FXP Task 1: TechFite Case Study

Brent Royal

C850 – Emerging Technologies

Western Governors University

A. Summarize an organizational need in the case study, including the scope of the need.

TechFite is an organization that works out of Houston, Texas and is the supplier of medical devices for NASA. Given that there is already a predisposition about the current cybersecurity infrastructure in place, the Chief Information Officer for TechFite has concerns about the two-firewall system and its ability to properly support the amount of network traffic in a secure manner. With TechFite working hand in hand with NASA, security is a top priority. As a result, the CIO would like for staff to research alternative security solutions that would provide top-notch security.

While security is important, it is also equally important that the security solution be Federal Information Security Management Act (FISMA) compliant. For the security solution to be FISMA compliant, it must meet US federal law guidelines centered around information security and protection by utilizing the National Institute of Standards and Technology (NIST) framework. Compliance across international boundaries is also an integral component for expansion as TechFite is looking to partner with space programs in other space countries, such as European Space Agency, the Canadian Space Agency, and the Japanese Space Agency.

Honeypots should be distributed to detect and deflect attackers from the sensitive data being handled and collected over the network, assuring that the honeypots have no real data associated with them. Also, the cybersecurity framework needs to have the ability to send alerts to the networking team should a threat be detected on the network. Amongst these threats would be denial of service attacks and/or advanced persistent threats.

B. Propose an emerging technology solution to address the organizational need from the case study. Provide justification that classifies this technology as emerging.

Based on the business need of TechFite, my recommendation for the organization would be to implement Amazon Web Services (AWS) as a cloud platform. Not only does AWS meet the requirements of FISMA, it is also secure. With security being a top priority, I believe AWS would be a perfect solution to meet the organization's needs. Large amounts of data can be handled with very minimal to no bandwidth concerns. The services provided by AWS are inexpensive, reliable, and scalable. On top of that, AWS is a pay-as-you-go cloud service so TechFite would only pay for what they truly need. AWS offers an array of tools that can be utilized, including, AWS Glue, Amazon Elasticsearch Service, EC2, etc. There is a need for data to be stored for extended periods of time, logs to be monitored, and real-time alerts of incoming threats to be detected on the network.

Another added benefit of deploying AWS as a cloud solution for TechFite would be the utilization of the Bad Bots component which automatically set up a honeypot. Bad Bots utilizes Access Handler AWS Lambda as a function to detect and deflect attackers by extracting its IP address and adding it to the AWS WAF block list (2019, Architecture Overview).

AWS can be considered an emerging technology solution for TechFite because there are many tools and features that AWS has to offer that the organization could benefit from and many organizations that currently utilize this cloud platform are still trying to figure out how the solution can be implemented into their current systems to meet their business needs.

C. Explain the steps of the adoption process that you recommend the organization use to integrate the new emerging technology, including a description of why each step is necessary and how each step relates to the organization.

Currently, there are various Tech Firms that offer technology consultations. It is recommended that Techfite advises such a Firm prior to selecting a vendor for any CWS installation. Upon receiving the recommendations of the selected Tech Firm's consultation, Techfite will then complete a purchase agreement with the selected vendor, after the vendor will then proceed with the installation of the CWS. First off, upon inception, system configurations and operations shall be accomplished with very little impact so that Techfite is able to configure the system to meet their specific needs. Second of all, the Techfite must be sure that the system administrator is aware of the systems capabilities, and configurations. (MacDonald, 2017).

Because of the use of NIST framework, installation phases will be as follows. Phase I, A risk assessment will be carried out by Techfite in order to asses and prioritize cybersecurity vulnerabilities. Phase II, Protection of Techfite's critical infrastructure will be accomplished by deploying the CWS system (Schlimmer, 2017). Phase III a scan will be performed in order to detect any suspicious cyber security events that could be perceived as malicious attacks. Following the detection of any suspicious events, a responsive procedure will be mobilized with an established timetable (Schlimmer, 2017). After the process improvement plan is initiated, lessons learned will be evaluated in order to improve upon the system in the future. Phase IV after the threat has been neutralized; system recovery procedures will begin. For a successful process, Techfite must ensure that it is well versed in each of the four phases, and ensure each phase is carried out precisely. Consistent tracking is paramount to guarantee the system adheres to each of the requirements of phases (Schlimmer, 2017).

As with anything, there are varied risks when it comes to implementing a system. First and foremost is cyber security. In order to evade this risk, the vulnerabilities must be prioritized and assessed, and impede any workarounds. Another common risk that frequently occurs is the

loss of information due to attacks. To best avoid delays, it is recommended that the CWS be adopted as soon as possible to mitigate the risks that have already been identified.

D. Describe both a positive and a negative impact that your emerging technology solution could have on the people or current processes in the organization, providing examples for how to address the negative impact.

While AWS would be a great technology solution for the organization, it could also have its negative effects as well. Because AWS is automated, it requires less human interaction to function. As a result, this may reduce the number of positions available for employees and result in layoffs and restructuring within the organization. There are advantages and disadvantages to an occurrence such as this. An advantage would be the operational expenses more than likely decreasing. Money would be saved for payroll expenses because of the cut in employees in the cybersecurity department. Another advantage would be accuracy. Errors would decrease if the system were more automated. A disadvantage would be highly skilled workers no longer working for TechFite. This could lead to extra training expenses for the employees who are continuing to work for the organization. The learning curve for the employees trying to fill the shoes of someone else who previously worked at the organization could lead to a decrease in productivity while they are learning their new roles and responsibilities. Another disadvantage would be employees potentially losing their worker morale because of fear they could be affected next as part of the restructuring of the organization. This could lead to employees exploring other job opportunities. Lastly, the restructuring could make TechFite appear as an unstable company in the public eye, which could potentially deter investors.

E. Compare your emerging technology solution to an alternative technology solution, providing at least two advantages and two disadvantages that each technology may have for the organization.

In comparison, there are a number of cybersecurity systems out there. One that comes to mind is HEWLETT PACKARD ENTERPRISE Secure Compute Lifecycle. The main goal of HEWLETT PACKARD ENTERPRISE Secure Compute Lifecycle is to ensure a server is not able to boot should it become compromised, threats are detected, and data is secured safely upon the designated server (HEWLETT PACKARD ENTERPRISE, n.d.). Nevertheless, the traffic and capability that is supported by the HEWLETT PACKARD ENTERPRISE Secure Compute Lifecycle is substantially less than that of CWS and is therefore not recommended to be used by Techfite. Furthermore, the HEWLETT PACKARD ENTERPRISE Secure Compute Lifecycle has less assets than CWS. For instance, HEWLETT PACKARD ENTERPRISE doesn't provide firewalling or like services. Because Techfite requires sophistication that will adapt to the mission and expansion of its security to further guarantee the information systems, as well as the vast data traffic. Because of the firewall necessity on top of the other comparisons, CWS is the best solution.

F. Recommend a method that can be used to determine whether adoption of the proposed emerging technology solution will be successful or unsuccessful, based on the needs of the organization.

The primary goal for the implementation of a cybersecurity solution is to mitigate the risk of a security attack in the most efficient manner. A risk-based approach would be a very effective way to measure the impact of technology within an organization (Chant, 2017). There is a common misconception that a compliance checklist or auditing process is the most effective

method of measuring risk of technology impact. This approach overlooks the importance of remaining abreast of advanced cyber threats. As Chant states, “Accurately measuring the effectiveness of security initiatives requires security experts to extensively assess the risk profile of their organization’s entire IT infrastructure. This means identifying the immediate risks and their impact to key business operations, implementing the relevant controls and processes to remediate them and putting in place a robust governance framework along with agile security operations to continuously manage, and reducing the organization’s risk profile to an acceptable level (Chant, 2017).”

Cybersecurity teams should not only view this risk-based approach through a technology lens, but also from an operational lens, which is where other departments within TechFite would come in. With a risk-based approach, TechFite would be able to focus more on the operational risks within the organization.

One of the metrics to measure the impact of the technology is by calculating the Analytical Production Time. This measure is calculated by measuring the amount of time it takes to gather data and comparing it to when the data was analyzed (Chickowski, 2015). Another measure that can be utilized is to perform case studies in an effort to make better informed business decisions. This can be done by comparing the older manual method of conducting business to the newer automated method to make business decisions.

References

Petters, J. (2019, April 1). What is FISMA Compliance? Regulations and Requirements. Retrieved July 1, 2019, from https://www.varonis.com/blog/fisma-compliance/

(2019) Architecture Overview

https://docs.aws.amazon.com/solutions/latest/aws-waf-security-automations/architecture.html

Chant, B. (2017, April 10). How to Measure the Effectiveness of Security Programs. Retrieved November 27, 2017, from www.infosecurity-magazine.com/opinions/how-measure-effectiveness-security/

Chickowski, E. (2015, March 16). 10 Ways To Measure IT Security Program Effectiveness. Retrieved November 30, 2017, from www.darkreading.com/analytics/10-ways-to-measure-it-security-program-effectiveness/d/d-id/1319494?

Cser, A. (2017, September 1). Vendor Landscape: Cloud Workload Security Solutions, Q3 2017. Retrieved November 27, 2017, from pages.cloudpassage.com/rs/857-FXQ-213/images/forrester-market-overview-cloud-workload-security-management-solutoons-automate-or-die.pdf

HEWLETT PACKARD ENTERPRISE. (n.d.). Server Infrastructure Security Solutions. Retrieved November 30, 2017, from www.HPE.com/us/en/solutions/infrastructure-security.html?pp=false&jumpid=ps_d6y3q8aebi_aid-510353130&gclid=CJj0zfXR5dcCFUMXGwodaCYKSg&gclsrc=ds

MacDonald, N. (2017). Market Guide for Cloud Workload Protection Platforms. Data centre. Retrieved November 27, 2017, from www.scribd.com/document/342875700/Gartner-Market-Guide-for-CWPP-2017.

Schlimmer, S. (2017, October 2). Simplify NIST Cybersecurity Framework Adoption. Retrieved November 30, 2017, from www.infosecurity-magazine.com/opinions/simplify-nist-cybersecurity/