# Cyber Awareness: Importance of Backups

HEALTHY STEPS HAWAI'I
WORKING TOWARDS A HEALTHIER HAWAI'I

# What are backups?

- Backups are a copy of data stored separately from the original.
- They prevent data loss from numerous ways
  - Hardware failure
  - Software malfunction
  - Malware
  - User errors
- Types of backups
  - Full backups
    - Full copy
  - Incremental backups
    - Only data that has been modified since last backup
    - Faster; requires less processing and storage
  - Differential backups
    - Similar to incremental, but copy all data since last full backup
    - Balanced between efficiency and restoration

HEALTHY STEPS HAWAI'I
WORKING TOWARDS A HEALTHIER HAWAI'I

# What is the purpose of backups?

- Provide business and individuals to recover data, minimize downtime, and prevent financial losses
- Simple, but extremely effective for worst case scenarios
- Duplicating the data creates a safety net for your information
- How can I implement a backup practice into my business or personal information?
    - 3-2-1 rule

HEALTHY STEPS HAWAI'I
WORKING TOWARDS A HEALTHIER HAWAI'I

# 3-2-1 Rule

- 3 copies of data maintained at a minimum
  - 1 primary
  - At least 2 backups
- 2 different mediums
  - Multiple media forms
    - External hard drives
    - Network attached storage (NAS)
    - Cloud storage
- 1 off-site copy
  - One copy of data should be physically stored in a separate location
  - Helps prevent local disasters: theft, fire,  and floods

HEALTHY STEPS HAWAI'I
WORKING TOWARDS A HEALTHIER HAWAI'I

# Maintaining Proper Backups

- Backups should be tested regularly to maintain data integrity
  - Incrementally multiple times over a 24 hour period
  - Less sensitive data can be once every 24 hour period or even longer
  - Context is important when maintaining data
- Verification of backup completeness
  - Ensure all critical data is accounted for
- Performance Testing
  - Evaluate how quickly data can be restored from backup for organization or your needs
- An old backup is better than none at all
- Provides resilience against a wide range of threats from physical to digital attacks through diversification of storage

HEALTHY STEPS HAWAI'I
WORKING TOWARDS A HEALTHIER HAWAI'I

# Encryption

- Equally important for ensuring backup data is secure
- In-transit encryption
  - Protects data while moves from system to backup location i.e cloud provider or server
- At-rest encryption
  - Secures data while stored in the backup location to protect against unauthorized access to the data
- Encryption is another blanket of security that further prevents unauthorized parties from accessing data
- Particularly important for HIPPA and GDPR regulations

HEALTHY STEPS HAWAI'I
WORKING TOWARDS A HEALTHIER HAWAI'I

# Backup Retention & Archiving

- Determining the length of retaining backups is also critical
  - Longer duration = increased storage costs
  - Potentially allows additional methods of unauthorized access
- 4 key pillars of backup retention
  - Regulatory Requirements
    - Industries have specific policies related to specific data, less of concern for individuals
  - Operational Needs
    - How far back you need to access the data for operational duties, less of concern for individuals
  - Storage Costs
    - Longer retention requires more storage costs, depends on type of data
  - Security Risks
    - Unnecessary data can undermine data prevention loss
- Tiered Retention Policy is a baseline
  - Keep different types of backups for different amount of intervals

HEALTHY STEPS HAWAI'I
WORKING TOWARDS A HEALTHIER HAWAI'I

# Questions?

Please feel free to reach out to us at healthystepshi@gmail.com if you have any questions or would like to see any new topics!