What are the best strategies to follow to ensure business continuity

Family

What are the best strategies to follow to ensure business continuity? Business continuity is an activity performed by organizations that ensures the smooth flow of business operations to customers, suppliers and other stake holders. It is most relevant in an event of disaster and thus seeks to ensure that the organizations image, profitability, operations, vision and mission are not compromised when any kind of calamity strikes. This usually means drawing up a business continuity plan which includes detailed instructions and steps to take when an organization is hit by an internal or external disaster. Some of the strategies should include drawing up a contingent plan regarding the financial, IT, logistics, management and telecommunication departments and ensuring that employees are well-aware of such procedures. In conjunction to business continuity plan is a disaster recovery plan which aims at focusing solely on managing disaster when it is occurring and outlines steps to follow immediately afterwards. Business continuity and disaster risk management are interdependent to a large extent although business continuity is more holistic and provides a more comprehensive view of how to manage an organization effectively after a disaster and thus takes a more long-term approach (O’ Hehir 37-44). The best strategies for pursuing business continuity include critically analyzing the business continuity plan. This means critically assessing that the pan is workable, realizing that management has a big role in carrying out the plan to its full execution and understanding that each and every department of the organization needs to have a practical contingent plan and resources to deal with any kind of interruption. Over the years organizations have only paid attention to information security and their IT departments and thus have neglected other departments in the process. It is therefore important to understand that although managing information security is vital, other departments should also be closely scrutinized. Business continuity plans should also include assessing risk against its cost effectiveness, providing a detailed financial forecast for emergencies and successfully communicating the contingent plan to employees. One of the most important strategies in outlining such a plan would be to effectively analyze a threat; this could be as simple as a water breakage or as technical as a high level information technology threat. When a potential threat is recognized, a holistic and comprehensive security environment can be created in dealing with it effectively. Also, it is important to realize that the business continuity plans should be put to test physically in order to assess their success rates. This is an important factor for maintaining and continuously developing an efficient business (O' Hehir 37-44). Which one of the three security approaches (Prevention, Deterrence, and Admonition) is in your opinion the best one to improve information security within an organization? Why? Besides having a business continuity plan, it is essential for an organization to invest its time and money in adopting the best security approach. Essentially, there are three security approaches to choose from namely Prevention, Deterrence and Admonition. Prevention works by eliminating the course of danger entirely. For example in case of computer security, this could mean that the physical computation law would in itself prevent the Java applet to write to another random memory location. Deterrence works by displaying the potential to " attack" as undesirable. It discourages parties to violate any rule simply by showing that the attack would not be in the best interest of the parties. In other words, it increases the risk associated with the act and reduces the benefits that might have accrued by attacking. Admonition, by its name acts as a warning and is simply polite requests not to violate the rules or pose as unnecessary threat. If this is done again and again, eventually this may lead the party to adopt a deterrence approach simply by making the attack undesirable, as mentioned above (Miller 1-4). Prevention approaches are the best strategies to adopt when managing information security. Baskerville and Sainsbury also suggest that prevention techniques are the best because they are the least expensive (31-32). Preventing the threat altogether would be less expensive than trying to recover the cost or improvising other strategies. In a world where information technology is going through rapid changes continuously a business cannot always be sure what exactly would pose as a threat, therefore in addition to prevention money should also be spent on recovery aspect as well (Baskerville & Sainsbury 31). Coles- Kemp & Theoharidou also suggest that though the traditional approaches to security are important in information security management, they lack in trying to understand the cultural elements of an organization which may pose insider risk to the organization. The authors suggest that although prevention approaches are important too, understanding and influencing cultural responses is also an important exercise to reduce the risk of a threat to an organization (70).

Works Cited Baskerville, Richard & Sainsbury, Robert. “ Securing Against the Possibility of an Improbable Event: Concepts for Managing Predictable Threats and Normal Compromises” Proceedings of the 5th European Conference on i-Warfare and Security. Eds. Bill Hutchinson. UK: Academic Conferences Limited, 2005.

Coles-Kemp, Lizzie & Theoharidou, Marianthi. “ Insider Threat and Information Security Management” Insider Threats in Cyber Security. Eds. Christopher Probst, Jeffrey Hunker, Dieter Gollmann and Matt Bishop. Heidelberg: Springer, 2010. O’ Hehir, Mike. “ What is a business continuity planning (BCP) strategy?” The Definitive Book Of Business Continuity Management. Eds. Andrew Hiles. West Sussex: John Wiley & Sons Ltd, 2007. Miller, M. “ Computer Security: Fact Forum Framework". Web. 19 Jan. 2011.