Assignment week

Business

The focus of risk mitigation is to assist the organization’s department of security administration with identifying a list of potential problems that could potentially cause hostile action during the life span of the company. This effort helps the company investigate response strategies for the qualitative and quantitative risk analysis Based on my findings founded for my Case Study 1 & 2, this study will outline my risk amalgamation strategies.

Wealth my mitigation strategies I will discuss each Individual issues and rank the problems according to how severity and frequently the issue

I Nils Is extremely Important, Decease In order to Implement an detective RISK occur. Mitigation Strategy for my case study I must first be able to identify reoccurring issues. I strongly believe the my swift actions will put me and my company, 23rd Engineer Company in a better situation, because I’m than able to thoroughly analyze the high-risk items and determine the best course of action for my company. Risk Mitigation Strategy No Risk Description Mitigation Strategy Impact Likelihood Leadership Conflict Clearly defined each and every manager roles and responsibility.

Main senior previous will track and monitor other personnel whom are in a management possession.

Med Med 2 Reporting and monitoring requirement, and how will they address Set a time limitation and guidelines to address how response time and limits to how long it might to for papers to stay at one location. Also require a log for to transfer and sign documents. Med 3 Lost of capital Utilize partner assess. Focus more on insuring customer information are kept in a secure

location. Financial data is back up and monitor frequently High Low 4 Market risk Concentrate on existing organization

High 5 High levels of malingering Possible compensation, rewrite company polices, allow management utilize engagement survey Med 6 Outdated Software license to seek Ana Have employees to take the initiative to learn other types of technology skills Just in case other employees are absent from work or on a vacation.

Med 7 Logic errors and computer bugs Establish a team to assess the situation while another form of team tries to continue working on the next iteration. Ensure that system testing is conducted and tested during every stage of the project High PHASE 2:

With today advance technology, trying to eliminate the risk will always be a losing battle. So finding an end result or an alternative for eliminating risk is pointless. As an intelligent species, risks are everywhere and there also involved with everything we do. So when it comes to managing security technologies that are associated with specialized production and individual growing support, the only substitution we have for eliminating risk is by managing the security risks themselves.

The process for most businesses can be a huge financial burden because when it comes to information technology (IT) everything is often considered as a continuous process.

Methodology After taking several moments to decide on what type of methodology I would use for my company (23rd Engineers Company), I

concluded the Qualitative Method would be the best approach while using methodologies and other elite practices located in the NIST.

I was able to Justify my reasoning by evaluating the total time it would have taken me to calculate the total cost; highlight any areas that show the likelihood of any form of risk occurring in the near future. Reducing any changes and the impact f risk is extremely vital and should be considered more vital to business, than losing capital when a risk has occurred. For businesses, the primary goal is to alleviate as much rills as possible Ana develop Deterred resealing your Dustless process.

Ho purpose, According to Walsh (20014), " There are a total of 9 steps that should be utilized when performing after conducting a Risk Assessment; characterization, threat identification, vulnerability identification, control analysis, likelihood of exploitation, impact, risk determination, recommendations for control, and results" (Walsh, 2014).

As we progress forward, a few specific requirements such as software and data, information and hardware must be obtained in order to identify the type of system needed.

The collected information is vital when determining the type of classifications and what is needed to insure the items or information is being secured. When it comes to threat identification, are level of threats is categorize according to the natural, human and environmental. When it comes to outlining the organization as a whole, meaning companies and leadership practice, network protection, data security, personal computers, and

response should all be included when organizing collected data in order to expose system sensitivity.

All of these practices should be oppressive practice in order to address the risk assessment method. As we take another look at methodologies, we should remain aware that there are no explicit requirements when establishing a risk assessment.

Your security administrator should be well experience when trying to determine the best solution for your organization during it risks assessment phase. In addition, once you have distinguished your results, your company should take the time to think the restriction ND try not to be bias during the operation.

Although some solution is provided during the risk assessment, please keep an open mind that some recommendation may appear to be to seem well but they’re not. Try selecting the best suggestions that fit your situation. In the end, the best route is to make your company flexible and possess the capability to be resilient when face with the difficult option in order to mitigate risks. It is never wise for a company to replicate the same types of risk assessment because; every situation and the solution are different from organization o organization.

Bear in mind that the best risk assessment methods are always selected when trying to establish an effective risk assessment. So like I said before, I strongly believed that the qualitative method was the best solution for my company. PHASE 1: With today society, a large range of risks often shadows

every decision we make. Risk can be clear and define by the situation at hand or how we associate the terms in order to categorize the conditions.

For today purposes, according to Rouse (2013) risk can be outlined, as “ a risk is the process of identifying potential hazards an organization may face and analyzing methods of response if exposure occurs” (Rouse, 2013).

Risks are a composition of our everyday life. From the moment we take part in our morning ritual; waking up, brushing teeth, driving to work/school, and catching a bus, we exposed ourselves to a large variety of risks. What makes dealing with risk so unlace Is ten concept AT along Walt rills unconsciously. We go tongue our ally routine without thinking about the possibility of what may occur.

On the other hand, we often try to go out the way to seek risk (implement new security systems, defining the risk management fundamental, installing new product on our computers, or clicking non-familiar mail) try to find ways that would allow us to exploit some of the risks that are polluting the system Company Selection For the case study I decided to stick with something I am familiar and perform a risk valuation on 23rd Engineer Company. 23rd EN is a military organization that provides ongoing mission outline for other supporting companies.

My area of focus will cover Management, incident response, Network Protection, and security areas such as: data, physical, and personal computers. Reason: I selected this organization based on the series of incidents that occur quarterly. Due to constantly routine missions and low available employees, the organization lacks the abilities to implement an

effective risk management system that will aggressively reduce the high level of risk. In addition, since my employment I have noticed that a majority of risk go unnoticed or failed to be resolved.

Management Practices: Management should delegate or define the roles and Job descriptions of each and every employee that are assigned to the organization.

The Job description should be outlined and based on the information security policy that is in place. All company’s documents should be categorized and based off the level of security. Policies should be reviewed and over-see by the security team. Confidential and non-confidential information, regarding previous and current employees should be segregated. After employees are released from the organization, all employees’ personal data should be stored for a maximum of 26 months.

Risk assessment should be performed every quarterly to insure they are in compliance with current organizational policies. System Security Measurement: All network traffic should be encrypted. Modification should be only made and configure by the designated organization security system administration. Each modification should be (signed, dated, and list the type of modification being made) logged. Due inability to gain access to the system, there is a lack of need and urgency to insure the system is running the most current up-to-date security patch. I strongly suggest that security administration performs routine security patch updates.

Scanning: Every quarterly the retina scanned should be tested based off a stressful condition. This will alleviate current concerns and reassure security

system administrator that tender are no conceivable errors Ana current system patches are Tunneling properly. Employee Training and Exercise: Staffs should undergo training so that they are able to work all departments. This will alleviate and form of scandals or errors that have not been covered by the primary employee assigned to that department. Information Awareness exercise should be conducted annually.

The exercise will insure the workers are training based off the currently level of risk. In addition, access to information should be limited and base on a need-to-know bases. Workers should only acquire the appropriate amount of information needed to complete their Job. Insure that security clearance has been conducted before allowing the employee the chance to work with confidential information. Information Security Exercise: Due to natural or man-made disaster, all system data will be recorded and stored on the CUSPS portal.

Information will be easy obtained and backed up every three to four hours.