE0Q6AEwCGoVChMIy-mrqIjByAIVhgeOCh09owx2#v=onepage&q=4%20BASIC%20STRATEGIES%20OF%20information%20security%20RISK%20CONTROLLING%20of%20E%26Y&f=false

Google Books,. (2015). *Proceedings of the International Conference on i-Warfare and Security 2006*. Retrieved 14 October 2015, from https://books.google.co.in/books?id=Zkdg632DVy0C&pg=PA21&lpg=PA21&dq=controlling+of+information+security+risk+through+Mitigation+of+E+%26+Y&source=bl&ots=Zw_VJSmUMz&sig=ikmvoD0Rw3SVNgBVHo1nqJ7yZdw&hl=en&sa=X&ved=0CD4Q6AEwBmoVChMIwuqto4nByAIVSB2OCh2yHAc2#v=onepage&q=controlling%20of%20information%20security%20risk%20through%20Mitigation%20of%20E%20%26%20Y&f=false

Paessler.com,. (2015). *PRTG Manual: Sensor Notifications Settings*. Retrieved 14 October 2015, from https://www.paessler.com/manuals/prtg/sensor_notifications_settings

Paessler.com,. (2015). *PRTG Network Monitor - Intuitive Network Monitoring Software*. Retrieved 14 October 2015, from https://www.paessler.com/prtg

Sans.org,. (2015). Retrieved 14 October 2015, from https://www.sans.org/reading-room/whitepapers/legal/legal-system-ethics-information-security-54

SearchSecurity,. (2015). *How will the Cybersecurity Information Sharing Act affect enterprises?*.

Retrieved 14 October 2015, from http://searchsecurity.techtarget.com/answer/How-will-the-Cybersecurity-Information-Sharing-Act-affect-enterprises