Group E Business Proposal

John R. Wilson

Old Dominion University

CYSE 494 Entrepreneurship-Prof Studies

Professor Akeyla Porcher, MS Ed

03 March 2023

Group E Business Proposal

What is the problem you are addressing?

The modern-day world operates in a technologically enhanced environment with interconnected computer communication networks that brings not only important communication advancements for the human race but also provides opportunities for criminal elements to target unsuspecting individuals and businesses for their unlawful purposes known as cybercrimes. Therefore, the problem we are addressing is the need to effectively combat the rise of cybercrime because unless society understands the situation, the cybercriminal element will continue to effectively use the internet as a tool for their illicit purposes for monetary gain, notoriety, revenge, state sponsored espionage, terrorism, bullying, blackmail, etc.

"Cybercrime is the single most common form of crime" (Shaw, 2019) today and with these incidents it causes the victims to experience loss of time, fraud, destruction or theft of personal information or data, and even damage to their reputation. Criminals have many different reasons to use the internet for their criminal enterprise, the internet provides a more economical way to execute their criminal plans because computers are inexpensive to acquisition, access to internet is widely available, and you do not need to physically be at the scene of the crime to commit the wrongdoing. Whatever the reason, the best solution is through educating the public on cyber awareness and the best cyber security practices.

How do you know it's a problem?

We know this is a problem because of stats have consistently shown the issue is increasing significantly every year and had especially spiked during the worldwide Coronavirus Disease 2019 (COVID-19) pandemic. Since COVID-19, cybercrimes have reportedly risen 600% (Alvarez, 2021) targeting businesses, especially small businesses because they lack awareness, expertise, and resources (Paulsen, 2016) to effectively implement cybersecurity awareness with its employees and owners (Bada & Nurse, 2019). In addition, we have also seen a rise in cybercriminal activity against individuals. According to the Cybersecurity Infrastructure and Security Agency (CISA), "1 in 3 households unknowingly have computers infected with a form of malicious software, 47% of American citizens had their personal information exposed on the internet by cybercriminals, 65% of Americans who went online received online scam offers, and phishing is rated the number one cybercrime targeting individuals and businesses" (The Facts | CISA, n.d.). Because of constant poor cyber security practices of individuals ignorant to the pitfalls of poor safety practices, which is one of the main contributors of why cyberattacks happen successfully and regularly.

What are going to do about the problem?

In order to address the problems surrounding cyber awareness we have decided to create a non-profit business that creates a cybersecurity education and awareness program to help spread the mindfulness of cyber-related issues and to instill good cybersecurity practices for both individuals as well as businesses and institutions. By providing cybersecurity education this will

provide the consumer with a better general understanding of the kinds of attacks reported and also provide recommended steps to help them secure their own networks and device. Another issue similar to COVID-19, is that this crisis is not bound to a specific demographic, region, race, sex, religion but affects the entire human community; therefore, the responsibility is a society dilemma that can be solved if we choose to help each other to effect better cyber security and practices. We thought the best way to solve this problem is to get the community involved and to do this was to afford the information through a non-profit because we do not want to be held to the bottom line but instead to the community. By getting the community involved it will make a positive impact on their resilience to cybercrimes.

What barriers do you expect to confront?

The barriers we expect the company to hurdle on the subjects of credibility, funding, product understanding, marketing, and unforeseen problems.

As with any startup business, one of the businesses barriers is having complete financial literacy. Financial literacy is having a full understanding of where to raise capital, knowing how much money to raise or borrow, how to best use the money (salaries to attract employees, equipment purchases or rentals, physical office location, research, etc.), how and when to attract investors, and having and following a solid financial plan so that the business's accounts are balanced and have a chance to stay afloat for the foreseeable future. Another hurdle a new business needs to overcome is their credibility.

Credibility is another barrier that this business might encounter problems because the business is an unknown and has not cemented a solid positive reputation within the community. Credibility in this instance means to be trustworthy in your actions which illustrate the businesses honesty. Having integrity will keep current customers using your product, attract new customers, and even help you gain investors and loans form the bank. If you do not have credibility, then you will lose the trust of your employees and consumers you need for a better bottom line. You want your employees to believe in the company they work for because they will do a better job and enjoy doing the work.

Marketing is another consideration as it might prove difficult to know where to accurately promote your business, especially with a constrained starter business budget and marketing inexperience. As a business we should be thinking of what marketing tools can we best levy to expose the business; do we advertise on a billboard, social media, word of mouth, business cards, posters, or leaflets and what communities do we advertise to?

Another hurdle is the consumer understanding the value of our product. For instance, to some consumers, they might not understand the importance of the cybersecurity training as an investment in their safe internet experience.

The last hurdle the business anticipates are the unforeseen difficulties that we are not able to accurately forecast because of inexperience, not fully understanding the problem, or the questions did not exist until after the business is in operation. However, the company and its employees should be prepared to meet and resolve these challenges.

How will you know if you are successful?

Success can be measured in many different ways and in this case we can successfully measure it through successful increase of monetary capitol raised, how well the consumers are learning from our product, through data points such as consumer usage and effectiveness of the products ability to teach the information, how much community involvement we keep and the attraction of new members, and by what we give back to the to the communities in need (which are the low income families and senior citizens for which the majority of them do not understand the technology they are using nor how to protect it.). Again, we know that we need money to run the business, but we do not want to be solely run by the bottom line.

References

Alvarez, F. M. (2021, January 21). *Cyber Crime has been up 600% Since COVID-19. Is Your Business Secure?* CloudDB. https://clouddb.solutions/blog/cyber-crime-has-been-up-600-since-covid-19.-is-your-business-secure

Bada, M., & Nurse, J. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Information and Computer Security, 27(3), 393-410.

Paulsen, C. (2016), "Cybersecuring small businesses", Computer, Vol. 49 No. 8, pp. 92-97.

Shaw, J. (2019, September 2). *How the internet made it easier for all of us to be criminals, or victims*. Wired. https://www.wired.co.uk/article/julia-shaw-making-evil-internet-crime

Watters, A. (2023, January 27). *Top 50 Cybersecurity Statistics, Figures and Facts*. CompTIA. https://www.emerald.com/insight/content/doi/10.1108/ICS-07-2018-0080/full/pdf?casa_token=B0w-VC23bNoAAAAA:HDbW1Hnb_LMKp5sRk77dEcLsrsr6JVtzWVbDd1KXMm7BdMY2WAgk5pgnlmaS8KVzHwCfIrwJt2CFSNDNFmJHf1A9DfG_ZHEABescb-UqISX4sFu6G9k (Watters, 2023)