PROTECTING DATA FROM RANSOMWARE AND OTHER DATA LOSS EVENTS

A Guide for Managed Service Providers to Conduct, Maintain and Test Backup Files

OVERVIEW

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) developed this publication to help managed service providers (MSPs) improve their cybersecurity and the cybersecurity of their customers. MSPs have become an attractive target for cyber criminals. When an MSP is vulnerable its customers are vulnerable as well. Often, attacks take the form of ransomware.

Data loss incidents—whether a ransomware attack, hardware failure, or accidental or intentional data destruction—can have catastrophic effects on MSPs and their customers. This document provides recommendations to help MSPs conduct, maintain, and test backup files in order to reduce the impact of these data loss incidents. A backup file is a copy of files and programs made to facilitate recovery. The recommendations support practical, effective, and efficient back-up plans that address the **NIST Cybersecurity Framework Subcategory PR.IP-4: Backups of information are conducted, maintained, and tested.** An organization does not need to adopt all of the recommendations, only those applicable to its unique needs.

This document provides a broad set of recommendations to help an MSP determine:

- items to consider when planning backups and buying a backup service/product
- issues to consider to maximize the chance that the backup files are useful and available when needed
- issues to consider regarding business disaster recovery

CHALLENGE

Backup systems implemented and not tested or planned increase operational risk for MSPs. The impacts of data loss events can include one or more of the following:

- loss of productivity
- revenue/customer loss
- negative reputation and brand impacts

APPROACH

NIST Interagency Report 7621 Rev. 1, Small Business Information Security reinforces the need for file backups to enable businesses to “resume normal operations after an event." To help small businesses, and the MSPs that support them, effectively conduct, maintain and test backup files, the NCCoE identified capabilities that mitigate the risks identified in the Challenge section. Each MSP should consider the business value or dependence it has on the data it controls to determine the appropriate capabilities. In addition, if the MSP is storing customer data (operational or backups), it should take into account any customer data retention requirements.

RECOMMENDATIONS (Planning, Implementations, Testing)

PLANNING

Planning is an iterative process critical to help an organization optimize and balance costs and operational needs. The following recommendations are based on guidance from NIST Special Publication (SP) 800-53, Rev 4, for controls CP-2, Contingency Planning; and CP-9, Contingency Planning-Information System Backup. When creating a backup plan the following considerations and operational issues should be addressed:

- **Identify the files to back up.** Prioritize files based on business value. For example, an organization may not be able to backup all files due to cost, size, or accessibility. Examples of key files are event logs, user files, and applications. See NIST SP 800-53, Rev. 4, AU-9, Protection of Audit information, for more information.
  - Various cloud services may require different backup techniques. For example, the data backup technique for an office collaboration platform may differ from a customer relationship management (CRM) service. In some cases, the data may not be readily available to back up. In those cases, an alternative approach may be required.
  - Customer data files stored by an MSP may need to be backed up. Consider the customer file retention policies and prioritization needs.
- **Determine restoration time.** Establish the desired timeframe to restore files and applications to minimize negative impacts to the organization's mission or business operations–known as recovery time objective (RTO).
  - Issues that may impact the ability to meet RTO include the internet bandwidth available, any off-site backup facility bandwidth, file transfer limitations and hardware file transfer limitations.
- **Determine file backup timing.** Determine maximum age of the backup files to enable operations to be reestablished with minimum acceptable interruption of operations–known as the recovery point objective (RPO). Acceptable backup file age may vary based on the file types and business process impacted (operations, human resources, accounting, for example).
- **Determine the relationships among systems** to understand any dependencies or order of restoration requirements.
- **Determine what set of backup files and other information need to be secured offline** and the update intervals that satisfy the RPO and RTO for those files. This data and information may include passwords, digital certificates, encryption keys, and other information needed to reestablish business operations quickly.
- **Plan to save more than one backup file** to safeguard your information. (See United States Computer Emergency Readiness Team backup recommendations)
  - To increase the chances of recovering lost or corrupted data, follow the 3-2-1 rule:

    3 – Keep three copies of any important file: one primary and two backups.
    2 – Keep the files on two different media types to protect against different types of hazards.
    1 – Store one copy – or "go bag" – off-site (e.g., outside the home or business facility).
- **Develop response and recovery processes and procedures** that utilize the backup files and backup systems. See Section 5 of NIST SP 800-184 Guide for Cybersecurity Event Recovery for additional recommendations.

- **Determine the appropriate technical approach to generating backups** (automation, manual processes).
  - See the Capabilities section below for a discussion of the type of backup technologies that may be considered.
  - Printed copies of some data/files may be sufficient as well as secure.
- **Determine workplace relocation options.** Fire, flood, or other catastrophic events could require temporary or permanent office relocation, and not all backup capabilities will be portable. See NIST SP 800-53 Rev 4, SC-37 Out-of-Band Channels, for more information. See offline backup recommendation above.
- **Identify any regulatory and legal data retention requirements** such as chain of custody, that may affect the backup plan and technical approach. See NIST SP 800-86 for additional information regarding forensic techniques.
  - Be sure to identify customer files/data retention and care requirements, ensuring that those with RPO/RTO and/or specific custody/retention requirements are treated appropriately.
- **Test the planning for recovery** for both individuals and the entire organization. See Section 3.3 of NIST SP 800-184, Guide for Cybersecurity Event Recovery, for plan recommendations.

IMPLEMENTATION RECOMMENDATIONS

- **Integrate the appropriate technologies into the operation** (noted in Capabilities and Technologies section below).
- **Keep a set of systems completely disconnected from the business network** (offline or on a separate/fire-walled network or located outside the office) for use during a recover/emergency situation.
- **Prepare a "Go Bag" for data recovery.** Keep a copy of critical data–including passwords and security keys, in a separate, secure and accessible location to facilitate recovery operations in the event of a data loss incident. Paper copies of some data may be necessary.
  - Be sure to retain credentials for cloud-hosting providers in printed format and/or electronic forms off-site and offline, such as cloud service authentication personal identification numbers, encryption keys and web browser cookies.
- **Physical diversity capability.** Consider an alternative recovery site in case the primary facility is unavailable for recovery activities

TESTING/MONITORING

- **Test (both manual and automated) the response and recovery processes, procedures and technologies** to:
  - verify backup file integrity
  - ensure effectiveness and efficiency of recovery processes and procedures
  - develop lessons learned. Lessons learned from tests may include:
    - time to retrieve files from off-site (cloud or data center across the internet)
    - whether file retrieval time is directly related to file sizes
    - time to restore files to systems,
    - time to rebuild systems,
    - degree of understanding regarding the responsibilities and authorities among the personnel involved.
    - effectiveness of the processes and procedures

    - identification of gaps (technical and procedural)
  - conduct automated testing that may include testing the various aspects of the backup technologies such as automated restoration, file recovery, and network connectivity
  - provide similar lessons through tabletop test exercises
- **Monitor (both manual and automated) the backup systems and files to:**
  - ensure backup files are created
  - ensure backup files can be successfully recovered and are usable
  - monitor automated testing for success/failure enables proactive management.

CAPABILITIES AND TECHNOLOGIES

To effectively conduct, maintain and test backup files to reduce the impact of data loss incidents, consider the following capabilities:

- **Storage technologies**
  - **Cloud storage** is a service offered to enable off-site file storage (internet connected) in a managed facility and information technology (IT) infrastructure. This may include services such as virtual shared drives or offline updatable storage along with encryption, regulatory compliance, backup from/to anywhere, and redundant file storage. However, cloud storage may identify dependencies such as file download capacity limitations, internet access (availability, bandwidth), and restoration time limitations, as well as lack of geographic location control which may affect domestic and international regulatory compliance.
  - **Local hard drive storage** includes server storage typically included in the operational IT infrastructure network or devices physically attached to the workstations and/or servers. Options may include write once read many (WORM) drives, and universal serial bus (USB) drives, as well as network segmentation to restrict access to the backup files. However, planning for local storage may identify dependencies such as lack of location/physical diversity, hardware and software failure management and software patch management.
  - **WORM storage** includes non-rewriteable technology such as compact disk (CD), digital versatile disk (DVD), and specialized solid-state drive. Files/data written to these types of drives cannot be modified, providing effective file/data protection at the hardware level. However, planning for WORM storage may identify dependencies, including susceptibility to the same physical risks as other IT hardware, and the need to store/protect the devices securely and manage them appropriately.
  - **Removable media storage** includes hard drives, solid state drives, CDs and DVDs (rewritable and nonrewritable), USB (thumb drives), and magnetic tape. Planning for removable media storage may identify dependencies similar to on-site and WORM storage. Removable media storage may also apply to use with a go bag as described above.
- **Automated backup system**
  Endpoint, servers, cloud services, and network based – these capabilities include agent and agentless systems as well as on-premises and cloud-based backup capabilities. Planning for automated backup systems may identify dependencies similar to local storage and cloud storage.

- **Encryption and key management**
  Encryption is recommended for data at rest and data in transit to prevent disclosure of data (inadvertent or malicious). Encryption technologies include disk encryption, data file encryption typically included in data loss prevention, and data transmission using Transport Layer Service and HTTPS. Planning for file/data encryption may identify dependencies such as encryption key management to prevent file/data loss. Encryption key management includes controlling use and access to the encryption keys for the life of any encrypted files. Refer to the Recommendation for Key Management, NIST SP 800-57, Part 1, Sections 5.1, 5.2, and 8 for additional information regarding encryption key management; sections 6.2, 8.2.2, and 9.5 for encryption key storage management; and section 9.4 for encryption key backup recommendations. Part 2 and Part 3 of NIST SP 800-57 provide additional details on organizational and application specific key management.
- **Cloud-based backup service providers**
  These capabilities provide backup file storage in each vendor's cloud/data center(s), for example. The services may include on-premises appliances, agent or agentless techniques to identify files to be stored for backup, such as frequency; data type, full or incremental; and various levels of security (encryption, geographic diver-sity). Planning for cloud-based backup services may identify dependencies similar to cloud storage.
- **Backup of data processed in cloud services**
  The capabilities provide backup file storage for the data maintained within each cloud service. Planning for cloud service data backup may identify dependencies similar to cloud storage. A combination of the capabilities listed above may be required to backup data/files stored in cloud services. The combination may be determined on a case-by-case basis.

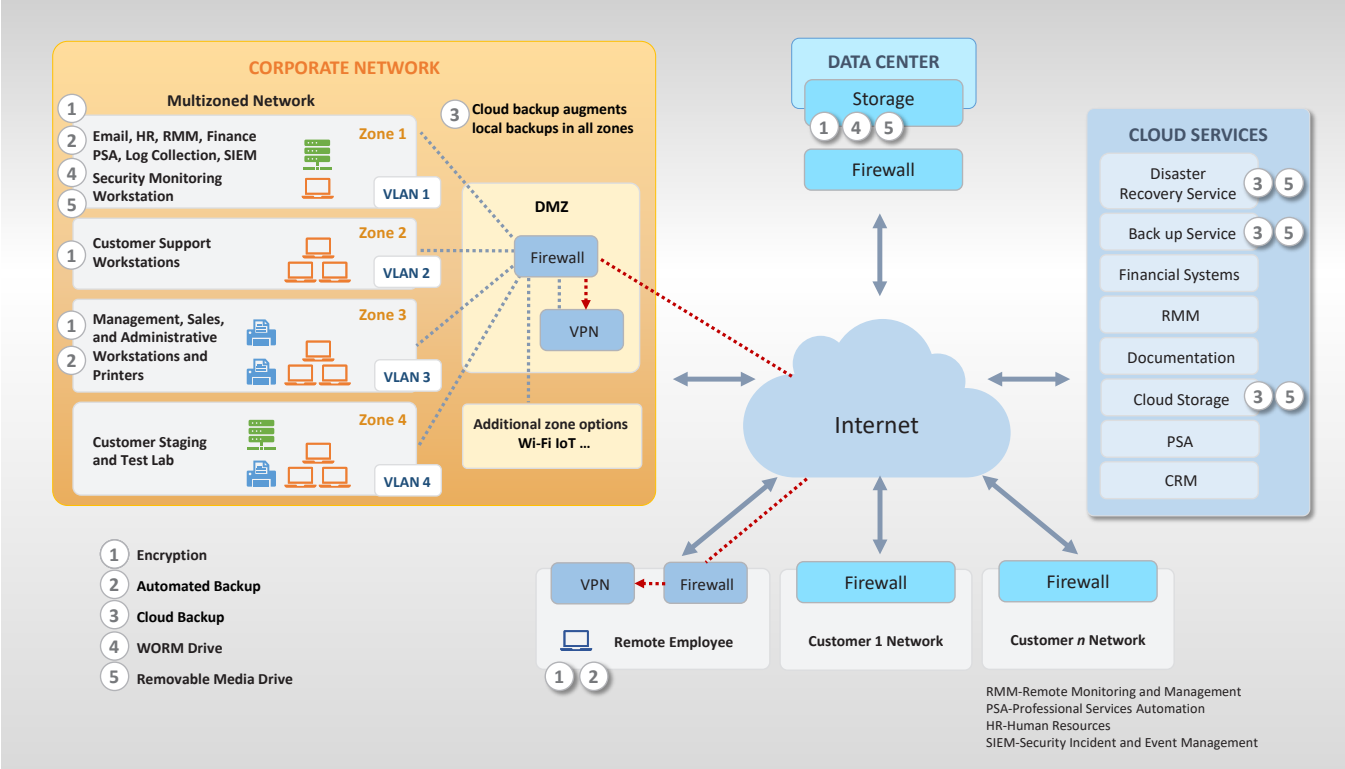
The following NIST publications describe solutions and implementation guides that include the capabilities listed above:

- NIST SP 1800-11, *Data Integrity: Recovering from Ransomware and Other Destructive Events*
- NIST SP 1800-25, *Identifying and Protecting Assets Against Ransomware and Other Destructive Events*
- NIST SP 1800-26, *Detecting and Responding to Ransomware and Other Destructive Events*

ARCHITECTURE

The diagram below illustrates a typical MSP IT infrastructure (including cloud services utilized by MSPs) and highlights where the capabilities listed in the previous section can be implemented to effectively conduct, maintain, and test backup files. Organizations leveraging the reference architecture should adhere to the standard cybersecurity recommended best practices listed in NIST SP 1800-11, Section 6.3.1, Deployment Recommendations.

ARCHITECTURE DIAGRAM



CONCLUSION

Preparing an organization to create and restore backup files can help mitigate the damage from ransomware attacks or other types of data loss incidents. The deployment and implementation recommendations described above can help MSPs conduct, maintain, test and monitor backup files to restore files/data and systems with minimal impact to business operations. The capabilities and technologies described may be used to implement policies and techniques required to achieve the goals of a backup plan. The architecture diagram illustrates the various networks, subnetworks and cloud services where data/file backup technologies may be deployed to achieve the goals of the backup plans. Throughout the document NIST publications were referenced to provide additional details to support planners and technology integrators.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have feedback on the architecture or the relevance and usefulness of this document, please email smb_nccoe@nist.gov.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.