asifma

*Growing Asia's Markets*

# Data Vaulting: ASIFMA considerations for improving data recovery

**June 2022**

## Disclaimer

The information and opinion commentary in this ASIFMA paper – *Data Vaulting: ASIFMA considerations for improving data recovery* – (Paper) was prepared by the Asia Securities Industry and Financial Markets Association (ASIFMA) to reflect the views of our members. ASIFMA believes that the information in the Paper, which has been obtained from multiple sources believed to be reliable, is reliable as of the date of publication. As estimates by individual sources may differ from one another, estimates for similar types of data could varywithin the Paper. In no event, however, does ASIFMA make any representation as to the accuracy or completeness of such information. ASIFMA has no obligation to update, modify or amend the informationin this Paper or to otherwise notify readers if any information in the Paper becomes outdated or inaccurate. ASIFMA will make every effort to include updated information as it becomes available and in subsequent papers.

**ASIFMA** is an independent, regional trade association with over 165 member firms comprising a diverse range of leading financial institutions from both the buy and sell side including banks, asset managers, accounting and lawfirms, and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, and competitive Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strengthand clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the U.S. and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.

## Executive Summary

- Regulators are increasingly concerned about the potential for destructive data events, such as a ransomware attack on a financial institution.
- Data vaulting is coming to be seen as a potential solution that will improve firms' cyber incident response and recovery capabilities.
- However, data vaulting has technical limitations which may hinder their ability to provide firms the capabilities needed to meet regulatory expectations for restoration.
- There are principles that regulators should consider before prescribing data vaults.
- Authorities should focus on expected outcomes following a destructive data loss event and avoid prescribing solutions for data recovery which may limit financial institutions' ability to make use of various solutions.

**Background**

As digitisation in financial services has advanced, regulators are becoming more concerned about the potential for a cyber-attack that may result in the unavailability of infrastructure or critical data such that established recovery solutions would not allow for restoration of services within an acceptable time frame. The resulting disruption could not only have negative impacts for consumers and the affected firm but could erode consumer confidence and reduce trust in the wider financial system. If severe enough, such a catastrophic cyber-attack could have financial stability implications. Concerns over the impact of cyber-attacks on data availability and recovery have resulted in several jurisdictions encouraging firms to develop data vaults as an additional layer of resilience to be used in the most extreme situations. While the way different regulators characterise data vaults may vary, their typical objective is to provide additional secure copies of critical data and 'other' objects (e.g., host objects) to protect against compromise in the production environment. To achieve this objective, these vaults are expected to be physically and logically isolated (air-gapped) from the production environment and used in addition to existing back-ups (as a result they are sometimes referred to as a tertiary vault).

While the regulatory focus on restoration and recovery is justified, the industry believes the focus should be on achieving expect outcomes rather than on the models, methods or solutions used to achieve those outcomes. Requirements for financial institutions to follow specific models or concepts for their data backup capabilities could inadvertently reduce restore capability options by diverting firms from more effective approaches.

**Data vaulting initiatives**

- U.S. Sheltered Harbor

  The U.S. Sheltered Harbor was created to "protect customers, financial institutions, and public confidence in the financial system if a catastrophic event like a cyberattack causes critical systems—including backups—to fail. Implementing the Sheltered Harbor standard prepares institutions to provide customers timely access to balances and funds in such a worst-case scenario"[1]. The policy intent behind Sheltered Harbor is, if, for instance, if firm A's critical systems went down and couldn't be recovered, firm B could recover the data firm A backed up leveraging the common data vaulting

[1] https://shelteredharbor.org/

standard SH created for retail customer accounts and retail brokerage protected under Federal Deposit Insurance Corporation.
However, this is conceptual, and the approach is untested. While Sheltered Harbor presents a useful standard for the data to safeguard, it did not lay out how firms might build an end-to-end solution to support service recovery. The approach is limited to providing a snapshot of customer balance data for use in a resolution situation and the industry does not consider it to be a core tool in their cyber incident response and recovery planning.

- Hong Kong Secure Tertiary Data Backup
  The Hong Kong Association of Banks (HKAB) published Secure Tertiary Data Backup (STDB) Guidelines. The Guidelines set out principles for financial institutions to follow as they design tertiary vault solutions for critical data in the event of a destructive cyber-attack. Later, the Hong Kong Monetary Authority (HKMA) requested banks to assess the need for setting up a STDB to counter the risk of destructive cyber-attacks following the HKAB STDB guidelines.
  The scope of data captured by HKAB STDB is a wide set of critical data. The project shifted from an initial focus on retail accounts protected by the local deposit protection insurance scheme, to an effort to bolster financial institutions' wider cyber incident response and recovery (CIRR) capabilities. While the industry appreciates STDB Guideline's flexible approach that does not prescribe a specific solution, the Guidelines still position data vaulting as a core solution for incident response which is problematic given that it suffers from many of the limitations set out in this paper.
  The industry is also aware that authorities in the EU and the UK are considering the merits of data vaulting.

**Definition of data vaulting**

For the purposes of this paper, data vaulting refers to 1) solutions typically designed with some form of sector-wide or multi-firm utility, i.e., a common design intended to be used by more than one firm[2]; and 2) solutions used by a single firm. Data vaulting at firm level refers to firm-specific solutions or requirements for storing copies of their backup data in an environment that is expected to be offline, physically, and logically isolated (air-gapped) from the production environment and core backup environment, typically on some form of hard copy media that must be reconnected for the data to be accessed.

**Limitations of data vaulting**

While a data vault may sound like a prudent approach, there are several limitations to data vaulting which require further exploration and discussion. Data vaulting may still play a role in financial institutions' resilience strategies in specific scenarios; however, it is questionable whether data vaults will be able to deliver fully on the regulators' objectives, especially where a financial institution is answerable to multiple regulators under different locations/jurisdictions.
In relation to destructive cyberattacks, some of the problems or limitations with data vaulting include:

- They are not ideally suited for recovery of data within data loss tolerance levels. Data vaulting may provide a level of protection by physically and logically separating the data from the infrastructure it is used in, but it also reduces the speed at which a firm is able to restore the recovery data into the production environment compared to online backup. Therefore, recovery using data from the data vault may fail to help firms meet the planned or regulatory-mandated Recovery Time Objective (RTO) and firms may still need to invest in idle resources at a tertiary site for faster recovery. For instance, Gartner research describes a situation in which a large quantity of backup data must be transferred from a public cloud environment to an on-premises environment as resulting in

[2] The U.S. Sheltered Harbour is an example of sector-wide or multi-firm data vaulting. The Hong Kong Association of Banks (HKAB) 's Secure Tertiary Data Backup Guidelines lay out principles that could be used for data vaulting solutions at the firm level or sector wide.

"catastrophic restore times".[3] Long restoration times make data vaults better suited to a resolution scenario rather than as a resilience tool for recovery.

- Data vaulting as a form of offline storage does not achieve zero data loss and presents problems for achieving Recovery Point Objectives (RPO). Namely, physical, or logical separation makes achieving synchronisation of data or sufficiently frequent duplication of the data to the vault or offline storage more difficult. Data loss should always be expected when recovering from a catastrophic cyber event involving destructive data. However, a data vault approach may increase the extent of definite data loss[4] between the backup and the live data at the point of the destructive data event.
- There are also limitations to how segregated a backup can be in a data vaulting solution, or any other offline storage. Every time data is transferred to one of these solutions, it must be connected to the production environment creating an opportunity for any malware to propagate across into the backup storage environment. The more frequently backup copies are updated, the more frequent the opportunity for contamination will be.
- Some data vaulting solutions are designed as an industry recovery tool with the expectation that one firm will be able to recover another firm's data and use it to service customers or markets. The storage of critical data in a resolution scenario could be of value, for instance, in ensuring accurate records for the execution of deposit protection insurance. Or, in the event of an incident at a smaller firm, the existence of records of customer accounts or other data in a standard format could be used by a larger firm to absorb those customers and provide account services like in Sheltered Harbor. However, this benefit will likely be limited to smaller firms rather than for large financial institutions. In the event of a prolonged outage at a major institution, there will be legal, technical, and liquidity issues created by one firm absorbing the large number of customers of another firm. These would likely be too great to overcome even if the necessary data were recoverable. For example, having relevant account information is not sufficient to service a client. The absorbing firm would still need to be able to identify the customer, including compliance with relevant know-your-customer rules, as well as to have the human and technology resources needed to service the account. This is the case for the U.S. Sheltered Harbor initiative (see above).

**Looking beyond data vaulting: Regulatory requirements on offline backup and available solutions**

IT and cybersecurity regulations increasingly require firms to maintain some form of offline backup including, but not limited to, data vaulting.[5] For example, in its 2021 Technology Risk Management Guidelines, the Monetary Authority of Singapore requires financial institutions to ensure that any confidential information is stored in backup media which is itself stored offline or at an offsite location.[6] The EU's forthcoming Digital Operational Resilience Act (DORA) similarly proposes to require firms to use an operating environment which is "not directly connected" to their main environment to restore backup data.[7] Many of these rules draw on the Financial Stability Board's (FSB) Cyber Incident Response and Recovery (CIRR) Guidelines which tell firms to "backup and store critical data in offline systems" and to "restore backup data kept in another system, which is segregated (either physically or logically) from the main system".[8]

---

[3] Gartner, "How to Recover from a Ransomware Attack Using Modern Backup Infrastructure", June 2021, p.34.

[4] Definite data loss results from the gap between the last point at which the data was backed-up and the point at which the production environment is compromised. The more frequent the backup the smaller the definite data loss is likely to be as the maximum period between backup and potential corruption is reduced.

[5] For example, see Hong Kong Monetary Authority Secure Tertiary Data Backup, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210518e1.pdf

[6] https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf See 8.4.4.

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN see Article 11

[8] FSB CIRR, paragraphs 16 and 30 https://www.fsb.org/wp-content/uploads/P191020-1.pdf.

While there may be a role for vaulting or offline storage (e.g., satisfying long-term retention requirements or as a fail-safe in the event of disasters other than ransomware, such as hardware failure or natural disasters[9]), there is a need for a clear understanding of the role these solutions can play, including their limitations, in a recovery scenario. Without this understanding, regulators that prescribe specific technical solutions may unintentionally limit financial institutions' ability or willingness to explore alternative solutions which better achieve the desired outcome. The FSB paper gives a clue as to what that outcome is when they ask firms to store backup data offline to "effectively shield the data asset from unauthorised access and data corruption by intentional or unintentional alterations".[10]

With this outcome in mind, financial institutions can leverage multiple solutions to "effectively shield the data asset from unauthorised access and data corruption by intentional or unintentional alterations". For example, some FIs are exploring data immutability which is achieved by storing data in an immutable manner such that the state does not change or deviate once constructed. Any changes that the data owner makes result in the deployment of a new version rather than modifying the existing version, thus leaving the original untouched. The previous version can therefore continue to exist forming a record of change and access to copies of data in their previous states. Some of the benefits of immutability include:

- The continuous chain of record that results from using immutability – which is online – means that it is not necessary to store backup data in an offline environment in order to ensure its integrity. This characteristic makes immutability a better tool for allowing firms to achieve restoration comparatively faster and meet their return to operation targets.
- Immutability will have positive implications for the confidentiality, integrity and availability of data. For instance, data immutability helps to protect against the most common causes of data loss and data manipulation including:
    - Malicious activity such as viruses and ransomware
    - Administrative errors or purposeful sabotage
    - Application bugs

Other resilience solutions include (i) additional detection mechanisms for storage devices so that if suspicious patterns remain undetected at the source host, no backup data is recorded nor replicated further, as well as (ii) proper segregation of backup traffic and backup/storage/restore control plans.

**Principles to consider regarding vaulting or offline backup**

As concerns about destructive data events continue to grow, more authorities are likely to consider whether data vaulting or offline solutions should be recommended or even prescribed in order to increase the industry's cyber incident response and recovery capabilities. However, before any new recommendations, regulatory requirements, or industry projects are enacted, we recommend that the following regulatory principles are considered

- Have a clear desired outcome – It is important for regulators to have a clear purpose and statement of the problem to be solved, as different data vaulting constructs or offline storage solutions are suitable for different use cases.
- Focus on what is most critical – If the objective of the vault or offline storage is to increase a financial institution's CIRR capabilities, it is important to focus on only that which is most critical to the firm. Overly broad requirements for what should be included within the scope of backup will result in significant inefficiencies ultimately reducing the ability of the financial institution to build resilience by forcing it to focus on creating unusable duplicate infrastructure.
- Have a clear statement of the data to be captured – Data prioritisation will be necessary when exploring any vaulting or offline storage solution, especially at the level of an industry solution. The challenge of capturing retail current/checking account data is different than payments data, for

[9] Gartner, "How to Recover", p.17.
[10] FSB CIRR, paragraph 16.

example. From an early stage, it is necessary for the project to identify the scope of critical data to be considered, noting that a single solution is unlikely to be fit-for-purpose for capturing all types of critical data. For instance, transactional data changes rapidly and therefore will require much more frequent backup in order to reduce the extent of definite data loss in a recovery scenario. Alternatively, configuration data changes much more infrequently and therefore make a better candidate for longer term storage.[11]

- Set clear expectations for the time required to restore – While an offline solution may seem the best option from a security perspective, it radically decreases the usability of the system for short term restoration. Regulatory mandated RTOs will often not be achievable using such a solution for which the financial institution would need to rely on more traditional resilience capabilities. It should also be made clear that financial institutions often architect to meet their RTOs in the form of applications, not data. Ensuring the integrity of data and achieving complete recovery of any lost data will almost always take a longer period of time.
- Align governance and oversight with existing incident management governance – Proper governance is necessary in a restoration scenario to ensure the integrity of the data. Such governance should be incorporated or aligned to the financial institution's existing incident response processes or other response and recovery processes. Duplicate governance of technology/data restoration is likely to lead to confusion and possibly further incidents if separated from the financial institution's wider response.

**Conclusion**

The financial sector recognises the growing risk that destructive data events pose, and many firms are independently pursuing uplifts to their data recovery capabilities as a result. Existing methods of data backup may no longer provide all the capabilities firms and regulators require. New technologies such as immutability are now being explored in greater depth as a result. To allow for these new technologies to come to the fore, authorities should adopt an outcome-focused approach and avoid locking in solutions or legacy practices or any other actions which may limit financial institutions' ability to innovate.

[11] On different data types see DTCC et al "Cyber threats and data recovery challenges for FMIs" 2021 p.3. https://www.lch.com/system/files/media_root/Cyber-Threats-and-Data-Recovery-Challenges-for-FMIs.pdf

# Terminology – Glossary

| Term | Description | Source |
|---|---|---|
| Immutable | Data that can only be written, not modified, or deleted for the retention duration. | Immutable - Glossary \| CSRC (nist.gov) |
| Air gap | An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control). | air gap - Glossary \| CSRC (nist.gov) |
| Isolation | The ability to keep multiple instances of software separated so that each instance only sees and can affect itself. | Isolation - Glossary \| CSRC (nist.gov) |
| Data Vaulting | Data vaulting is a security practice that relies on a segregated environment which contains copies of the data and that provides the needed protection against accidental / deliberate modification or deletion of high value data.<br><br>The objective of the vault is to create a protected copy of data that can be trusted in extreme disruption circumstances. It is disconnected from the production and core backup environments in order to increase the chances of successful recovery shall the production network environment be compromised. | |