Benefits and challenges of technologies – cyber security and risk management

With the improvement in technology, businesses are prone to new challenges that are unique, which need different and more advanced management. Many surveys indicate that although businesses continue to increase their investments and dependencies in IT resources, they aren't doing to enough to protect themselves from technological risks. Protiviti's survey indicated that businesses are prone to ten major risks due to advancing technologies: The biggest threat being the information security, followed by cloud computing, risk management and governance, regulatory management, technology integration and upgradation, resource and infrastructure management, fraud monitoring and disaster recovery (Protiviti, 2012).

Businesses monitoring their technological advancements with efficient risk management and IT security programs and audits succeed in their endeavors. With better technologies companies develop better and effective communication, increase productivity and save business costs by automating operations and processes. Classic examples of effective communication via advanced technologies include high speed internet with high end computer technologies which aid in video conferences and meetings to communicate effectively and remotely. This in turn reduces the travel costs and time for the business leading to higher productivity (Digicult, na).

Due to the efficient technologies' companies will be able to better market their business models and reach out to the greater level of the community. Use of social media techniques to advertise improves the quality of the business product. Out of all technology protects businesses from cyber attacks and viruses. The business data will be quickly compromised if companies don’t strengthen security on networks and computers. Hence the technological advancements provide endless benefits if efficient management plans are carried out.

The benefits of technology cannot be quantified as a direct ratio between the return and investment. It is a complex calculation which should include indirect benefits. For example, using a high-speed internet as discussed above doesn’t guarantee high yield for the business. The better use of that technology might aid in better success rate. Similarly, there are other important issues with advancing technologies that must be addressed by the companies as discussed below.

Cybersecurity is critical in today’s world where we need to control the safety of every party and protect one from attackers/hackers who steal personal information and other parties who collect personal knowledge of the user without the user’s consent. There are several risks in the cyber world on sharing own content and using the services of the websites such as social networks and using the cloud services. Cybersecurity risks arise from the usage of the internet and on sharing information on the Internet as it is an unsecured medium. Importance of not exercising cyber security solemnly are many such as losing money and data, data leakage, hacked, infected with virus and worms. Information leakage is the biggest threat that can ever be and is the primitive consequence of the world in cybersecurity (Steven and Bulter, 2016).

Risk management is where cyber security issues and risks in the business have to be handled. In IT security management the risks must be identified, defined, quantified, and managed. It is especially more and more concerning for the companies to invest in such solution to pro identity a level of safety for their private data which could contain sensitive information, public data regarding their customers and analytical data all at the same time. Companies need to invest in an all-purpose system which can fully operate in the given conditions of the requirements that are presented as a challenge to the companies.

Information Technology plays a critical role in many organizations in risk-assessment and risk management process. When you own a business or organization, it is essential to have a risk analysis and assessment of what lies ahead of you in the industry. IT helps you with that. With data analytics, tools to foresee the growth and recommend methods and inclusion of technology, the information technology be practiced as an enabler for the risk-evaluation manner. It is always implemented to identify risks in the business, with dealings, and IT helps you to reduce or manage those risks and to develop a plan and action in the event of a crisis. Thus, the role of information technology in the risk-assessment process is enormous. It is the most strategic capital and valid information provider which helps the business to succeed. Risk assessment involves measuring potential risks, monitoring, and controlling the chances to meet the targets and objectives and to cause low risk in the dealings of the business.

Cybersecurity and risk management can be considered as the parts of the same coin. Both serve their purpose to safeguard the private data while the significant differences being in the area of implementation. Risk management can be considered as the development of contingency plan which in some cases can be viewed as a sort of a last case defense strategy while cybersecurity essentially is the first line of defense against the attacks to the information or the data.

For my company, as an IT manager, I would start by upgrading the current system to the specific standards while all the physical access point would be secured. New all in one data protection tools will be implemented which will contain software such as data encryption, network management and security, anti-virus and firewall and a level based access system which will allow only a certain amount of data available to a particular person is permanently safeguarding the rest of the data. I would also invest in cloud services as a data backup center and protect the data from any corruption during any attacks or system failure.

Organizations should be producing the constant risk management and appraisal and a plan to get out and dodge those risks and be adapted for risky professions. Risk management should be there in an organization. It consists of following, orient, decide, and act on the events that may lead to risk. The company will separate the risk and manage it in a better way. Risk analysis should be done majorly on the analysis phase of the chance to avoid and be prepared for the opportunity and in case of also unforeseen risks. The better approach is the approach where we implement continuous risk management.

References:

1. Bitsight, 2017. The Standard in Security ratings. The Top 10 Cybersecurity Articles Of 2017: A Recap. Retrieved fromhttps://www. bitsighttech. com/blog/cybersecurity-articles
2. Digicult, na. The benefits technology brings to your business. Retrieved from http://digicult. it/digimag/benefits-technology-brings-business/
3. Microsoft Technet, na. Responding to IT Security Incidents. Retrieved fromhttps://technet. microsoft. com/en-us/library/cc700825. aspx
4. Protiviti, 2012. 2012 IT Audit Benchmarking Survey. Retrieved from https://www. protiviti. com/US-en
5. Steven B. Lipner and Butler W. Lampson, 2016. Risk Management and the Cybersecurity of the U. S. Government Input to the Commission on Enhancing National Cybersecurity. Retrieved fromhttps://www. nist. gov/sites/default/files/documents/2016/09/16/s. lipner-b. lampson_rfi_response. pdf
6. UW-Madison Cybersecurity Risk Management Policy. Retrieved fromhttps://it. wisc. edu/wp-content/uploads/Cybersecurity-Risk-Management-Policy-2017-03-14_Final-for-ITC-First-Reading. pdf