Proposal

Nyiesha Pettaway

Old Dominion University

CPD/CYSE/WCS 494

Professor Porcher

March 3, 2023

A security consultation is a service provided by security experts or consultants who assess an organization's or an individual's security posture and provide recommendations on how to improve it. The consultant typically conducts a comprehensive review of the organization's or individual's security controls, processes, and policies to identify any vulnerabilities or areas for improvement. They then provide recommendations for changes or enhancements to improve the overall security posture. The consultant may also provide education and training on best practices for cybersecurity and risk management. The goal of a security consultation is to help the organization or individual understand and mitigate the risks they face and protect their assets and information from cyber threats. The purpose of this proposal is to provide insight into security problems faced by homeowners and small businesses, display evidence, describe barriers, and offer a working solution in combatting the lack of security.

Because they often lack the knowledge and resources to secure their digital assets properly, small businesses and individual homeowners are increasingly becoming targets of cyber-attacks. The consequences of a successful cyber-attack can be devastating, leading to financial loss, reputation damage, and other significant consequences. Our company specializes in providing expert security consultation to small businesses and individual homeowners. We understand that security is a top priority for everyone, and that's why we offer personalized consultation services tailored to meet the unique needs of each of our clients. Our team of skilled employees can conduct security analysis and install appropriate software to safeguard against potential threats.

Multiple reports and studies indicate that small businesses and individuals are highly targeted by cyber-attacks. For instance, a 2021 report by Verizon reveals that small businesses are the targets of 28% of all data breaches. Similarly, a study by Security Magazine shows that 43% of cyber-attacks target small businesses. Knowing this data allows our business to provide comprehensive security consultation services to small businesses and homeowners. The solution to combatting these security issues include offering a security analysis, appropriate software installation, and basic cybersecurity lessons tailored to the needs of the customer. In addition, providing a range of consultation options, including one-time, monthly, quarterly, and annual services. Our team will comprise of Certified Ethical Hackers (CEH), Network Engineers/Administrators (IT Specialist), and Cybersecurity Analysts to identify, patch, and explain the steps taken to secure the customer's digital assets.

Security analysis for small businesses typically involves identifying potential vulnerabilities and threats to the organization's digital and physical assets, and developing strategies to address them. Here are some steps that can be taken as part of a security analysis for small businesses:

1. Identify assets: Determine what assets your business has that need to be protected, including physical assets such as equipment and inventory, as well as digital assets such as customer data and intellectual property.
2. Identify vulnerabilities: Assess the potential vulnerabilities that exist within your organization, such as weak passwords, outdated software, or unsecured networks.
3. Assess risk: Determine the likelihood and potential impact of each identified vulnerability and threat to your business.

4. Develop a security plan: Create a plan that outlines how your business will address the identified vulnerabilities and threats, including policies and procedures to mitigate risk and improve security.
5. Implement security measures: Implement security measures such as access controls, firewalls, and antivirus software to protect your organization's assets.
6. Educate employees: Train employees on the importance of security and how to follow security procedures to reduce the risk of security breaches.
7. Monitor and update: Regularly monitor your security measures and update them as necessary to keep up with new threats and vulnerabilities.

Overall, a security analysis for small businesses should be tailored to the specific needs and risks of the organization and should involve ongoing monitoring and assessment to ensure the effectiveness of security measures.

Installing appropriate and necessary security software and providing basic cybersecurity lessons are important steps that small businesses can take to protect their digital assets from cyber threats.

1. Installing Security Software: Installing appropriate and necessary security software such as antivirus and anti-malware programs, firewalls, and intrusion detection systems can help protect small businesses against various types of cyberattacks. It is important to select security software that fits the specific needs of the business, such as the size of the network and the type of data being stored.
2. Providing Basic Cybersecurity Lessons: Educating employees on basic cybersecurity practices such as creating strong passwords, avoiding suspicious emails and links, and regularly updating software can help reduce the risk of security breaches. This can be done remotely or in-person through training sessions or workshops.

Both steps should be tailored to the specific needs of the business and should be implemented as part of a larger security plan that includes ongoing monitoring and assessment of security measures. Regularly reviewing and updating security software and educating employees on new cyber threats and best practices can help ensure the ongoing effectiveness of security measures.

As a company, there are five major barriers we expect to face. Firstly, small businesses and homeowners may not be aware of the risks of cyber-attacks or may not see the need to invest in cybersecurity. Another significant barrier is the cost of our services, which may be prohibitive for some customers. In addition, difficulties may be experienced when convincing customers to invest in cybersecurity due to their perception of cybersecurity as a non-core expense. Also, because there are other security companies specializing in helping homeowners and small businesses, we face strong competition from other cybersecurity service providers in the market. Lastly, difficulties in keeping up with evolving cybersecurity threats and technology are expected.

In analyzing success metrics, we will track our success based on the number of customers we serve and the feedback we receive. Positive feedback and customer retention will be strong indicators of our success. Additionally, we will track the number of successful cyber-attacks prevented, and the impact they could have had on our customers' digital assets. Also, increased

revenue and profitability are both indicators of success. Lastly, strong reputation and recognition in the market as a trusted cybersecurity service provider.

References

Comerford, L. (2022, May 25). *Why small businesses are vulnerable to cyberattacks*. Security Magazine RSS. Retrieved February 26, 2023, from https://www.securitymagazine.com/blogs/14-security-blog/post/97694-why-small-businesses-are-vulnerable-to-cyberattacks

Cybersecurity consulting services in the World of IOT : NEC Technical Journal. NEC. (n.d.). Retrieved March 1, 2023, from https://www.nec.com/en/global/techrep/journal/g17/n02/170214.html