Yohannes Ejigu
CPD494
Prof Akeyla Porcher
March 29 2023
Old Dominion University

Proposal: Chary - Small Business Cybersecurity Class

Introduction:

For small companies to better safeguard their sensitive data from cyber-attacks, Chary is a program that provides cybersecurity training. We'll go over the issue, the fix, obstacles, and program evaluation in this proposal.

Problem:

One of the most severe concerns that small businesses confront is cybersecurity. Smaller organizations may have worse security practices than bigger corporations, making them more appealing to hackers. Cyberattacks may lead to the theft of sensitive information, financial losses, and brand harm. Small companies are particularly vulnerable to cyber attacks because they typically lack the means to hire full-time cybersecurity personnel.

Moreover, small businesses may lack the software or technological infrastructure needed to protect their data, leaving them more vulnerable to assaults. Many small businesses continue to utilize obsolete operating systems or software that may not receive regular security updates, making them more exposed to cyber attacks. Small businesses may also be uneducated about the most recent cybersecurity threats and best practices, making them open to social engineering attacks such as phishing emails and phony websites.

Context:

Many studies have found that hackers typically target small businesses. A 2020 Verizon investigation found that small businesses were responsible for 28% of data breaches, with each breach costing anything from hundreds of thousands to millions of dollars. Many small businesses are ignorant of the risk, or they lack the resources or expertise required to implement cybersecurity defenses.

The increased susceptibility of small business owners to cyberattacks is a concerning development. Hackers have turned their attention to small businesses in recent years because they may take advantage of their lack of cybersecurity tools and resources. 88% of small businesses feel they are not vulnerable to cyberattacks, despite the fact that 58% of small businesses have had a data breach in the past year.

Solution:

Small company owners who take Chary's cybersecurity course will be given the information and abilities necessary to safeguard their enterprises from online dangers. A variety of subjects, such as spotting possible attacks, making safe passwords, installing firewalls, and instructing staff on cybersecurity best practices, will be covered in the class. The initiative will also give information to assist small firms in evaluating their cybersecurity risk and provide suggestions for improvement.

The course will teach participants about cybersecurity through a practical and hands-on approach, concentrating on typical cyberattacks including phishing scams and ransomware assaults and how to handle security problems. Also, the most recent cybersecurity innovations, such as endpoint security, intrusion detection, and cloud security, will be explored, with an emphasis on how to deploy them effectively and efficiently to guarantee a strong and modern security architecture.

The best practices for conducting security audits, creating efficient cybersecurity policies and processes, and educating staff members about cybersecurity will also be covered. Chary will provide continuous assistance via an online platform, which includes access to a community of cybersecurity professionals, online training modules, and frequent updates on the most recent cybersecurity risks and best practices, to provide ongoing access to cybersecurity resources.

Barriers:

Many obstacles may stand in the way of small enterprises implementing cybersecurity safeguards. A big barrier is a lack of money for security investments. Lack of knowledge about the dangers and significance of cybersecurity is another problem. Small business investment in cybersecurity may also be hampered by time restraints and conflicting objectives. Chary will offer budget-friendly, simple-to-implement solutions to these problems that are suitable for small businesses.

Also, a lack of experienced cybersecurity employees to develop and maintain their security measures may be a problem for small organizations. Small firms may find it difficult and expensive to hire and retain cybersecurity personnel, which forces them to rely on outside security companies that could not provide them with solutions that are specifically suited to their needs.

small enterprises might not have the technological know-how necessary to successfully adopt cybersecurity measures. Because they do not have the time or resources to research the most recent security trends and technology, small company owners may find the complexity of today's cybersecurity solutions to be intimidating.

Assessment:

By counting the number of small companies enrolling in the cybersecurity course and listening to their feedback, Chary will gauge the program's effectiveness. We'll keep tabs on how many small firms adopt the cybersecurity precautions our program suggests. A follow-up evaluation will be performed to gauge the success of the steps taken by these companies and pinpoint areas for development.

Chary will also keep track of how many cyber incidents the small businesses that took our cybersecurity course reported. By investigating these occurrences, we may spot patterns and trends and modify our software to counter new dangers.

The total effect of our curriculum will be evaluated by counting how many fewer cyber incidents small companies that took our training reported overall. To assess the program's success in reducing cyber risks for small firms, we will compare this data to industry benchmarks.

Chary will routinely ask small company owners and other stakeholders for input in order to maintain the program's efficacy and continued improvement. We will make changes to the content and materials of the program based on this feedback to suit the changing demands of small companies and maintain the program's value and relevance.

Conclusion:

In conclusion, Chary provides a crucial remedy for the issue of escalating small-business cyber attacks. Chary seeks to arm small company owners with the information and abilities they need to safeguard their organizations from cyber dangers by offering inexpensive and useful cybersecurity training, tools, and continuous assistance. The program deals with the difficulties small firms have in putting cybersecurity safeguards in place, including financing, knowledge, and technological know-how. Chary will continually enhance and modify its resources to suit the changing requirements of small businesses by evaluating the program's efficacy through attendance, feedback, and effectiveness in minimizing cyber incidents. The Chary initiative is an essential step toward protecting small companies' sensitive data in the future from cyber attacks.

References

Schipul, R. (2021, March 16). Nine Practical Ways To Protect Your Company From Hackers And Phishing Attacks. Forbes. https://www.forbes.com/sites/theyec/2021/03/16/nine-practical-ways-to-protect-your-company-from-hackers-and-phishing-attacks/?sh=5de115cd4e44

Rahmonbek, K. (2022, March 1). Small Business Cyber Security Statistics. strongDM. https://www.strongdm.com/blog/small-business-cyber-security-statistics.

Chubb. (n.d.). 5 Ways to Protect Your Small Business From a Cyber Attack. Retrieved from https://www.chubb.com/us-en/businesses/resources/5-ways-to-protect-your-small-business-from-a-cyber-attack.html.

"2020 Data Breach Investigations Report," Verizon, 2020.https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf [Accessed: 28-Mar-2023].