Project #1:

GAP ANALYSIS

DeBora King

CSIA 485 7980

Practical Applications in Cybersecurity Management (2178)

November 5, 2017

University of Maryland University College – Fall Semester, 2017

INTRODUCTION

Imagine doing business these days without computers. Managing people, processes and technologies would be virtually impossible. Computers have allowed us to do things like payroll, research and technology faster, better and more efficiently. This efficiency comes with a cost – being interconnected with the world wide web (also known as Internet connectivity). The Internet is a blessing, but it also brings vulnerabilities. Just as we can access the tools needed to manage businesses, people with ulterior motives can access business systems. Focusing on cybersecurity is essential to help guard against potential harm to network systems. This white paper will support and expand on three categories already addressed by the company's Chief Information Officer: 1) people, 2) processes and 3) technologies. The objective is to equip leadership with research material that will assist in making decisions for each department's budget based on integrating cybersecurity as a standard for the company.

ETHICAL CONSIDERATIONS

Just as our country is governed by laws and rules to protect its citizens, companies should set policies and guidelines to protect its stakeholders. Companies may be bound by its commitment to clients (internal and external), employees (which includes contractors and business partners), and property (real and/or intellectual). In a perfect world, we can trust that all clients' data is secure, all employees are honest with company property and knowledgeable about company vulnerabilities, and that perils to our network are nonexistent. This is not the case in today's world of technology. A company responsible for safeguarding client data should be prepared to layer defenses in an effort to dismayed unwanted traffic trying to gain access to valuable information. Some of the most dangerous exposure is within the company, from employees who know information about network systems and use it for their personal gain, to disgruntled staff, to untrained personnel. According to a Security Intelligence article, Aidan Knowles states the consequences involved when a company neglects to put policies in place. “They are subject to lawsuits and damage to their reputation,” says Knowles (Tough Challenges in Cybersecurity Ethics, 2016).

BEST PRACTICES

Forbes reports that the increase in cyber crime was expected to go up to $600 billion in 2016 (Best Practices in Cyber Security, 2016). Let’s couple each investment category with best practice recommendations from the aforementioned Forbs article.

- **People** – policies should be in place to inform employees of the rules and expectations required by the company. In addition, social engineering is used by hackers to gain access to systems or information through manipulating individuals. Training and policies, such as role and rule based policies and password policies can diminish exposure to such exposure. Vetting employees and separation of duties should also be a practice, in addition to setting up exit procedures. A former employee should not have continued access to the company’s systems.
- **Processes** – data encryption is a way of camouflaging critical information to deter hackers from seeing data in plain text. Regular system backups will be very helpful to the company’s recovery. According to a Department of Defense article by Amaani Lyle, It’s not a matter of if a company will be attacked, but when

(DoD News, 2016). Ensuring that backed up data is housed off the premises is equally as important as frequent backups. Prevention of data leakage and theft through access control is a great use of the product.

- **Technologies** – The DoD article states that investment in network defense is worth it. NSA invests in the following solutions to guard against cyber crime:
    - Windows 10 security features
    - Whitelists (trusted websites)
    - Host-based security/intrusion prevention system to address antivirus protection
    - Controlled administrative privileges

RECOMMENDATIONS

The following technologies for information securities are recommended by Gartner:

Cloud Access Security Brokers; Endpoint Detection and Response; Nonsignature Approaches for Endpoint Prevention; User and Entity Behavioral Analytics (UEBA); Microsegmentation and Flow Visibility (halts attackers in the act after they have accessed the system); Security Testing for DevOps (provides automation and transparency through configuration); Intellegence-Driven Security Operations Center Orchestration Solutions (ISOCS "detection and response"); Remote Browser (the ability to isolate malicious activity resulting from email, URLs or websites); Deception tools (staging false vulnerabilities to trap intruders in an attack); and Passive Trust Services (addressing the Internet of Things [IoT])

REFERENCES

Knowles, A. (2016, October 12). *Tough challenges in cybersecurity ethics*. SecurityIntelligence. Retrieved from https://securityintelligence.com/tough-challenges-cybersecurity-ethics/

Harrison, K. (2016, May 3). *The best practices in cyber security for small-to-medium-sized businesses*. Forbes Entrepreneurs. Retrieved from https://www.google.com/amp/www.forbes.com/sites/kateharrison/2016/05/03/the-best-practices-in-cyber-security-for-small-to-medium-sized-businesses/?client=safari

Lyle, A. (2016, October 20). '*Not if, but when': NSA official discusses importance of cyber vigilance*. U.S. DoD.
Retrieved from https://www.defense.gov/News/Article/Artilcle/980031/not-if-but-when-nsa-official-discusses-importance-of-cyber-vigilance

Panetta, K. (2016, June 16). *Gartner's top 10 technologies for information security*. Gartner. Retrieved from http://www.gartner.com/smarterwithgartner/gartners-top-10-technologies-for-information-security/