

Watavien Favors

Professor Porcher

CYSE 494

21 June 2023

Addressing Cybersecurity Challenges through Comprehensive Services

In today's rapidly evolving digital landscape, organizations face increasing cybersecurity challenges that threaten the integrity, confidentiality, and availability of their sensitive information. Our cybersecurity consulting company aims to address the pressing problem of inadequate cybersecurity measures within organizations, specifically focusing on the education of the higher-ups of the company, vulnerability assessments, secure network configurations, and network monitoring. The context of this problem is the rise in cyber threats, data breaches, and malicious activities targeting organizations of all sizes and industries. Numerous high-profile incidents have highlighted the severe consequences of inadequate cybersecurity practices, including financial losses, reputational damage, and compromised customer trust. Surveys and industry reports consistently reveal a lack of awareness and preparedness among employees and a need for proactive measures to ensure robust cybersecurity defenses. To tackle these challenges, our consulting company proposes a comprehensive suite of services. First, we will provide employee education programs specifically tailored to the individuals higher up in the company who have more authority, such as CEOs, Chief Technology Officers, and anyone else who makes management decisions within the organization. This education aims to empower these individuals with the knowledge and skills to identify and mitigate cyber risks. The programs will include interactive training sessions, workshops, and online resources, tailored to

different roles and levels of technical expertise. Second, our team will conduct thorough vulnerability assessments to identify potential weaknesses in an organization's infrastructure, systems, and applications. Through meticulous analysis and testing, we will provide organizations with a detailed assessment of their vulnerabilities, along with actionable recommendations to strengthen their security posture. Third, we will assist organizations in implementing secure network configurations. This will involve reviewing and optimizing existing network infrastructure, including firewalls, routers, and switches, to ensure proper configuration, access controls, and encryption protocols. Our experts will work closely with IT teams to develop robust network architectures that minimize potential attack vectors. Finally, our company will offer proactive network monitoring services to detect and respond to potential security incidents in real time. Through continuous monitoring and analysis of network traffic, we will identify anomalous behaviors, intrusions, and emerging threats. This proactive approach will enable organizations to respond swiftly, minimize damages, and mitigate the risk of data breaches.

While we are confident in our ability to deliver effective cybersecurity services, we anticipate certain barriers that we may encounter. One such barrier is resistance to change from individuals who may think they are already sufficiently educated on cybersecurity or may not see the value in participating in educational programs. Overcoming this resistance requires effective communication and stakeholder engagement, highlighting the importance of continuous learning and updating knowledge in the rapidly evolving cybersecurity landscape.

Another barrier is budget constraints, which often limit the allocation of resources for cybersecurity initiatives. Adequate investments are crucial for implementing effective cybersecurity measures. Finally, the existing organizational culture can pose a barrier to

implementing cybersecurity measures effectively. A culture that does not prioritize cybersecurity or lacks awareness of potential threats can undermine efforts to improve cybersecurity defenses. In conclusion, our cybersecurity consulting company aims to address the problem of inadequate cybersecurity measures within organizations by providing tailored education, vulnerability assessments, secure network configurations, and network monitoring. While barriers such as resistance to change, budget constraints, regulatory compliance, and organizational culture may be encountered, we are committed to overcoming these barriers and delivering effective cybersecurity solutions to empower organizations to mitigate cyber risks and strengthen their security defenses.

Literature:

The Problem and What we are Doing to Solve it:

The problem that has been increasing and increasing has been cyber-attacks. The number of cyber-attacks have increased over the last couple of years because of the advancement in technology, and the lack of education of employees specifically those in management roles. There are agreement reports that have concluded that the number of scams in mower tags rose once the pandemic started. The world economic forum reported that the pandemic led to a 50% increase in cyber-attacks, which was between the 31st of December 2019 and the 14th of April 2020. These attacks not only lead to emotional stress. It leads to financial loss as well. The average ransomware pay for the second quarter of 2020 was \$178,254. Which was a jump up 60% compared to the first quarter of the year (Harjinder 2021). But many attacks could've been avoided. Because of the pandemic, a lot of people were working from home, which led to a level

of unpreparedness by some of these companies, and because of that, their security lacked leading to their systems being infiltrated (Harjinder 2021). And this goes back to employee education, because if the higher-ups in these companies were educated on the situation, and more aware of what working at home could lead to, they could've prepared a little better, and educated their employees that are under them on the upcoming events and how to prevent some of the stress or loss that the world was going through. Not all cyber-attacks are ransom related but still lead to some kind of financial loss. Below is the financial loss resulting from cybercrime in 2019 (Bell 2020).

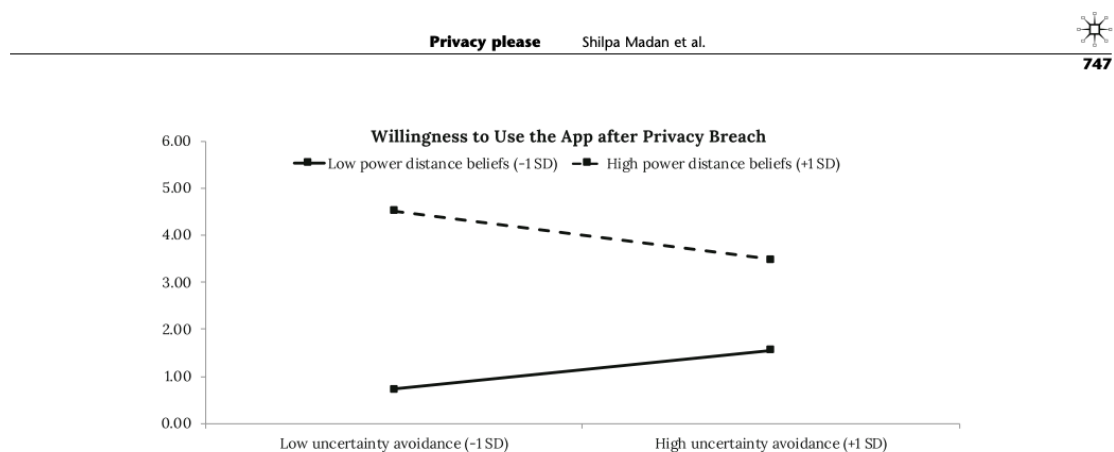
2019 Cybercrime Cost Statistics

By Victim Loss			
Crime Type	Loss	Crime Type	Loss
BEC/EAC	\$1,776,549,688	Employment	\$42,618,705
Confidence Fraud/Romance	\$475,014,032	Civil Matter	\$20,242,867
Spoofing	\$300,478,433	Harassment/Threats of Violence	\$19,866,654
Investment	\$222,186,195	Misrepresentation	\$12,371,573
Real Estate/Rental	\$221,365,911	IPR/Copyright and Counterfeit	\$10,293,307
Non-Payment/Non-Delivery	\$196,563,497	Ransomware	**\$8,965,847
Identity Theft	\$160,305,789	Denial of Service/TDoS	\$7,598,198
Government Impersonation	\$124,292,606	Charity	\$2,214,383
Personal Data Breach	\$120,102,501	Malware/Scareware/Virus	\$2,009,119
Credit Card Fraud	\$111,491,163	Re-shipping	\$1,772,692
Extortion	\$107,498,956	Gambling	\$1,458,118
Advanced Fee	\$100,602,297	Health Care Related	\$1,128,838
Other	\$66,223,160	Crimes Against Children	\$975,311
Phishing/Vishing/Smishing/Pharming	\$57,836,379	Hacktivist	\$129,000
Overpayment	\$55,820,212	Terrorism	\$49,589
Tech Support	\$54,041,053		
Corporate Data Breach	\$53,398,278		
Lottery/Sweepstakes/Inheritance	\$48,642,332		

Note: 2019 cybercrime cost statistics courtesy of the FBI (FBI, 2019).

In 2020, there were close to 4,000 reported breaches where the hacker exposed billions of personal records worldwide. These breaches lead to bigger financial losses for these bigger

companies. It brings along fines from the people that regulate, customers could stop using or supporting that company because they had a huge security breach, their whole reputation will go down, and lastly, the people affected may want to sue, and that would just add onto the money. The graph below shows how it differs in different cultures whether or not, they would continue to support and use a company's product after a security breach. And low-power cultures they usually may feel violated, and feel as the company didn't do enough to protect their data which leads to them not wanting to associate with them anymore. While high-power cultures are the complete opposite, they believe that they are the ones who gave them their data so it is kind of out of their control and in the long run will continue to use the product.



They say that the cost of these bridges could reach up to \$5 trillion by the year 2024, which is coming up. One of the biggest breaches was the Cambridge analytical leak. 87 million Facebook users were affected by politically targeted advertisements. These types of ads have the power to threaten democracies (Madan 2023).

Our company will do everything in our power to try and reduce the amount of data breaches in cyber-attacks happening within the company. On top of keeping employees educated, we offer to connect with IT teams and monitor networks and make sure that all network

configurations are in place to prevent this kind of stuff from happening. Vulnerabilities are what is being searched for, periodically doing these vulnerability scans can lead to risk mitigation. Vulnerability scans help you find the weakest link in your networks, showing, where in your system, there is a risk for an attack.

How employee Education will be helpful:

There has been a large rise in the number of corporate malware phishing attacks. From the year 2020 to now the number has increased by at least 450%. Now a lot of people think that was because of Covid and how everything kind of went online. To give you another example in 2019 there were around 260,000 attacks at this one company and two years later, that number jumped up to 720,000 corporate now we're fishing attacks. It has been said that employees are one of the top risks within companies (Shine 2022). Educating your employees specifically, your higher-ups, or people who do any kind of management, will benefit your company because these higher-ups will serve as role models. Them furthering their knowledge will help the person under them. By actively participating in cybersecurity initiatives, they set the tone for prioritizing security measures throughout the company and encourage other employees to adopt best practices. This top-down approach creates a positive impact on the overall security posture of the organization. The advantages of educating high-ups in cybersecurity extend beyond cultural influence. Studies have highlighted the importance of executive leadership in resource allocation and decision-making related to cybersecurity (Herath & Rao, 2019). Informed high-level employees can better understand the implications of cybersecurity investments, advocate for necessary resources, and make informed decisions to mitigate risks effectively. Furthermore, cybersecurity education for high-ups enables them to play an active role in incident response and

crisis management. In the event of a security incident, executives who are well-versed in cybersecurity principles can provide valuable guidance and support to the incident response team, facilitating a coordinated and efficient response (McIlwraith, 2021). When doing more research, I found out that if you look at the numbers, it suggests that between 60 and 85% of information security incidents are coming from people in the organization. Mainly because of their lack of knowledge, user error, or just ignorance. Lack of knowledge is the main reason to advocate for educational programs.

Barriers:

As organizations grapple with the escalating cybersecurity challenges in today's digital landscape, the need for effective cybersecurity measures has become paramount. Our company aims to address the pressing problem of inadequate cybersecurity measures within organizations by focusing on educating higher-level personnel, conducting vulnerability assessments, implementing secure network configurations, and offering network monitoring services. But as we know there are going to be many things in our way when trying to implement these things. A big thing is a resistance to change: Implementing robust cybersecurity measures often encounters resistance from employees and organizational stakeholders. This resistance can stem from a reluctance to adapt to new practices or a lack of awareness regarding the significance of cybersecurity. A study by Von Solms and van Niekerk (2013) emphasizes the importance of fostering a security-aware culture within organizations. Overcoming resistance to change requires effective communication, stakeholder engagement, and clear demonstrations of the benefits of the proposed cybersecurity measures. To implement these things, you need money which you may not always have. Adequate investments are crucial for employee education,

vulnerability assessments, and the implementation of secure network configurations. However, competing priorities and budget constraints often hinder organizations from dedicating adequate funds to cybersecurity. To address this barrier, organizations can consider cost-effective alternatives, such as leveraging open-source tools or partnering with cybersecurity consulting companies that offer flexible pricing models. The existing organizational culture can pose a barrier to implementing cybersecurity measures effectively. A culture that does not prioritize cybersecurity or lacks awareness of potential threats can undermine efforts to improve cybersecurity defenses. Angus McIlwraith discusses the importance of employee behavior in information security and emphasizes the need for a culture that encourages vigilance and responsible information handling. Shifting the organizational culture toward cybersecurity awareness requires top-down support, continuous training, and regular reinforcement of security practices. Implementing comprehensive cybersecurity measures, such as secure network configurations and network monitoring, often involves dealing with technical complexities. Organizations may lack the internal expertise required to implement and manage advanced security technologies effectively. Partnering with cybersecurity consulting companies can help bridge this gap by leveraging their specialized knowledge and technical capabilities. Another reason why these education programs should be put in place.

Conclusion:

In conclusion, our cybersecurity consulting company recognizes the escalating cybersecurity challenges faced by organizations in today's rapidly evolving digital landscape. The rise in cyber threats, data breaches, and malicious activities targeting organizations of all sizes and industries highlights the urgent need for robust cybersecurity measures. Our

comprehensive suite of services aims to address the problem of inadequate cybersecurity measures within organizations by focusing on education, vulnerability assessments, secure network configurations, and network monitoring. We empower organizations to strengthen their security defenses and mitigate cyber risks. The education of higher-level personnel, such as CEOs, Chief Technology Officers, and decision-makers within organizations, is a crucial aspect of our approach. By providing tailored education programs, including interactive training sessions, workshops, and online resources, we empower these individuals with the knowledge and skills to identify and mitigate cyber risks. This top-down approach creates a culture that prioritizes cybersecurity and sets an example for other employees, fostering a security-aware environment. We are dedicated to partnering with organizations to navigate the complex cybersecurity landscape and ensure the integrity, confidentiality, and availability of their sensitive information.

How the Problem/Innovation Relates to Material Outside of my Major:

The problem addressed by your cybersecurity consulting company and the proposed innovation of providing employee education, vulnerability assessments, secure network configurations, and network monitoring aligns with concepts and knowledge covered in several classes that I've taken outside of my major. Here's how the material covered in those classes relates to our problem and innovation: My Digital Literacy course provided me with a foundational understanding of digital technologies and their impact on society. It helped me recognize the significance of cybersecurity in the digital age and understand the need for robust measures to protect sensitive information. English Composition and American Writers Experience may not have a direct link to cybersecurity, but they developed my communication

and writing skills. Effective communication is crucial in the cybersecurity field, as you need to convey complex technical information to both technical and non-technical stakeholders. Our ability to articulate the importance of cybersecurity measures and the value of your proposed innovation was enhanced through the skills gained in these courses. Introduction to Criminology provided me with a broad understanding of the causes and consequences of crime. While focusing on traditional criminology, the concepts covered can be applied to cybercrime as well. Understanding criminal behavior and motivations is essential in developing effective cybersecurity strategies and addressing the human element in cyber threats. Digital Basics and Photography 2 are art courses, but they have honed my creative and visual communication skills. In cybersecurity, visual representations, such as diagrams and infographics, can be effective in explaining complex concepts, network architectures, and security configurations to clients and stakeholders. Introductory Oceanography and Earth Science which are science classes are seemingly unrelated to cybersecurity, these courses contributed to my understanding of risk assessment and the importance of proactive measures. Just as scientists study natural processes and predict potential hazards, cybersecurity professionals assess vulnerabilities and anticipate potential threats to prevent attacks. Public Speaking was a great class to take. Effective communication is a crucial skill in cybersecurity, especially when trying to educate employees about cybersecurity best practices and risks. Public speaking skills acquired in this course can be valuable for delivering impactful cybersecurity awareness programs and conveying technical information to non-technical individuals. Intro to the Visual Arts can foster creativity and critical thinking skills. These skills are valuable in the cybersecurity field, where innovative problem-solving and the ability to think from an adversary's perspective are essential in devising effective defense strategies. By incorporating these connections, I can demonstrate a broader

interdisciplinary perspective and showcase how my background in various subjects contributes to my understanding of the problem and your innovative solutions in cybersecurity.

Success Measurement:

Success in addressing the identified problem will be measured through several key indicators. First, we will evaluate the effectiveness of our employee education programs by assessing the level of awareness and adherence to cybersecurity best practices among participants. This can be measured through pre-and post-training assessments, surveys, and feedback mechanisms. Additionally, track the number of reported security incidents or policy violations before and after training. For vulnerability assessments, success will be determined by the number and severity of vulnerabilities identified and the organization's ability to remediate them effectively. We will use industry standards and benchmarks to categorize the severity of vulnerabilities and regular follow-ups and reassessments will help track progress over time and ensure that organizations maintain a strong security posture.

The success of our secure network configurations will be measured by monitoring the frequency and impact of security incidents, such as successful intrusions or unauthorized access attempts. We will compare incident data before and after the implementation of secure network configurations to measure improvements, a reduction in such incidents will indicate the effectiveness of our solutions. The effectiveness of our network monitoring services will be assessed by tracking the average time to detect and respond to security incidents, as well as the overall reduction in incident severity and impact. This will determine the impact of our proactive monitoring. Not only will we determine effectiveness using numbers and statistics, but we will also gather feedback from clients to understand their perception of the effectiveness of your

cybersecurity innovation. Satisfaction surveys, interviews, or focus groups to assess overall satisfaction with your services will be conducted. This will identify areas for improvement and measure the impact on client confidence and trust. To implement this innovation, it will not be cheap but in the long run, it may be worth it. We will assess the financial impact of your cybersecurity innovation on client organizations and compare the cost of implementing your services with the potential financial losses and damage from security incidents avoided. This analysis can provide insights into the cost-effectiveness of our innovation.

How to Make it Happen:

To turn our innovation into reality, several steps need to be taken such as resource allocation, creating a robust infrastructure, developing tailored education programs, comprehensive vulnerability assessments, and collaborations with different organizations and their IT teams. To establish and operate the cybersecurity consulting company effectively, adequate resources must be allocated. This includes financial resources to cover operational expenses, hire qualified personnel, acquire necessary technology and equipment, and conduct research and development activities. Building this cybersecurity consulting company requires a team of highly skilled professionals with expertise in cybersecurity, risk assessment, network engineering, and incident response. It is essential to recruit individuals with extensive knowledge and experience in the field who can effectively deliver the proposed services. The team should include trainers who can develop and conduct employee education programs, vulnerability assessment experts, network security specialists, and incident response analysts. And to support the delivery of our services, a robust infrastructure is needed. This includes hardware and software resources for conducting vulnerability assessments, network monitoring tools, and secure communication channels. The infrastructure should be designed to handle the volume of

assessments and monitoring activities for multiple clients simultaneously while ensuring the confidentiality and integrity of the collected data. With each client's needs being different from each other, establishing partnerships and collaborations with organizations of various sizes and industries is crucial. These partnerships will enable our consulting company to understand the specific needs and challenges of each organization and tailor our services accordingly. Building strong relationships with clients is essential for effective implementation and long-term success.

A huge part of this innovation is the educational advancement for the higher-ups so developing comprehensive and tailored education programs is vital to address the specific needs of organizations and their employees. These programs should cover a wide range of topics, including cybersecurity awareness, best practices, social engineering, password hygiene, and incident reporting procedures. The education programs should be interactive, engaging, and accessible through various mediums, such as in-person training sessions, workshops, online resources, and e-learning platforms.

To conduct thorough vulnerability assessments, our consulting company must employ industry-standard tools and methodologies. This includes utilizing vulnerability scanning tools, penetration testing frameworks, and risk assessment methodologies. The assessments should cover all aspects of an organization's infrastructure, systems, and applications, including network devices, servers, databases, web applications, and endpoints. The process of implementing secure network configurations would require close collaboration with the organization's IT team. Our consulting company should have the expertise to review and optimize existing network infrastructure, including firewalls, routers, switches, and intrusion detection systems. This involves ensuring proper configuration, access controls, and encryption protocols, as well as addressing any vulnerabilities or misconfigurations identified during the assessment phase. As

far as proactive network monitoring goes, our consulting company needs to deploy advanced monitoring tools capable of analyzing network traffic, detecting anomalies, and identifying potential security incidents in real time. This requires continuous monitoring, log analysis, and event correlation to ensure timely detection and response. Additionally, the company should establish incident response protocols and procedures to guide the handling of identified security incidents. In conclusion, bringing our cybersecurity innovation to fruition requires assembling a skilled team, establishing a robust infrastructure, developing tailored education programs, conducting comprehensive vulnerability assessments, optimizing network configurations, and implementing proactive network monitoring. By addressing these key requirements, our consulting company can effectively address the problem of inadequate cybersecurity measures and contribute to a more secure digital landscape for organizations.

A look back:

From this project, I have learned the importance of addressing cybersecurity challenges within organizations to protect sensitive information from cyber threats. The rise in cyber-attacks, data breaches, and malicious activities highlights the urgent need for robust cybersecurity measures. One of the key lessons learned is the significance of educating high-level personnel within organizations. By providing tailored education programs for CEOs, Chief Technology Officers, and decision-makers, we empower them with the knowledge and skills to identify and mitigate cyber risks. This top-down approach creates a culture that prioritizes cybersecurity and sets an example for other employees, fostering a security-aware environment. we have also recognized the barriers that can hinder the implementation of cybersecurity measures. Resistance to change from employees and stakeholders, budget constraints, and

existing organizational culture can pose challenges. Overcoming these barriers requires effective communication, stakeholder engagement, and clear demonstrations of the benefits of cybersecurity measures. In terms of what I would have done differently, I would have emphasized the importance of continuous learning and updating knowledge in the rapidly evolving cybersecurity landscape. Cyber threats are constantly evolving, and organizations need to stay updated with the latest trends and best practices to effectively defend against them. Continuous education and training programs should be an ongoing effort rather than a one-time initiative. Additionally, I would have focused more on the technical complexities involved in implementing secure network configurations and network monitoring. Organizations may lack internal expertise in these areas, and partnering with cybersecurity consulting companies with specialized knowledge and technical capabilities can help bridge the gap. Overall, our project has highlighted the critical role of comprehensive cybersecurity services in addressing cybersecurity challenges within organizations. By providing education, vulnerability assessments, secure network configurations, and network monitoring, we aim to empower organizations to strengthen their security defenses and mitigate cyber risks.

References

- Bell, L. E. (2020). Identifying Financial Loss Caused by Social Engineering (Order No. 28087890). Available from ProQuest Dissertations & Theses Global. (2448121325).
<http://proxy.lib.odu.edu/login?url=https://www.proquest.com/dissertations-theses/identifying-financial-loss-caused-social/docview/2448121325/se-2>
- Franklin, C., Jr. (2003). Vulnerability scans mitigate risk. *InfoWorld*, 25(37), 26-29.
<http://proxy.lib.odu.edu/login?url=https://www.proquest.com/trade-journals/vulnerability-scans-mitigate-risk/docview/194375715/se-2>
- Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105, 102248.
<https://doi.org/10.1016/j.cose.2021.102248>
- Madan, S., Savani, K., & Katsikeas, C. S. (2023). Privacy please: Power distance and people's responses to data breaches across countries. *Journal of International Business Studies*, 54, 731-754. <https://doi.org/10.1057/s41267-022-00519-5>
- McIlwraith, A. (2021). Information Security and Employee Behaviour.
<https://doi.org/10.4324/9780429281785>
- Shine, D. (2022). Strengthen weakest link to help fight cybercrime: Employee education crucial, compliance expert says. *Automotive News, Suppl. NADA DAILY FRIDAY*, 26(1).
<http://proxy.lib.odu.edu/login?url=https://www.proquest.com/trade-journals/strengthen-weakest-link-help-fight-cybercrime/docview/2640099923/se-2>
- Von Solms, R., & Van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security*, 38, 97-102. <https://doi.org/10.1016/j.cose.2013.04.004>