PWNIUM

Teddy Y., James C., Peyton D., Emily K., Charles A., Kyle G.
Computer Science and Information Technology
Advisors: David Corcoran and Wendy Yagodinski

Problem Statement

Due to the lack of cybersecurity measures, there was a fear of an attack at Fernwood. An attack could result in loss of revenue, reputational damage, and loss of productivity. Our job was to identify current data security risks, implement detection/protection measures, and propose policy changes.

Customer Needs/Specifications

Customer needs:

•Update/Create policies

•Multi Factor Authentication

•Help creating more secure passwords

•Plan for backups

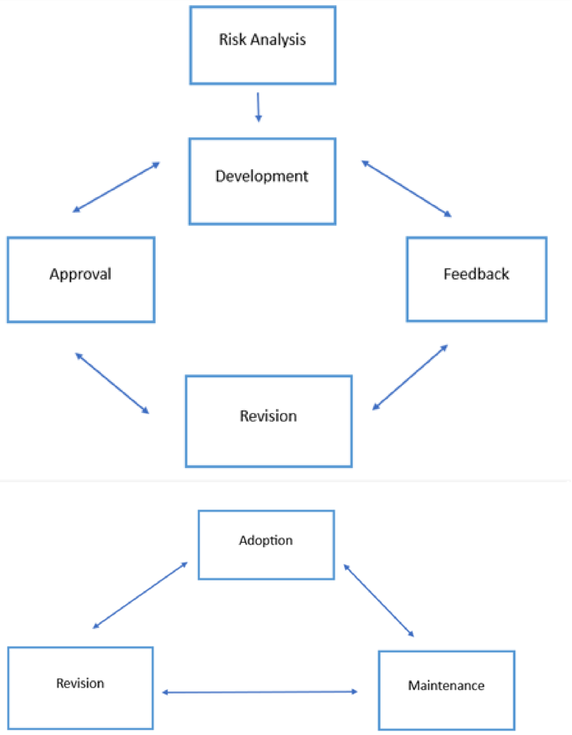
•Help create a culture of data security awareness

Customer specifications:

•Keep in mind limited budget

•Chosen systems need to be automated due to limited staff

Process



Final Product

- Password policy
- Multi-factor authentication policy
- Incident response plan
- BYOD policy
- Cybersecurity awareness training
- Phishing simulation campaigns
- Physical security proposals
- Data backup scheme
- End-user data backup policy

Challenges

One of the biggest challenges we faced was the limited budget:

- budget for the year is determined in advance
- Left us a limited budget to work with for physical security and trainings

Another challenge we faced was the implementation of policies and rolling out training. In the beginning we wanted to implement the policies soon after we completed them.

- Didn't take into consideration the educational training that would need to take place to ensure everyone was on the same page
- External forces -our point of contact was out of commission for over a month so policies that we wanted to roll out were put on hold

Lessons Learned

We learned a lot about how small businesses operate, as well as how IT and cybersecurity infrastructure applies to small businesses (especially those that are nonprofit). More generally, we learned about creating administrative cybersecurity policies and the process for implementing them.

Conclusion

Our implementation plan was broken down into small, medium, and large implementations. The small implementations can be completed within a month. These are free changes that are focused on policy changes. Medium implementations that would take one to six months to implement fully. These changes would be focused on training and preparing for an attack. The cost of these changes depends on what training plan the company decides to go with as well as what backup server is chosen. Large implementations would take six months to a year to complete. These implementations have a jump in cost because these are focused on physical security aspects such as cameras and locks. Ultimately it is up to Fernwood to implement.

Acknowledgments

We would like to thank Joe Metz and all the staff members at Fernwood for being so welcoming and allowing us this opportunity. We would also like to thank David Corcoran, Wendy Yagodinski, and fellow classmates for all their guidance and advice that helped us overcome all the challenges we encountered throughout this process.