OLD DOMINION UNIVERSITY
CYSE 494 / WCS 494
Entrepreneurial Proposal

Dylan Bell

Group J will be proposing to address the absence of information security standardization on public and private organizations infrastructure. Our proposal will address the training of handling sensitive data, addressing active and passive threats in a specified environment. There can be a measure of high risk of misuse that stems from the lack of education in cyberspace and cybersecurity, and the development of secure information technology.[1] With additional guidance on computer and physical security these risks can be minimalized.

Without a solid standard base of security, there has been a detrimental worldwide economic impact over several trillion dollars in the past few years, affecting all aspects of an organization's business operations. One of the largest and worst data breaches in the United States was the Yahoo data breach. This breach, which holds the record for affect the most people was conducted by a team of Russian hackers who targeted Yahoo's database.[2]

The Russian hackers used backdoors and cookies to steal vital information from Yahoo's users. The personal identifiable information that was stolen was[2]

- Names
- Email addresses
- Phone Numbers
- Birthdates
- Passwords
- Calendars

It is estimated that over three billion users were affected in this breach which resulted in Yahoo being fined and sued for millions of dollars. The Yahoo breach is just one example of how there is a lack of security understanding and testing that can lead to weaknesses in the system, and how it could affect millions of people worldwide.

To effectively address the problem at hand, our group proposes a few action steps to help evaluate a business's strengths and weaknesses. We would begin by performing a penetration test on their systems and provide the organization with the results. After presentation of the results, we would then make recommendations on how to improve their systems, by education training, recommendations of tested products which would provide a better security platform. We would then provide a re-test of the system and evaluate the progress and environment until their vulnerabilities come to an acceptable level or non-existent.

There will be expected situations and barriers that will cause a few setbacks. These situations, depending on the size may have impact upon a company and could cause higher startup costs, economies of scale or syndication. As each situation comes up, we would shift our recommendations to address.

A survey by CWJobs reported that only a small portion information technology decision makers surveyed are satisfied with their employee's abilities to use new technology properly. This survey brings employee training to the forefront. Proper employee training could make sure that employee's abilities meet the organization's expectations and minimize the risk of employees causing a breach which could cost the organization time, money and reputation.

One barrier that may be met is communication. Most organizations have employees that are not as tech savoy as other employees. Our group proposes to keep communications simple and to the point so that all employees can comprehend the training and instructions that are given to them. This would deter any confusion which could cause a crack in the communication and security systems. We also propose to keep communications based around the expected outcomes and goals that they are trying to achieve.

In regard to the actual testing, we would run a penetration test, which is a simulation of a cyber-attack on the system in question to show if and where there are any vulnerabilities. To perform the test, we would define the scope of the test, to include the goals you want to reach and gather intelligence. In analyzing how the application will respond to the intrusion attempts, we will run static and dynamic analysis. The static analysis estimates the way an application's code would behave while running and a dynamic analysis is the inspection of the application's code in a running state. After these are ran, we would gain access by using web application attacks to uncover any vulnerabilities.[3] The results of these tests would be compiled into a report and presented to the company.

In this report, we will highlight the vulnerabilities that were found. In our findings we will supply a guide which will provide the information on each breach, including how it was created and exploited. This should provide an understanding that this test was successful and show how the next test would find fewer vulnerabilities. It is our belief that for a organization to have a solid baseline of cyber competency, it must have less than the recommended acceptable risks given to the vendor at the time.

An obstacle that we anticipate running into is the ability to secure sensitive data that our client has provided us. Since we will be a publicly advertised company, we may be a target for a data breach ourselves. We will have to put a plan in place to secure this data properly. Another obstacle that we may face is the challenge of effectively presenting the need for our products to the decision makers of the companies, who may not understand the need for our product.

With our proposal, the organization's decision makers will have an accurate account of their security system and its vulnerabilities. We will provide training, any products to the organization as needed to develop a better cybersecurity system. We will also provide the organization screenshots of any sensitive data breaches so that they can inform their clients and mitigate the damages.

We will know if our proposal is a success by retesting the organizations' security systems and analyze the results to ensure that there are fewer or non-existent vulnerabilities. We will also check on the staff and ensure that they are satisfied and applying the training we provided.

References

1. https://healthitsecurity.com/news/weak-healthcare-cybersecurity-employee-training-affects-it-security
2. https://www.upguard.com/blog/biggest-data-breaches-us
3. https://www.imperva.com/learn/application-security/penetration-testing/