## 

DAT 515 Final Project Milestone Six

Michael Surdek

Southern New Hampshire University

In order to protect customers’ personal financial and identity information, Third Star Financial Services will be required to add security frameworks and other restrictions on top of the standard implementation process. The approach to doing this is a layered security framework which protects data at all levels from the outside in. This framework includes security measures along the perimeter, network, platform, application, data, and user levels. It also spans various critical business dimensions such as privacy, confidentiality, integrity, and trust.

To secure the perimeter of the organization, Third Star should install a firewall where secure and insecure networks such as the internet meet. All network traffic, whether inbound or outbound, will flow through this firewall which protects against many common threats. The security for networks themselves should be provided by a Virtual Private Network (VPN) which establishes an encryption tunnel for users and devices to exchange information. It will also be important to ensure platform security regarding actual devices by only using verified and trusted operating systems, file systems, and servers, and by protecting physical access using secure passwords or even biometrics.

Security in regards to applications, data, and users themselves is best managed by restrictions to access control and other defined entitlements that protect against traditional and emerging security threats. Third Star should use a Roles-and-Rules-Based Approach to access control which involved enacting “complex and flexible policies and processes that are based on user identities, roles, resource entitlements, and business rules.” (Berson pp 281) The roles-engineering aspect of access control must include the following considerations:

* Organization role (employee, contractor, customer, partner, etc.)
* Segment role (business domain)
* Team role (software developer, analyst, etc.)
* Channel role (platform, entry point, application, etc.)

In order to further secure the application, data, and user levels of the layered security framework, additional restrictions regarding entitlements and security technologies such as encryption and a Public Key Infrastructure must be implemented. Entitlements across the organization must be defined in terms of functional and data components at both coarse and fine grained levels. Functional entitlements cover coarse grained services and applications and fine grained transactions, methods, and interfaces. Data entitlements cover coarse grained URLs, filed, and databases and fine grained records, attributes, and fields. Technologies that include encryption and other conceptual components are an additional level of security at the application, data, and user layers of the framework. Key concepts that Third Star must consider are eXtensible Access Control Markup Language (XACML), Public Key Infrastructure, Policy Enforcement/Decision/Administration Points, and the separation of duties in regards to the enforcement of policy based access control decisions.

On top of implementing best practices to secure customers’ personal financial and identity information, Third Star must take some common data management ethics issues into account to further protect their customers, prospects, and partners. Although it can be enticing and can lead to operational and business benefits for the company, analytic projects and machine learning algorithms should only be undertaken after thoroughly consider possible negative social implications such as discrimination. Additionally, Third Star must ensure that targeted marketing and communication does not cross the lines into manipulation or harassment. Third Star and all business users of customer’s personal information need to understand the difference between influencing and manipulating a customer. For example, an agent should not show up outside a prospect’s place of employment because they discovered the prospect’s company from their email address. Finally, all mass external communications must include the opportunity for individuals to change or remove their privacy preferences with Third Star, including email type preferences and the option to opt-out entirely. These preferences must be directly connected to the customer data hub and incorporated into all necessary programs and applications so that the customer’s preferences are not violated.

References:

Berson, Alex. Dubov, Larry. Master Data Management & Data Governance. McGraw-Hill

Education. 2020.

DAMA International. “The DAMA Guide to The Data Management Body of Knowledge.”

Technics Publications, LLC. 2010.