



Preparing For and Recovering From Ransomware

Definitions

- Malware

mal·ware

/ˈmɒlwɛr/

noun COMPUTING

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

- Ransomware

ran·som·ware

/ˈrɑnsəmˌwe(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"

What does Ransomware do?

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

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).



OK



WARNING!

Your personal files are encrypted!

11:58:26

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open <http://maktubuyatq4rfyo.onion.link>
or <http://maktubuyatq4rfyo.torstorm.org>
or <http://maktubuyatq4rfyo.tor2web.org>

How does ransomware infect my devices?

Common infection vectors

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

Ransomware Prevention Checklist

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

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

Response Options

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

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

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

Response Option #3 (Accept the Loss)

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

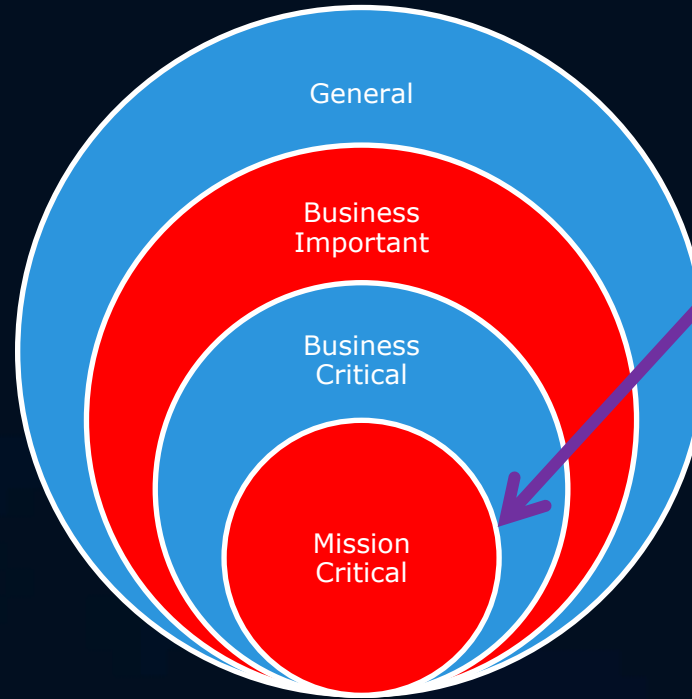
Response Option #4 (Pay Ransom)

- 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

Questions?

Identification and Classification of Data Types

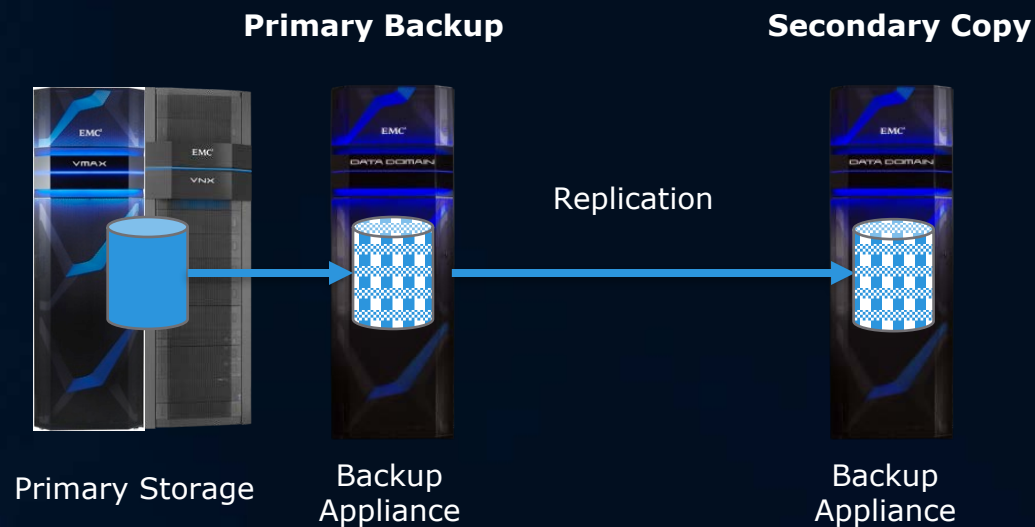
- **Mission Critical**
 - Failure of organizational operations.
- **Business Critical**
 - Disruption of certain functions. Suffer serious financial or legal damages.
- **Business Important**
 - Organizational functionality at either reduced or delayed levels.
- **General Information**
 - Normal operational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

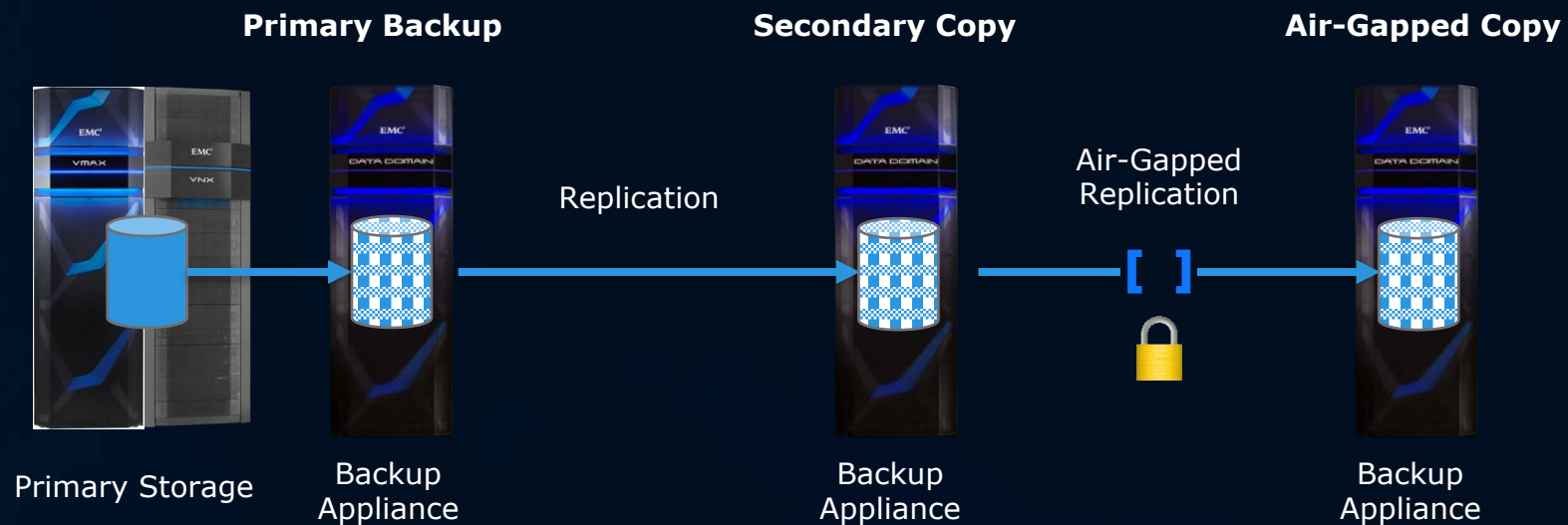
Disk Based Backup with Secondary Copy

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



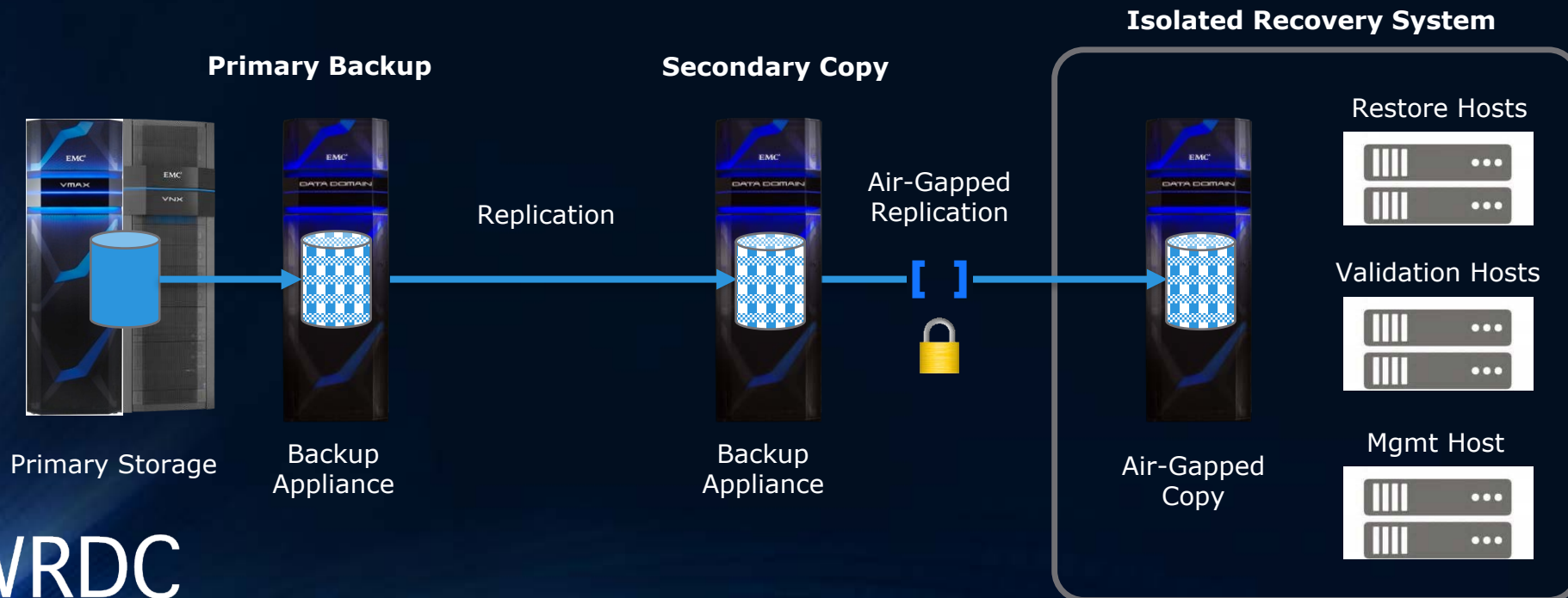
Disk Based Backup with Secondary Copy Using Air-Gap

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



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



The Common Elements of any Recovery Solution

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

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