Cybersecurity Risk Analysis Firm

Paper proposal

Tajae Bennett

Professor: Akeyla Porcher

CYSE 494

October 5, 2022

The internet today has developed the ability of connecting friends and families from all over the world. The internet also makes it possible for people and businesses to complete their daily tasks in a more efficient and timely manner. Since the internet provides all these benefits to people and businesses all over the world, cybercriminals have used this opportunity to target those who are vulnerable. Cyber criminals use attacks such as malware, social engineering, and password attacks to target businesses. These Cyberattacks have become so problematic to both small and large businesses in which businesses are finding themselves paying thousands of dollars in order to repair damages that were caused by cyberattacks. With the huge threat of cybercrimes such as cyber-attacks looming, our new business firm will seek to provide support to small businesses within our communities. This cybersecurity risk analysis firm will offer support and services to businesses within our local communities by offering basic cyber security training to employees. Conducting basic cybersecurity training for all employees is the most important goal of our business. This is because the number one cause of cyber-attacks in a business is due to employee's errors. Employees tend to make common mistakes in the workplace such as clicking on email links that are from an unrecognizable source, accessing customers' sensitive information on an unsecure wifi network, using passwords that are relatively weak, and using software that is not updated on a regular basis. It is impossible to prevent cyberattacks, but with proper employee training and guidance, employees within a workplace can reduce the possibility of a business getting attacked.

When legislators are consistently making and passing new legislation bills in order to combat an issue, then we know that issue is problematic and urgent. Cyberattacks consistently cause businesses to lose significant amounts of money and in some cases, it can cause businesses to close due to bankruptcy. Take the colonial pipeline attack for example where thousands of American lives were affected. Cybercriminals gained access to the pipeline data and held it for Ransom. The pipeline business had to make a payment in bitcoin which is worth millions of dollars in order to get their business back to normal. When small businesses see attacks such as the colonial pipeline, they often believe that cyber criminals only attack large businesses that are worth millions of dollars. According to Raineri and Resig from the Journal of Applied Business and Economics "Small businesses are easy victims of cyberattacks due to their limited resources and insufficient training. Furthermore, many small business owners ' attitudes diminish their need for safeguards because they think that they are not likely to be attacked." By small businesses thinking their assets are not worth enough to attract cyber criminals, they often face lawsuits, lost revenues, legal fees, and reputation damage when they become a victim of cyber-attack.

Our business firm's goal is to get small businesses to change their attitude and take cybersecurity threat more seriously. A business needs to know that cybercriminals do not discriminate in which they will attack a business of any size. In fact, cybercriminals enjoy targeting small businesses because of the lack of security knowledge employees and owners possess. The firm will offer support and services by following the National Institute of Standard and Technology guidelines in helping small businesses to have a better understanding of cyberattacks. The firm will also train small businesses on how to mitigate and react to a cyberattack if one does take place.

The firm will also aim to safeguard a small business long term. This means that the firm will help small businesses in creating a cybersecurity long term plan. In order to create a cybersecurity plan, one must know the type of services or products their customers offer. One must also know how their customer businesses operate on a day-to-day basis. Getting firsthand

experience on how small businesses operate, the firm will be able to see vulnerabilities by observing how our customer business handles day to day operations. These vulnerabilities may include our customers using software that are outdated, lack of encryption when storing customer and business sensitive information, and employee awareness. The firm will then conduct a risk assessment in which we will rank our customer assets and data on a scale ranging from 0 to 1. 0 on the risk analysis scale will represent least likely and 1 will represent most likely. Assets and data that are ranked closer to 1 (most likely) will be issues that need immediate attention due to its high risk of data breach. The next step is to get our customer to develop a security strategy. This means that roles and responsibilities within the business should be divided among employees. Proper access control mechanisms should be implemented in which only certain employees have access to a particular set of data. Regularly backing up business data should be implemented in case data is lost during a breach. Lastly, multi factor authentication should be implemented. This method reduces unauthorized access to a business computer network and data. With a cybersecurity plan that follows these core principles, a business will be prepared to detect, recover, and respond to a cyber-attack after it has occurred.

The number one barrier that our business firm could potentially encounter is stubbornness from our customers. Some businesses could be stubborn in which they could refuse to invest in the right software and hardware that is required to protect their assets and sensitive data. Investing in cybersecurity services does not generate revenues for small businesses, so small businesses tend to invest their money only where they can make profits. In other words, small businesses as a whole do not see cybersecurity as a main priority. A business in general regardless of the size will prioritize generating as much revenues as they can with spending little or no money. This mindset and attitude from small businesses is what leads to many different types of cyberattacks. If our customers do not allow cybersecurity professionals from our firm the freedom of experiencing day to day operation firsthand, then this can become an issue. The firm can only provide support and services based on what we have been told by our customers if firsthand observation is not granted. This means that the firm could potentially be offering services to areas of our customers' business that does not need attention. And the areas that do need attention are left vulnerable to cyberattacks.

In order to know if our firm is successful in helping small businesses with cybersecurity support and services is to compare data. One can compare the number of mistakes employees made before and after they were provided basic cybersecurity training. By comparing these two data, it should be evident if employees were properly trained to prevent common mistakes that often lead to cyber-attack. For example, is there a reduction on clicking links in emails that are from an unrecognizable source? Are employees using stronger passwords that consist of letters, numbers, and symbols? These are some ways our firm can determine if we are successful in providing basic cyber security training to our customers. Our firm can also be judged on how well our customers follow and implement their long-term cybersecurity plan. The firm can analyze how often our customers back up their business data and how often software is being updated in order to prevent vulnerabilities. Determining how well our customers use the access control matrix is vital to our success. Access control is very important when it comes to security in businesses. If all employees have access to business data, one can not effectively determine if an attack is internal or external. Lastly, calculating the time our customers take to detect and respond to a cyberattack if one does occur can tell us how the efficiency of the cybersecurity plan that we helped our customer to create.

References

Raineri, E. M., & Resig, J. (2020). Evaluating Self-Efficacy Pertaining to Cybersecurity for Small Businesses. *The Journal of Applied Business and Economics, 22*(12), 13-23. http://proxy.lib.odu.edu/login?url=https://www.proquest.com/scholarly-journals/evaluating-self-efficacy-pertaining-cybersecurity/docview/2497240123/se-2