Data Backup Programs

Why are data backup programs important?

Ransomware attacks, data corruption events, and hardware failure can quickly render mission-critical data inaccessible or unusable - potentially producing immediate and devastating consequences for the affected institution. A robust data backup program ensures that critical business systems and data, including core processing, network administration, and customer records, can be recovered when these events occur. These programs are the backbone of an institution's ability to restore services and maintain operational continuity.

Effective backup programs go beyond simply saving files- they must also include protections against ransomware, test restorability, and allow for off-network restoration if the primary environment is compromised.

Data backup program basics

According to the FFIEC, decisions to implement any particular methodology for backing up data, including the use of replication, should be "based on the risk and criticality of the systems and data."[1] The CSBS Ransomware Self-Assessment Tool (R-SAT) outlines eight key control considerations for implementing and maintaining an effective data backup program. These control considerations are applicable for core processing, network administration, and other data driven critical services, such as trust services, mortgage loans, investments, image files, email services, etc.

- **Ransomware and extortion-resilient procedures**: Ensure that backup procedures include isolation, segmentation, and protections to protect malware from accessing or encrypting backup data files. This may involve utilization of immutable (unalterable) storage methods, air-gapping techniques, and endpoint protections on backup architecture.
- **Distinct authentication methods for access to backups**: Restrict access to backup environments using unique login credentials that are separate from those used for access to the primary network. This can assist in creating an audit trail and can help limit threat actor access when stolen network user or administrative credentials are used to gain access during an attack.
- **Daily full system backups**: Full system backups (not just incremental backups) should ideally be performed at least daily. This procedure helps to ensure that a complete, reliable copy of the data environment is always available. If full data backups are not feasible, the institution should categorize its data by criticality, decide the nature of data to be included, and determine the appropriate frequency of backups to ensure that current, critical data is available when needed.
- **Redundant media types to store backups:** Ideally, institutions will maintain at least two copies of backups stored on different media types (i.e., disk, cloud, flash drive, etc.) and, most ideally, hold them in separate, secure locations. This will help to ensure accessibility in the event of failure of the mechanism(s) utilized to access, read, and restore backup data.
- **Offline or immutable backups**: Ensure that at least one backup is held offline in an air-gapped environment or in an immutable format. According to IBM, "*Air gapping* refers to the physical separation of computers and networks, while *air-gapped networks* are networks that have been

[1] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - VI.B.4- Backup and Replication Processes. June 2021.

isolated from all external networks, including cloud and wi-fi. Air-gapped networks are disconnected from the internet and provide a strong layer of protection from a broad range of cybersecurity threats."[2]

- **Off-network restoration capabilities:** Establish procedures for immediate restoration of backups in a separate, off-network environment in the event primary systems are locked down or otherwise unavailable.
- **Annual backup testing:** Data backup systems should ideally be tested at least annually to confirm that successful data restoration can be reliably performed. Backup testing can be accomplished as a stand-alone process or it may be incorporated into the institution's larger business continuity or incident response testing exercises. Backup tests should be documented, and any identified deficiencies should be remediated.
- **Validation of backup sterility:** Before restoration, verify that backups are free from malware to prevent possible cross-contamination and reinfection. This includes scanning backups before use and verifying the integrity of the backup data.

Other data backup program considerations

Reassess backup and recovery strategies

According to the FFIEC, backup and recovery strategies should be reassessed as technology and threat environments evolve. More advanced duplication and backup methods may be appropriate for real-time or high-volume systems. These advanced methods, including cloud and mirroring, provide high data availability to the institution. Moreover, "Management should maintain an accessible, off-site repository of software, configuration settings, and related documentation. Even standard software configurations can vary from one location to another. Differences could include parameter settings and modifications, security profiles, reporting options, account information, customized software changes, or other options. Failure to back up software configurations could result in inoperability or could delay recovery."[3]

Determine appropriate data retention periods

Appropriate retention periods should be determined for each iteration of data backup. Protections should be in place to prevent the replication of malware and data corruption, the risk of which is enhanced with the use of near real-time data replication systems, as malware can be replicated undetected. According to the FFIEC, "Even with diagnostic tools, management could be unaware of an event that causes data integrity issues until well after it happens, as data could appear uncorrupted but later determined to be inaccurate. Management may determine that the backup of critical data files should be subject to longer retention periods to ensure the ability to recover a backup prior to a corruption event."[4]

Develop appropriate cyber resilience processes

Finally, the FFIEC notes that, "Entities should develop **appropriate cyber resilience processes** (e.g., recovery of data and business operations, rebuilding network capabilities and restoring data) that enable restoration of critical services if the institution or its critical service providers fall victim to a destructive cyber-attack or similar event. Business continuity management (BCM) should include the ability to protect offline data backups from destructive malware or other threats that may corrupt production and online

[2] IBM (Flinders, Mesh and Smalley, Ian). *"What is an air gap?"*. October 14, 2024.
[3] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Business Continuity Management Booklet – IV.A.3 – Data Backup and Replication. November 2019.
[4] Ibid.

backup versions of data."[5] Institutions that rely on third-party service providers, including cloud service providers, to manage their backup and replication processes should validate and ensure the provider maintains satisfactory processes that address, among other considerations, inventories of backup media; processes for testing backups; capabilities to restore to a previous trusted state; protections against malware, destruction, and corruption; and policies, procedures, and standards that document methodologies, prescribe personnel responsibilities, and promote consistent performance.[6]

[5] Ibid.

[6] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - VI.B.4- Backup and Replication Processes. June 2021.

Data Backup Programs
Questions Board Members Should Ask

Below are some questions you may ask management to ensure that the institution's data backup program is sufficient to allow the institution to restore critical business systems and data in the event of a ransomware attack, data corruption event, or hardware failure.

1. ***Explain the controls our institution has in place for data backups.***

   WHY THIS IS IMPORTANT: Backup procedures ***include isolation, segmentation, and protections*** *to protect malware from accessing or encrypting backup data files. This may involve utilization of immutable (unalterable) storage methods, air-gapping techniques, and endpoint protections on backup architecture.*

   Access to backup environments should be restricted *using unique login credentials that are separate from those used for access to the primary network. This can assist in creating an audit trail and can help limit threat actor access when stolen network user or administrative credentials are used to gain access during an attack.*

   Full system backups (not just incremental backups) should ideally be performed at least daily*. This procedure helps to ensure that a complete, reliable copy of the data environment is always available. If full data backups are not feasible, the institution should categorize its data by criticality, decide the nature of data to be included, and determine the appropriate frequency of backups to ensure that current, critical data is available when needed.*

   Ideally, institutions will ***maintain at least two copies of backups stored on different media types*** *(i.e., disk, cloud, flash drive, etc.) and, most ideally, hold them in separate, secure locations. This will help to ensure accessibility in the event of failure of the mechanism(s) utilized to access, read, and restore backup data.*

   Ideally, ***at least one backup should be held offline in an air-gapped environment or in an immutable format****. According to IBM, "Air-gapped networks are disconnected from the internet and provide a strong layer of protection from a broad range of cybersecurity threats."*[1]

   Procedures should be established for ***immediate restoration of backups in a separate, off-network environment*** *in the event primary systems are locked down or otherwise unavailable.*

   Data backup systems should ideally be tested at least annually *to confirm that successful data restoration can be reliably performed. Backup tests should be documented, and any identified deficiencies should be remediated immediately.*

   Before restoration, the institution should ***verify that backups are free from malware*** *to prevent possible cross-contamination and reinfection. This includes scanning backups before use and verifying the integrity of the backup data.*

[1] IBM (Flinders, Mesh and Smalley, Ian). *"What is an air gap?"*. October 14, 2024.

2. ***Does management periodically reassess the institution's data backup strategy?***

   WHY THIS IS IMPORTANT: According to the FFIEC, ***backup and recovery strategies should be reassessed as technology and threat environments evolve****. More advanced duplication and backup methods may be appropriate for real-time or high-volume systems. These advanced methods, including cloud and mirroring, provide high data availability to the institution. Moreover, "Management should maintain an accessible, off-site repository of software, configuration settings, and related documentation. Failure to back up software configurations could result in inoperability or could delay recovery."*[2]

3. ***Does management consider data retention periods for each iteration of data backup?***

   WHY THIS IS IMPORTANT: ***Appropriate retention periods should be determined for each iteration of data backup.*** *Protections should be in place to prevent the replication of malware and data corruption, the risk of which is enhanced with the use of near real-time data replication systems, as malware can be replicated undetected. According to the FFIEC, "Even with diagnostic tools, management could be unaware of an event that causes data integrity issues until well after it happens, as data could appear uncorrupted but later determined to be inaccurate. Management may determine that the backup of critical data files should be subject to longer retention periods to ensure the ability to recover a backup prior to a corruption event."*[3]

4. ***Does the institution maintain appropriate cyber resilience processes that enable the restoration of critical services if the institution or its critical service providers fall victim to a destructive cyber-attack or similar event?***

   WHY THIS IS IMPORTANT: According to the FFIEC, "Business continuity management (BCM) should include the ability to protect offline data backups from destructive malware or other threats that may corrupt production and online backup versions of data."[4] *Supporting processes should allow for the recovery of data and business operations, the rebuilding of network capabilities, and the restoration of data.*

   Institutions that rely on ***third-party service providers****, including* ***cloud service providers****, to manage their backup and replication processes should validate and ensure the provider maintains satisfactory processes that address, among other considerations, inventories of backup media; processes for testing backups; capabilities to restore to a previous trusted state; protections against malware, destruction, and corruption; and policies, procedures, and standards that document methodologies, prescribe personnel responsibilities, and promote consistent performance.*[5]

---

[2] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Business Continuity Management Booklet – IV.A.3 – Data Backup and Replication. November 2019.
[3] Ibid.
[4] Ibid.
[5] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - VI.B.4- Backup and Replication Processes. June 2021.