What is the problem you are addressing?

In general,the existence and frequency of cyber attacks is an undeniable reality in today's interconnected world. With the increasing digitization of businesses and the rapid expansion of technology, organizations face a multitude of cyber threats that can cause severe damage and disruption. Cyber attacks can result in financial losses, theft of sensitive data, reputational damage, and legal liabilities. The sophistication and frequency of these attacks continue to escalate, making it crucial for businesses to prioritize cybersecurity. To effectively mitigate the risks posed by cyber attacks, organizations need comprehensive cybersecurity solutions. Creating a cybersecurity consulting company that offers multiple services is necessary to address the diverse and complex nature of these threats.

There is a multiple range of studies which indicates that 88-90 percent of security breaches are results of human error. In all cybersecurity organizational correlations, humans are considered the weakest links. Here the lack of awareness in recognizing a potential threat is what is to blame. Not being able to understand the magnitude of the potential attacks, not being able to follow password rules, not able to recognize phishing emails and social engineering techniques used by hackers, lack of safe internet practices and little to no knowledge of privacy and data protection methodologies are some of the problems that need to be addressed to minimize or eliminate cyber attacks that are caused from human educational problem.

In the fight against cyber threats, there are also areas where problems can arise that can damage the overall security posture of an organization. Some of them are potential weaknesses in network infrastructure, systems, and applications. Networks , systems and applications are exploited by malicious actors all the time. This exploitation can escalate and lead to unauthorized access, data breaches and service disruptions. For these reasons, vulnerability assessments are necessary to mitigate it.

During a cyber attack, the first posture that will be hammered is the area of defense, where securing network configuration is vital. Without properly configured firewalls, organizations leave their networks vulnerable to unauthorized access, data breaches, and the spread of malware; an absence of encryption exposes data to interception and unauthorized viewing; and weak access controls can lead to unauthorized individuals gaining entry to critical systems and data. In short, insecure network configuration can increase cybersecurity risks such as financial loss and compromises of data security.

Other than problems that can arise because of regulatory requirements and non compliance in meeting the industry standards, lack of network monitoring can also create problems in the tasks of identification of anomalous network behavior or patterns and potential internal threats that may indicate a security breach or emerging cyber threat.

How do you know it’s a problem?

Generally speaking, the increase in frequency and sophistication of cyber attacks on businesses across industries highlight not only the existence of the problems, but also the urgency in tackling them. The rising number of data breaches, ransomware incidents, and other security breaches and everything that follows are real-human

problems that need a solution. Some problems are more apparent than others. For example human errors are one of the leading causes of security incidents, that is the lack of employee education and awareness contributes to this problem, making organizations more susceptible to social engineering attacks, phishing attempts, and other forms of cyber manipulation. Not being able to maintain a strong security posture associated with undiscovered vulnerabilities that exposes an organization to risks and unauthorized access are also known problems. Here not being able to timely monitor and detect network activities can allow malicious activities to go undetected.

What are going to do about the problem? (solution)

To address the challenges posed by cyber threats and the identified problems, an entrepreneurial solution could be the establishment of a comprehensive cybersecurity consulting firm that offers a range of services. This firm would prioritize employee education programs to enhance awareness and understanding of potential threats, safe internet practices, and data protection methodologies. By providing regular training and knowledge-sharing sessions, employees can become a strong line of defense against cyber attacks, reducing the risk of human error as a weak link.The firm should also specialize in vulnerability assessments, conducting regular audits to identify weaknesses in network infrastructure, systems, and applications. This would enable organizations to proactively address vulnerabilities and implement necessary patches or updates, minimizing the potential for unauthorized access, data breaches, and service disruptions. In addition, the cybersecurity consulting company would focus on assisting organizations in implementing secure network configurations, including properly configuring firewalls, implementing encryption, and establishing strong access controls. By ensuring that networks are robustly protected, the firm can mitigate cybersecurity risks, such as financial loss and data compromises, stemming from insecure network configurations. Moreover, it would also offer network monitoring services to detect and respond to security incidents in a timely manner. Continuous monitoring of network behavior and patterns can aid in identifying potential threats and enabling swift incident response, thereby minimizing the impact of cyber attacks and internal threats.

What barriers do you expect to confront?

As a barrier to new companies in general and a small cybersecurity consulting firm specifically in our case, In finding the entrepreneurial solution to address the identified problems in cybersecurity, several barriers may be expected. Firstly, there could be resistance from organizations to invest in comprehensive cybersecurity measures due to budget constraints or a lack of awareness about the potential risks they face. Convincing them of the importance of employee education, vulnerability assessments, secure network configurations, and network monitoring may require significant effort. Additionally, navigating the constantly evolving cybersecurity landscape and keeping up with emerging threats and technologies could pose a challenge in delivering effective and up-to-date solutions. Finally, establishing trust and credibility as a cybersecurity consulting firm in a competitive market could be a hurdle, as clients may have concerns about the reliability and effectiveness of the services provided.

How will you know if you are successful?

The success of the solutions provided can be measured through several key indicators. Firstly, the level of employee engagement and awareness regarding cybersecurity practices will indicate the effectiveness of the employee education programs. Second, regular assessments of employee knowledge, incident reports, and a decrease in human-related security incidents can serve as metrics for success. For vulnerability assessments, the number and severity of identified vulnerabilities, along with the timely implementation of necessary fixes, will determine the efficacy of the service. The success of secure network configurations can be measured by conducting regular security audits and penetration testing to ensure the absence of exploitable weaknesses. Lastly, the effectiveness of network monitoring can be assessed by the timely detection and response to security incidents, reduction in incident response time, and the ability to mitigate potential threats before they cause significant harm. In general, continuous feedback from clients, ongoing monitoring of security metrics, and a reduction in cybersecurity incidents will also serve as tangible evidence of the success of the provided solutions.