Analysis of commdev organization’s implementing new changes to the business model...

Business, Risk Management

Impact analysis

In this section, we will explore the changes CommDev organization needs to incur when implementing new changes to their business model.

Organizational Impact

Compromise in clashing laws and regulations: With the implementation of the Sustainable Community Partnerships Programme (SCPP) has bought in substantial impact on the operations of CommDev. A qualitative assessment in the form of face to face interview with the managerial positions of CommDev have bought the following impact to attention that since SCPP has its operation in other countries, it forces the CommDev to comply with the respective country’s laws to continue business. In doing so, some of the local regulations comes in clash with Australian regulations, especially privacy laws.

Technical (System) Impact

Risk of information compatibility performing work with personal devices: By current doctrine, a lot of daily information gathering, sharing, and collecting is performed by the staff’s personal smartphones. The cause of this is speculative, with one staff member mentioning the reason to be to reduce effect on budget, since staff using personal devices prevents CommDev to invest on providing personal devices to employees, saving costs. However, the impact of doing so results in compatibility issues in recording files in their appropriate formats.

Security Risks faced in handling work assignments on personal devices: Following incompatibility, personal devices have been a carrier of harmful malware, leading to affecting main CommDev systems. There is record of a man coming from an international assignment, whose phones might have contained such virus, which led to affecting the information systems of the headquarters in Melbourne.

Difficulties in upgradation of main information system: Implementation of new business modules such as the SCPP has led to upgradation of the IT infrastructure of CommDev to account for the new data and the processing that is needed to be performed from such new modules. In doing so, Microforce, the custom-made information system of CommDev has been subject to new functionalities. These new patches are roving to be incompatible with the existing patches, causing perfectly working functionalities to get bugged in the process. The situation with Microforce has been raised to a critical level that the senior management had to be informed, who in turn have consulted the IT Manager to consider replacing Microforce with another information system.

Control assessment

Some of the controls the CommDev should implement in the managerial and the technical aspect are as follows: CommDev does face lack of control over the workings of its employees. One instance being where the human resources team decide to implement their own IT functionality and invest on cloud computing instead of waiting for the chain of command to come up with a professional solution from the organization’s IT team. In such a case, deterrent controls such as an official warning to the employee will send them a stern message in operating outside company boundaries. If employees or the department in question keeps persisting on operating on their own, CommDev would have no other choice but to terminate their employment.

Furthermore, to prevent such authorization from slipping away, a regular involvement of the senior management, as well as regular audits will allow managerial positions to keep track of the daily performance of each of the teams working for CommDev. Lastly, newer functionalities will incur increasing documentation at the administrative level. In such a case, using cloud system as a backup for substantial documentation will be an advisable solution.

Technical Controls

CommDev does contain significant technical situations, ranging from corrupted software manhandling major servers to imperfect patchwork and incompatibility issues of their main information system. Hence, warnings from the information system, Microforce will allow IT team to detect the bug before it corrupts the system causing loss of valuable data, time and money. In the instance a virus has corrupted the system, regular system patches will help in remedying the situations Along with patches, compensating controls such as regular checking of CommDev equipment by the IT department and record of logs of functionalities will help in easier detection of irregularities. As per recovery, cloud backups too help in this case in providing a larger space for maintaining backup of database without compromising space of the CommDev server itself, keeping the server space free for dedicating the freed memory space for performing other IT functionalities by Microforce.

Likelihood analysis

Regarding CommDev, there are two of these significant areas of the organization whose business processes are more risk prone and require. They are as follows:

1. The Microforce System

Risk: Newer patches to handle newly implemented business functionalities of CommDev might create compatibility issues with existing software.

Probability of Occurrence: The frequency of occurrence would range from an occasional level of software issues propping up only during new installation of patch, to regular inconsistencies in data presented and kept lingering even after patching of software is completed.

Category Ranking: (Medium). If data keeps getting corrupted on a regular basis, not only it hinders daily operations of CommDev, it could provide incorrect analysis to the managerial team who rely on this data to aid them in their decision making. Hence, mitigation of this risk should be considered as one of the top priorities.

2. Personal Devices used in Workforce

Risk: Personal devices of each employee used for CommDev work purposes prone to security problems and data sharing inconsistencies.

Probability of Occurrence: The occurrence of this risk is currently very frequent. Personal devices are used for current operations, especially international settlements of CommDev to facilitate data sharing and communications, hence risks associated to it will occur on a frequent basis too.

Category Ranking: (Medium to High) CommDev has already faced cases of data misinterpretation due to incorrect recording via using wrong file formats. Furthermore, foreign use of personal devices has led to viruses being cropped up in main servers of the information systems as the file is shared from an employee’s personal device to the main database. Hence the risk assessment team urges CommDev to change this policy to using a standard device platform provided by CommDev itself. Investment on such a business module will outweigh the cost of mitigating the risks caused when malicious software corrupts a whole server, leading major loss of capital in recuperating from a virus attack.