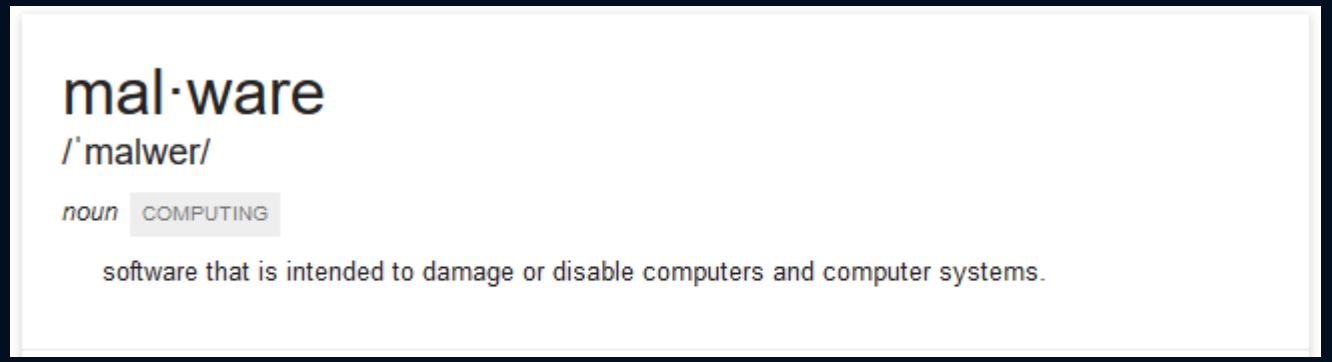
NWRDC
Northwest Regional Data Center

# Preparing For and Recovering From Ransomware

# Definitions

- Malware



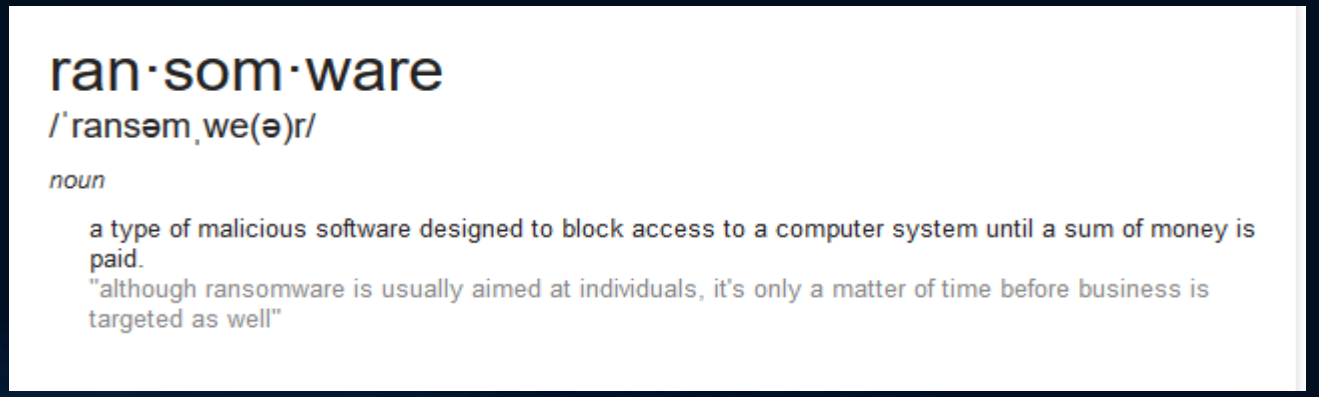
mal·ware

/ˈmalwer/

*noun* COMPUTING

software that is intended to damage or disable computers and computer systems.

- Ransomware



ran·som·ware

/ˈransəmˌwe(ə)r/

*noun*

a type of malicious software designed to block access to a computer system until a sum of money is paid.

"although ransomware is usually aimed at individuals, it's only a matter of time before business is targeted as well"

NWRDC
Northwest Regional Data Center

# What does Ransomware do?


- Usually locks infected devices , displays large banner
- Tries to propagate itself throughout your network, via any means available
- Makes $$$


NWRDC
Northwest Regional Data Center

# How does ransomware infect my devices?

## Common infection vectors

- Phishing
- Infected removable media
- From other compromised machines
- Being introduced via other malware

NWRDC
Northwest Regional Data Center

# Ransomware Prevention Checklist

- User Education
- Vulnerability Management Program
- Anti-Malware Solution
- Security Reporting System
- Incident Response Plan
- Data Backup & Data Restore Plan
- Patching
- Permissions

NWRDC
Northwest Regional Data Center

# Post Ransomware Infection Checklist

- Disconnect everything
- Determine scope of the infection
- Determine the Ransomware Strain
  - https://id-ransomware.malwarehunterteam.com/
- Note all mapped network connections
- Note cloud based storage, SAN , etc.
- Determine infection vector and remediate it

NWRDC
Northwest Regional Data Center

# Response Options

- Restore your files from backup
- Attempt to decrypt encrypted data
- Accept the loss
- Pay the ransom (Not recommended)

NWRDC
Northwest Regional Data Center

# Response Option #1 (Restore)

- Locate your backups
- Ensure all files you need are on the backup media
- Verify integrity of the backups (corrupted files/encrypted files/missing files)
- Check for previous versions stored in the cloud / Air-gapped Backups
- Restore your files from backups

NWRDC
Northwest Regional Data Center

# Response Option #2 (Attempt to Decrypt)

- Determine the strain and version of the ransomware
- Locate a decryptor; there may not be one for newer strains
- Attach storage media that contains encrypted files
- Decrypt files

NWRDC
Northwest Regional Data Center

# Response Option #3 (Accept the Loss)

- Remove the ransomware if possible
- Backup encrypted files for possible future decryption (optional)

NWRDC
Northwest Regional Data Center

# Response Option #4 (Pay Ransom)

- Attempt to negotiate a lower ransom and/or longer payment period
- Determine acceptable payment methods for the strain: Bitcoin, Cash Card. etc.
- Obtain payment, likely Bitcoin
- Locate an exchange through which you wish to purchase Bitcoins
- Setup an account/wallet and purchase Bitcoins
- Reconnect the infected system to the internet; pay ransom

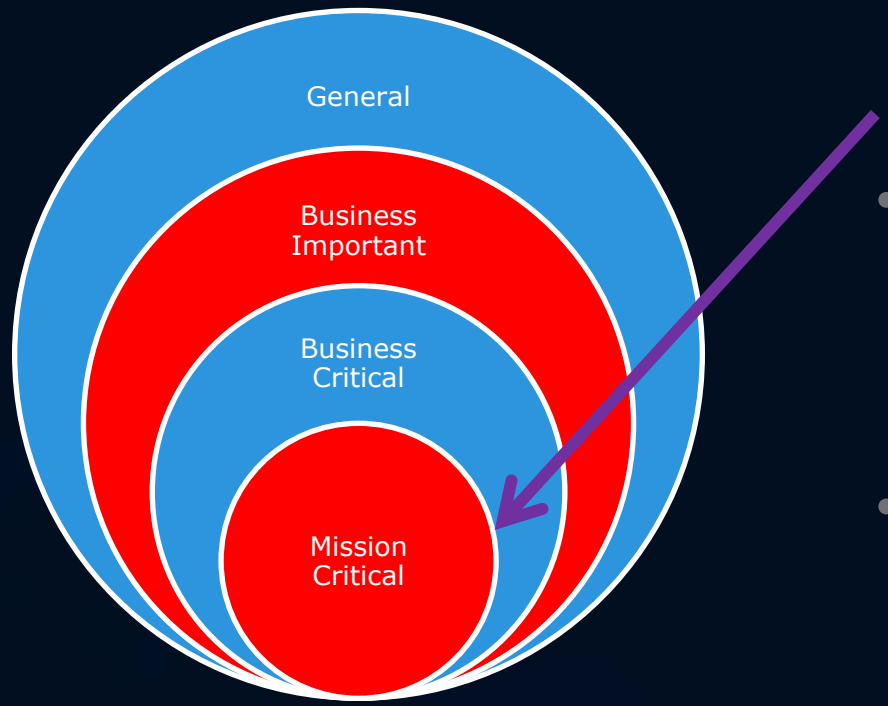
NWRDC
Northwest Regional Data Center

# Questions?

NWRDC
Northwest Regional Data Center

# Identification and Classification of Data Types

- Mission Critical
  - Failure of organizational operations.
- Business Critical
  - Disruption of certain functions. Suffer serious financial or legal damages.
- Business Important
  - Organizational functionality at either reduced or delayed levels.
- General Information
  - Normal operational functions continue. Lost data can be recreated.

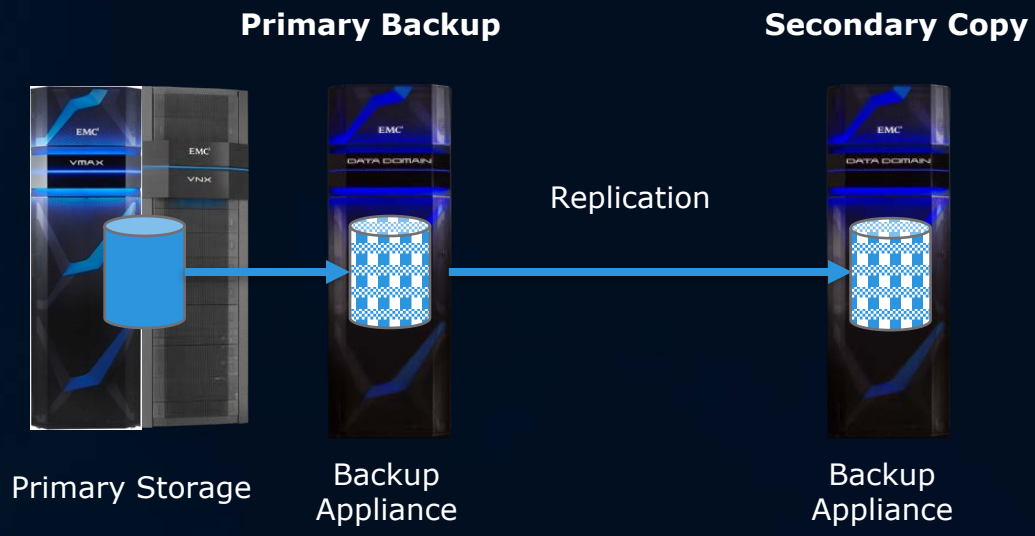



- Protect the "heartbeat" of the business first
- Prioritize top applications or data sets to protect
- Usually less than 10% of data
- Start with a core set and build from there

NWRDC
Northwest Regional Data Center

# Disk Based Backup with Secondary Copy

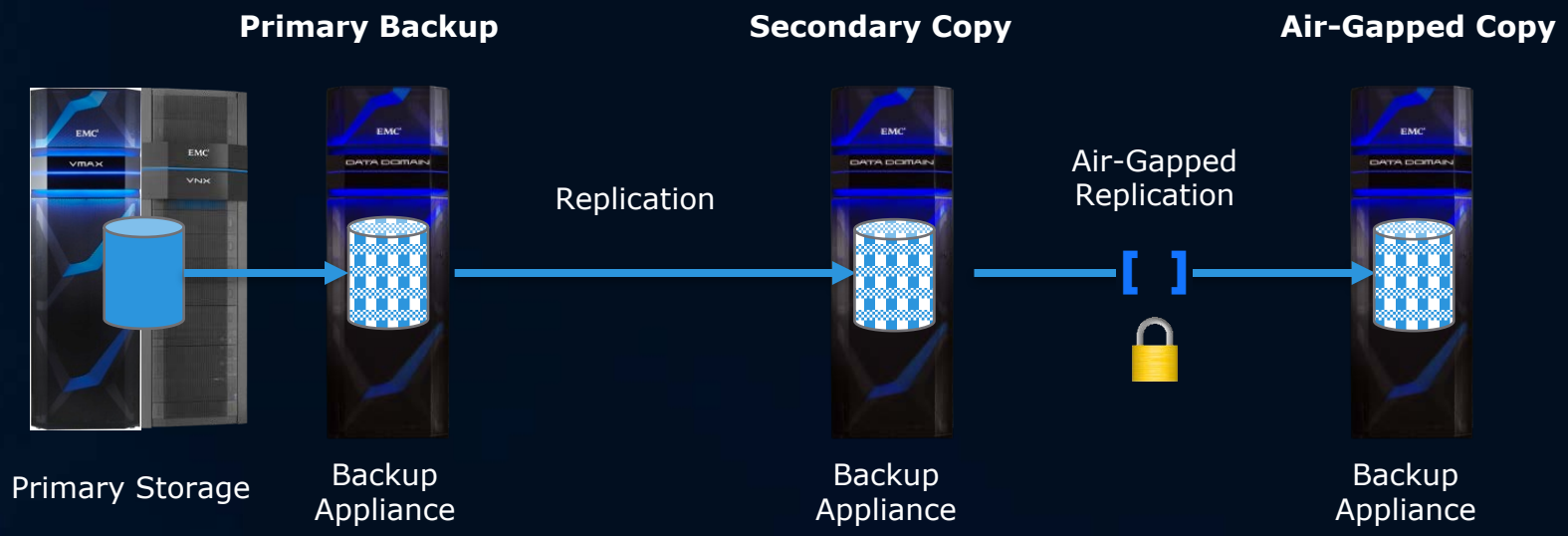
- Create Backup of Data
- Replicate Backup to Secondary Copy ( local or remote location )




NWRDC
Northwest Regional Data Center

# Disk Based Backup with Secondary Copy Using Air-Gap

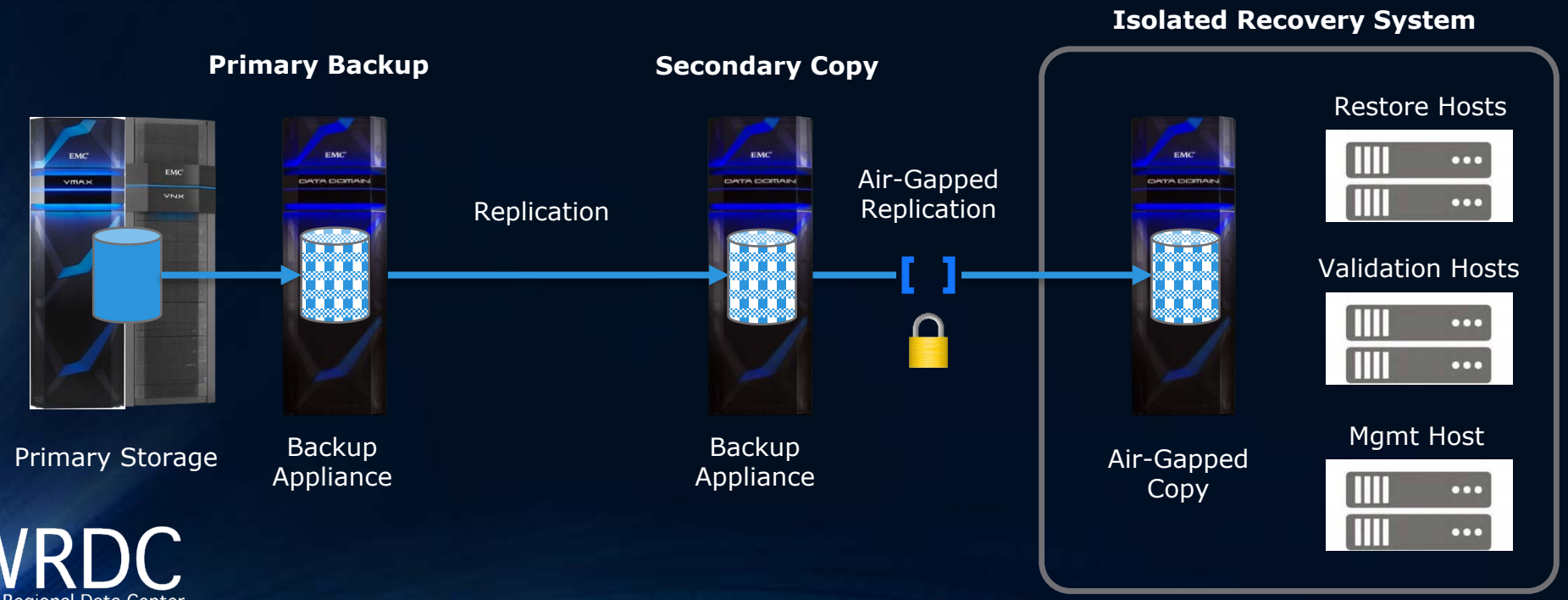
- Create Backup of Data
- Enable Link and Replicate to Isolated System ( local or remote location )
- Complete Replication and Disable Link




NWRDC
Northwest Regional Data Center

# Isolated Recovery Solution

- Create Backup of Data
- Enable Link and Replicate to Isolated System ( local or remote location )
- Complete Replication and Disable Link
- Restore Data into Isolated Systems and Validate
- Enable Link and Initiate Restore into Production




NWRDC
Northwest Regional Data Center

# The Common Elements of any Recovery Solution

- Planning and Design
- Separation and Data Movement
- Validation Procedures
- Recovery and Remediation

NWRDC
Northwest Regional Data Center

For questions or additional information, please contact:

Tony Fondo
Information Security Manager
tony_fondo@nwrdc.fsu.edu
850-645-3529

Steve Oropallo
Storage and Recovery Services Manager
steve_oropallo@nwrdc.fsu.edu
850-645-3575

NWRDC
Northwest Regional Data Center