Good example of essay on risk management in business

Business, Company

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Management

Security management is very essential for any given company‘ s growth and expansion. The information technology managers are solely responsible for this because as it is the major form of communication in an industry. In security management, it is critical to analysis the business environment, needs of the company and the available defense mechanisms. In a business setting, the major problem is to determine the exposure and vulnerability of a business. Exposure and vulnerability in computer security can be achieved by conducting audits in computer security. It involves regular review of network administrator’s logs. Reviews of the current security patches are also required to be undertaken. In addition, firewalls settings, use of external auditors and policies of incorporating third party auditing company need to be looked at critically. Hiring a consultant in computer security management is considered the most important step as it eliminates conflicts of interest and unforeseen bias among the IT managers. It is challenging to evaluate

your own environment and thus, the consultant becomes the better option. External auditors provide assurance that the established controls, technologies and set policies are working as envisioned. Security audit depends on the size of the business and the industry. It is essential to do risk analysis management in computer security auditing.

The second action in security management is to get to get support from the management levels. This is because security affects every level of a business. In some cases the top management officers can compromise company data and guards that might result into stealing of keys of their offices. The company chief executive officers may delegate duties and even appoint staff to positions such as chief security officers. Therefore, getting buy-in of top management is critical in achieving IT security in a company.

The forth action is to mitigate the identified risks after the analysis process that identifies the vulnerable areas. Mitigation process can involve: educating the users on the security processes to be observed, regular review of IDs and privileges. It is recommended disabling the IDs users that are no longer company as fast as possible. Finally, security can be enhanced by developing and implementing policies to track security related risks. The forth action is to collaborate with the users to achieve security within the company. The staffs need to be constantly remained on the importance of logging off after using the computers. They are also need to be made aware of the security risks available. User training is thus necessary. In the training, the staffs would be capacity built on their impacts on the computers and precautions to take when surfing. Finally, it is important to recognize that security is an on-going process that reviews computer usage and the current

technologies available in the market so as to keep updated on security issues.

Summary of Risk Mitigation

Risk mitigation is essential as helps prevent surge in computer risks for a company that mighty result into lose of very useful data and exposure to confidential information to hackers. The risk analysis exercise identifies possible exposure and vulnerable areas that to be made to prevent the posed risk by the vulnerability. The most important action in risk mitigation is to educate the users on how to mitigate the risk and practice safe surfing. In case a staff leaves a company, it should be a norm to promptly disable his/her access to the company data. Ex-employees have always been threat to company data especially if they did not leave in good term with the management. All active tools of the user have to be terminated; they include payroll system and other services that use IT.

Part 4

Pre-disaster planning is very essential for any organization to continue running its business. The entire stakeholders in the company have to be prepared to mitigate the effects that can be caused by the strike of the potential disaster. Planning measures, recovery mechanisms and training of the staff on how to behave in emergency is critical as it would keep the staff in business. Disaster planning and drilling are necessary in business sustainability. Early warning mechanism has to be established and monitored constantly. The company must be insured so as to minimize losses in case a disaster strikes.

Part 5

It is important to acknowledge that the information technology (IT) leaders are basically in charge of organization’s communication system because they are directly and indirectly involved in the process. The managers have to put in place mechanisms to manage effective performance of the IT leaders in a company. The company can put in place codes of conduct that regulate the conduct of the IT staffs. They have to be managed by other sub-managers that monitor the activities of the IT staffs. The company can easily manage the IT department by having a control serve within the system that checks the use of the computers. The manager in charge of the department would be responsible for checking and monitoring the server. It has to be managed by a professional in the department who is loyal to the company. The company has the overall responsibility to foster loyalty of not only the IT staffs, but the entire company staffs.

Part 6

There are numerous fraudulent activities that have surfaced at a Home Depot Inc. It is a large breach of data whereby the fraudulent are using the credit card and debit card information to hack into bank accounts of unsuspecting persons. The fraudsters take advantage of the data breach to advance their stealing habits from people’s bank accounts. The actions has triggered widespread complain from customers across the banking institutions. Hackers are able to access accounts that do not belong to them and withdraw cash.

Questions

- How can the IT department promote security of an organization?

- What regulations and legislations can help the IT department to run more efficient?

- Describe the life cycle of a disaster

- What is the importance of disaster preparedness? How can it be improved?