

WCS494 Academic Paper

Amanee Garcia

WCS 494 Entrepreneurship in Cybersecurity, Professional Studies, and World Languages &
Cultures

Akeyla Porcher

12/10/23

As the years of age go by technology advancement has been planned and created to make life easier as the generations of the population grow. With this growth that also includes the natural stages of life as we all know that the generation below us becoming more advanced in technology as time has changed. With having more access to the world virtually it includes high levels of cybcrime daily. It is crucial that society stays aware and informed with how to protect themselves by providing them with a cybersecurity application for guidance.

The targeted audience for this innovation will be created for the elderly group from the age range of 50 and older because they are the primary target in today's world. The idea for the app is to keep this age group cautious from individuals that perpetuate to gain from the lack of cyber knowledge the elderly have.

Not too many people take steps into learning about cyber security for themselves unless they are in the situation and need help. It is important to know how to avoid threats before they become part of your life, and it feels like you have no knowledge of where to start. Many scams or threats are advancing so quickly that it is hard to tell the difference between legitimate calls, emails, or messages compared to phishing that replicates other companies where it may seem like true information. A great example would be online banking, amazon shopping, or even links that open personal information to a database that allows others insight. The elderly will be the main target due to their lack of familiarity with the use of technology. The statistics in the use of technology for the elderly has increased over the pass couple of years which is closing the gap of use but increasing the potential for cyber threats.

With our innovation we will be addressing the problem of elderly not being knowledgeable on how they are apart of the cyber world in protecting themselves and how to be more aware of popular methods on how to see and avoid cyber threats. We will create this app as a profitable

app but advertise a free 7-day trial to make sure that the catering party knows what is in store. This free trial will gain audience attention and let them experiment with the app to see if this fits what they are looking for. The app will have a friendly and welcoming page that starts with just a name request, age bracket selection with an optional email address to get email alerts for updates and keep track of visitors. Even though our target audience is elderly we want to be able to see what other ages are interested in the information or experiencing cyber issues. The next steps would be a small questionnaire that lets the app get to know the user. A few example questions including: “how important is cybersecurity for you?” How much do you know about cybersecurity?”

Once that is filled out, we will broadcast current cyber issues and common cyberthreats that are taking place. This will be an informative page that will keep the elderly aware of what is going on in the world daily to see what new phishing alerts that they may become a victim too potentially. In addition for categories, we will include a menu drop down as well as subcategories for cyber information example being hints on self-protection, reliable websites for additional protection, spam, and phishing help. We want to guide the elderly in a simple but easy way with as much information as possible based on their need. In order to be more help, we will have a search button at top of the page and also a chat box for quick responses on matters they may have missed. Since this is profitable, we will have employees working the application in order to respond and keep the application up to date with new information. The problem that we will be solving is the lack of education the elderly have in cybersecurity awareness, the support they need to be self-motivated to learn on how to stay protected but also avoid potential cybercrime that is happening to large groups of people, and methods to know how to proceed in a case of a cyberthreat on their own personal devices or identity.

The first scholarly source is by sage journals called “The Role of Cybersecurity knowledge and Awareness In cybersecurity Intention and Behavior in the United States,” which will describe how gender, education, age and other factors predict the knowledge of cybersecurity awareness. As the modern society is aware that cybercrime can happen in an instant moment many are not knowledge about what cybersecurity precautions to take for their own protection.

According to Lee & Chua (2023), “Cybersecurity plays an important role in guaranteeing and protecting people who use the Internet in their daily lives” (p.1). The role of cybersecurity is just giving people the opportunity to understand the world of technology and while using the internet have knowledge on steps to take to avoid cybercrime. The data taken to get a perspective on what individuals know is by collecting research on what is currently in place to provide the information needed for those in the United States to being informed on the topic. “Increased Internet use and smartphone ownership/usage is associated with a higher level of cybersecurity knowledge. Individuals with a higher level of Internet and smart device usage are likely to have a higher level of cybersecurity knowledge.”

With the age being a factor, many middle age and young teens are well established on how to maneuver through technology and create a safe space to conduct their work without feeling vulnerable. They also can be more aware of potential cyber attack methods that the elderly become victim to because they are unfamiliar with the methods used for phishing.

The main goal in this is show the importance of cybersecurity awareness because it protects individuals from falling victim to cybercrime and businesses fraud lack of detection that can potentially hard the customer. In contract with our innovation, we will be providing similar

insight into why it's important and how to better prepare yet avoid cybercrime while using technology.

Defining Cybersecurity is another scholarly journal that provides great insight into our entrepreneurship endeavor. This article was written by a collected group of individuals, Dan Craigen, Nadia Diakun-Thibault, and Randy Purse describing that the word cybersecurity can mean several different things to different groups of people. (Craigen, Diakun-Thibault, and Purse, 2014) stated "Based on the literature review described in this article, we found that the term is used broadly and its definitions are highly variable, context-bound, often subjective, and, at times, uninformative."(p.13) With our innovation the purpose will be to be informative and guide the targeted audience to want to know more about cybersecurity because the effect of knowing its advantages will be the key to safe use of technology.

The Elderly, become the first attempted victims because of the lack of knowledge on cybersecurity because they are trusting and believe that a phone call that sounds official or email is to help but it could be the exact opposite. A quote that was mentioned in the article that is an example of self-education states "Humans must defend machines that are attacked by other humans using machines." (p.13) With having people majoring in cybersecurity or the betterment of the internet usage creating safety for its users, it also become crucial that those using the technology are willing to dig deeper into the meaning. It does not mean they have to have an interest in the cyberworld, but they should take interest on staying protected while using these machines we call "technology." The first steps are admitting that we don't know what we would do if we were taken advantage of by a simple phone call or a hyperlink that redirects to a scam that collects personal information leaving the simple user exposed.

Cybersecurity is a study that requires more than just one discipline in order to have a successful plan and execution when defending the world from cybercrime. In our entrepreneurship endeavor we experienced while brainstorming that it will take more than just the knowledge of cybercrime but other perspectives to serve the audience and make an impact.

The scholarly journal, “Interdisciplinary Cybersecurity: Rethinking the Approach and the Process,” written by Michelle Peter, Jacob and a T. Yang provides the aspects of multiple disciplines and how they contribute creativity and ideas into businesses. Holts states, “A holistic approach to cybersecurity is one that considers the many disciplines that produce cybersecurity professionals – technical and nontechnical alike, in a coherent fashion.” (p.3) Each discipline has an expertise in different fields that can contribute to cybersecurity and the full understanding of who and how it affects the world. By having understanding in multiple discipline, it advances the decision-making process.

Due to the cybercrimes advancing throughout the world it requires more than just cybersecurity to be hands on with preventative measures. They need interdisciplinary approaches to be able to coincide ideas and cognitive skills to keep up with the increase of users which also increases vulnerability. Peter, Jacob, & Yang (2020), stated “This vast increase in the number of internet users raises concern in terms of vulnerabilities and emerging threats by ideologically motivated offenders to cause harm and further their political and social agendas.” (p.4). With the knowledge of users feeling more reliable on the internet for shopping, banking, social media and other reasons it opens the risk for more advanced cybercrimes to take place easier than ever before.

With our innovation it makes sense to create an application sense everyone has a cell phone and uses it for almost everything. With their card numbers saved to accounts, personal

information saved to webpages, banking information app installed on phone leaves individuals exposed but many think because of a passcode or logging out is enough. With the application it will give hints and tips of the best passcodes, lock methods, security features to be self-aware of how something so convenient still needs protection. With the target age group of 50 and older it will help set up strong passcodes and reminders since memory declines with age for many.

“Senior Citizens and Cybersecurity Awareness,” by Carlene Blackwood-Brown, Yair Levy, and Steven Terrall at the College of Engineering and Computing Nova Southeastern University, focused primarily on seniors and exposure to cybercrime. “One in five American senior citizen is a victim of online financial fraud, costing more than \$2.6 billion per year (Willis, 2015). (p.15). With seniors receiving social security and other pensions they usually fall victim because of the confirmed income is known across the world and not many are helped with managing their income. This is not the only issues that are addressed when it comes to cybercrime but also the mental state it contributes to once they are at risk. “Senior citizens who are identity theft victims suffer devastating effects (Jones, 2001): Loss of all their life savings, Feelings of shame for being victims, Decreased self-confidence, Exacerbated illnesses to include premature death.” (p.15).

With having the statics of the mental abuse the elderly have to deal with once they are cyber attacked is the best reason for why our innovation targets this age group. With the application it will increase self-confidence, protect their set income, build a sense of safety, and avoid stressful situations with our support. To know that we can provide insight on what to look out for with the words or questions asked by telemarketers that just don’t seem right or alarming. To know what sights to pay attention to when buying items or providing card information or

even logging in and remembering to log out if on an unsecured website can decrease the number of victims.

Frank Cremer, Barry Sheehan, Michael Fortman, Arash Kia, Martin Mullins, Finbarr Murphy, and Stefan Materne wrote a scholarly journal called “Cyber Risk and Cybersecurity: a Systematic Review of Data Availability” providing data on cybersecurity and availability of cyber risk and analysis. In the article they state, “Despite the increasing relevance for the international economy, the availability of data on cyber risks remains limited. The reasons for this are many. Firstly, it is an emerging and evolving risk; therefore, historical data sources are limited (Biener et al. 2015). It could also be due to the fact that, in general, institutions that have been hacked do not publish the incidents (Eling and Schnell 2016).” This statement is an example of cybercrime that takes place but are not reported or tracked properly in order to know the patterns. With not being aware of the potential risk it minimizes the research on cybercrime and those that experience the risk I chose this article because it shows the lack of control and evidence of this emerging crime it has on the users.

With our innovation we will be able to track the users base on age gap and most popular used subcategory as well as current cybercrime issues. In order to stay informed as an individual they will need a common site that provides just enough information on the cybercrime potential and what is being used to incriminate.

Identified studies are divided into three categories: datasets on the causes of cyber risks, datasets on the effects of cyber risks and datasets on cybersecurity.” With these categories they place everyone including insurers, business, and individuals in one study in order to create predictions for future crime. With these predictions it helps discipline create a potential product

for security and protection before they encounter the risk but as stated all reported crimes are not listed but show the increase and growth of cybercrime.

Roland Trope wrote a scholarly journal called “There’s No App for That: Calibrating Cybersecurity Safeguard and Disclosures.” The first sentence intrigued me as well as the title since we have decided to create a application for cybersecurity. Trope (2012) stated, “the term “cybersecurity” has become an oxymoron like “military intelligence” and “bug-free code.” This statement rung a bell in my head because it is a group that study and observe cybersecurity but as well contribute to helping those that have no knowledge of what is used in today’s world. I look at technology as a privilege but many misuse it because they are unaware of the risk of having it means when not informed correctly on the potential cybercrime.

Many companies as discussed in the journal choose to not discuss breaches with the consumers or employees because it creates fear and the loss of trust for the standard they are held to. With not mentioning the crime it leaves the severity unknown and excludes the proper steps to avoid future crime within the disciplines leaving them as well unprepared. With the increase of cybercrime, it puts individuals at an disadvantage because they already are not knowledgeable of the seriousness of what cybercrime can do but also do not know what steps to take to avoid it.

An example used to show the side effect of cybercrime was mentioned in the article by a bank, called Comerica. Trope (2012) mentioned after the breach it took them over an hour to stop the distribution when it went to court, they stated “The district court, after a bench trial, held Comerica liable for reasons that should be of interest to counsel advising clients on the scope of cybersecurity safeguards they should implement.” (p.6). With not being aware of potential breach it left not only the company but user open for fraud and theft with their funds. If there was

proper training on avoidance and protection it could of took less time to solve the issue and lead to less issues.

Nicole Radziwill wrote a scholarly journal called “Cybersecurity Leadership,” it displays how to lead with cybersecurity input to organizations with a business mindset in leadership. Hasib (2014) states “Particularly in production and critical infrastructure environments, attention to cybersecurity must be incorporated into quality and risk management efforts because attacks can result not only in diminished quality of outputs, but also in damage to expensive physical assets.” Leadership has to be involved with the efforts to protect society even though it can affect the environment financially we need to make sure that the business product is seamless and worth using. With leadership they include details that close the gap for the unknown in cybersecurity. With several disciplines it gives different of insight on the product and the usability of the product.

Our entrepreneurship will include several disciplines because we understand providing the knowledge is not the only way to success. To involve the user, we have to connect with their minds and teach them how to be leaders in their protection and security when it comes to their personal information.

The main goal is to create an application that provide cyber knowledge while including other disciplines to make the process less complex. The other disciplines that will have a large impact in the business is psychology, marketing, finance, leadership, and engineering. With a join effort the user will feel heard, understood and supported by the resources to be successful.

Psychology plays a major role into the information and how it comes across through the application. To be able to understand the elderly age bracket of 50 and older will allow us to create empathy for their need and not what we think they will need. By finding studies of their

fears and capabilities of learning and memory will not make them feel like they are not smart but just that they are not up to date with the world changes as many in the younger age group are.

With the business plan we have to also think about image which is joint with psychology and marketing. The marketing will be determined based on audience and what do they do most on the technology they use. Facebook is a large social media platform that all age ranges us to stay in touch with what is going on with others and join groups for similar liking. With our Marketing we will focus on Facebook advertisement, Magazines in facilities that the elderly are most commonly known to go, and even to events that cater to older members. Newspaper can also be a nice touch because many of the elderly audience still have and read newspapers because that is what they are accustomed to.

Finance will be used within our innovation to know what is being spent in order to gain. The more we spend on the product for advertisement purposes we should have a goal to double that which finance will be capable of keeping track of money spent and made. With our application being a 7-day free trial, they can create a suspected subscription once there is a pattern of downloads. With tracking the subscriptions, we can determine the monthly income and be able to edit and ask the opinion of the users of what else is needed or is not helpful in order to keep updating the application. Since we will be having a chat box and a search at the top we will also need staff which finance will determine who is needed and the cost of having the help.

Last but not least is Leadership, this is an important role because it is similar to a person being an overseer of the everyday business. A leader will know how to communicate expectations, changes, updates, and any news to keep everyone on the same page. A leader is able to combine all the disciplines listed and use them jointly to be able to work as a team. In our

group we had three cyber majors and one interdisciplinary study major, and the gap was filled with these multiple disciplines being studied.

The overall success will be determined by the users because they will be the party that downloads, pays monthly and gives guidance on what is needed or changed. The application being profitable will let us know that we have loyal customers and customers that are benefiting through their confidence and safety for cybersecurity. To know the revenue, we will monitor the downloaded application and subscriptions but also views on the Facebook page that give customers access to leave comments and concerns.

An effective innovation is an innovation that helps society in some form of way. I would suggest that our innovation for creating a business plan to help the elderly is already a step in the right direction. In order to know if we are effective with the use of the app and its purpose, we would need to collect data from the cybersecurity analysis for the rate of the elderly affected by cybercrime about every 6 months to a year. If the rate of cybercrime decreases and the elderly are not as high on the vulnerability and risk rating, then we know that the impact has help avoid cybercrime.

Another way that involves the user, so they can be heard is to give surveys every couple of months on the application. The survey will go from the range of the speed of the application, to how easy is the app to use, to what concerns does the customer have. With the customer feeling like they are being heard will build good relationship and trust that they can rely on meeting the customers needs to our fullest capability.

I would like for it to be effective enough that this app is talked about among many groups of individuals that can self-promote how it changed their lives and have others join the experience. Eventually facilities may ask for us to come out and speak on the benefits of the cyber application that we call All Safe because even though it targets a specific group it is not limited to only information for them. With the more marketing ability, the more profit we will be able to make to upgrade features and have around the clock assistance on monitoring changes in the economy as well as the application.

To make an innovation project into reality it starts with several brainstorming ideas. Brainstorming begins with thinking about what is needed in the world to make life easier for the everyday person. No idea is a dumb idea at this point of the process because it adds creativity that can be useful. The second steps is planning, it is when ideas become one and can either be combined or removed from the process. When planning it considers who is the audience, what is the goal, and why is do we need to create this innovation. Business plans work better when there are multiple disciplines playing a role in this process because it adds knowledge to the final idea that maybe one discipline may have neglected. This is how our team came up with our entrepreneurship endeavor.

Our application is called ALL SAFE, it is to not just to be a temporary fix for problems but an instruction manual that never gets old for cybersecurity. We had to choose an age group that is the most vulnerable but also the worst affected when they experience cyber-attacks. With the journals we used early they support this statement because it doesn't only affect them financially but also mentally and emotionally leading to severe consequences like death due to the stress.

With the knowledge and notes of what we want our development to serve as and be catered to can help us move onto making it reality. The app will educate the attended audience with general information about the importance of cybersecurity and taking the first steps into awareness. We will have the app like a newspaper but online form with recent events that occurred with cyber threats to business that people use whether it's a dating app, amazon, or even a bank. As we draw in the elderly with this type of information since it is current and interesting news that isn't usually commercialized, we will continue with then providing information on cybersecurity. This information will be by providing guidance on how to use technology safely, word choice for fraudulent request from unknown numbers, and even security features to protect important personal information. It will be an app used to help with determine what to do in a questionable situation when it comes to using technology.

With having so much useful information on an application we will make sure the website flows seamlessly without any hiccups or delays. With the site being simple to use we have to create a design that provides where each item will be located and displayed. With going into detail on the app we will offer a read more that will not redirect but have webpages that are safe to get more information from on the specific topic. A feature we could offer is a thumbs up or down which will let us know how to continue to provide just enough information to gain knowledge and awareness but not confusion the minds of the reader. We must remember that with age the memory holds less unless repetitive as well as be judged quickly with too much information that is not helpful. To be able to develop we will need a group of individuals to interview the elderly and ask what their dislikes on apps they are currently use and what do they like the most so we are able to incorporate that into what we are offering since this is an informative app we must keep them involved and reoccurring visitors.

Once we collect all the important information up and running, we will be able to have a trial period where assign different disciplines to review and give feedback on the system and its features. In order to have a great app we need professional opinions that are not within the same discipline to give their perspective on how useful and easy to use the business idea actually is. Once the trial is complete, we will market the product through Facebook and create a page that will be for groups that have experienced cybercrime or have questions that will redirect them to the app for further assistance.

The next steps for our entrepreneurship will be not just have an app but service those in companies and try to have them advertise the product to other age groups to spread awareness. The steps in order to achieve this goal is to continue to market to the intended audience and show support in several avenues. I believe that it is important to continue to try to work with other disciplines when it comes to the aspect of closing the gap because it takes more than just information to keep subscribers involved and want to continue their memberships. We will need to offer seminars and video chats for classes that also show a sense of presence in the future. The more the audience knows there is a person behind the development that just wants to build a strong group of individuals they tend to stay involved and give better feedback.

In this class I learned that just because interest or majors are different it does not mean that we cant have the same end goal. With an end goal it may take different paths to get their but it still leads to the same destination which is a great example for this class and the project as a whole. I do wish we interviewed a couple of elderly members we may know to understand how they feel about technology and see what their daily day looks like whether that's using technology or not. I feel like getting to know their uses and their fears could of made the paper more personal but also the idea behind our business idea. I also next time would consider making

the project a nonprofit and seeing what avenues we would be able to explore that won't build a profit but maybe a large follow base and decrease cybercrime.

In conclusion, Cybercrime is not going to end with an invention to make other more informed on the matter, there will always be someone out there finding ways to work a system for their own beneficial gain without concern of who they left as a casualty. It starts with all people finding ways to educate themselves with the things that they use that put them at risk. The cybersecurity world has grown around the world because the need for it will always increase as technology becomes the main source in the world.

Technology is used no matter where we go whether that is in school, work, or using the gps to get to an unfamiliar location we still make ourselves vulnerable. Vulnerability can cause a loss of confidence and safety that does not go away in one night or once the situation is over. With the application called ALLSAFE that our team created was for these people that never forgot the time they were at risk, or received phishing emails, or scam calls wondering how my information got out or what did I apply for to get my number on this list. There are several answers but the most important one, is a safe mindset and cybersecurity a step in the direction for your precaution.

Work cited

Lee, Claire Seungeun, and Yi Ting Chua. "The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States." *Crime and Delinquency*, 2023, pp. Crime and delinquency, 2023.

Craig, D., Diakun-Thibault, N., & Purse, R. 2014. Defining Cybersecurity. *Technology Innovation Management Review*, 4(10): 13–21. <http://timreview.ca/article/83>

Jacob, J., Peters, M., & Yang, T. A. (2019). Interdisciplinary cybersecurity: Rethinking the approach and the process. *Advances in Intelligent Systems and Computing*, 61–74. https://doi.org/10.1007/978-3-030-31239-8_6

blackwood-brown , C., levy, Y., & terrell, steven. (2014). *Senior citizens and cybersecurity awareness - nova.edu*. senior citizens and cybersecurity awareness. <https://www.nova.edu/gwep/igti/presentations/2016-igti/senior-citizens-and-cybersecurity-awareness.pdf>

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022, February 17). *Cyber risk and cybersecurity: A systematic review of data availability - the Geneva Papers on risk and insurance - issues and practice*. SpringerLink. <https://link.springer.com/article/10.1057/s41288-022-00266-6#Sec3>

Trope, Roland L. "“There's No App for That’: Calibrating Cybersecurity Safeguards and Disclosures.” *The Business Lawyer*, vol. 68, no. 1, 2012, pp. 183–195.

Radziwill, N. M. (2018). Cybersecurity leadership. *Quality Management Journal*, 25(2), 109–109. <https://doi.org/10.1080/10686967.2018.1436356>

