

Data Security v/s Data Usage

Amol Gote | Course Title | 04/04/2020

*"The world's most valuable resource is no longer oil, but data." (The Economist 2017).* Growth in amount of data that is been collected has grown exponentially. In 2020 each person on earth will generate an average of about 1.7 MB of data per second and there will be around 40 trillion gigabytes of data (40 zettabytes). Enterprises across world big or small ensure that they could collect as much information as possible from the end users or their customers, so that they can define their advertising, marketing, product, customer support etc. strategies based on data insights. This data makes these enterprises powerful, but with power there comes responsibility of securing this vast amount of data. So it has become a big challenge across all these corporate organizations on how to leverage the maximum potential of collected data through various analysis, but in doing so ensure that the data is secure. People may argue that maintaining harmony between these two sets of activities is difficult, but in my opinion there is a way to main the balance between these two processes. Lot of the data driven companies like Amazon, Apple have benefited by maintaining the balance.

Typically in an organization there is a chief data officer (CDO) or Chief information officer (CIO) who is responsible for maintaining the overall organization data safe and secure. There are other executives from different business units within an organization who need to access the data for their data scientists to analyze the data associated with their business or application. The data insights could provide the executives inputs for deriving certain business decisions, it could help them analyze any particular issues and take corrective action to resolve the issue. It helps them in identifying patterns which can help them in organizing the inventory or adjust production quantities. It could help in deciding sales targets for group or an individual. Like these are tons of benefits which can be derived from the existing data a particular application or business might be collecting. So it is of prime importance that the CIO provides access to the respective business units the required data.

CIO’s organization in process of providing secure data access, must avoid any loop holes which will expose the data, ensure proper access controls are in place, identify safeguards to protect data, ensure data quality and accuracy. For securing data they first need to identify which one to secure, this is where data categorization in to PII, PHI etc. can be helpful. There are lot of things that need to be accomplished to ensure appropriate data access and this can be achieved with appropriate data governance framework. *“There are four ways in which data governance and enterprise data management boost cyber security those are Identify data at risk, Identify and classify sensitive data e.g. PII, PHI etc., Identify sensitive data users for ensuring consistent data access processes and Ensure safer access to sensitive data.” (ISACA Journal May 2017).* Apart from this CIO office also need to ensure they abide by all the privacy laws depending upon the industry they are aligned to, these include FTC Act (Federal Trade Commission Act), HIPPA (Health Insurance Portability and Accountability Act), Gramm–Leach–Bliley Act (Financial Services Modernization Act). Recent laws include GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act). To prove that perfect balancing act can lead to lead to greater success of an organization lets cite some industry specific examples.

Let’s consider first the data breach example, First American Financial, one of the largest title insurers in US, reportedly exposed more than 885 million sensitive documents online. Exposed sensitive information included bank/credit union account numbers, mortgage records, tax documents, wire transfer receipts, Social Security numbers and photos of drivers’ licenses. The breach occurred because of incorrect web application design and without any security authentication guards in place. “*Essentially, a link to a webpage with sensitive information is created and intended to only be seen by a specific party, but there is no method to actually verify the identity of who is viewing the link. As a result, anyone who discovers a link to one document can view it—and can discover any of the other documents hosted on the site by simply modifying the link by incrementing the number.” (Forbes May 2019).* The company took immediate action to address the situation and shut down external access to the application. Major issue with this breach was access without authorization and other was insufficient process validation which happens when web application does not enforce appropriate business rules. In this case security team need to ensure flow control which ensure each step is performed in specific order by end user. Appropriate data governance framework especially ***Pillar 3 – Privacy, Compliance and Security*** would had been of significance over here to avoid the breach. It talks about protecting sensitive data through access management and enforces regulatory and compliance requirements which could have helped in discovering the security lapse.

Bibliography

<https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>

<https://kommandotech.com/statistics/big-data-statistics/>

<https://hostingtribunal.com/blog/big-data-stats/#gref>

<https://www.cio.com/article/3234884/what-is-a-chief-data-officer.html>

<https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/boosting-cyber-security-with-data-governance-and-enterprise-data-management>

Forbes May 2019 - <https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/#5449a1e5567f>

<https://www.bankinfosecurity.com/report-sec-investigates-first-american-data-exposure-a-12910>