

# PROTECTING YOUR DATA FROM RANSOMWARE AND OTHER DATA LOSS EVENTS

**Recommendations on How to Conduct, Maintain, and Test Backup Files** 

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 small- and medium-sized business customers. This document provides **recommendations to help MSPs conduct, maintain, and test backup files** to reduce the impact of these data loss incidents. The deployment and implementation recommendations in this document can help MSPs restore files/data and systems with minimal impact to business operations.

## **BENEFITS OF IMPLEMENTING EFFECTIVE BACKUP STRATEGIES**

- Minimizes impact of data loss incidents.
- Improves business operations and resiliency.
- Highlights a commitment to security for MSP clients.

### **RECOMMENDATIONS**

When creating a backup plan, the following considerations and operational issues should be addressed:



#### IDENTIFY FILES AND PROCESSES FOR BACKUPS

- Prioritize files based on business value and operational needs.
- Identify what backup files/data to secure offline. Consider producing multiple backup file copies.
- Identify any regulatory and legal data retention requirements, such as chain of custody, that may affect the backup plan and technical approach.
- Determine if automated or manual processes are best for generating backups, including hard copies.
- Retain copies of credentials, including personal identification numbers, encryption keys, and web browser cookies.



#### DETERMINE FREQUENCY OF BACKUPS

- Establish a desired time frame to restore files and applications to minimize negative impacts to the organization's mission or business operations-known as recovery time objective.
- Determine the maximum age of the backup files to enable operations to be reestablished with minimum acceptable interruption of operations– known as the recovery point objective.



#### **TEST BACKUP RECOVERY PLAN**

- Develop response and recovery processes and procedures that utilize the backup files and backup systems. Conduct tabletop exercises to identify opportunities for improvement.
- Determine workplace relocation options: e.g., fire and flood could require temporary or permanent office relocation; not all backup capabilities will be portable.
- Test planning for recovery: Test individual systems and the entire operation (if possible).
- Monitor the backup processes for failures and consistency.

# For detailed information on implementing a backup solution visit www.nccoe.nist.gov/msp

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. LEARN MORE ABOUT THE NCCOE Visit https://www.nccoe.nist.gov/

CONTACT US smb\_nccoe@nist.gov