Data Security and Compartmentalization

Rajalakshmi Thiruthuraipondi Natarajan

rajalan11@gmail.com

Abstract

Data Compartmentalization is a practice of analyzing the data collected and managed by the organization for its sensitivity , breaking them into smaller portions and isolating them into respective buckets and applying layers of security as needed to avoid any unintended access or data breaches or leaks and provide relevant ownership for accountability and ease of maintenance. These restrictions apply to accessing the information both internally and externally. The company might employ one more method to categorize and secure the data to restrict the access by an individual or an application, or flow of data to other downstream systems. Depending on the need, relevant security and scrambling techniques, such as access control, encryption, data masking, etc., might be employed to protect the data from unauthorized access and/or safely transmit the data.This needs to be a continuous process, where the data is revisited in regular intervals and reclassified as needed so as to avoid over-utilizing the resources or cause serious hindrance to the company's performance, without compromising the application efficiency and data integrity.

Keywords: Data Security, Cybersecurity, Data Compartmentalization, DataIsolation, access control. Need-to-know access, Information Sensitivity, Data Masking and Encryption, Data Scrambling, Data accountability

Introduction

Every information has a certain sensitivity associated to it. It can be as open as "the sky is Blue" or as secretive as "A secret among two people is, one too many" and it is both legal and moral responsibility to rightly identify and protect them accordingly. Any operating company will have a bundle of raw and processed and information ranging from public statements to inform the general audience and attract new investors to research documents, which might be the next big thing that would put the company on the map and each of these information needs to be rightly identified and exposed or hidden. These restrictions are not only for folks outside the organization, but even within the organization, even could be within the same department. These restrictions are needed by the company to control who knows what and when, since unintended leak might cause damages anywhere between misinterpretation or misunderstanding to proprietary information getting into the hands of competitors leading to serious financial damage.

This is a collaborative effort between business, controllers and IT team to identify and implement the security and isolation. While the source datais usually generated or collected by business, it is the controllers' responsibility to define and manage the access and the IT team's job to implement the solution. Since no application can work in silos, not only should the data be secure from accessing, but also allow it to be used by the necessary users or application for its functions.

Need for Data Isolation & Security

Every business, big and small will have different teams and divisions performing their stipulated tasks for the common benefit of the company as a whole. Yet not all need to access every information that enters the organization. It not only poses a security concerns, but also the efficiency, since too much

irrelevant information would bog down the team in finding the right information for doing its job, not to mention the high chance of mismanaging or misinterpreting or out right misusing the information, posing a nightmare for the security team to protect the organization from threats, both internally and outside.

Data Security

Data security needs no introduction or justification. There are rules and laws at every level directing the organizations on how the data needs to be maintained and the penalties that they must face for failing to do so. Hence companies spend a substantial number of resources and budget improve their security. A breach in data security can be the most damaging to a business, possibly more than a bad product and the threat to the data is real and constant. These threats can be from both external parties such as hackers and internal, like their own employees or contractors.

As mentioned, each division has a specific set of tasks and need relevant information to execute it efficiently. At the same, they have little to no business in having the information outside their purview. For instance, the company's quarterly financial statement after earnings call is a public information and should be accessible to everyone. The employee benefits should be an internal information and should likely be available to all employees within the organization. At the same time, the price negotiated with a supplier is a very confidential and should be available to a specific set of users, probably in the purchasing and department and no one else, even within the company. From the example mentioned above, it is evident that each type needs different levels of security. Having a uniform security might prove to be costly or even counterproductive.

Resource Management

"Too much of anything is good for Nothing". Flooding the team with lots of data will result in wastage of valuable time and resource to find and process the right data for its operations. One might argue that a wholistic knowledge would be beneficial, but quite often, it's not. It can be an automated system or a manual labor, to get to a required set, the whole bunch needs to be scanned, relevance understood and eliminate unwanted information to get to the needed information. To keep up with the need, the company might have to add more resources, either in the form of better systems or more personal to achieve the target.

Example, for AP reporting team, the data needed is the transactions and journals related to Payable invoices and their payments.Feeding the team with all the journals and/or the transactions from other domains, is not only a security issue, but also would be an overhead since most of this information would be irrelevant and waste resources and cause fatigue.

Protection, Integrity and Control

This is an add-on to the above needs. As mentioned, not all data needs to be secured the same way. There are certain set of data that needs to be protected with the highest possible security and others, though not a public information, if compromised, will not cause much of a damage. Hence the need to bucket the data accordingly so that it can be secures as needed. The criticality of the data needs to be determined based on, its value to the division or the company and to others, based on which selective access can be provided to intended parties.

Data integrity indicates how accurate and clean the data is. Exposing the data to a large number of people or resource, increases the chance of it getting corrupted, resulting in inaccurate results or waste valuable resource validating and correcting the data. This can potentially result in loss of confidence in the

data and by extension the company and cause damage financially and to its reputation. Even while finding a solution, it is equally hard to trace back to the problem and provide a permanent fix, until when, the company needs to go into damage control mode.

Finally, control. Any organization would like to be in control of the narrative. Each person or a division can view the same information differently and infer differently. This might lead to multiple versions of incorrect information spreading resulting in gossip or panic. The damage would be even bigger if the same gets outside the company. Once misinformation is spread, it is extremely hard to correct and control this and the damage might already be done. Hence it is extremely important that such sensitive information is only with the responsible team, who has a much better understanding and would know what, when and how to spread the information.

Data Accountability

Data Accountability is holding an individual or a team responsible for anything that happens with the data that they manage. A data in a common pool, while is easy to access, also is exposed to unwarranted access and modification. In an unfortunate situation of data corruption or breach, there will be chaos and finger pointing with no clear ownership. There is also the case of stepping on each other, where the data might be altered to suit one division, which might render it useless for a different division. For instance, Items should be controlled by material management team it is responsible to validate the request and make this information available to anyone who might need it. However, any change to the item should be in full control of this team, if not each team might make changes as needed for them and cause some serious problems to a different team and none the wiser.

Compliance

Compliance is an unforgiving need in every corner of any business. The are rules and regulations defined at various layers on how to manage the data in an organization. Failing these regulations would result in a range of repercussions like loss of confidence, monetary impact, federal audit, legal issues, etc. There are various compliance laws that each industry needs to uphold. For instance, form Medical Industry, the HIPPA law restricts a patient's medical information being accessing aby anyone except the medical professionals, not even by the patients themselves. This is a classic example of a data isolation need, where the medical history made available only to doctors and nurses, whereas the billing information available only to accounting team and any overlap or leak in either side is a serious breach of data leading to heavy fines and penalties.

Implementing Data Compartmentalization

There are several methods that can be adopted to segregate and protect the data and there is no one solution for all, not one right way. There are several factors, such as, data type, mode, accessibility, sensitivity, etc., determines how to effectively isolate the and secure the information. While most products come with its own provision for controlling the data, it is vital that the IT team along with business, evaluate the landscape and come up with solution that is best suited for the business, which can be one or combination of various methodologies.

Functional Isolation

This is the criteria of segregating the data based on the division or personal's job. Each department in a company would be responsible for a specific set of operations and hold data for completing their task. While there might be some information that would overlap with other teams, there will some information

that would cater specifically to the team which others are not privy to. The amount such data might differ between teams, but howeversmall, such information should be isolated and made available only for valid users.

Regional Isolation

This type of isolation kicks in when there are data restrictions based on geography. When a business has a global presence, there could be rules, both from government and internal on the availability of data within and across its boundaries and for various reasons such as non-competence, security, local reliability, etc. This can be as large as a union level, which might group several countries or as small as state or county level. While this information might get consolidated and finally bundle up at the organization level, the operational level information has to be bucketed. For example, in Oracle applications EBS, there is a concept of operating unit, which is usually set up to represent a country and every user can access data only for the operating unit that they are associated to.

Control Isolation

Control Isolationis a horizontal criterion that would be a sub-section of above two conditions. This is based on the level of authority one might have within their section. This type typically will have higher level of clearance compared to others even within the same team or division. These data would be very sensitive and have the highest security and audit. Example, In the payables team, while the regular team would have access to create and process invoices, there would be a set of admins, who are responsible for maintaining the bank accounts and cash disbursement information, which other are not authorized. These types of data would usually have rigorous audit and monitoring as it might have serious consequences.

With the data properly segregated, next logical step is to protect and provide controlled access to this data and ability to create, modify or view this data.

Access Control

This is the most common type of control, where users are created with a specific access control along with various levels of permissions to handle the data, such as edit or view or any other operations. Again, taking Oracle Applications as example, the functional and regional ability to access a data is determined by the responsibility assigned and the MOAC set-up respectively. Without these assignments, the user is denied any ability to view or edit these sets of data.

Another option could be the at the network level, which can either be applied individually or in conjunction with the user access. The data can be secured in a secure network and must be logged into a VPN or a secure remote system to access the data.

Data Encryption and Scrambling

Data Encryption is a technique, by with the information is digitally protected and a valid decryption key is needed to manage it. This can be applied to a whole data set or just a column in in a larger table depending on the sensitivity. This is usually employed when the accessing user is to be made aware of the existence of the data which out providing the actual data or allowing only certain privileged users to access the information.

While accessing suppliers, the banking information is usually encrypted, there by allowing the IT and payables team to access the supplier information and can check and validate if the bank information entered for their operational and support purposes yetwon't be able to see the actual bank details. The

complete access will be limited to master data creation users who will have the decryption key linked to their user and can view and update bank details.

Conclusion

Data has always been a valuable commodity and off-late more organizations and customers a have started realizing this fact. With the growing customer demand for “quick and easy” in every walk, more and more data are collected and maintained by the companies to satisfy the needs, and it becomes all the more important for these companies to manage the data properly to gain customer confidence and grow. With the increase in digital marketing, more industries have a global presence and operate and service from/to every corner of the world, using distributed systems, it has become a complex, yet mandatory, to secure the information and control the same. In a risk of ending in a low note, no matter the design and precaution, there is always a chance that there might be a gap, however, with careful considerations and continuous monitoring, the damage can be detected and controlled swiftly and effectively.

References

1. Security Engineering: A Guide to Building Dependable Distributed Systems, Chapter 8. Multilateral Security
https://www.cl.cam.ac.uk/archive/rja14/Papers/SE-08.pdf

2. R. Khan, K. Ghanem and F. Coffele, "Digital Security by Design: A Review of Combined Hardware-Software-Based CyberSecurity with Compartmentalization," 2023 IEEE International Workshop on Technologies for Defense and Security (TechDefense), Rome, Italy, 2023, pp. 181-186, doi: 10.1109/TechDefense59795.2023.10380808.

3. S. W. Leibholz, "Solutions for the Grand Challenges of Information Security: Protection Against Rogue Insiders, Dynamic Compartmentalization and True Quantum Encryption," 2007 IEEE Conference on Technologies for Homeland Security, Woburn, MA, USA, 2007, pp. 129-132, doi: 10.1109/THS.2007.370033.