Business Impact Analysis

Student’s Name

Institutional Affiliation

Course Name& Code

Instructor

Date

Business Impact Analysis

The priority areas for Amerigo business analysis will include: customer needs and business opportunities, the organization’s capability to address these needs, system design and optimization, staffing issues, technology options (including internal and external ones), one-time costs required to implement data collection system, ongoing maintenance costs required to maintain data collection system. This analysis will provide a solid foundation for developing a data collection system. It will also provide the opportunity to compare and contrast various options as well as identify potential risks, costs and benefits of each possible solution (Quoquab, Mohamed Sadom & Mohammad, 2020). Once the analysis is complete, the next step is to identify and prioritize those solutions that provide the most significant benefits. Once the highest-value options have been identified, it will be necessary to perform a cost/benefit analysis for each one. This will help determine which solution makes the most sense from a business perspective—as well as which solution is best suited for addressing your specific needs. Once the most appropriate solution has been identified, it will be necessary to perform a feasibility study. This will determine whether or not the solution is technically feasible and whether or not it can be implemented within your current budget constraints. If so, then it’s time to begin testing out your new system. The testing phase of the project will help you determine whether or not the solution is working properly and whether or not it’s capable of addressing your business needs. If any changes need to be made, they can be made at this stage (as opposed to once the new system has actually been implemented). Once testing has concluded and all issues have been resolved, it will then be necessary to begin rolling out the new solution.

The procedure that should be taken in the event a problem occurs is: notify the appropriate technical personnel, notify the appropriate department managers within the organization, take necessary steps to prevent damage to existing information and systems, take necessary steps to protect the privacy of personal information (Shahid et al., 2018). The first thing that should be done is to notify senior management. Next, it should be done by the appropriate technical personnel within your data collection system team. Once they’ve verified that there is indeed a problem (and thus an issue), they will pass this information along to their supervisors. In addition, depending on how serious the issue is (and how much of a threat it poses to your business or reputation), they may want to contact you as well. Make sure that they do this secretly and not in an overly-flippant manner. If you hear about the issue from your supervisors, it’s time to notify the appropriate department managers within the organization. Once contact has been made with these managers, it’s time to take steps to protect the privacy of personal information. This could mean choosing to implement a security program, limiting access to certain data (such as not releasing any information during a crisis until the crisis has been resolved), or taking any other measures necessary to ensure that there is no damage done to existing information or systems (Shahid et al., 2018). Once these steps have been implemented, the next step is to gather information about the business impact of the problem. The impact on your current operations will be determined using an adverse scenario analysis. This will help you determine just how much damage has actually been done to existing information or systems as well as how much business value has been lost due to the problem. It’s important that you take a worst-case scenario approach here—even if it means acting as though all of your information has been completely compromised. Once this step has been completed, it will then be necessary to determine (using a contingency planning approach) what steps should be taken in order to get back up and running as quickly as possible. Once the necessary steps have been outlined, it will then be time to get your system back up and running as quickly as possible. If you have backups, then you can simply take them and place them in a place that only a few people know where they are. It’s also important that you stay ahead of the game here by implementing contingency measures (such as taking files from your system before problems occur) so that you aren’t completely paralyzed. In the case of an actual disaster, the response procedure will be quite similar to how it would be for any other disaster—so make sure that everyone on your team is informed about what to do and where to go.

The priority of specific responses and their relevance to the organization’s process depends on the nature of which they are presented. For example, if data can be collected in only one way, then the response would be to ensure that this method continues to be kept in working order. Alternatively, if there are several different ways in which data can be collected, then it will be necessary to look at all (or at least a few) of these options. For example, if an organization were conducting research into a new drug in order to find a cure for cancer, the top priorities would likely include: keeping drug test subjects healthy and alive, identifying additional potential patients for the study (i.e. collecting data on all healthy people within the same age range as the subjects that have been given the drug), and finding a way to analyze this data quickly and efficiently. It would be necessary at this stage to identify how much of a threat any of these areas hold. If they’re crucial to dealing with the issue, then they will be top priorities—as will ensuring that existing data isn’t lost in the process of implementing these new measures. Once it has become clear which areas are not essential to dealing with the problem, it will be time to begin implementing new responses. As previously mentioned, this process can be done in a number of different ways (depending on what’s needed). These might include looking at all of the options, implementing a trial-and-error approach (i.e. trying different things out until you find something that works), keeping existing processes in place and identifying potential second sources of data (i.e. performing all of the necessary steps to gather data in other ways because they are no longer feasible), or creating a new system altogether (such as creating a new system based on an entirely different technology). This is one area where it’s important to communicate with each other and make adjustments as soon as possible (as opposed to waiting until everything is complete). If you’re not communicating to make adjustments as necessary, then you might be leaving yourself vulnerable to a problem that could envelop your entire business (and cause a substantial amount of damage). It’s important that you stay ahead of the game by implementing changes as they become necessary. The ultimate goal is to prevent problems from occurring in the first place, but this can’t always be accomplished (thus making it necessary for the organization to be prepared for these emergencies).

It’s important to understand how quickly the organization must react in order to recover as quickly as possible. For example, if there are several steps that need to be taken in order for an issue on a computer system to be resolved, then it will be necessary for everyone on staff (as well as the appropriate system administrators) to work together in order to make these changes as quickly as possible (Shahid et al., 2018). In other words, this is where communication is key. In addition, specific considerations must be made when it comes to recent technologies that might be used within the organization. It’s important that you understand how easily your systems can be compromised by new technologies (such as something running on a new web server). As a result, it’s important that you work hard to ensure that your systems are secured in a way that keeps them protected from any potential threats. If your systems can be compromised by new technologies (i.e. if they run on parts of the web server), then it will be necessary to look at all of the options available for keeping them safe. For example, this might include applying the latest security updates or making sure that your web server is up to date. If you fail to do this, then you might find yourself exposed to a potential threat by an attacker (who will be looking for any system that is susceptible). As a result, it’s important that you take precautions and ensure that your systems are secure. It’s also important to note that the more recent technologies are introduced into an organization, the more there is a chance for things to go wrong. As a result, it’s necessary to take precautions and make sure that your systems are protected by proper security measures.

The leader of an organization may have access to data that is crucial to the organization’s future (i.e. their own personal information). As a result, it will be necessary for them to clearly understand how this data can be kept safe and protected from any potential threats (Dhillon & Coss, 2019). When it comes to technology, the leader will be responsible for ensuring that any new systems introduced within the business are secure and reliable. As such, the leader must ensure that these systems are taken care of properly (i.e. if they’re not up to date, then there is a risk that they could fail at any point). In order to do this, it’s important that they communicate these needs with the appropriate people within their organization. Additionally, the leader will be responsible for ensuring that any new technology is implemented in a manner that protects the personal information of others within their organization (Khan et al., 2020). As previously mentioned, there is a chance for personal information (which could be a major threat) to leak from the organization if something goes wrong. It’s important at this point in time to keep everyone informed of potential threats by implementing proper security measures. If the appropriate measures aren’t taken, then there is the potential for an organization to come under attack from a potential threat (thus resulting in a substantial amount of damage) (Al-Charchafchi, Manickam & Alqattan, 2019). As a result, it’s important that the appropriate steps be taken to ensure that personal information is protected at all times.

Reference

Quoquab, F., Mohamed Sadom, N. Z., & Mohammad, J. (2020). Sustainable Marketing. *The Palgrave Handbook of Corporate Social Responsibility*, 1-24.

Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). *Applied Sciences*, *12*(4), 1927.

Khan, W. Z., Rehman, M. H., Zangoti, H. M., Afzal, M. K., Armi, N., & Salah, K. (2020). Industrial internet of things: Recent advances, enabling technologies and open challenges. *Computers & Electrical Engineering*, *81*, 106522.

Dhillon, S., & Coss, D. L. (2019). INFORMATION PRIVACY LITERATURE: ISSUES AND CHALLENGES. *Journal of Information System Security*, *15*(3).

Al-Charchafchi, A., Manickam, S., & Alqattan, Z. N. (2019, July). Threats against information privacy and security in social networks: A review. In *International Conference on Advances in Cyber Security* (pp. 358-372). Springer, Singapore.