Computer Science Capstone

Name

Institution

**Table of Contents**

Computer Science Capstone

## Proposed Solution

Information is the life force of Target Corporation, and as a result of advanced technology, that info can be effortlessly distrubuted among coworkers, customers, and providers. The massive technological dependence introduces additional risks and threats to those systems which have to be addressed (Kuipers & Fabro, 2006). The proposed solution to improve the security at Target Corporation includes two strategies: an attribute-based authentication and layered security.

### Attribute-Based Authentication

The organization has to improve their security by formulating multiple levels of authentication and protection by introducing additional check and access points. Target Corporation should provide an authentication protocol that addresses the authentication, authorization, and access to all company resources (Abrams & Bailey, 1995). The first aspect is the virtual traffic manager who comes in between an access point and an application to introduce an additional identity verification. The virtual traffic manager will ensure the user identity is validate with other info correlation. It is a multi-factor authentication strategy that checks each user's digital key and their necessary personal credentials that give them the right to access confidential information.

As well as the PKI and personal credential, an attribute database check can be used to add another level of security. The attribute database performs a check for an assortment of personal identifiers such as the employment status and level can be identified from the human resource database. Also, the permission levels can be verified from the clearance database, and content permissions can be determined from the corporate databases that hold a user's department. In addition to identity verification, the credentials determined by the attribute

database check also determine the info a user is allowed to access in the system instead of giving everyone corporate level unrestricted access (Abrams & Bailey, 1995).

**Layered Security**

For an adequate security infrastructure, once identity has been verified there has to be several layers of security at the application layer. Applications today focus more on their operations and neglect to address the security requirements since they are created with a focus on the business-specific requirements. The assumption is that another team will address the security needs of the application. It is conceivable that an application is deployed with known security holes that the current security infrastructure cannot conceal. Some of these holes can be solved through security patches, but that may take a long time after the system is already dispatched in the entire corporation which exposes the company to cyber-attacks. Therefore, a majority of attacks focuses on application security since they are most times deployed with security holes that provide access points for hackers.

It is vital to creating an interconnected multi-layered policy to deal with the threats which guarantee the security of Target Corporation's sensitive info. By tradition, companies concentrate their defensive protocols on the outer limits in the conviction that this makes it challenging for hackers to gain access to the company information and systems. On the other hand, once this boundary is penetrated, the hackers have somewhat unlimited control within the network. Tough, boundary defenses on its own also do not handle the threats that originate from the inside. Therefore, it is prudent for Target Corporation to come up with a multilayered security approach that concentrates on the privacy, reliability, and accessibility of the business-critical info that has to be secured.

The layered security addresses this vulnerability by enforcing real-time policies such as clear, safe session administration, and URL encoding. Also, a virtual web application firewall (vWAF) can be used for application-level security by applying security measures to

web traffic, examining and deflecting security attacks such as SQL injections, while at the same time sifting the outbound traffic to disguising personal identifiable information like users' physical address (Kuipers & Fabro, 2006). Also, there are some more critical protocols like system hardening, and log administration.

**Solution Justification**

The adoption of the attribute-based authentication provides a three-layered identity verification solution through the use of a username and password, PKI digital certificate, and the security clearance level (Abrams & Bailey, 1995). Furthermore, it is possible for Target to include more attributes to their identity authentication process. Finally, the strategy provides the IT personnel with clear info on what users are accessing, particularly which users are accessing the sensitive information and verify if they have the necessary credentials to have that access.

On the other hand, layered security ensures that the application layer is secured even if attackers can bypass the authentication layer. Depending on just one security layer is not prudent anymore given the level of sophistication in security attacks. Target Corporation has to focus on the info that has to be protected and construct several layers of security around. The final solution can be referred to as a defense-in-depth strategy (Kuipers & Fabro, 2006). A layered method to security guarantees that if a single level is affected during a cyber-attack, the other levels will counterbalance and preserve the safety of the company assets. In sequence, all layers must comprise several measures positioned to protect the security of the info.

## Time Line and Resources

### Time Line

The timeline for the project counting the final documentation is roughly six months when the multi-layered security solution is fully operational, as presented in Table 1 and Figure 1.

*Table 1* Milestones (Tasks)

| Task | Possible Start Date | Projected End Date | Duration (In Days) |
|---|---|---|---|
| **Research** | 11/1/2018 | 11/15/2018 | 14 |
| **Feasibility Study** | 11/15/2018 | 12/12/2018 | 27 |
| **Initial Plan** | 12/12/2018 | 12/26/2018 | 14 |
| **Evaluating the Current Security** | 12/26/2018 | 1/10/2019 | 15 |
| **Identifying the Security Measures** | 1/10/2019 | 1/24/2019 | 14 |
| **Selecting the Security Providers** | 1/24/2019 | 2/6/2019 | 13 |
| **Hiring a Team** | 2/6/2019 | 3/3/2019 | 25 |
| **Implementing the New Protocols** | 3/3/2019 | 3/17/2019 | 14 |
| **Testing** | 3/17/2019 | 4/8/2019 | 22 |
| **First Draft of the Documentation** | 4/8/2019 | 4/15/2019 | 7 |
| **Final Draft of the Documentation** | 4/15/2019 | 4/22/2019 | 7 |

| | | | |
|---|---|---|---|
| **Post-Implementation** | 4/22/2019 | 4/29/2019 | 7 |

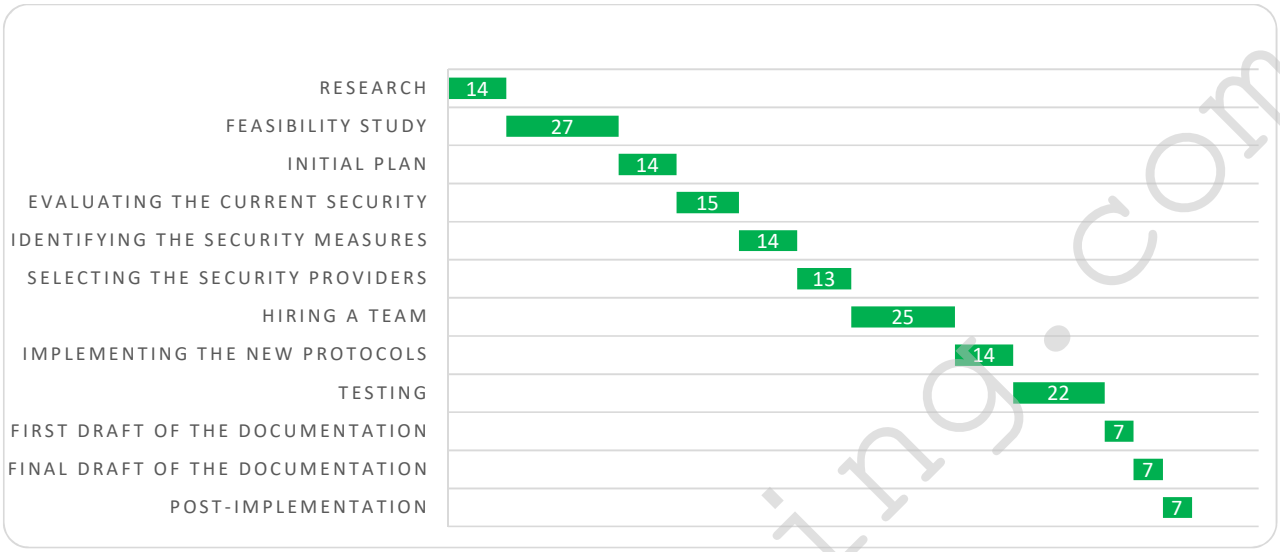


*Figure 1* Gantt chart

The entire process involves twelve tasks that are essential in realizing a more secure system for Target Corporation. The first step involves researching the attribute-based authentication and layered security. This stage ensures the most modern and practical approach is selected. A variety of implementation options are identified, and the most suitable is selected such as an off-the-counter solution or separate solutions. A feasibility study is performed to evaluate the proposed plan and determine if it is financially and technically practical. Once the proposed solution is determined to be feasible, then an initial plan is designed to act as a guide throughout the implementation process. Next, the current security protocols are analyzed to determine their main strengths and weaknesses. It is essential that only the weaknesses be addressed, and the strengths maintained. After which the security measures are determined to handle the weaknesses. Once the security requirements have been determined, the suitable providers are selected which is either a single provider for an off-the-counter single solution or several providers for individual solutions.

Also, a competent IT team has to be hired to handle the next steps. The selection of the team is a crucial stage since the team's actions, and work ethic will determine the success of the project. The team implements the newly proposed protocols and begins testing to ensure the security measures are effective during an attack. The testing will involve launching several cyber-attacks on the new system to identify any security holes and attempting to fix them. Throughout the project, there is documentation of each step but at the end of testing an initial draft of the documentation is created. On review, the draft is corrected and becomes the final documentation. The last step is post-implementation, which is a continuous process of maintaining the system to ensure it is up-to-date with any new security threats (Selcuk, 2017). Also, post-implementation involves training current and new users on the security measures and best practice that ensure Target Corporation remains secure.

**Resources**

A majority of the hardware and resources required to implement the layered security have been listed in Table 2. Although their resources are subject to change since it is possible to find a single solution that provides more than one resource, for instance, antivirus software could also include anti-spam capabilities.

*Table 2* Hardware and Software Resources

| | |
|---|---|
| Software | Antivirus Software |
| | Network Firewall Application |
| | Anti-spam Application |
| | Network-Based Intrusion Detection System (NIDS) |
| | Identity and Access Management System |
| | User Authentication System |
| | Email Security |
| Hardware | Access Control |

| | |
|---|---|
| | Hardware Firewall |
| | Alarm Systems & Intrusion Detection |
| | Biometrics |
| | IP Cameras |

**Risk and Cost-Benefit Analysis**

Performing risk and cost-benefit analysis of architectural features such as security is one of the most challenging activities since the benefits may be challenging to assess (Boardman, Greenberg, Vining, & Weimer, 2017). IT personnel usually security choices, but non-IT managerial staff always question whether their investment in security which is very expensive is worth the money (Butler, 2002). The total cost of implementing both the attribute-based authentication and layered security, regarding licensing and implementation costs, can be very high for each computer, reliant on agreements with the specific vendors. In the case of Target Corporations, they suffered a massive security breach that led to multiple effects on the company's overall performance and total revenue (Heagney, 2018). The hackers were able to steal more than $20 million.

Furthermore, the attackers stole customers' debit and credit numbers that they used to steal from each of them separately. The attackers gained access to customers personally information (PII) such as their emails, physical addresses, and phone numbers. Consequently, Target Corporation will be less skeptical of spending much money on security. There are two main benefits of implementing attribute-based authentication and layered security. The first benefit is that it reduces the window of opportunity attackers may have when targeting the Target systems which makes them less vulnerable (Butler, 2002). It is likely that without the security measures, the company has a sure likelihood of facing another data breach or operational outage within five years. The second benefit is that attribute-based authentication

and layered security minimizes destruction of endpoint systems since malware is removed in the location it was identified thus the damage is rectified remotely (Butler, 2002). These two benefits, collectively, significantly decrease the time spent on tedious IT administration.

## Current and Future Trends Analysis

One of the most significant tendencies is that everything is going mobile. It is the age of smart devices. Mobile devices are being used widely to connect with others, for e-commerce, and to keep records of sensitive info (Kukreja, 2015). Furthermore, the use of mobile payment software and e-wallets to send and receive money has changed people's outlook on the concept of money and money management. Consequently, cybercriminals have identified a new security risk since massive amounts of data stored on mobile devices consist of payment details used in performing online financial transactions.

Over the years, there has been a development of even more sophisticated tools that can detect attacks, which has forced cybercriminals to advance their knowledge and tools to be able to work around the advanced detection tools (Kukreja, 2015). Cybercriminals are working non-stop with the goal of identifying and exploiting various components. Their efforts have been somewhat successful since several organizations have fallen victim to the zero-day exposures. A zero-day weakness refers to an application's security error that is the software owner and creator are unfamiliar with even when the software has been sold. A zero-day exploit gives the attacker a way of causing massive damage that could be as serious as installing malware in company software that allows them to gain illegal access. Furthermore, software components are usually interconnected which means access to a single component may increase the attack-surface and provide the attacker access to even more exploitable components.

Another significant trend in the technological realm is virtualization and cloud environments (Kukreja, 2015). Virtualization makes up a significant portion of cloud

environments. It involves the partitioning of a physical layer into multiple virtual layers or machines. Virtualization assists in providing computing resources such as software and data within the cloud setting. It can also be referred to a software-defined network. Unfortunately, virtualization results in the creation of a complicated architecture of layers whereby every layer has to be protected. In recent years, the technological progression of virtualization in the cloud setting has resulted in an upsurge of the number of security issues being reported.

**Impact the Technology Trends Have On the Project**

Given the popularity of mobile devices, Target Corporation will have to come up with mobile applications where their customers can access their services. Also, the mobile apps will allow staff members to access the company systems remotely with only their credentials. Consequently, the popularity of mobile devices has resulted in a growing need for software security for mobile apps. When Target Corporation eventually develops and launches their mobile apps, they should have them evaluated before launching them within the company and to their customers to reinforce their security (Kukreja, 2015).

Unfortunately, zero-day exploits are very hard to prepare for since they are software defects (Kukreja, 2015). Although, once an exploit has been identified it is crucial to inform the vendor so that a security patch is prepared and dispatched. Also, it is essential to prioritize security requirements when selecting the vendor to avoid falling victim to the zero-day vulnerabilities.

The popularity of cloud technology will force Target Corporation to consider migrating their legacy systems to the cloud environment. Consequently, the company will rely heavily on the core functions since it offers more straightforward deployment and administration, ameliorates disaster recovery, and reduces the overall expenses through minimizing hardware needs. Therefore, the migration to the cloud will introduce new security

risks in the form of complex virtualization layers that necessitate the use of proper security tools (Kukreja, 2015).

**Financial Impact Analysis**

As more cyber threats come up that are focused on the operational integrity and critical information resources, it can take time and again appear as though the company is under threat from an ever-growing list of attacks. Company assets can be in various forms, and the information they hold can be highly valuable. It is usually very essential that procedures are in place to safeguard and protect the assets and that the security measures are suitable and cost-effective (Garg, Curtis, & Halper, 2003).

Target Corporation consultants are skilled at recognizing vulnerabilities, coming up with policies, and rectifying the network to guarantee that the company is safe. The security team utilizes several risk measurements that are suitable to the scope of the company and worth of the resources; they can fashion appropriate requirements of the security measures for the company (Garg et al., 2003). The implementation team possesses the experience and expertise to detect and modify the company's security situation to ensure that risks, which are always underlying, are extenuated. The advanced resolutions provided help minimize the security budget without making conciliates to the class of the Target Corporation's pro-active security. The security measure put in place ensure a competent, non-stop exterior and interior security with instantaneous monitoring, device administration, event correspondence, and examination of the company's infrastructure and vital apps (Garg et al., 2003). The strategy guarantees that any cyber threat is pro-actively handled and attacks are extenuated.

References

Abrams, M., & Bailey, D. (1995). Abstraction and refinement of layered security policy. *Information Security: An Integrated Collection of Essays*, 126-136.

Boardman, A. E., Greenberg, D. H., Vining, A. R., & Weimer, D. L. (2017). *Cost-benefit analysis: concepts and practice*. Cambridge University Press.

Butler, S. A. (2002, May). Security attribute evaluation method: a cost-benefit approach. In *Proceedings of the 24th international conference on Software engineering* (pp. 232-240). ACM.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, *11*(2), 74-83.

Heagney, G. (2018). *Target Corporate*. A Bullseye view. Retrieved 8 October 2018, from https://corporate.target.com/about.

Kuipers, D., & Fabro, M. (2006). *Control systems cybersecurity: Defense in depth strategies*. The United States. Department of Energy.

Kukreja, M. (2015). Top 6 Tech Trends That Will Affect Software Security In 2016 | Synopsys. Retrieved from https://www.synopsys.com/blogs/software-security/top-software-security-technology-trends-for-2016/

Selcuk, S. (2017). Predictive maintenance, its implementation, and latest trends. *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture*, *231*(9), 1670-1679.