Academic Paper

Hannah Bass

CPD/ CYSE 494

Old Dominion University

4/21/2023

Problem and Innovation Overview

Cybersecurity is an ever-growing field with a tremendous need for skilled workers and upon initial thought, one might think that cybersecurity is only needed within big businesses and government agencies. This is an inaccurate way of thinking and could be seen as feeding into delusion; more accurately, small businesses also need cybersecurity. Just because these businesses are small does not mean that they will not encounter personally identifiable information (PII) which must be properly secured. Additionally, small businesses have much more to lose if they fall victim to a cyber-attack. They are called small businesses for a reason. Most of their funds are pushed toward getting their business up and running. Their focus is most likely on marketing, product fulfillment, and creating a profitable atmosphere. Cybersecurity tends to be an afterthought when resources are strained.

Having a cybersecurity presence in small businesses is a reasonable goal in theory. However, expecting this outcome without guidance, training, or tools can potentially set the business up for failure. How much do these companies know about cybersecurity? Do they add a mixture of capital letters, symbols, and numbers in their passwords? How many employees and owners use at least eight alpha/numeric characters for their password? Are they informing their workers about phishing schemes? Is there a set of workers dedicated to securing the networks? All these questions seem like common knowledge to those who study cybersecurity, but this is not always common knowledge amongst laypeople. There must be a way to help them not only combat ignorance but also the issue of no cybersecurity.

My group's entrepreneurial venture could potentially combat this problem through the use of Virtual Reality (VR) to conduct training for the general staff and specialized training for

the cybersecurity team, since VR already widely exists. VR is widely known because of its use in video games. Everyone has that friend that uses the VR headset, that gets too into the game and ends up punching a wall. VR, however, does not start and end with video games. This technology has already started being used in learning efforts. For example, pilots often use simulations to practice flying and landing airplanes. Nothing is stopping cybersecurity from doing the same.

Virtual reality training for cybersecurity is the main idea, but this entrepreneurial effort is deeper than that. Our company will mostly serve as a software-based company. This means that companies have the chance to hire our company to create specialized software that uniquely aligns with their cybersecurity goals. Nevertheless, there will also be other premade software available for purchase that includes the basics of cybersecurity training. Basic cybersecurity training does not include specific training for an already established cybersecurity professional. Essentially, this sort of training is to educate already established workers in real time. This software will be offered at a discounted price to ensure accessibility. While this might work for some companies for the time being, it will be made abundantly clear that purchasing uniquely made software is highly recommended to provide training to a cybersecurity professional based on certain company standards. A basic training package will be designed for those who are in desperate need of a quick and affordable adjustment. For this reason, those who choose to purchase the basic training software will be offered a discount on the eventual purchase of uniquely made software specific to their business. All software sold will come with regular updates and vulnerability patches to ensure security. If our business is preaching cybersecurity but does not practice cybersecurity, we would be considered hypocrites.

In the spirit of accessibility, our company will also provide the option to rent VR headsets that are required to utilize the software we offer. The rental periods can be short-term, long-term, or even rent-to-own. This is especially useful for companies running on limited resources and cannot afford a headset. Regardless, of if a company chooses to rent or own, the software will work across different devices and produce outstanding results.

Literature Review

As mentioned earlier, there is an ever-growing need for cybersecurity. One journal outlined the release of President Biden's executive order related to cybersecurity in the United States (Koseff, 2023). This executive order will encourage companies and government entities to work together to enhance security efforts and prevent cyber incidents that result in large amounts of data loss (Koseff, 2023). Essentially, this executive order diminishes any division between the private sector and government as it pertains to cybersecurity (Koseff, 2023). It is recognized that a considerable amount of the cyber realm is connected to the private sector and therefore they need to not only keep up with the varying threat landscape but also work with the government sector to maintain security in their products/services (Koseff, 2023). This says a great deal about the need for a cybersecurity presence within companies.

Presumably, the breaking down of barriers between the private sector and government sector to enhance cybersecurity will put a never-before-seen expectation on companies. If companies have little to no cybersecurity presence now, then they will be expected to have one in place now. Companies now have the government in their corner and are being recognized as a vital component in keeping the nation secure. Government guidance will only work in the private sector's favor. Whenever these sorts of initiatives occur, one can expect the number of job openings to skyrocket, leaving most companies without the proper amount of workforce to meet

added expectations. This translates into an even greater need for capable cybersecurity professionals. To create skilled cybersecurity professionals, proper training and education must be in place and available. VR has the potential to create this caliber of cybersecurity professionals with ease. Traditional learning can take years to achieve, which is exactly why something has to give. Fast-paced careers require expeditious environments capable of keeping up.

Another journal talks about cybersecurity as it relates to small businesses (Raineri & Resig, 2020). Small businesses tend to be easy targets when it comes to anything negative related to the cyber realm (Raineri & Resig, 2020). This is because small businesses assume that being a target in a cyberattack is unlikely for them, thus they neglect training (Raineri & Resig, 2020). Unfortunately, criminals already know the lack of readiness these businesses have in the face of cyberattacks (Raineri & Resig, 2020). Additionally, these small businesses do not have employees who are specifically knowledgeable in technology or cybersecurity (Raineri & Resig, 2020). Verizon found that 43% of small businesses experienced a cyberattack and 60% of those businesses had to shut down because of the cyberattacks (Raineri & Resig, 2020). Prince and King found that although the majority, 98%, of small business owners felt as though they put security as a priority, only 43% actually put security measures in place (Raineri & Resig, 2020).

Unquestionably, the cybersecurity landscape in small businesses could be better. The overarching theme, however, is that they do not have the proper training. A company, like ours, that provides software specifically tailored to small businesses to conduct training through VR would alleviate the issue of non-cybersecurity compliance for small businesses. This would alleviate pressure on owners worried about how to enforce cybersecurity training because it would be prefabricated in a ready-to-use form. Additionally, small business owners would not

have to consider travel to various locations to complete these pieces of training, for themselves or their employees. Ultimately, our software-based company cuts out the middleman and fast-tracks efforts. Experiencing the training through VR also allows the individual to get an all-encompassing idea of what it might be like to promote proper security measures and experience cyberattacks. Normal training modules can be great to enforce concepts, but experiencing cybersecurity in the metaverse will provide an enhanced experience that will stick with the individuals forever. Most importantly, small business owners will sleep better at night knowing they have at least tried to avoid being a part of that statistic of small businesses that had to shut down due to a cyberattack.

Cybersecurity is considered an interdisciplinary career, meaning that it involves many disciplines to combat a unique problem. Some of these disciplines include computer science, psychology, criminology, law, and even mathematics. Perhaps, this entrepreneurial effort can look past the use of VR in cybersecurity and look at how other careers are using this groundbreaking technology to prove to all that VR has to offer. The effectiveness of VR training programs has been researched to improve surgical performance in conducting incredibly important or risky procedures such as colonoscopies (Sugden et al., 2012). Within this specific research study, there were a total of 50 physicians with varying levels of experience (novice, intermediate, and experienced) in performing the colonoscopies (Sugden et al., 2012). The specific device used to carry out the VR training program is known as the Olympus ENDO-TS1 VR colonoscopy simulator and includes an array of advanced technologies such as haptics and quality resolution (Sugden et al., 2012). As a result of the study, it was found that the educational program created for VR colonoscopies was successful in improving performance, as long as the

program was created specifically for the individual and the feedback provided was abundant (Sugden et al., 2012).

Medical professionals can utilize the VR tool to practice any number of procedures. The question, however, is whether VR can be used in the same manner, for cybersecurity specifically. For example, if someone does not get a colonoscopy, they run the risk of having colon cancer and not knowing it. Whereas, if businesses do not have cybersecurity in place, they run the risk of being hacked by cybercriminals, and losing the personal information of their customers which also puts the customer at risk. Meanwhile, when cybersecurity is not enforced, there is a risk of this data getting into the wrong hands or even worse, outages of critical infrastructure. This leaves both the business and the consumer having to pay the price for cybersecurity not being in place. Healthcare is pushing forward with VR training for colonoscopies, but cybersecurity is not pushing the VR training option at all. Perhaps it is time for cybersecurity to take notes from the medical field and utilize VR in training programs.

To further provide examples of VR being used for training purposes, one can look at the use and potential use of VR training for anti-trafficking and what it has done for the general public (Borrelli & Greer, 2021). The California Cybersecurity Institute is fully invested in making a fully functional VR training apparatus to prevent trafficking (Borrelli & Greer, 2021). It was found that the use of VR training provides people with a learning experience that is impactful when users are given the power of decision-making (Borrelli & Greer, 2021). This is because the person undergoing the training can repeat situations in a VR environment as many times as they want. One concept known as “Edgar Dale’s Cone of Experience”, (Borrelli & Greer, 2021, p. 3) states that 90% of learning is accomplished through experience. With that being said, it is important to note that in order for VR training to be successful, there needs to be

coupled in-person learning, storytelling, and re-playability (Borrelli & Greer, 2021). However, concerning cost, VR training is affordable in comparison to in-person training (Borrelli & Greer, 2021).

Surely, just as the example of VR training for colonoscopies can provide insights, Anti-trafficking VR training also provides insights. VR training is quite robust in what it does for advancing people's learning. It is astounding that they found a way to implement VR training to accomplish their own needs. This just further emphasizes the need for cybersecurity to hop on the same trend. The works involving the California Cybersecurity Institute (CCI) also provide good advice on what to include in a VR training program. So, if an entrepreneur, like us, is looking to create their own VR training program but for Cybersecurity in businesses, they might take what CCI has done and incorporate it into their own program. In our case, it would be helpful to consider storytelling that requires an individual to make decisions while in the simulation, re-playability, and provide an introduction course that goes over basic information on cybersecurity.

While it is evident that VR training programs do exist, the skills in the cybersecurity workforce need to be analyzed. Are current employees in the cybersecurity workforce skilled enough? Are there enough people trained? Looking at the problems in the cybersecurity workforce can help answer these questions (Hill, 2020). Hill (2020) describes the problem perfectly by acknowledging that the problem is that there are not enough workers ready to fill the open positions, there are not enough workers skilled enough to keep up with the rapidly changing cybersecurity environment, and there are not a lot of businesses that can keep up with the cost of finding and maintaining a skilled cybersecurity taskforce. Skilled workers do not only need to know about cybersecurity when entering the workforce, but they also need to know about the

business's mission (Hill, 2020). This is so that when they are working, they will be able to provide security that works appropriately for the business (Hill, 2020). Businesses also need to understand that they must invest money in training alongside their cybersecurity presence (Hill, 2020). Furthermore, without a competent cybersecurity workforce, businesses run the risk of tampering with the economy by losing profit, compromising the availability of services, and disheveling customers' privacy (Hill, 2020).

Given the information, the point that cybersecurity training is vital, is reiterated once again. Businesses must decide if they are willing to run the risk of their businesses taking a beating. Money is hard to come by within small businesses, so, understandably there is hesitation in investing money in cybersecurity training. However, if the business has a source that provides the training for them, then they are doing their part in making sure that the workforce gap closes. This software we provide is all-inclusive and can elevate a business's capabilities. It is time to take the matter of training seriously and try out this new and improved type of training program brought so conveniently.

An additional issue introduces the problem within the workforce gap and also focuses on how training institutions simply cannot keep up (Beveridge, 2021). A solution to increasing the amount of realism used within the training is by incorporating simulations (Beveridge, 2021). As the world progresses, there is a push towards online learning in an array of fields and when they are not coupled with experience, learning is not as impactful (Beveridge, 2021). Virtual training is becoming an avenue for cybersecurity training that allows individuals to harmlessly practice skills while increasing their abilities to comprehend especially when the realism within the simulation is high (Beveridge, 2021). This is beneficial due to the harm that could come from accidental damage to systems that could thus be costly (Beveridge, 2021). Additionally, the

nature of the VR training is flexible, engaging, and responsive by giving constant feedback which leads students to reduce stress levels and increase their amount of enthusiasm (Beveridge, 2021). Critical thinking skills are also more likely to be developed thoroughly in those who go through simulations (Beveridge, 2021).

A company that offers virtual reality training software to businesses interested in developing their cybersecurity workforce can be a reality. This company will offer impactful learning and training that will impact the individuals involved forever. Mistakes in cybersecurity are costly and these mistakes cannot be blamed on employees if the business has not taken action in providing their workers with the proper knowledge to succeed. The employee could practice on a business's actual system to figure out the specific controls themselves but that truly is not a viable option. The employee could break the system or feel as if they are not in the proper space to grow as a cybersecurity professional simply because they are stressed out practicing in a live environment. This is a high-stress way of learning; there are real consequences to the failure involved. Furthermore, it is evident once again that VR training has the capability of impacting learning significantly, especially when there is feedback involved.

For an aspiring VR software development company to succeed, there must be information available to show this has the potential to be successful. The preceding information helps to solidify this potential. The technology acceptance model (TAM) provides a way of showcasing how customers amongst varying populations feel about technology (Manis & Choi, 2019). It was found that the market for VR hardware is expected to grow at a compounded annual rate of 56.1% and this proves to be useful in showing that there is a potential for developers, marketers, and firms to have an advantage in the market (Manis & Choi, 2019). The study also found that the response to whether or not the public views VR as use useful was

neutral (Manis & Choi, 2019). Within the writing, usefulness is defined in relation to technology and is whether or not the user finds the technology to be advancing or constructing and with most of VR being involved with gaming it is expected to have a lower score for usefulness (Manis & Choi, 2019). As for ease of use, the public found VR to be easy (Manis & Choi, 2019). Knowing this about the usefulness and ease of use shows the content being presented within VR needs to not only be developed further but also filled with relatable content (Manis & Choi, 2019).

Courses Outside of Cybersecurity That Relate to the Innovation

While the innovation in question focuses on software for VR training, it is still useful to look at works that discuss VR hardware. There seems to be positive growth in the market for VR hardware and this can be perceived as good news for developers like us too. If the hardware market is doing well, there has to be software involved with the hardware to make a VR experience happen. Perhaps it can be expected for the market to be viable for our company which offers specialized software for VR as well. Additionally, what was found about VR hardware being easy to use shows positivity for this innovation as well. Innovations should not create more work for people or be difficult to use. This might prevent someone from buying the product and could stop the up-and-coming business before it is even able to take off. The whole idea is to make training easy, and it is good to know for sure that the hardware will not be an issue for the small businesses that are the targeted market. Furthermore, it was said that VR needs to have engaging content for it to be considered something that is useful in everyday life. It is good that our cybersecurity training is engaging in the sense it immerses the user into an experience that gives great results within their cybersecurity program. This will hopefully make our innovation be perceived as useful once it hits the market to thus drive its success.

When someone majors in cybersecurity, they presumably take a lot of cybersecurity courses. The assumption is that most courses are in are mostly in hacking, policy, networking, practice using Linux, and programming. This is somewhat true, but there is a bit more to a major in cybersecurity than just this. There are other classes involved that are outside of the cybersecurity major that is required to make a well-rounded cybersecurity professional and even play a role in this future company that creates software for small businesses. Some of these courses are often found in the early stages of one's college career. These classes are commonly known as general education courses because everyone must take them. The most notable courses that have aided this entrepreneurial venture for me, include college writing, public speaking, and criminology.

College writing courses may be everyone's least favorite, but it truly does play a crucial role in developing skills as a cybersecurity professional and an entrepreneur. If colleges left the requirement of a writing course out of their curriculum, it would be very hard for someone to communicate their development in writing. Unfortunately, there is no way to get out of not writing down the development. Furthermore, college writing prepares an individual to conduct research. The development also requires research and without it, individuals run the risk of failing before even starting. Most of this writing presented is research that proves that Virtual Reality training software for cybersecurity will be a good product to sell to small businesses. Being able to write does not stop at the development of a product either, after the venture is successful writing is going to be a vital component to communicate with potential clients.

Public speaking is another one of those courses that most people dread. Rightfully so, nobody likes to stand in front of complete strangers and speak. The speaking prompts in this course are often difficult for most people as well and require some sort of level of confidence.

Yet this course is intensely important in preparing students for the real world regardless of one's major. Specifically, for this product public speaking is going to be involved when presenting the idea to investors. People must be able to express their products clearly and in a way that sparks the interest of investors. Public speaking has many tactics that are useful in accomplishing this. Some of these tactics include standing up straight, looking people in the eyes while you speak, avoiding the use of "um" and "uh" during the speech process, and sounding lively. When anyone speaks with confidence, others show a return of confidence. Similar to writing in this way, as writing does not end with presenting the product, public speaking does not end with presenting the product. Speaking in front of a crowd is a continuous venture for an entrepreneur; there will be speaking in front of employees, in front of clients, and even at events.

Finally, criminology is another course that is required to be taken that relates to this product as well. Criminology is known as the study of crime and within this course, taxing questions such as why people commit crimes are thoroughly reviewed. For example, within the course, I learned that people with certain personalities or even genes are more likely to commit crimes; criminology is closely tied to cybersecurity for this reason. Cybersecurity professionals must be able to think like a criminal to stop a criminal. The whole point is to always be ahead of the criminal committing the crime to protect the network. This makes this course related to this specific product because this must be something covered within the VR training software to ensure that companies are getting considerable training. Furthermore, as seen above, VR training is starting to be used in the prevention of crime trafficking.

While courses within a cybersecurity major are extremely interesting, the other courses outside of the major are also taken for a reason. They prepare individuals for success no matter what path they choose to take in life. More specifically, however, they prepare entrepreneurs and

cybersecurity professionals to have the appropriate skills to make their businesses that much more successful. Entrepreneurs need as many tools of success that they can get their hands on. Innovation is exciting and so is VR training software for cybersecurity.

How to Measure the Success of Innovation

There is a clear indication that this innovation is possible and viable, and for this innovation, there are a few ways to analyze success. An obvious indicator is what the net profit of the business is each year. Success will show a return on investment thus the profit will be larger than the amount of money that is spent on making the innovation possible. Another way to measure success is to conduct customer satisfaction surveys. After each transaction, the customer will be sent a survey to see how they feel about the product. A Likert-type scale can be used to assess and analyze customer responses to several narrow-field declarative statements proposed to customers as a customer satisfaction survey.

Another point of measurement will be the overall success within the virtual environment. After going through the resources, there needs to be a storytelling or a decision-making element within the training program to make it the most impactful. This means that there is a correct way to progress through the training. The correct way fully finishes the task and forwards a message of success to the users, when the users are unsuccessful at the task they are to complete, they receive feedback to repeat the training until they get it correct. Satisfaction surveys in the form of statements graded with a Likert-type scale can again be used here to assess and analyze user satisfaction. The sorts of declarative statements involved with this survey will be more related to how the user felt while being immersed in the VR environment.

Turning the Innovation into Reality

There are ways to make sure the innovation is viable and successful, but innovation requires steps to be turned into reality. For this innovation, there are quite a few things that would be needed to turn it into reality. First, it would need a set of software developers that can produce not only a VR program but also capable of keeping up with a high amount of work. There will have to be several teams of developers to keep up with demand and to ensure that the work is being done effectively. Second, there would need to be a set of cybersecurity professionals that are highly skilled in cybersecurity to ensure that the content within the program is accurate and relevant. The cybersecurity team would need to also include a separate team dedicated to protecting the networks within the company itself. It would be ridiculous for our company to promote cybersecurity training if it did not have its own cybersecurity team. Thus, an additional set of employees would be needed solely for testing the products before they are provided to customers. Additionally, there would also need to be a marketing team that is tasked with making sure that the company is being represented in all forms of media.

The third step is that there would need to be a set location where the company is based out of. Our company could potentially have one main location with many employees having the option to work from home, though additional technology will need to be available to make this a reality. This means there would need to be company-issued laptops for employees to remotely access the Virtual Private Networks (VPN) and a system that is capable of remotely tracking the employee's workday. These are only a few technologies that would need to be added to make remote work acceptable. Furthermore, there would need to be a database center (which could be virtual), testing environments, and more. With technology comes many avenues of repair. This is

where a dedicated information technology (IT) team would be needed to make sure the technology is running smoothly.

Our venture would also need a human resources (HR) department, which would handle all employee relations concerns, but we would also need a customer service team to be tasked with handling all customer service questions and concerns. This ensures that the company is keeping customer satisfaction at the top of its priority list. There are a lot of employees involved to make this innovation fully successful, but a lot of this is necessary to ensure that a company is capable of running at full capacity and seeing high success rates. At first, the company is going to be considered a small business, so the employees in each group are going to be limited. The focus, in the beginning, is going to be software development and gaining customers.

Furthermore, there needs to be a set amount of VR headsets available for rent for our customer base. Our company promises that customers can rent VR headsets if they feel that purchasing of a VR headset is not within their budget constraints. So, the company would want to start with approximately 250 headsets. This would ensure that there are enough to be rented out to each of the business employees that need to undergo virtual reality training. As the company progresses, more and more headsets can be purchased to be available to rent. The headsets would need to be maintained in many ways as well. Each headset would need to be checked before and after the rental to ensure that it is working properly. Another innovation would be a recycling program for our company to donate broken or unrepairable headsets too, as they do wear out from use. Lastly, there would need to be some sort of system to keep track of how many headsets are being rented out, and by whom.

Next Steps

Cybersecurity and its everchanging environment need VR training to ensure small businesses are capable of keeping up and maintaining a secure environment. Most of the next steps for this innovation are to fine-tune the details to ensure that it will viable business. The next step for our entrepreneurial venture is to figure out a budget, look at the laws associated with the technology and innovation, research the market, and figure out what the mission of the innovation is. All the researched information will go into the pitch of the product in front of a group of investors. Even if the innovation never leaves the bounds of this entrepreneurship class, it will still hold a valuable learning experience for me and my peers alike.

Personally, for me, this innovation has helped me reach goals that are part of a program that I am a part of. The program is known as ODU SFS CyberCorp LeADERS. The L stands for leadership, the e stands for ePortfolio, the A stands for Academic internship, the D stands for Diversity, the E stands for entrepreneurship, the R stands for Research, and the S stands for Service learning. I have created an innovation with my group that allows me to fulfill the entrepreneurship portion of the program, which not only prepares me to be a contributing member of society but will also prepare me to be a great leader in the cybersecurity job force.

Overall, though the next steps involved with this innovation is to revel in the feeling of accomplishment for what was done in this course. I came into the entrepreneurship class thinking that there was no way, a normal everyday person like me, could think of an innovation. It is extremely difficult to step outside of your self-made constraints, but I was able to do that alongside my group members. I am extremely happy with the outcome, and I hope my group members feel the same. Maybe one day VR cybersecurity training will become reality and it helps people achieve all that they are hoping for.

References

Beveridge, R. (2021). *Efficacy of Increasing Realism in Cybersecurity Training* [Ph.D., Robert Morris University]. https://www.proquest.com/docview/2512684617/abstract/7BF20C581E414998PQ/1

Borrelli, D., & Greer, B. T. (2021). The Next Step: The California Cybersecurity Institute's Anti-Trafficking Virtual Reality Immersion Training. *Anti-Trafficking Review*, *17*, Article 17. https://doi.org/10.14197/atr.2012211711

Hill, T. P. (2020). *Cybersecurity Workforce Issues: A Skills Gap or a Leadership Gap?* [D.B.A., California Southern University]. https://www.proquest.com/docview/2522829832/abstract/3A839B57BBA94CF9PQ/1

Koseff, J. (2023). Upgrading Cybersecurity Law. *Houston Law Review*. https://dx.doi.org/10.2139/ssrn.4364356

Manis, K. T., & Choi, D. (2019). The virtual reality hardware acceptance model (VR-HAM): Extending and individuating the technology acceptance model (TAM) for virtual reality hardware. *Journal of Business Research*, *100*, 503–513. https://doi.org/10.1016/j.jbusres.2018.10.021

Raineri, E. M., & Resig, J. (2020). Evaluating Self-Efficacy Pertaining to Cybersecurity for Small Businesses. *The Journal of Applied Business and Economics*, *22*(12), 13–23.

Sugden, C., Aggarwal, R., Banerjee, A., Haycock, A., Thomas-Gibson, S., Williams, C. B., & Darzi, A. (2012). The Development of a Virtual Reality Training Curriculum for Colonoscopy. *Annals of Surgery*, *256*(1), 188–192. https://doi.org/10.1097/SLA.0b013e31825b6e9c