Cyber Cadets: Entrepreneurship Research & Analysis

DaRon Briggs

Old Dominion University

CYSE 494 Entrepreneurship in Cybersecurity

Dr. Brian K. Payne

June 20, 2022

The Innovation Overview: Cyber Cadets

During my development team's entrepreneurship endeavors in relation to cybersecurity, we noticed there are quite a few cyber related problems that plagued everyday technology users that needed to be addressed. These issues ranged from lack of cyber awareness to lack of proper computer training to common cyber errors that leave users and their sensitive data vulnerable to cyber-attacks. We realized as cybersecurity and STEM students and practitioners that not all civilians and workplace personal have had the luxury of being properly introduced to proper and safe cybersecurity practices and vulnerability prevention methods as we have been throughout our academic endeavors. Our goal then became to develop a product that end-users could use to overcome these problems to live a safer digital lifestyle. The product we decided to create was in the form of a mobile phone/tablet application that would teach inexperienced and novice users of common cybersecurity practices and terminology that they will need to know to protect themselves and their various communities online while mitigating the possibility that they fall victim to a cyber-attack. The application we are developing, which my development team and I named Cyber Cadets, seeks to educate users in an engaging manner through cyber related tutorials and interactive activities where users of all demographics can build knowledge without the stress of finding a teaching facility or instructor. We plan of providing this application for free on the Google Play Store, Apple App Store, and the Windows store to reach a wide variety of individuals and groups. We plan to include incentives within our application to get users to regularly use the Cyber Cadets application so that they will build strong cyber awareness in hopes of broadening their cyber knowledge and mitigating vulnerabilities.

The Problem(s)

The number of cyber vulnerabilities and cyber-attacks will continue to grow around the world as many societies look to technology to aid in daily life operations. Banks, hospitals, school systems, and even much of the early 21st century's social lives revolve around the use of technology and the internet. As the various branches of work and social communities continue to intertwine their ways of life into technology users have to become accustomed to using the various forms of technology and online skills effectively and efficiently. Alas, this is not the case as many users have been put into positions where they are not entirely tech savvy, particularly those who come from demographics that did not grow up using technology or those who did not have the means nor opportunities to access such cyber world devices. In order to keep up with the digital word boom of the early 21st century and be productive in their daily lives these novice cyber users must try and use the technology to the best of their abilities regardless of if they even understand how the technology works and how to properly use it. However, by these inexperienced users engaging in online activity they are potentially exposing themselves, and those on their shared network, to cyber-attacks if they do not know the proper tactics to protect themselves online. The type of cyber threats novice technology users may fall victim to range from pop up malware on untrustworthy websites, to being tricked into downloading viruses to a computer from fraudulent lookalike sites, to phishing schemes that try to get the target to divulge sensitive information to what they believe is a trustworthy source. Regular everyday users tend to overlook these vulnerabilities due to negligence or them not being properly trained to identify them. My team and I's goal are to create an application that will help users recognize these various types of vulnerabilities and cyber-attacks and guide them on

how to overcome vulnerabilities through an engaging and fun app that they can learn from on a daily basis. The Cyber Cadets apps will include tutorials on a different range of topics such as types of cyber-attacks, internet of things and their vulnerabilities, and even the importance of virtual private networks (VPN's) and how to use them. A portion of the app will also be dedicated to interactive activities that will challenge the app user's comprehension from the tutorials to see if they can accurately use what they have learned under the tutorials section in everyday life scenarios.

Spotting Potential Attacks

Some cyber device users fall victim to cyber-attacks simply because they do not know what they are an or how to spot these attacks. Some of the more common cyber-attacks such as phishing and trojan horse attacks are the type of cyber-attacks can be prevented if the user was properly exposed to resources that trained users on how to spot them. Phishing attacks are a socially engineered forms of cyber-attacks that rely on deceiving the user into clicking on the email and its various attachments which in turn installs some form of malware or relies on the user divulging sensitive information to the fraudulent party which they intend to use without proper authorization. According to Wright (et al., 2014), approximately 500 billion emails are sent over email platforms daily, and of those 500 billion emails 80%, or 400 billion, are malware infested, spam related, or phishing emails. This means that for every 10 emails a person receives, only 2 of those emails are legitimate communication emails from another authorized a potentially trustworthy user. Phishing emails tend to incorporate terms and phrases such an urgent, warning, deadline to get susceptible users to act urgently and respond to the email as fast as possible without taking the time to analyze the message by putting deep thought into

what is being asked and how it is being presented. A social study performed noted that the longer an inexperienced user attentively looks at a phishing email, the more likely they are to think the email is valid and fall for the scheme the attacker has laid out (Harrison et al., 2016). One of my team's goals through the use of tutorials interactive is to help users understand how they can spot and manage potential cyber-attacks before they happen. We plan to be the alternative to training that simply lectures individuals on how to limit cyber vulnerabilities and prevent themselves from becoming victims of cyber-attacks. By creating narrative scenarios and mini games that incorporate different cyber related attacks, users of our app will have the ability to apply what they have learned in our tutorials while also enjoying the engaging and teachable activities that accompany the tutorials.

Password Troubles

Cyber technology users, both experienced and inexperienced, often expose themselves to dangers they do not realize they have involved themselves in until it is too late. For example, many users often create and use passwords that are capable of being compromised through various methods such as a brute force password attacks, which guesses at potential passwords until the user's password is correctly guessed. Inexperienced users typically do not think of creating passwords that are complex as they may view it as unnecessary and foolish to create tough passwords they will not remember. Having to add a combination of special characters and numbers accompanied by lowercase and upper-case letters can prove challenging to those who want to use easy passwords they have been using for years on end. Also, non-technology savvy/experienced users tend to not change their passwords often, unless processed by the platform's system to do so, which can lead to their passwords being stored in password

cracking systems for later hacking by various attackers. According to Grobler (et al., 2020) the importance of creating complex passwords is not often communicated to the end-users who are creating the passwords. This lack of proper communication on the "why" behind the necessity for such complex passwords leads users to becoming frustrated and adding special characters or numbers to the end of their passwords instead of mixing them throughout. For example, user who is creating a password for the first time on a site/platform might want to use the password "ilovepoodles" but due to system requirements they add the special requirements to the end of the password to get "Ilovepoodles1!". Although "Ilovepoodles1!" is a stronger password than "ilovepoodles" it is not as strong as a password such as "1L0vep00dle$Two"; which mixes in uppercase letters, lowercase letters, symbols, and letters all throughout the password making it harder hackers to guess and or use a password cracker. The addition of multiple factor verification, such as onetime password or biometrics, when paired with a strong password can greatly improve online security for platforms that requires credentials to gain access (Yin et al., 2020). With multi factor verification, even if the user's password is compromised the attacker will still need access to the second verification method in order to fulling compromise the user's account. The lack of understanding why strong passwords and multi factor verification are important causes many cyber related judgement errors. Yet these are the type of problems that are easier to prevent than having to assist a user when their credentials have been compromised by an outside party. So in Cyber Cadets we plan to aid users through daily tutorials and interactive activities that will only take a few minutes a day, and over time user's will gain more and more knowledge on how to protect their credentials.

Fortifying Cyber Defenses

I, along with my team that created Cyber Cadets, believe we can elevate the knowledge of common users around cybersecurity practices and techniques that are overlooked by exposing them to various topics in our application. As no singular cyber defense method 100% percent safe from being penetrated by outside forces, adding layers on layers of protection lessens the chances that a user will become a victim of a cyber-attack. While a technological literate person may know of multiple different ways to fortify the cybersecurity defenses, novice users may have only been exposed to defenses such as anti-malware/virus protection software, if even that. Two of the more affordable and easier to use forms of cyber defenses my team and I plan to reveal to the Cyber Cadets application users are virtual private networks, also known as VPNs, and encryption and decryption tactics. The use of VPN's and the use encryption and decryption may elevate a user's cyber domain to where their sensitive information is less likely to be compromised when data is in transit. Virtual private networks were originally created for use by businesses and private organizations but have been adopted for use by both governments and civilian usage. VPN uses a technique called tunneling which incorporates the use of encrypting data between the client, or end user's device, and the server providing the service ((Himanshu, 2017). There are a variety of VPNs available to users to use, also the use of encryption and decryption keys could prove useful for companies and private users who have to transmit important documents such as tax reports or health related paperwork. Encryption works by the sender hiding the message using receiving user's public key, which multiple people may have access to, and the receiver uses their private key, which they should only have access too, to decrypt the hidden message (Batamuliza &

Hanyurwimfura, 2021). Cloud computing is starting to become a prime user of encryption and decryption in their storage mediums (Batamuliza & Hanyurwimfura, 2021).

Building an Understanding of Cyber Security

We, the Cyber Cadets team, believe that cybersecurity is an everyone problem not just an issue for the information technology (IT) specialists and network and security personal. In this ever so growing technological word, users must have some sense of what kind of technology they are manipulating when engaging in online ad cyber affairs. Having an understanding of what they are engaging with will also give users a better sense of how to protect themselves from those who are trying to take advantage of them while also allowing users to mitigate their vulnerabilities. According to Arabo & Serpell (2019) applying real world scenarios to a concept taught in cybersecurity yield better comprehension results versus teaching only concepts and ideas. The latter statement is one of the ways the Cyber Cadets development team plan to create the application, as we do not want users to only use is application because it is apart of some training program for work. We want users to actual enjoy what they are learning and feel as though they can use what they have learned on Cyber Cadets in their daily lives, where knowledge can actually make an impact. Interactive activities are a huge part of developing knowledge in any concept, including cybersecurity. Competition and games related to cybersecurity have also been shown to exponentially improve comprehension rather than only using traditional linear teaching methods(Fernández-Caramés & Fraga-Lamas, 2020).

Interdisciplinary Aspect of Cyber Cadets

In regard to the product application known as Cyber Cadets that my team and I look at it leans on a lot of concepts from cybersecurity from how to spot and mange cyber-attacks, to how to limit self-imposed errors, to learning how to develop stronger cyber defense techniques. Overall, we tried to incorporate as many topics as we felt necessary that were not too complex to understand for those who did not have a background in cybersecurity. However, we had to borrow topics from other disciplines to properly develop the product known as Cyber Cadets and how it was going to function.

One aspect of Cyber Cadets that needed to be thought through was how we were actually going to create the application and implement our ideas onto. Due to most of the team being cybersecurity majors, we had little experience in actually coding on an expert level to where we could develop an application worthy of the end user's time. We decided to move forward with planning the application while our goal would be to hire someone or preferably a group of app develops who could aid us in our project. This interdisciplinary aspect is drawn more from the computer science field, which can often be associated with cybersecurity as both are STEM fields.

The actual promoting Cyber Cadets and creating slogans for the application would stem from the business interdisciplinary field, in generally the sub-field known as marketing. Under the business side we had to determine how much the application would cost and how long it would take to fully build the application. We calculated that the cost of creating the application could range from anywhere from 100k USD to 500k USD, and the development process could

take as long as 6 months to 2 years in length. Also, by making our application free we had to think how ere we going to generate money to continually fund the development and maintenance of the app. Having outside companies put their adds within our app was the decision we thought was best, as we have seen a plethora of other teaching applications such as Quizlet and Duolingo have small advertisements appear in between segments on their applications.

Two of the other disciplines we had to learn from to develop Cyber Cadets was the education and psychology. We had to figure out what were effective ways of teaching cybersecurity topics to those who may not be as interested in the topic. We did not the app to be boring and we wanted it to have some uniqueness to it that other cybersecurity teaching platforms did not use. Psychological we had to develop an engraining way to get users to actually learn from the app while also feeling as they have a reason to come back to the app daily. That is why we decided to do create small tutorials similar t teaching platforms like BrainPOP and Duolingo that have users learn their skill in small bits over a large period of time, that way they could fit Cyber Cadets lessons into their already busy daily life without having to spend long hours staring at their device screen.

One of the last disciplines we used in the making of Cyber Cadets was the use of graphic design. We created an application logo along with how the app will look at the end. The application known as Canva was used to create most of the imagery used within the application. This allowed for decently crafted visuals without the need to hire a graphic designer, and gave our team complete create design over the visuals of the app.

Effectiveness of Cyber Cadets

In order to determine if our app innovation is successful, the Cyber Cadets development team will carry out a series of tests and analyses to see if our app does indeed accomplish what it intends to do. First, we will start with gathering a small control group of in-between 100 to 1000 people to see how they interact with the app. These testers need to be from a plethora of different background and demographics; old, young, middle-aged, rural areas, urban areas, lower class, middle class, some without higher education, and some without higher education. Next, we will collect feedback on if they plan to continue to use the application in the future along with asking them about the challenges they faced while using the app and if they felt as though certain topics were difficult to understand or not explained well. Within the app itself there will also be a certificate test that can be completed to see if users were able to adequately retain and comprehend the information that was presented throughout the app. We will also look at the comments and reviews posted in the Google Play Store, Apple App Store, and Microsoft Windows Store to see if any feedback is presented that was not from the initial test groups. The app rating on these latter named stores will also be taken into consideration upon determining the effectiveness of the app to see if any changes need to be made. I also would like to add an analytics software into the app to gauge how users are using the app, and to see how much time users spend on the app and what sections are viewed the most. A leaderboard system may also be implemented in the future for completed tasks and time spent within the app, this will also serve as a measurable for analysis. Lastly how many sponsors we receive for the app will be a true visible representation of how effective our app is in the eyes of other organizations.

Turning Cyber Cadets into a Reality

In order to turn the innovation Cyber Cadets into a reality, the team and I will have to gather many different resources in personal. The first major obstacle is funding for the application. At minimum it appears to cost around a 100k USD to build an application for a mobile device without any self-input. We will either have to do fundraising style events, online and in person, or take out a loan from a bank supported by the money the Cyber Cadets development team invests into the application themselves.

This brings up the second part of bring Cyber Cadets to reality, hiring an app developing team. I would prefer we hire a company that has a decent track record in developing applications for clients and has a portfolio of live applications we as a team can interact with to gauge the developer's potential and style. We would then have to agree to a contract with the company on how long they will develop the app for and how many developers will be working on developing Cyber Cadets, as this will impact the overall funding needed for the application.

While the app is being developed, the Cyber Cadets team will need to design if we will hire an actual graphic designer to design the logos for our application. The logos we created for free using the Canva app are not professional done and an experience graphic designer can aid us in designed an eye-catching logo and banner that we can use. They can also help with designing and formatting the visuals for our website and social media platforms.

We will need to register a domain name and hire a website developer so that we can be contacted about any issues or partnerships for the application. Here is where we will have the web designer and graphic designer intertwine to come up with a visually appeasing and

functional website. We also will need to look for sponsorships and partnerships, as having these will be a great way to fund the app going forward. We will also look for partnerships to be embedded within Cyber cadets under the certificates portion of the application. Our goal is for those who fund our app through advertisements to support our incitive program by providing rewards when certain levels within the app are completed to give users more of an incitive to use the application. These incentives can be presented in the form of coupons or an online raffle ticket for which they can win a prize.

Upon the completion of the application of the application, we will run a series of beta testing to see what bugs present and what ideas need to be added or removed from the application. After we complete testing, we will look to launch the application on the various app stores. Yet, before we officially launch, we will have to hire two new sets of personal. One set of personal will be the application, website, and social media maintenance teams as they will be responsible for keeping all our platforms up to date and free of bugs and issues. Followed by the hiring of the latter teams, the Cyber Cadets development team will have to hire a help desk. The help desk team will be tasked with troubleshooting any problems users may be having with the application. The available troubleshoot options will be available in the form of online chat and phone call. The help desk team will also support this innovation by receiving any complaints about the app users may have, which in turn can be forward to the development team and ap maintenance teams.

The last step in turning Cyber Cadets into a reality would be to market the application then launch it. Marketing it om a multitude of social media platforms is ideal when first starting

off. Eventually the goal would be to be marketing across television commercials and radio stations.

Next Steps

The next steps for now while working on the innovation Cyber Cadets is to fully flush out the details of how the team wants the application to look. Right now, we are still in the pitching stage, which means we can make as many edits to the project as we want at the moment without losing any financial resources. We also will need to start acquiring financial resources so that when we are reading to actually approach another organization or app development company with our idea, we will have the resources to develop a quality product. We can also approach the local entrepreneurship centers in the Hampton Roads area to see if they assist with resources that will help us develop Cyber Cadets.

WORKS CITED

(Wright et al., 2014)

Wright, R., Jensen, M., Thatcher, J., Dinger, M., & Marett, K. (2014). Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance. Information Systems Research, 25(2), 385-400

(Harrison et al., 2016)

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails How attention and elaboration protect against phishing. Online Information Review, 40(2), 265-281

(Grobler et al., 2020)

Grobler, M., Chamikara, M., Abbott, J., Jeong, J., Nepal, S., & Paris, C. (2020). The importance of social identity on password formulations. Personal and Ubiquitous Computing, 25(5), 813-827.

(Yin et al., 2020)

Yin, X., He, J., Guo, Y., Han, D., Li, K., & Castiglione, A. (2020). An Efficient Two-Factor Authentication Scheme Based on the Merkle Tree. Sensors (Basel, Switzerland), 20(20), 5735.

(Himanshu, 2017)

Himanshu Monga. (2017). An approach to Virtual Private Networks and security. International Journal of Advanced Research in Computer Science, 8(5), 343.

(Batamuliza & Hanyurwimfura, 2021)

Batamuliza, J., & Hanyurwimfura, D. (2021). Identity based encryption with equality test. Information Security Journal., 30(2), 111-124.

(Arabo & Serpell, 2019)

Arabo, A., & Serpell, M. (2019). Pedagogical Approach to Effective Cybersecurity Teaching. In Transactions on Edutainment XV (Lecture Notes in Computer Science, pp. 129-140). Berlin, Heidelberg: Springer Berlin Heidelberg.

(Fernández-Caramés & Fraga-Lamas, 2020)

Fernández-Caramés, T., & Fraga-Lamas, P. (2020). Teaching and Learning IoT Cybersecurity and Vulnerability Assessment with Shodan through Practical Use Cases. Sensors (Basel, Switzerland), 20(11), 3048.