Cybersecurity Innovation: Cybersecurity Awareness group

Connor Williams

Department of Cybersecurity

ENTR 494: Entrepreneurship in Cybersecurity

Professor Akeyla Porcher

November 21, 2022

Cybersecurity Innovation: Cybersecurity Awareness Group

Introduction

Cyber-crime is a problem that is growing in scale. As technology progresses, criminals are adapting to the cyber world and finding innovative ways to exploit technology to commit cyber-crimes. Cyber-crime is a criminal activity that is carried out by means of computers or the internet. Common cyber-crimes are phishing scams, website spoofing, ransomware, and malware. Many people fall victim to cyber-crimes and do not have the knowledge to protect themselves or how to respond to a cyber-crime incident. Technology is always improving and cyber-crimes become more sophisticated along with it. Being secure on the internet can be complicated and the knowledge to keep yourself safe needs to be readily available to all people.

My team's innovation is a cybersecurity awareness group. Our awareness group would host workshops to educate people on how to become more cyber aware. We would work with businesses, organizations, and individual people who need help with improving cybersecurity or responding to issues with cybercrime. The goals of this project are to close the skills gap in the field of technology and to raise awareness of cybersecurity and how to deal with cyber-crime. The gain from this awareness group would not only benefit the companies, but also educate those who are unaware of the actual facts of cyber-attacks and how they happen. The workshops will be treated as a training course to inform businesses as well as individuals what to look out for, and the differences between unsafe treading, and safe treading online. As many successful ideas need options, we are also proposing a protocol handbook within our cyber awareness program that can be useful for the businesses who seek to have information at their fingertips. This can not only give insight on how to prevent or recognize cybercrime, but also to understand how to handle the crime after it has been committed. With the growth of technology rapidly changing, and the new ways cybercrimes are being committed, this program can be helpful to everyone.

Literature Review

Cybersecurity Knowledge: Individuals

One of the focuses of our innovation is to help individual people expand their knowledge of how to stay safe in the cyber world in order to help prevent cybercrime. Many people do not have the knowledge they need to stay safe online and to protect their personal data. The information can be hard to find and can take time and energy to implement. For the less technically savvy individuals, the information can also be confusing. People are also becoming more and more reliant on computers and technology in their everyday lives. It can be very hard for people to keep up with technological advancements. Cyber criminals continue to get smarter and use technology to their advantage. Cyber criminals target people who don't have the knowledge to defend or keep themselves safe. Many people just don't have the time in their day to become a cybersecurity expert. Our innovation will bring knowledge to one place and make it easy for people to be able to implement cybersecurity into their daily lives.

A study was done among students of Majmaah University to assess the cybersecurity awareness of the students. The study was done using a 50-question questionnaire that included "demographics (5 questions); Internet usage (10 questions); the use of security tools, such as anti-virus and firewall (7 questions); phishing awareness (5 questions); cryptology (8 questions); browser security (5 questions); social networking (4 questions); and cybersecurity knowledge (6 questions)" (Alharbi & Tassaddiq, 2021). Some of the findings of the study showed that a significant amount of people were lacking some core cybersecurity fundamentals. It also found that 30% of the students did not have any form of antivirus software on their devices.

Additionally, 21% of students did now know the risks of “installing free software from unreliable and unknown sources” (Alharbi & Tassaddiq, 2021).

As the study showed, there are a significant number of people who do not have a lot of knowledge about cybersecurity and are in need of education or training on common cybersecurity practices. Our business would be an organization that would help people who do not have that knowledge. We would host workshops and seminars to help educate people. By providing handbooks and access to online resources, people would be able to have something they can reference in order to improve and maintain their cyber security.

Cybersecurity Knowledge: Businesses

Businesses are a target audience of our organization. We want to help businesses improve their cybersecurity capabilities and to help startups with the basics of cybersecurity. Many small businesses may not be able to afford staffing a full information technology (IT) staff to handle their cybersecurity needs and one cyber-crime incident can be devastating to small start-up businesses. This would be different than helping individuals and we would be more involved with the business because cybersecurity for businesses is more complicated. Businesses are responsible for a lot of their customer’s data and need to take steps in order to ensure that their customers data is secure. As a customer you trust that the data you give to businesses, like your credit card information and account passwords, is safe and secure. People can lose trust in an organization if they do not take the steps to secure customer data.

An analysis was done on the directors of ASX 100 companies (the top 100 companies listed in the Australian stock exchange) on the cybersecurity skills and knowledge of the directors. They found that only 1.8% of these company directors have cybersecurity experience and that “those directors are distributed among only 5 per cent of ASX 100 companies” (Phair &

Alavizadeh, 2022). They also found that “78 per cent of directors have neither cyber nor technology-related experience and background” (Phair & Alavizadeh, 2022). This shows that many companies have leaders that do not understand cybersecurity. Many of them may understand the importance of cybersecurity but do not understand how and what they need to do to stay secure as a business. Our innovation would be able to help people like company directors with cybersecurity consulting and to help close the knowledge gap in businesses. A focus of our innovation would also be to improve the employees’ levels of cybersecurity awareness by hosting workshops to train people that work for those businesses to take that knowledge back to their business and share it with others.

Cybersecurity Knowledge: Government Level

The government is not a target of our organization; however, it is important to understand how prepared the government is with cybersecurity because they write policies that directly affect the people and business that we are trying to help. The government works with businesses and also holds a lot of people’s personal information, such as their social security numbers, tax information, and medical information.

A study was done on American local governments on their preparedness and knowledge of how to respond to cyber-attacks. The study found that the United States government was under “frequent, if not constant, attack” (Norris et al., 2019). The study also found that government employees are not always aware of the best cybersecurity practices and recommends “greater cybersecurity awareness among local government employees” (Norris et al., 2019). The study also found that local governments sometimes lack the funding to improve their cybersecurity capabilities. They recommend that “local governments should be aware of and follow the latest cybersecurity best practices” (Norris et al., 2019). This is where the cybersecurity handbooks that we would make could come in handy. They would be available to anyone who wants them not just business and people. If a local government organization wanted to use our resources they could.

Impact of Cyber Crime

Helping people who have experienced cyber crime is an important focus of our innovation. Cyber-crime can impact people in many ways. It can impact people financially as well as have an emotional impact. Studies done have shown that in cases of fraud "not only that victims suffered significant financial damage, . . . but also that they experienced emotional and psychological impacts" (Notté et al., 2021). Cyber crime is not just focused at going after people's money. It can also be used to try and destroy someone's reputation. The impact could be financial loss due to people's reputation being tarnished that leads to them losing their jobs (Notté et al., 2021). Online sex crimes are also another form of cyber-crime. A form of online sex crimes is called escalated sexting. Escalated sexting is when a person's personal "images get into the hands of someone other than the intended recipient" (Notté et al., 2021). This can lead to a damaged reputation and "in the longer term, victims might develop feelings of paranoia" (Notté et al., 2021). The impact of cyber-crimes is similar to crimes committed offline in the physical world. Cyber-crimes can create impacts that differ from traditional crimes. Cyber-crimes can reach more people because of the way the internet works. Unlike traditional crimes, cyber-crime can have a wider reach. Victims of cyber-crime that have had their reputations targeted can find that a wider audience is reached through the internet. Cyber-criminals that post compromising or reputation damaging materials on the internet can have more widespread and lasting damage. Things on the internet can prove hard to remove so crimes like online sex crimes can place reputation damaging information on the internet for a long time and continue to impact the victims for years. “Victims suffer from double, triple or even quadruple hits; it is the accumulation of different types of impact, enforced by the limitlessness in time and space, which makes online crime victimization so extremely invasive” (Notté et al., 2021).

Cyber-crimes impact business as well as individual people. The impact that cyber-crimes have on business can be different than the impact on an individual person. The internal staff costs that businesses have “neutralizing a cybercrime incident tend to be rather low.” (Paoli et al., 2018). The cost to business with “non-personnel costs are also usually low” (Paoli et al., 2018). Most business reported having no costs “for replacing hardware and software after suffering illegal access, data/system interference, or cyber extortion” (Paoli et al., 2018). Overall, the direct financial cost to the business for cyber-crimes is very low. The impact that cyber-crimes have on businesses are that they can cause harm to their internal operation as well as “the services to customers, reputation and privacy” (Paoli et al., 2018). The ways that cyber-crimes can impact a business financially is how much a business spends to protect themselves against cybercrime. (Farahbod et al., 2020).

Cyber-crime can also impact the economy. The economy drives this world and there are many things that can affect the economy. The effect that cyber-crimes have had “cost the global economy from $300 billion to $1 trillion” (Farahbod et al., 2020). The impact of cyber-crimes on the economy can lead to increases in the cost of goods and services overall. When the economy is suffering the public suffers too as a result.

Increase in Number of Cyber-Crimes

Crime has always been a risk people faced every day for as long as societies have been around. Cyber-crime is a form of crime that has been on the rise ever since the inception of the internet. As time has progressed and technology has improved, cyber-crime has been growing exponentially. As more people have access to technology and the internet and businesses and people become more reliant on such technology to go about their daily lives, cyber-crime has become much more prevalent. Since the Covid-19 pandemic in 2020, cyber-crimes took off even more than they have before. More people started working from home and using the internet to do things that they would normally have done in person. More things have become available on the internet and people are relying on the internet to conduct business meetings, shop for groceries, bank, buy fast food, etc. Since more people are working online from home, “cybercriminals are maximizing the new opportunities related to the rapid increase in working from home” (Monteith et al., 2021). During the beginning of the pandemic “over 116,000 coronavirus themed new domain names were registered” (Monteith et al., 2021). Of these domains, 2000 of them were malicious with over 40,000 of them associated with malicious URLs. The UK saw a big “increase in cybercrime during the pandemic” (Monteith et al., 2021). These increases affected individuals more than organizations. With cyber-crimes becoming more prevalent cyber criminals are able to reach people who don’t have the information they need to stay safe. These cyber-criminals often try to scam their victims rather than trying to hack them. The victims of cyber-crimes “may not be sufficiently suspicious, may not be able to detect fraudulent messages, or may not pay sufficient attention to stop a fraudulent process” (Monteith et al., 2021).

Importance of Cybersecurity

Cybersecurity for the average person may not be that important. Not many people think about cybersecurity as a part of their daily lives. Going on the internet should be treated as a place where someone may try to steal your information. Like going out at night there is a chance that you can get robbed and most people take precautions when going out to keep themselves safe. When on the internet you can be at risk for cyber-attacks, cyber scams, or cyber-crimes. It is important for people to take precautions to keep their personal data secure. Businesses also must take cybersecurity very seriously and it should “be considered a critical and core element of any organization” (*Digital defenses: The importance of cybersecurity in entrepreneurial ventures in the digital age* 2022). The main focus for business should be to keep their stored data, to include customer information, safe and secure from cyber criminals.

Cybersecurity Awareness Training

A lot of what we will be doing as a company would be basically cybersecurity awareness training. What we strive to do is to help educate individuals and businesses on the best cybersecurity practices. The workshops we would host would help train people to the basics and standard practices that is required for safe and secure use of the internet. There are some issues with cybersecurity awareness training that we would try to mitigate as best as possible. An issue with many cybersecurity awareness programs is that people may “feel bored with mandatory security training programs that force them to watch uninspiring lectures” (Zhang et al., 2021). Since we would be working with businesses some employees may be required by their employer to attend workshops if they are partnered with us. To mitigate this feeling of boredom we would make our workshops more interactive and not like a lecture that they are sitting in a classroom listening to. Another problem is that “security training programs are not designed to accommodate a variety of learning styles and employee needs” (Zhang et al., 2021). We could mitigate this by offering a variety of training to appeal to different learning styles. Some people are able to learn by just listening to information while some people may need to be more hands on with their training for it to be effective. We would incorporate hands-on training with real life scenarios. Having participants open email accounts with examples of phishing scams or malicious attachments are methods to provide varied training tailored to specific businesses.

Overview of Innovation Related to Classes Outside of Major

PHIL 230E: Introduction to Ethics

Our innovation relates to a couple of classes I have taken outside of my major. I took an introduction to ethics class. This class had covered a lot of morality and ethical questions. Ethics is what a person believes to be right and wrong. This relates to our innovation because of what we are doing. Since our project is based around cyber-crime and helping people who have experienced cyber-crime as well as cybersecurity consulting ethics are a big part of our entrepreneurial efforts. Cyber-crime is something that most people believe as ethically wrong and what we are doing to trying to combat cyber-crime by closing the knowledge gap in cybersecurity. We also have to worry about if what we are doing is ethically right. We don't want to be spreading misinformation that would lead to someone being a victim of cybercrime.

COMM 101R: Public Speaking

In public speaking I learned how to speak in front of other people. I also gained confidence in speaking to other people. Our business model would require us to speak to other people or hire other people to speak in seminars and workshops. Being able to get your point across in an effective way that is efficient and able to be fully understood by a broad audience is important. If we were to hire other people to speak in front of other people, we would still need to ensure that they know how to speak in front of other people in an effective way. Speaking to people is something that you will do every day as an entrepreneur. This project will require us to speak to business people and businesses to understand their needs.

MIL SCI

Each semester, I have taken a Military Science course as part of Old Dominion's Army Reserve Officer Training Corp (ROTC) program. In the classes I have taken for ROTC I learned a lot about leadership and what it takes to be an effective leader. As an entrepreneur you are a leader in a business. A failure to lead the people in your company will lead to your company failing. In ROTC I learned that there is a process to becoming a leader. One of the things I learned is the operational process which is plan, prepare, execute, and assess. As an entrepreneur you must have a plan for everything that your company does. You then need to prepare. For our innovation our preparation would include things like preparing the material that we would cover in our workshops. Executing is just doing the thing that you planed and prepared for. Assessing is the actions taken after executing to determine what can be improved. You assess the planning, preparation, and the execution. You assess to see what you did right and what you did wrong so you can see what you need to sustain and what you need to improve.

ROTC has taught me the importance of the chain of command. In the civilian sector the chain of command isn't as regimented as it is in the Army but it is still important. You follow the chain of command for a lot of reasons. One of the main purposes is succession of command. This is the plan for if someone isn't around or if something were to happen to someone in a leadership position. This tells you who is in charge of what position if someone were to go down. For example, if one of your team leaders at your business gets sick, who is the person that will be the team leader for the day? Or if the CEO of a company dies or retires who is the new CEO? The chain of command is also important for management purposes. It is a lot harder to manage 40 people than it is to manage 3 or for. In the Army it is set up so that you only have to manage 3-4 people and they manage the people under them. A platoon has 40 people in it. The Platoon leader manages the 4 squad leaders. The squad leaders manage their 2 team leaders, and the team leaders manage their 3 team members.

How to Determine if our Innovation is Effective

With our innovation there is a problem that we are trying to solve that we cannot eliminate completely. Our focus to try to reduce the amount of people impacted by cyber-crime by educating people who have experienced cyber-crime. The goal is to help people and businesses that want to improve their security against cyber-crime. To know if our innovation is effective requires us to follow up with our customers. We could also look at the cyber-crime rates to see if they have declined, however, that is very large in scale and it would be hard for us as one organization to have a large impact on the cyber-crime rates. If we were to pick an area where we have a lot of customers, we could take a look at the cyber-crime rates in that area and we may have an impact on local cyber-crime rates and victimization.

Cybersecurity awareness is preventative, and as such, difficult to determine its effectiveness since it's designed to prevent something that is inevitable. Just as bank provide bank-robbery training to their employees, the goal is to educate the employee on how to reduce risk and actions to take after and incident. Completely eliminating cyber-crime is unrealistic. Part of the training is to educate individuals and businesses on the fact that eventually they may be targeted for cybercrime. Cybersecurity awareness training is designed to give employees the basic tools to operate safely in cyberspace.

To really determine if our innovation is effective would require us to reach out to the individuals and businesses that we have helped with cybersecurity and cyber-crime. For individuals we could send out emails that include surveys and or questionaries. The surveys could ask questions about if they have had been affected by cyber-crime since they came to one of our workshops. The questionaries would be sent out a couple months or maybe even a couple years after they attended a workshop or seminar. The questionnaire could include topics that we have covered like cybersecurity practices to see if people retained the knowledge that we shared. For businesses we would work closely with them to see if they have experienced any recent cyber-attacks. Many businesses are constantly under attacks from people trying to gain access to their systems. If they have had successful attacks in the past, we could look at the number of attacks that they have successfully thwarted.

What is Needed to Turn our Innovation into a Reality

Since our innovation is a cybersecurity awareness group the first thing we would need is good cybersecurity information. To turn this into a reality we would do research and get training on cybersecurity. Since our entrepreneurial group has cybersecurity and cyber-crime majors, we already have a lot of good information, however, we want to provide people with the best information possible. To make this a reality we would need to become experts in the cybersecurity and cyber-crime fields. This would require continual training and education on our part to stay abreast of the most current cybersecurity practices and tools.

The second thing we need to turn this into a reality is money. We would need some amount of capital to start our business in order to have the necessary equipment to conduct the workshops. To do this we could go to investors or use fundraising. Another way to raise some money would be to take out a loan to get the business started. By taking out a loan we could get some money that we could use to start our business and we could pay off that loan with money raised from the business. This money would be used to pay for the training we would need to give to any employees we hire as well as used to fund our workshops needs.

The third thing we need is to start hosting workshops. At first it would just be our team running the workshops. We would need to make course plans for what we plan to teach. In order to host these workshops, we need somewhere we could host them. For businesses, we could possibly host them within the business space if they have a large enough group of employees to train. However, for workshops targeted to individuals, we would likely have to rent out space to host the workshops. We would then need to be able to reach out to business and people in order to get people to come to our workshops. This would entail advertising costs and possibly sales or promotion staff to reach out to businesses to secure attendees. After we raise some money from the business, we could hire people to teach the workshops and then start hosting seminars that will be similar talking to a bunch of people on a stage.

We need good marketing in order to reach out to people and businesses. I am not a marketing expert so we would need to hire someone or another company to handle marketing. At first it would just be us doing all the marketing in order to reach out to the people and businesses to get people to come to our workshops. Without people being interested in coming to the workshops we don’t have a business. We need to get the word out about what we are doing in order to get people to come. This might entail hiring promotional support to reach out via social media, direct calls to businesses, or even television advertisements. We also need to make sure we are targeting the right people. We need to conduct research on the people to understand what people we need to target with our marketing. The next thing that is needed is research into other businesses that are doing similar things. To be competitive we need to understand what other companies are doing with cybersecurity training.

There are some things that are required by law for us to legally operate a business. Some states require that businesses are required to register in the state that the business is based out of. This will require us to file for state registration and obtain a business license. We will also have to check with federal and local governments to see if they require us to register with them. The federal government does not require registration but local governments may. If we are to hire employees, we need an employer identification number which we would also have to apply for.

The final thing that is needed is insurance. Workers' compensation is mandatory in most states in order to hire employees. We also need liability insurance to protect against any potential lawsuits. For our offices, we also would need commercial property insurance. Health insurance may be needed depending on the number of our employees and possibly.

Steps After Business is Started

After we start our business, the next step is to grow our business. After we make some money, we will buy our own office building that will have office rooms as well as rooms that we host our workshops in. We will hire a full staff so we can focus on running the business while other people execute the workshops and seminars. We will start renting out places across the country to host workshops on the road. This will be to reach new people all across the country to grow interest in our business.

We will continue to research into cybersecurity and cyber-crime in order to keep our education material up to date. We will start to work on our cybersecurity handbooks that have all the information that is talked about in the workshops. These handbooks will be given out in our workshops and also be available for sale to anyone who wants to have one.

We will get started on a website and online training programs. Having in-person training is good for a lot of people but some people don't have the time or don't want to attend an in-person training program. Being able to take training courses online or just have informational videos will help people who want to learn on their own time. The website will also have information on our workshops and allow people to sign up online. We will also be able to sell informational handbooks on the website or possibly create an online version of our handbook that stays updated. The online handbook could be free for a certain time period for workshop attendees and a monthly fee could be charged for continued access. We can also use the website for fundraising and marketing.

The final next step is following up with our customers. This will allow us to gain feedback from the people who are attending our workshops in order to be able to provide the best information and training that we can. Our end goal is to provide individuals and business with the information they need to stay safe in the cyber realm.

Self-Reflection

This project took a lot of work as a team in order to come up with an idea that worked for all the team members. Originally, I did not like the idea but we had to compromise in order for everyone to be able to participate in a way that was related to their major. Working as a team for this project was hard because all of the assignments were individual. Working together and producing separate projects taught me to be able to work as a group but also be able to understand that individual effort is important. The online format of the class also provided some hurdles as it took some coordination in order to "meet" with our group and make decisions.

Our project has value in not only the innovation but also the process that it took for us to turn ideas into assignments. Working as a team is important for everything in life and things become much easier when you are able to bring ideas together. The value in our project can be found in our research. The facts about cybersecurity and cyber-crime show how much the world needs cybersecurity. Much of what we do today is reliant upon online systems and the internet. Fewer and fewer things require a physical presence, and people can be "virtually" robbed simply by having their identity stolen, banking accounts compromised, or credit card information hacked from an online retailer.

I learned a lot from this project. Most importantly was teamwork. I also learned about what it takes to be an entrepreneur. An entrepreneur in my opinion is an innovative leader. To be an entrepreneur you must be able to lead your business to success. I learned a lot from my own research that I did for this paper. I already knew a lot of the facts about cybersecurity but cyber-crime facts gave me the most value out of this project. Learning about the impact that cyber-crime has on people makes cybersecurity even more important to me.

If I were to do anything differently it would be to work better as a team. At first, I didn't understand why we were working as a group if we were to produce different assignments, however, I see the importance of that now. Working as a group teaches teamwork, shared perspectives, and producing our own assignments shows the importance of individual effort.

References

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2), 23. https://doi.org/10.3390/bdcc5020023

Digital defenses: The importance of cybersecurity in entrepreneurial ventures in the digital age. (2022). *Strategic Direction*, *38*(2), 24–26. https://doi.org/10.1108/sd-12-2021-0159

Farahbod, K., Shayo, C., & Varzandeh, J. (2020). CYBERSECURITY INDICES AND CYBERCRIME ANNUAL LOSS AND ECONOMIC IMPACTS. *Journal of Business and Behavioral Sciences, 32*(1), 63-71. http://proxy.lib.odu.edu/login?url=https://www-proquest-com.proxy.lib.odu.edu/scholarly-journals/cybersecurity-indices-cybercrime-annual-loss/docview/2426140034/se-2

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current Psychiatry Reports*, *23*(4). https://doi.org/10.1007/s11920-021-01228-w

Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2019). Cyberattacks at the Grass Roots: American local governments and the need for high levels of cybersecurity. *Public Administration Review*, *79*(6), 895–904. https://doi.org/10.1111/puar.13028

Notté, R., Leukfeldt, E. R., & Malsch, M. (2021). Double, triple or quadruple hits? exploring the impact of cybercrime on victims in the Netherlands. *International Review of Victimology*, 026975802110106. https://doi.org/10.1177/02697580211010692

Paoli, L., Visschers, J., & Verstraete, C. (2018). The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium. *Crime, Law and Social Change*, *70*(4), 397–420. https://doi.org/10.1007/s10611-018-9774-y

Phair, N., & Alavizadeh, H. (2022). Cybersecurity skills of company directors — ASX 100. *Journal of Risk Management in Financial Institutions*, *15*(4), 429–436.

Zhang, Z. (J., He, W., Li, W., & Abdous, M. H. (2021). Cybersecurity Awareness Training Programs: A COST–benefit analysis framework. *Industrial Management & Data Systems*, *121*(3), 613–636. https://doi.org/10.1108/imds-08-2020-0462