**Data Functional Areas - Data Security Management**

Chase Rawson

Department of Technology, Granite State College

DATA 520: Data Mining, Cleaning, and Visualization

Dr. Tony Sulpizio

February 22, 2023

In the world of data analytics, organizations have adapted to more modern data management techniques. Most commonly, data collection comes entirely from the internet and technology. In turn, this data is processed and managed, and data analysts use the results to make concrete decisions that will affect their organization’s future. Now with technology, data records can be saved so data analysts (and the general public when viewing the results) can look back over a specific period to view historical data records. Unlike a locked file cabinet at a desk or in a secure storage room, the architecture used to view historical data can be modified by anyone when connected to the internet; there needs to be some data security implemented. The National Institute of Science and Technology defines “data security as the process of maintaining the confidentiality, integrity, and availability of an organization’s data in a manner consistent with the organization’s risk strategy.” (“Data Security,” n.d.). To prevent any incident, each organization must have a policy that outlines a plan to have a secure data architecture and a plan in place if their data has been compromised in a network attack. Implementing data security may sound simple, but many steps need to be considered, as requested by outside parties.

The first step is to question what data security is and how data must be protected. To accomplish this, the policies of protecting data come from the stakeholders, regulations, and concerns related to the growth of a business. Managing data security is needed to inspire data stakeholders to trust the organization to secure their data in the safest ways. It is the right of students, clients, patients, fellow business partners, and taxpayers to know how an organization is respecting their privacy and their right for their identity to remain confidential to those looking to attack the data architecture. Government regulations also play an essential role in the data security management process, “regulations are in place to protect the interests of some stakeholders. Regulations have different goals. Some restrict access to information, while others ensure openness, transparency, and accountability.” (Henderson et. al., 2017). Also, depending on the motive of the subject(s) attempting to steal confidential data, the concerns of the business or organization must be addressed due to their data possibly having a competitive advantage over other rival organizations. One example would be a beverage company; if The Coca-Cola Company has data about one of the sodas they manufacture and that data justifies the reason for its dominance in grocery stores, they would need to address ways to protect this data from rival companies such as PepsiCo, Inc. or a foreign beverage manufacturer who is looking to compromise their data to be used unethically to improve their sales. Coca-Cola would also need to identify, classify, and locate the sensitive data they need to protect them or lower the risk of these attacks. However, a way to effectively implement data security management does not just come with discovering these risks.

For organizations, especially the size of Coca-Cola and even the United States Government, tools will need to be used to protect the network architecture and the stakeholder data stored on those servers. As described by Michael Samuel Ofori-Duodu, DIT,

The use of devices includes firewalls, load balancers, intrusion detection devices, intrusion prevention devices, honeypots, antivirus, proxy servers, and change detection tools such as tripwire, among others … Countless techniques are under consideration to use by some organizations to help detect malicious insider activity. One such method is the use of a combination of anomaly detection and signature-based techniques to identify potential security breaches. (Ofori-Duodu, 2019).

Other tools that can be considered to use in conjunction is to ensure the website that is collected data is encrypted with HTTPS as well as metadata tracking and data masking/encryption. These tools can provide an in-depth strategy to prevent data breaches. Also, since most of the data will be managed by software, there needs to be a standard to expedite the install security patches, including patches for the devices in the organization interacting with the dataset. Some metrics that can be used to ensure these patches are installed are to calculate the percentage of computers with the most recent security patches and up-to-date anti-malware installed, as well as determining the percentage of employees with background checks and determining how many devices tested for disaster recovery. Performing security audits are also a great way to determine what cybersecurity tasks need to be completed and implemented in the organization. (Henderson et. al., 2017). Although these tools are guaranteed to detect and protect data from external (and possibly internal) threats, we must also discover how to implement data security management concerning internal organizational culture.

Depending on the industry and how sensitive the stakeholders’ data is to others, implementing data security management should begin with a risk assessment. This assessment should include training employees to understand the policies surrounding appropriate internal data usage, ensuring all regulations are followed, and a sense of urgency to ensure the organization follows all requirements at all times. This would be included with any rules already established that provide a hierarchy of which employees are accessing the resources they only need, also known as least-privilege access or access management, “granting database, network, and administrative account access to as few people as possible, and only those who absolutely need it to get their jobs done.” (“Why is data security important,” n.d.). If a specific organization, or government, were at fault for not preventing a network attack that compromised their stored data, the stakeholders would most likely sue them for damages. The lack of legal documentation, agreements, and data security management policies publicly viewed by stakeholders would be disastrous for the organization and likely result in a losing court case. Some organizations have developed these policies to determine the level of confidentiality of the data they have stored to determine (what they believe) is proper data security.

Two great examples of data security management are Harvard University and Marquette University. Harvard’s policy focuses on data security management when conducting research and instructs researchers and information security officers on effectively managing the stakeholders’ data. The purpose of these rules, as stated,

This policy is mainly focused on protecting confidential research data because of applicable laws and regulations, agreements covering the acquisition and use of the data, and University policies. To protect research data appropriately and effectively, the University’s researchers, research oversight bodies, and Information Security Officers must understand and carry out their responsibilities related to data security. (“Harvard Research Data Security Policy,” 2012).

Marquette’s security policy is somewhat different and more flexible; understanding that every research project conducted is unlikely to meet what Marquette deems as data security, but still gives preferences to what they believe is effective data security management (“Data Security for Data Management Plans,” n.d.). This includes preferences regarding the data environment, user access, data management, storage, and transmission.

The purpose of data security management has helped spark a conversation on our focus to protect the collection of our data. Our transformation to a more digital world, along with the many different regulations passed to enforce data privacy, has brought many challenges to organizations regarding how much privacy is needed. In previous days when the internet was nonexistent, data security management was protected using physical controls. However, nowadays, data security management has been enforced logically using many different tools to protect cybercriminals, acting as agents of a foreign nation or as agents of a competitive rival organization. As data security management evolves, new tools and regulations are shaping to enforce data security management to a world where maybe cybercriminals become nonexistent; we can only hope.

**References**

*Data Security for Data Management Plans*. (n.d.). Retrieved February 23, 2023, from <https://www.marquette.edu/research-sponsored-programs/documents/data-management-planning-security-overview.pdf>

*Data Security*. NCCoE. (n.d.). Retrieved February 23, 2023, from <https://www.nccoe.nist.gov/data-security>

*Harvard Research Data Security Policy*. Harvard University. (2012). Retrieved February 23, 2023, from <https://files.vpr.harvard.edu/files/vpr-documents/files/hrdsp_10_14_14_final_edits.pdf>

Henderson, D., Earley, S., Sebastian-Coleman, L., Sykora, E., & Smith, E. (2017). *Dama-Dmbok: Data Management Body of Knowledge* (2nd ed.). Technics Publications.

Ofori-Duodu, Michael Samuel*, "Exploring Data Security Management Strategies for Preventing Data Breaches" (2019).*Walden Dissertations and Doctoral Studies. 7947.  
<https://scholarworks.waldenu.edu/dissertations/7947>

*Why is data security important?* IBM. (n.d.). Retrieved February 23, 2023, from <https://www.ibm.com/topics/data-security>