Security Risk Management

INSY 4325-001

With the advancement of technology organizations are adding more and more device which are connected to their network. Organizations are also growing and hiring more employees each with their own personal devices connected to the organizations network. Each one of these devices could cause a cyber crisis to the business. This why Organizations should take an active role in protecting its network and planning ahead. That's were security risk management comes in, it is the process of identifying analyzing and responding to security risks. It implies controls of possible future events that may or may not happen creating options that reduce or eliminate problems before they occur. It is a very critical part of an organization and should be implemented immediately. According to Norton "Cybercriminals will steal an estimated 33 billion records in 2023" (Norton, 2018). Organizations that implement will avoid a crisis compared to those that don't.

Security risk management begins with a risk assessment; you can't fix a problem without knowing the problem. This involves the analysis of vulnerabilities, threats and consequences and controls for risks. Vulnerabilities are anything that can give unauthorized access to threats. Threats are attacks that could compromise an organization, example of threats are Denial of service attacks, viruses, trojans and threat actors better known as hackers. Once the assessment is completed the risk treatment prosses begins. In this prosses the organization implements controls and responses to the risks. Once completed organizations monitor and evaluate its effectiveness.

Many organizations that did not implement security risk management have suffered in instances that could have been managed. There are many examples across different industries but to stay consistent this paper will focus on the Healthcare industry. These industries are a major target because health care businesses are not quick with upgrading their security and patient's personal information is valuable. First an employee of a county health center had his cellphone

and laptop stolen for his car the devices were not password protected. Both devices had patients name, phone number, address and type of disability. This instance could have been avoided if the Health center had planned ahead with a risk assessment and came up with a risk treatment that could have involved polices for device passwords and having patient's information only accessible on a secure network to a secure database. Another example is a plastic surgent posted before and after photos of patients on her website, but the code was made incorrectly which exposed the patient's personnel information. This could have been avoided by simply not posting personal information of patients on the website and doing tests before a website goes live. These are simple fixes but without a security risk management assessment Organization don't think ahead in order to avoid these mistakes.

Sometimes organizations do implement security risk management but unsuccessfully. An example from 2018 is of Hancock health a hospital that paid $55,000 to hackers after being attacked by ransomware locking them out of systems. By the time employees noticed it was too late. The hackers gave the hospital seven days to pay or the data will be permanently encrypted. Despite having back-ups, the hospital continued operations using pen and paper. They decided to pay the hackers in Bitcoin a virtual currency to unlock their data. They were unsuccessful in assessing the risk and the impact it would have on operations. Instead of using the back-ups which was part of their risk treatment they paid the hackers which not only motivates them to keep doing it, the hackers could have just not provided the key to unlock the data. Fortunately for the hospital they did but this risk could have been avoided with a successful implementation of security risk management.

In conclusion, cyber threats are growing and will affect organizations worldwide. Organizations should take an active role in keeping their assets and customers data safe. A

successful implementation of security risk management will benefit an organization. It might prevent or eliminate a future event that could be crippling.

Bibliography

Norton (2018). 10 cyber security facts and statistics for 2018. Retrieved November 20, 2019, from https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html.

Osborne, C. (2018, January 17). US hospital pays $55,000 to hackers after Ransomware attack. Retrieved November 20, 2019, from https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/.

The Doctor company (2014, October 13). Case studies: healthcare data breach risks. Retrieved November 20, 2019, from https://www.youtube.com/watch?v=VDrWbjgM3Ik.