Data-Driven Security for the Organisation

– Prakash Kumar Ranjan
Senior Manager - IT & Information Security Audit, Airtel Payments Bank, India
https://orcid.org/0000-0003-0319-1749 prranjan1990@gmail.com

Article History
Paper Nomenclature: Srutiny Tip (ST)
Paper Code: CYBNMV1N4SEP2019ST1
Submission Online: 6-Sep-2019
Manuscript Acknowledged: 10-Sep-2019
Originality Check: 12-Sep-2019
Originality Test Ratio: 1%
Peer Reviewers Comment: 14-Sep-2019
Blind Reviewers Remarks: 20-Sep-2019
Author Revert: 21-Sep-2019
Camera-Ready-Copy: 28-Sep-2019
Editorial Board Citation: 29-Sep-2019
Published Online First: 09-Dec-2019

We have heard now a new slogan which says "DATA is the new Oil". The reason behind that organisations uses this data to churn out new business vital information using various data analytics tool or telemetric. DATA is now "Crown-Jewel" to any organisation. Every Organisation has DATA which is vital for their organisational growth and business opportunities. Most of the organisation are building foundation for the security controls around Structured Data which is mostly stored in the organised storage like Database. But typically, more than 80% data are unstructured and is created by almost all the employees unless before where the data creator were less and data consumer were more, but now we all create some amount of data which is relevant for the organisation.

Keywords: Data Security | Cloud Adoption | Digital Information

Introduction

Organisation now have to protect the data from unauthorised access not only from external users but also from internal users as criticality of the data may be high for eg Data related to quarterly results is highly confidential only till it is announced in public domain by the Corporate, but before the announcement of the result, leakage of this data may impact the organisation badly and may also arise insider trading.

DATA Driven security embeds the security controls into the data itself so that these controls are intact to the data irrespective of the data being at rest or in motion or even while the data is being utilized/consumed in a running application.

In Data-Driven Security, data is always kept independent of the security of the infrastructure, be it device, application, network or the method of transport of data so that the controls are platform independent and exercise its security control irrespective of where it is being consumed. DATA LEAKS NOT ONLY puts pothole on reputation of the organisation but also leads to monetary loss/penalties /legal action. The new regulations require the organisation to build control around security of the data and the privacy of the data even if the data travels within the boundary of the organisation or data going outside the boundary of organisation or even crossing the boundary of the nation.

Broadly, the core DATA-DRIVEN Security solutions can be categorised into the following:

1. Data Classification
2. Data Loss/Leakage Prevention (DLP)
3. Cloud Access Security Broker (CASB)
4. Digital/Information Rights Management (IRM, DRM, ERM, EDRM)

Data Classification – Data Classification is a process of identifying and labelling the information/ data preferably on the sensitivity of the data. Most classification tools have element of machine learning based on content and context. This increases the effectiveness of DLP, CASB, EDRM tools. In this we prioritise the data itself and provides the information to the end user also about the nature of the data i.e if data is classified as Internal then it is expected from end user that this shall not be sent outside the organisation.

Data Loss/Leakage Prevention (DLP) - DLP is a security solution that performs realtime scanning of data at rest and in motion, evaluates that data against existing policy definitions defined in the tool, identifies policy violations and automatically enforces some type of pre-defined remediation actions such as alerting users and administrators, quarantining suspicious files, encrypting data or blocking traffic outright. Using DLP Solution , we can take action like we can put a policy that any internal

or Confidential data cannot be sent outside the Organisation so even if users sents email with internal data, DLP can proactively block the email from being sent outside and thus results in preventing the data leakage.

Cloud Access Security Broker (CASB) – Now we all know that Cloud adoption has increased multi-fold and data is no more residing only in your data centre but now residing in private or public cloud so we need to build control to secure our data residing in cloud. CASB helps in identifying, monitoring and controlling the enterprise data in Cloud Infrastructure and it extends control to the Cloud applications. It is also sometimes referred as Cloud DLP in terms of data centric security.

Digital/ Information Rights Management (IRM, DRM, ERM, EDRM) – Traditionally we used to enforce the security controls for the data which resides in our premises but now we need to enforce security control even on the data which has left our premises and is residing in other place because of business requirement. DRM embeds the security controls into the data itself. This controls remains active even if data is being used or worked and it also remains persistent during the movement of data. It helps the enterprise to have control over the data even if the data has left the boundary of the enterprise. Some popular controls of DRM is self-destruction of data or disallowing copy/paste/print of the document.

Scenario of DATA-CENTRIC Security: -

Bank normally send the file to Card vendors to print the cards from vendor location and this file contains all the card details like card number, embossing name, CVV, Date of expiry etc. This information is highly confidential and though the organisation signs NDA with the vendor but NDA is just a legal assurance, but it cannot protect the data from being misused. Though the vendor does not read the data and is used only for safe printing but what in case the employee at the vendor side leaks the data.

How the security of the document/ file be ensured?

Can we assume that after printing from the file, vendor has deleted the data from the device or from SFTP location?

Can the enterprise be 100% sure that data would not be misused in future? -NO

Solution – If we enforce DRM on the document or file, we can set the period of the life of the document itself. We can even recall or revoke access to information that we have shared to anybody. DRM maps the policy so that the document can be protected automatically whenever they are discovered, detected, downloaded or shared.

Emergence of Data Protection Laws

2018 has been a significant year for privacy and data protection laws in the world. Some of the popular data protection laws are: -

GDPR- The EU General Data Protection Regulation (GDPR) took effect on May 25, 2019 and is a regulation in EU law on data protection and privacy for all individuals citizens of the European Union (EU) and the European Economic Area (EEA). The GDPR aims primarily to give control to individuals over their personal data and simplifies the regulatory environment for international business by unifying the regulation within the EU.

CCPA- The California Consumer Privacy Act (CCPA) – a US law – which got passed in California in 2018 and takes effect on January 1, 2020. The CCPA applies to businesses (regardless of location) that collects personal information about California residents, including customers and employees.

Bahrain has also passed a new, comprehensive data protection law making it the first Middle East country to adopt a comprehensive privacy law.

One of the most significant privacy law developments of 2019 is expected from **India**. India's draft bill introduces specific rights for individuals as well as requirements processing entities have to meet. For example, businesses will need to implement organizational and technical safeguards regarding the processing of personal data, including for cross-border data transfers. The law also says to establish a Data Protection Authority for overseeing data processing activities.

Prakash Kumar Ranjan is currently Senior Manager - IT& Information Security Audit, Airtel Payments Bank, India. He was prior working at IDBI Bank and Canara Bank. He has experience of more than 6 years in Security Operation Center design and management ; IT Risk Assessment ; review and implementation of security solutions ; regulatory compliance. He is also having good exposure in Cross Border payment security along with exposure in security design and implementation in Banking and Financial organizations. He is active on various blogging platforms and writing articles on various topics related to Cyber Security.

prranjan1990@gmail.com

Annexure I

Submission Date	Submission Id	Word Count	Character Count
12-Sep-2019	1177017225 (turnitin)	1334	6931

ORIGINALITY REPORT

1%	0%	1%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

PRIMARY SOURCES

1	Johanna G. Tan. "A Comparative Study of the APEC Privacy Framework- A New Voice in the Data Protection Dialogue?", Asian Journal of Comparative Law, 2015 Publication	1%

Note: www.Cybernomics.in Uses a "Turnitin" https://www.turnitin.com which is an American commercial, Internet-based plagiarism detection service, a subsidiary of Advance and also offers plagiarism-detection service for newspaper editors and book and magazine publishers called iThenticate..

Reviewers Comment

Review 1: Protection platform that allows you to move to the cloud securely while protecting data in cloud applications.

Review 2: Data-centric and tokenization security solutions that protect data across enterprise, cloud, mobile and big data environments.

Review 3: Hardware security module that guards financial data and meets industry security and compliance requirements.

Editorial Excerpt

The article has 1% of plagiarism which is accepted percentage for publication The finding related to this manuscript "Data Driven security". Data is important for any kind of organization ,and its loss can lead to penalties, legal actions and monetary loss. so, data driven security is of grate importance as it embeds the security controls into the data itself. Hence ,looking at the findings of the article, it has been earmarked finalized for publication under the category of "**Scrutiny Tip**"

Scholastic Seed Inc.
www.scholasticseed.in

Citation

Prakash Kumar Ranjan
"Data-Driven Security for the Organisation"
Volume-1, Issue-4, Sep 2019. (www.cybernomics.in)

Frequency: Monthly, Published: 2019
Conflict of Interest: Author of a Paper had no conflict neither financially nor academically.