Group E Academic Paper

John R. Wilson

Old Dominion University

CYSE 494 Entrepreneurship-Prof Studies

Professor Akeyla Porcher, MS Ed

05 April 2023

Contents

Group E Academic Paper

Introduction

The modern-day world operates in a technologically enhanced environment with interconnected computer communication networks that brings not only important communication advancements for the human race but also provides opportunities for criminal elements to target unsuspecting individuals and businesses for their unlawful purposes known as cybercrimes. “Cybercrime is the single most common form of crime” (Shaw, 2019). Cybercrime causes victims to experience loss of time, fraud, destruction, theft of personal information or data, and even damage to their reputation. Criminals have many different reasons to use the internet for their criminal enterprise. The internet provides a more economical way to execute their criminal plans because computers are inexpensive to acquisition, access to internet is widely available, and people do not need to physically be at the scene. Therefore, the problem we are addressing is the need to effectively combat the rise of cybercrime because unless society understands the situation, the cybercriminal element will continue to effectively use the internet as a tool for illicit purposes for monetary gain, notoriety, revenge, state sponsored espionage, terrorism, bullying, blackmail, etc.

Similar to Coronavirus Disease of 2019 (COVID-19) pandemic, the cybercrime crisis is not bound to a specific demographic, region, race, sex, religion but affects the entire human community worldwide. Therefore, the responsibility to solve this obstacle is a societal dilemma that can be solved if we choose to help each other to effect better cyber security and internet practices through educating the public on cyber awareness and proper cyber hygiene.

What is the Innovation?

It is a fact that cybercriminals use the internet to callously exploit individuals considered to have low digital literacy and tech familiarity (Anthony, 2023). In order to address the problems surrounding the rising problems of cybercrimes against individuals, we

created a non-profit business responsible for spreading cyber awareness out to the communities that are considered easy prey for cybercriminals. The business would be responsible for the development of cybersecurity education and awareness programs to help spread the mindfulness of cyber-related issues and to instill effective cybersecurity practices.

It is widely believed that individuals who receive cyber awareness training experience fewer cyber related events than persons who have not. Research has found that “companies with an effective cyber awareness training program have fewer breaches than those who don’t” (Byrd, 2022). Cybersecurity awareness training is provided as an annual requirement for employees that work in large organizations like Amazon, Meta, and federal/state/local government organizations. Why are we not using the same research that large companies are utilizing and help educate our communities in need by providing similar type of training to individuals that are not as fortunate?

Our company believes that one of the strongest defenses against cyber-attacks is to educate and train users to be cyber resilient to the kinds of attacks that are known to target individuals that do not possess the financial capability to purchase high-end training. The focus of our business is to provide the consumer with a better general understanding of the kinds of cyberattacks reported and present recommended steps to better secure their own networks and devices. By providing a holistic cybersecurity education and cyber awareness program, the playing field will be leveled between victims and perpetrators.

Target Market

Who does the business target and where will this company operate? It is our vision to begin operations in the Hampton Roads region of Virginia, which includes the cities of Chesapeake, Hampton, Newport News, Norfolk, Portsmouth, Suffolk, and Virginia Beach. However, in the beginning, the company will not cover all seven cities of Hampton roads, Instead, we will concentrate on two of the poorest cities, Norfolk and Portsmouth; because

these two cities have the highest poverty rates in the region with 20% of Norfolk and 17% of Portsmouth live in poverty (Ley & Reyes, 2020).

As for the target audience, we strongly believe this business will be better suited for seniors and individuals that are underrepresented or reside in a low- or fixed-income areas that simply cannot afford to hire expensive information technology (IT) professionals to solve and repair their cyber problems. Seniors “are one of the most vulnerable groups who are prone to cyber-attacks” (Blackwood-Brown, 2017) and they make up 16.18% in 2022 (Roads, 2022) of the population in Hampton Roads. The underrepresented and poor make up approximately 7.71% or 35,287 families in the Hampton Roads area (Roads, 2022).

The Problem of Cybercrime (Review of Literature)

As processes in different organizations become automated, more of the infrastructure continues depending on technology. Automated systems are created by code, which can be accessible by cyber criminals as they breach systems. More processes continue being done digitally, which gives more opportunities for hackers to steal private information. Businesses continue falling under threats, which makes cybersecurity one of the most important aspects of security in the world today, according to Erendor & Yildirim (2019). In the digital age, there are vulnerabilities everywhere. Cybercriminals can target websites, computers, servers, and any technology that is based on code. From car alarms, power grids, security systems, airplane navigation, and communication systems;more products than ever before continue to be at risk for compromise by criminals. Due to the vulnerabilities, different organizations need the best online security strategies to identify and mitigate security threats for dynamic technological innovation. Organizations continue focusing more on cybersecurity as most firms cannot afford a data breach. A breach can cost businesses millions of dollars, which is the reason businesses focus more on mitigating risks as opposed to fixing breaches when they

occur. One of the ways that have been identified as a lasting solution against cybercrime is cyber awareness.

New technologies have led to new criminal opportunities in the digital world. Cybercrime is one of the fastest growing areas of crime today, which involves the use of computers and digital technology to commit illegal activities, such as identity theft, fraud, intellectual property theft, trafficking in child pornography, and violation of privacy. It usually occurs through the internet especially since the use of computers has become important in commerce, government, and entertainment. Cybercrime affects virtually every sector in the world meaning, from private citizens to small businesses and large corporations, and governments. According to Sabillon (2019), most cybercrime attacks are on cybercrimes effect some aspect of individuals' lives, governments, and corporations. The attacks are on the information attributes of the person or organization, which involves compromising the virtual elements of everyday life and databases that the organizations own. There is increased exposure to cybercrime at all levels of an organization due to the adoption of digital technologies. Individuals, corporations, and organizations can also incur massive losses after cybercrime due to effects such as blackmail, breach of intellectual property, compromising daily operations, undermining basic utilities, financial fraud, and loss of private and confidential information.

Causes of Cybercrime

There are many causes of cybercrime, which vary from one organization to another. The main cause is the lack of security assistance. As more people and organizations continue relying on digital technology, few are aware of the simple steps that one can take to increase cybersecurity. More people do not have easy access to experts and resources that they need to improve security. Simple steps like using strong passwords are crucial in preventing cybercrime. A lack of cyber awareness leaves users vulnerable to attacks (Lezzi et al., 2018).

They fail to follow simple steps when setting up security features; such as, creating strong passwords or multifactor authentication. It fails in preventing unauthorized access to personal data and accounts such as social media, emails, and banking. System vulnerability is also a main cause of cybercrime. According to Lezzi et al. (2018), cybercriminals are vigilant to spot weaknesses in different systems and can temporarily block websites, lead to full security breaches, complete crimes, or in other cases, conduct cyber terrorism. Some system vulnerabilities are very dangerous and can have detrimental effects on users. In some cases, employees share vulnerabilities online seeking assistance, which attracts criminals. Other criminals can have access to administrative credentials such as employee cards displayed publicly, which can lead to an attack on an organization's system.

The other main cause is a lack of risk assessment when using cyber technologies. Criminals want people to continue underestimating the vulnerabilities and consequences of cybercrime. As more users continue underestimating what may happen in case of a cyberattack, they fail to assess risks or come up with ways to mitigate them. It creates a bias where users think that the future of using digital systems will be similar to the present. For example, statistically, plane crashes are less likely to occur than car crashes. However, more people continue to have a fear of flying and will prefer driving when presented with the two options. It is similar to cybercrime where websites continue warning people that they are vulnerable to attacks. However, will rarely assess risks when using different sites and fail to implement basic preventive measures that are essential for enhancing security. Most of the causes of cybercrime are based primarily on ignorance, according to Ling et al. (2019). Users may lack basic information on security measures, fail to assess growing risks every day, or may not be aware of the existing vulnerabilities of a system and may ask for security information online, exposing them to criminals.

Cyber Awareness

From the causes of cybercrime, it is evident that most of the causes arise from a lack of information on cybersecurity. Cyber awareness refers to the process of educating and training users about security threats in cyberspace, how to prevent the threats, and what they may do in case of a security breach. It helps to introduce users to a sense of proactive responsibility when using digital technology to keep their personal and organizational information safe and secure. Cyber awareness helps people to know the security threats that they face and take responsibility for avoiding potential risks (Ling et al., 2019). Through cyber awareness, users are informed of the latest security threats and the best cybersecurity practices. Users gain information on the dangers of downloading infected attachments, clicking malicious links, interacting online, and sharing sensitive information. They are also aware of basic security features such as creating a strong password, avoiding writing passwords where they can be retrieved, the privacy of login cards in organizations, and other features that can enhance security. For organizations and governments, employees learn about the security features available in their systems and their responsibility in upholding the security features.

Effectiveness of Cyber Awareness in Combating Cybercrime

Human error is the main contributing factor behind many security breaches in different organizations. The organizations may have security measures for networks and systems in place but still, experience data breaches. Most data breaches are a result of human involvement, such as errors, social engineering, and the use of stolen credentials. Criminals exploit the weaknesses of the human element to infiltrate different systems and networks. Cyber awareness is effective in avoiding errors. According to Zhang-Kennedy & Chiasson (2021), cyber awareness can be effective in reducing up to 80% of the total breaches, which arise from the human element. It helps in educating employees in the organization about the malicious methods that cybercriminals use and how an individual can become an easy target. Programs

also educate the person on how to spot potential sources of threats, such as pop-up downloads on some websites (Hassan, 2023). The person is aware of the steps that they should take not to fall victim to the threats. Cyber awareness empowers users giving them the skills and knowledge to identify and avoid potential security risks before the breach occurs. It informs users of the changing threats especially since digital technologies are evolving each day.

Failure to conduct training in cybersecurity awareness can have detrimental consequences for an organization such as damaged reputation, loss of client trust, and blackmail leading to remediation costs for others (Lee & Shin, 2020). Cyber awareness is a successful cybersecurity strategy since it ensures that the possibility of threats does not arise due to employee vulnerabilities. It ensures that organizations can deal with security threats before they occur. The employees act as the primary line of defense against major threats.

Training and Education in Cyber Awareness

Cybersecurity has become the main priority for organizations of all sizes. Cyber awareness is one of the critical components of each firm's cybersecurity strategy. It involves using tools and techniques that can give employees the knowledge and skills on security risks and how to mitigate them. It helps the employees in understanding their responsibility concerning safety and security in the organization. Education and training involve informing and equipping users about cybersecurity and areas that criminals are likely to exploit. According to Corallo (2022), criminals have found that human behavior and emotions are the weakest links in cybersecurity for any organization. They exploit weaknesses to compromise security for businesses. After training and education, employees are quick to determine sources of threats such as suspicious links on social media (Corallo, 2022). They can significantly act toward reducing the risk of security breaches and incidents. It promotes a culture of an organization that is based on roving security and protecting data assets, which is necessary for the firm's sustainability. Every firm must invest in cybersecurity awareness training and

education to help in mitigating security risks. It ensures that the firm has the necessary security mechanism that can reduce security incidents and minimize losses associated with data breaches.

Training and education for cyber awareness are not reserved for security professionals and IT administrators in an organization, but should extend to other employees in every department. According to Zhang et al. (2021), the scope of training can vary depending on the role of the employees and their interaction with IT systems and networks. It should also depend on the functions of the organization and its digital infrastructure. However, every cyber awareness program must include email security because emails have become one of the most important tools for both formal and informal communication in organizations (Zhang et al., 2021). Most businesses require that employees have an official address to communicate with others, receive memos and information and communicate with clients. However, emails are also the beginning point of different sources of cybercrime such as malware, ransomware, and phishing. Dangerous ransomware and malware enter an organization's attachments and links via emails. Training involving email security helps in identifying unsafe attachments and links (Gale et al., 2022). Cyber awareness training should also involve social engineering and phishing. Cybercriminals are aware of human psychology. They can exploit human emotions and behavior to instigate attacks. The attacks can occur when a person is disclosing is creating accounts on the internet, transferring funds, offering system access, or sharing one's credentials among others. Training helps users in determining areas where they may be targeted and how they can be convinced to share information that can be used for breaches. It is important in spotting warning signs and avoiding falling victim to an attack.

Cyber awareness training also involves informing users of browser security. Web browsers are gateways to the internet that hold large volumes of data and personal information, which makes them hot targets for cybercriminals. Cyber awareness informs users of websites

that are safe to use online through internet security training. It includes the best practices when using specific browsers, social media policies, and sites that are allowed when using official company computers (Alruwaili, 2019). It also trains users on confidentiality when browsing and web safety. Training and education in cyber awareness are also effective in maintaining information security. It involves training users on how to store, share and delete sensitive information in a safe way. It informs users of their legal obligation to maintain information safety in an organization and the legal consequences in case of a breach (Dash & Ansari, 2022). Cyber awareness also informs remote work protocol, which is a new form of working for different organizations across the globe. It informs users of the security risks while working from home or remotely away from the organization's secure systems. It also offers knowledge tools that are essential when using removable media to address risks associated with a virus or malware infection, data exposure as well as data theft and loss. Other areas of cyber awareness include password security and incident response, which are crucial in avoiding and addressing threats respectively.

Cyber awareness is essential in addressing different areas of cybersecurity, which are effective in addressing cybercrime. Most organizations have engaged security experts in creating secure systems and networks, which have security measures that make it difficult to breach. However, most breaches come from the human element, exploiting human error and emotions. Cyber awareness is effective in addressing security threats arising from human aspects. It involves informing users of the available security measures, identifying potential risks, and avoiding them. Cyber awareness cannot be the solution to cybercrime but has proven to be a successful way to address potential risks. However, organizations continue facing security breaches associated with human-related incidents, indicating that there are improvements needed in implementing cybersecurity awareness in both training and education.

Organizations must continue prioritizing training and education on cybersecurity to increase cyber awareness.

How Cyber Awareness Relates to Material Covered Outside of the Cybersecurity Major

Cybersecurity awareness is not only applicable to those individuals who examine and work in the field of cybersecurity but is also essential to other academic areas. Sociology, Engineering, and the Heath Industry are just a few academic disciplines in which cybersecurity awareness can assist other academic areas outside of the cybersecurity major.

Sociology is defined as the study of human behavior in society, including how people interact with one another and the institutions and structures that shape them (Form, 2019). Therefore, sociology is related to cybersecurity in various ways. For instance, sociology could examine human behaviors through cybercrime. Cybercrime is a form of aberrant behavior that involves using a form of technology to commit crimes, such as identity theft, fraud, and hacking. Sociologists can study cybercriminals to better understand the social and economic factors that lead individuals to participate in such malicious activities. They can also explore the ways in which law enforcement agencies and other defense institutions respond to cybercrime and the social and cultural implications of these responses. Another area where sociology and cybersecurity intersect is investigating the broader social and cultural factors that shape cybersecurity. For example, sociologists can explore how gender, race, and socioeconomic status impact access to technology and the ability to protect oneself online. They can also examine how cultural attitudes toward privacy and security shape individuals' perceptions and online behaviors through their interactions online. For example, studying the difference between expectations users in the United States (U.S.) and Peoples Republic of China (PRC). Users in America expect a certain amount of privacy while online which is guaranteed by the U.S. Constitution. However, users in the PRC assume their data is

being monitored by the state as they are known to use sophisticated surveillance technologies that monitor online activity to identify potential threats to social stability. Additionally, the PRC has also implemented a country wide internet security system called, the Great Firewall, which is considered a system of internet censorship and control that restricts access to foreign websites and social media platforms (Ahmad, 2022); whereas the US values freedom of information and has not implemented a country wide internet firewall.

Another academic field that cybersecurity is related to is engineering. Engineering plays a critical role in the design, development, and implementation of secure systems and technologies within computers and other devices. Engineers are responsible for creating the hardware, software, and network infrastructure that form the backbone of modern information systems, and they must consider cybersecurity as a key component of their designs. For instance, engineers must make significant considerations of the security of the system during the development process, from design to final testing. This ensures the systems are using the most up-to-date algorithm's that are known to be resilient to hacking, that the data is protected both at rest and in transit, and that systems will stand-up-to and robust when confronted against various cyberattacks.

Lastly, cybersecurity is becoming increasingly important in the health industry due to the growing use of digital technologies and the need to protect sensitive patient information. Healthcare providers collect and store vast amounts of sensitive protected/personal health information (PHI) about patients, including medical records in a digital format that are shared across different systems and networks. Furthermore, healthcare providers are required to take steps to ensure that PHI is protected from cyber threats. Therefore, the Health Insurance Portability and Accountability Act (HIPAA), was formed to apply strict regulations and standards for the protection of patient data. Another concern in the health industry is the protection of medical devices and systems. Current medical devices, such as pacemakers,

insulin pumps, and other implantable devices, are now connected to networks and can be remotely controlled and monitored. Furthermore, these devices have the potential to create vulnerabilities for malicious actors to exploit. Healthcare providers must consider cybersecurity awareness to ensure that these devices are secure and that they can detect and respond to any potential security threats.

Possessing and understanding cybersecurity awareness has the potential for a lasting positive impact within the academic fields outside of the cybersecurity major. Through increasing awareness of cybersecurity risks and best practices, individuals and organizations can utilize this skill in the academic fields of Sociology, Engineering, and the Heath Industry and throughout a variety of other academic fields like Criminology, Psychology, and Law.

How to Determine Whether Your Innovation is Effective.

The profitability and effectiveness of an innovation can be measured in many ways such as continual upswing in positive money flow, growth of the business market share, and time usually two to three years (FreshBooks, 2019). As with any non-profit organization, the most important measure for this business to thrive and be successful is gaining overwhelming community support through buy-in. Community buy-in is gaining the trust and cooperation of the community about your business. With community buy-in there is a built trust the business will do something positive for the community, helps get everyone in the involved, aids in spreading the word about the program, and helps identify whom needs the assistance, because those in the community know more about their area than an outsider. Without community buy-in the business will not be successful no matter how much time, money, and materials you throw at the problem. For example, if a business were to attempt to open up an outreach program like feeding the hungry without the backing of the community (buy-in), it is very likely the business would fail. This is because trust was not built within the community, the

word does not get out, and there is no buy-in or interest within the community to support the business.

Another important metric that needs to be gauged is the continual success of raising monetary capital through new and continual investors. Finances can quickly cripple business if they run at a loss; specifically, non-profits organizations that need supporters to keep the positive cash flow. Because our organization is non-profit, does not equate the business should not generate a profit. As a matter of fact the business needs to make a profit in order for the organization to stay afloat during times of financial scarcity or insecurity, purchase of materials required for community give back, for the business to expand to other areas, and most importantly to have the ability to meet its financial obligations like paying employee pay checks, rentals on equipment or real estate (brick and mortar), insurance, lawyers' fees, licenses, advertisements, etc.

Other metrics the business can be measured is through data points such as the continual and repeating of returning customers, showing the business makes positive financial decisions with cash flow, how positive the experience and feedback the consumers feel about the services, consumer usage and effectiveness of the products ability to teach the information, how much community involvement we keep and the attraction of new members, and by what we give back to the communities in need.

What Do We Need to Turn the Idea into a Reality?

As with all business start-ups it requires a lot of planning and research to figure out if the idea will either move forward or die on the vine. Since the business is a non-profit organization and it will require some identical planning and information conditions as a for-profit business, such as the creation of a business plan, financial capitol, business name, business license, employees, a marketing campaign, etc. However, because our business is a non-profit, there are some additional requirements. According to the Virginia Chamber of

Commerce (2022), for a non-profit to be legally registered and operate in Virginia the business is required to apply for both state and federal tax exemption status, nominate a registered agent, form and recruit board members, produce bylaw policies, create a organization structure, prepare and file articles of incorporation, obtain an Employer Identification Number (EIN), and pay the startup state costs when starting the new business.

The first thing the business needs before attempting to turn this idea into a reality is the creation of a sound business plan. A business plan is basically a research paper that can help prove or disprove your idea and keep you focused on the needs of your creation. The plan can illustrate your financial requirements, prove you are taking your business seriously (which is important to potential investors and loan officers), assist in better understanding your competitors and customer base, and help focus your efforts. Additionally, the business plan can help attract potential investors, partners, and employees. Another important addition the plan illustrates is it helps you judge the success of your business by comparing the actual operation to the plan. Without the creation of a sound business plan, the organization would be without a proper professional compass to help successfully pilot through potential business landmines that would prevent the idea from succeeding.

Now that we have a sound business plan, the next portion of important business is obtaining the financial capital needed for startup costs such as, materials, marketing, required licenses, lawyer fees, etc. To obtain capitol the organization can attempt to attract investors through community meetings or pitching your business vision or through traditional bank loans or through state run organizations like the Virginia Small Business Financing Authority (VSBFA) that offers loans directly to the business. Another avenue to gain capital is through grants such as the Small Business Investment Grant Fund (SBIG) that can award upwards of $50,000 or even through individual donations through a website such as GoFundMe or Crowdfunder, or even through fundraisers like bake or garage sales.

Now that we have a business plan and some financial backing, we need to have the support of the community the business is targeting through community buy-in. Without community buy-in to the vision, the business will likely not do very well in the target area. You can get the community behind your venture if they agree there is a problem, and they approve with the way your company solves the dilemma. You can also garner favour through volunteering in the area and having discussions with the area's leadership like the religious leaders, community leaders, political leaders, etc. This illustrates that you understand the predicament and you can have a discussion as to how your vision will solving the problem.

Prior to advertising the business, we need to begin producing cyber awareness materials we will be using to educate the masses. The type of materials we will produce is a website that will house future customers to access our materials. If the poor areas do not have internet; then we should be prepared to have in-person group or individual classes so we can educate them on cyber awareness.

Now that we have a plan, financial backing, the community is behind the venture, and we have materials to showcase, we need to tell introduce the business to everyone and we do this through a strategic marketing campaign. Marketing is important here because it is great that we have all the startup needs for the business; however, if no one knows about the business and what we do, then how does the business get going. To remedy this, the business could start off with positing paper flyers in the community of the areas, like bulletin boards, we are servicing, building a webpage, place advertisements in the paper, and through word of mouth which is hopefully already happening if the community has buy-in.

Lessons Learned

The things I have learned from this project is that you cannot start a company and get it off the ground without teamwork. Teamwork is a vital part of the experience as it provides you with a sounding board for idea creation and practicality, keeps you on track, and can

keep the experience engaging. Again, businesses are not built alone, it takes an illustrious team of likeminded people that develop great and extraordinary businesses. I also learned is that I better thrive in a teamwork environment than an independent worker. I enjoyed pitching and defending well thought of ideas and solutions to the problems with a group. I enjoyed the way others brought their perspective ideas and thought of things that I would have never thought of in a million years.

Other lessons I learned from this project were that it took effective research to be able to write professionally and talk effectively about the innovation. You must investigate your topic to make sure that you can portray your innovation in a positive light and because you have researched your idea it can help you defend it against the unconvinced. Another lesson that I learned is how unique the paperwork is between for-profit and non-profit businesses. For instance, my wife has and runs a for-profit business, and the procedures and paperwork were minimal compared to that of a non-profit. A for-profit business needs a business license, proper industry licensure (cosmetology, barber, etc.), a space to work, and a business bank account. However, a non-profit has quite a bit of paperwork to fill out as it is required to not only possess what a for-profit business requires, but also, needs to submit for tax free status, have to appoint board members, etc.

Learning how to create and prepare an elevator pitch was another lesson learned. An elevator pitch is a 45-second to 2-minute short presentation on selling your idea, vision, product to prospective clients or investors. What I can do with this new skill is that I can transpose the elevator pitch to other areas like produce a bio elevator pitch to better sell myself to perspective employers. I could use a video version and upload it to an electronic portfolio, and I can utilize the same strategy to verbally pitch myself when meeting potential employers face-to-face at job fairs or interviews.

Conclusion

Cyber-crime is one of the largest faceless crime crises we, as a society, are facing today. This paper has highlighted the problem of the rampant cybercrimes against the technological illiterate by presenting an overview of the problem and providing an innovative solution through cyber awareness education and training, a short research using academic research information on cyber awareness training and cybercrime, how this business idea can be positively used outside of the information technology field, steps to determine if the idea will be effective, explains a plan on how to turn the business into a reality, and the lessons learned from this project assignment.

Lastly, I hope this innovative idea does do what is intended and that is to help those in need; because we as a society need to do a better job of not judging and instead choose to fight for the ones that cannot fight for themselves.

References

A. (2022, June 7). *How to Start a Nonprofit in Virginia | Chamber of Commerce*. Chamber of Commerce. https://www.chamberofcommerce.org/nonprofit/virginia

Alruwaili, A. (2019). A Review of the Impact of Training on Cybersecurity Awareness. International Journal of Advanced Research in Computer Science 10 (5): 1-3. ISSN: 7545-1254

Ahmad, K. (2022, November 1). *What Is the Great Firewall of China and How Does It Work?* Make Use Of. https://www.makeuseof.com/what-is-great-firewall-china/

Anthony, A. (2023, March 13). Cyber Resilience Must Focus On Marginalized Individuals, Not Just Institutions. Carnegie Endowment for International Peace. Retrieved March 22, 2023, from https://carnegieendowment.org/2023/03/13/cyber-resilience-must-focus-on-marginalized-individuals-not-just-institutions-pub-89254

Blackwood-Brown, C. (2017). An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills. Nova Southeastern University. Retrieved March 22, 2023, from https://nsuworks.nova.edu/gscis_etd/1047

Byrd, P. (2022, June 28). Why is Security Awareness Training Important? Hook Security Blog. Retrieved March 22, 2023, from https://www.hooksecurity.co/blog/why-is-security-awareness-training-important#:~:text=We've%20found%20that%20companies,of%20you%20in%20the%20industry.

Corallo, A. (2022). Cybersecurity Awareness in the Context of the Industrial Internet of Things: A Systematic Literature Review. Computer in Industry 137: 103614. https://doi.org/10.1016/j.compind.2022.103614

Dash, B. & Ansari, M. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy. International Research Journal of Engineering and Technology 9 (4). ISSN: 2395-0072.

Erendor, M. & Yildirim, M. (2019). Cybersecurity Awareness in Online Education: A Case Study Analysis. IEEE Access10: 52319-52335. DOI: 10.1109/ACCESS.2022.3171829

Form, W. (2019). sociology | Definition, History, Examples, & Facts. In *Encyclopedia Britannica*. https://www.britannica.com/topic/sociology

FreshBooks.com. (2019, March 19). *How Long It Takes for a Small Business to Be Successful: A Year-By-Year Breakdown*. FreshBooks. https://www.freshbooks.com/hub/startup/how-long-does-it-take-business-to-be-successful#:~:text=Most%20small%20businesses%20take%20at

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing Cybersecurity from the Boardroom: Challenges, Drivers and Ways ahead. Computer Security 121: 102840. https://doi.org/10.1016/j.cose.2022.102840

Hassan, M. (2023). Review on Cyber-Physical and Cyber-Security System in Smart Grid: Standards, Protocols, Constraints, and Recommendations. Journal of Network and Computer Applications 209: 103540. https://doi.org/10.1016/j.jnca.2022.103540

Lee, I. & Shin, Y. (2020). Machine Learning for Enterprises: Applications, Algorithm Selection, and Challenges. Business Horizons 63 (2): 157-170. https://doi.org/10.1016/j.bushor.2019.10.005

Ley, A., & Reyes, J. (2020, November 28). The Virginian-Pilot - We are currently unavailable in your region. Retrieved March 22, 2023, from https://www.pilotonline.com/government/virginia/vp-nw-fz20-census-problems-virginia-20201128-4tj5dwgiovdj7jrcsdeoorxstm-story.html

Lezzi, M., Lazoi, M. & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the Current Literature: A Reference Framework. Computers in Industry 103: 97-110. https://doi.org/10.1016/j.compind.2018.09.004

Ling, L. et al. (2019). Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior. International Journal of Information Management 45: 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Roads, G. H. (2022). *Greater Hampton Roads :: Demographics :: Region :: Greater Hampton Roads (MSA) :: Age*. Copyright (C) 2023 by Greater Hampton Roads. https://www.ghrconnects.org/demographicdata?id=281263§ionId=942

Sabillon, R. (2019). An Effective Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness Training Model (CATRAM). A Case Study in Canada. Journal of Cases on Information Technology 21 (3): 14. DOI: 10.4018/JCIT.2019070102

The Virginia Pilot. (2020, January 15). More of the Hampton Roads population is over 65. Here's why it matters. Retrieved March 22, 2023, from https://www.pilotonline.com/inside-business/vp-ib-census-boomers-0120-20200115-4eo4pf7verebxkf4jdkimvua5y-story.html

Zhang, Z., He, W., Li, W. & Abdous, M. (2021), Cybersecurity Awareness Training programs: a Cost–benefit Analysis Framework. Industrial Management & Data Systems, Vol. 121 No. 3, pp. 613-636. https://doi.org/10.1108/IMDS-08-2020-0462

Zhang-Kennedy, L. & Chiasson, S. (2021). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. ACM Computing Surveys 54 (1): 1-39. https://doi.org/10.1145/3427920