Cybersecurity Risk Assessment Firm

Proposal Proposal

Rafael Figueroa Medina

Old Dominion University

CYSE 494

Prof. Akeyla Porcher, MS Ed

9/30/2022

The internet has grown to become a significant part of our lives in which people utilize the internet to get their daily tasks done. With just a few keystrokes from a computer or even a mobile phone, people are immediately connected with the entire world and are instantly capable of doing a myriad of things. Although that brings many benefits, it also opens the door for a lot of cybercrimes to take place. "While most organizations consider people to be their greatest assets, those working in the field of cybersecurity acknowledge that people also represent one of their security threats" Cyber attacks are commonly exploited through social engineering, where these attackers use various different tactics to access people's electronic devices. Large companies like Yahoo, LinkedIn, Facebook and Starwood (Marriott) Hotel and Resorts are just examples of corporations being exploited through cyber attacks. Small businesses often lack the resources and organization to have an effective IT security program and when you add the extra risks with employees, it becomes a recipe for disaster. Common infractions like sharing passwords or leaving them posted near a station, connecting to public wifi networks on company devices, and clicking on random links from unrecognized emails are a few examples of small things that can lead to huge problems. One of the more recent attacks was that of the Colonial Pipeline. Half of the fuel supply to the United States was shut down for several days because of an exposed password. Understanding and coming to the conclusion that these threats very well exist, leaves companies worldwide to take a better internal look to see how they are conducting their own processes when it comes to IT security.

According to the U.S. Cybersecurity & Infrastructure Security Agency (CISA), "Small businesses may not consider themselves targets for cyber attacks due to their small size or the perception that they don't have anything worth stealing." Members in the U.S. House of Representatives hearing in 2017 said that the average cyberattack was about $30,000 in damages. They also said that "60% of small businesses that fall victim to a cyber attack close up shop within 6 months."

This is clearly an issue that is only growing as each day passes by. We understand that a lot of small business owners are starting their first business and they have limited knowledge and resources when it comes to cyber security matters. These small businesses probably dedicate their limited time and resources to other issues like supply chain. Cybersecurity therefore falls on the back burner where it does not get the recognition it deserves.With little or no recognition given to cybersecurity, businesses develop vulnerabilities that are then exploited by cybercriminals.

We plan on attacking these issues by offering a service that will serve to both educate and provide groundwork on what these small businesses should do in regards to their business and mitigating risks revolving around technology. The company provides a consultation service that conducts a cybersecurity risk assessment in accordance with the National Institute of Standards and Technology (NIST) Framework of other companies to assist businesses to understand, control and mitigate risks involving their assets and technology. This Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes.

The first thing regarding our service is to understand the business of our customer and get a better sense of the day to day dealings and processes. With this information we can accurately access the various assets that they utilize to conduct their daily business. We would then rank their most valuable assets and look at the different measures the organization is utilizing to safeguard those assets. From those assets we would create a risk management matrix, where we would look at various assets and talk about the various risks associated with each one, to include

the severity level and likelihood of happening and associate a score around it. The overall score will help serve as a guide on what assets would require more attention in order to keep it from getting exploited. There are also mitigation steps for each risk in order to provide information on how to better protect them. Some assets may have a monetary value in order to understand its value, along with the amount for a single loss expectancy as well as the annual rate of occurrence. With these figures, companies can better understand the annualized loss expectancy as well as the total cost of ownership in order to mitigate those risks.

Then there is another portion where we include the company's key performance indicators with those assets and we associate them in an area of the NIST Cybersecurity Framework Control (Identify, Protect, Detect, Respond, Recover), in order to provide a clear explanation of its importance, to include a policy suggestion and procedure. For example, Trade Secrets and Intellectual property may be assigned a control of Protect, because it's very important and sensitive data that must be safeguarded at all times. A policy suggestion may be the establishment of Non-Disclosure Agreements with a procedure on how to implement the policy in that specific organization and how often it should be reviewed and/or updated.

Some of the barriers we can expect to encounter from the very beginning is accreditation. Our employees will have to have certain certifications in order to have the competency and credentials in order to conduct Risk Assessments. Although it is not absolutely required for any specific area, these certifications will help establish a positive reputation with our customers. Those certifications are COMPTIA Security+, COMPTIA Pen Tester, Certified in Risk Information Systems Control (CRISC), Certified in the Governance of Enterprise IT (CGEIT), Chartered Enterprise Risk Analyst (CERA), and Control Objectives for Information and Related Technologies (COBIT). These certifications are not all inclusive, and are constantly changing and evolving. Another significant barrier would be the cooperation of our customers. Our service is centered around the information that is given to us by our customers, and we have to understand our clients current state of affairs in order to accurately address them. Money is another key issue that we can encounter. Understanding the law of scarcity and realizing that these companies only have so many resources to throw at these risks can be a potential issue in the service we provide our customer. Although our service is more consultation than implementation, we can expect to encounter issues if we can effectively mitigate a risk with the resources we have at our disposal from our customer.

We can measure the success of our services with our customers through various ways. One way can be to reassess these organizations and compare the outcomes from the initial one. Another can be at the bottom line in their finances. Our assessment may show a certain asset that is being underutilized and as a result of our assessment our clients are able to be more successful with implementing the new processes. Other measures can be technical in nature, like measuring the response times between the detection of a threat and when appropriate action is taken, average time of establishing updates of software, periodicity of cybersecurity training, and looking at user privileges and ensuring the least amount possible for users to conduct their job. In conclusion, our firm looks to provide a service to our community and assist them in their immediate goals, whether that is providing food and shelter for the community or protecting personally identifiable information and health information. We want our customers to understand the risks involving technology within their place of business and give them affordable solutions and processes in order to continue the growth and development of their organizations.

References

Dahbur, K., Bashabsheh, Z., & Bashabsheh, D. (2017). *Assessment of security awareness: A qualitative and quantitative study. International Management Review,* 13(1), 37-58,101- 102

Cisa Cybersecurity Awareness Program Small Business Resources. Cybersecurity and Infrastructure Security Agency CISA. (n.d.). Retrieved September 28, 2022, from https://www.cisa.gov/publication/cisa-cybersecurity-awareness-program-small-business-resources

Protecting small businesses from cyber attacks: The Cybersecurity ... (n.d.). Retrieved September 28, 2022, from https://www.govinfo.gov/content/pkg/CHRG-115hhrg26297/pdf/CHRG-115hhrg26297.pdf

Barrett, M. P. (2020, January 27). *Framework for improving critical infrastructure cybersecurity version 1.1*. NIST. Retrieved September 28, 2022, from https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11