L’importanza della protezione dei dati nel garantire una più efficace cyber resiliency

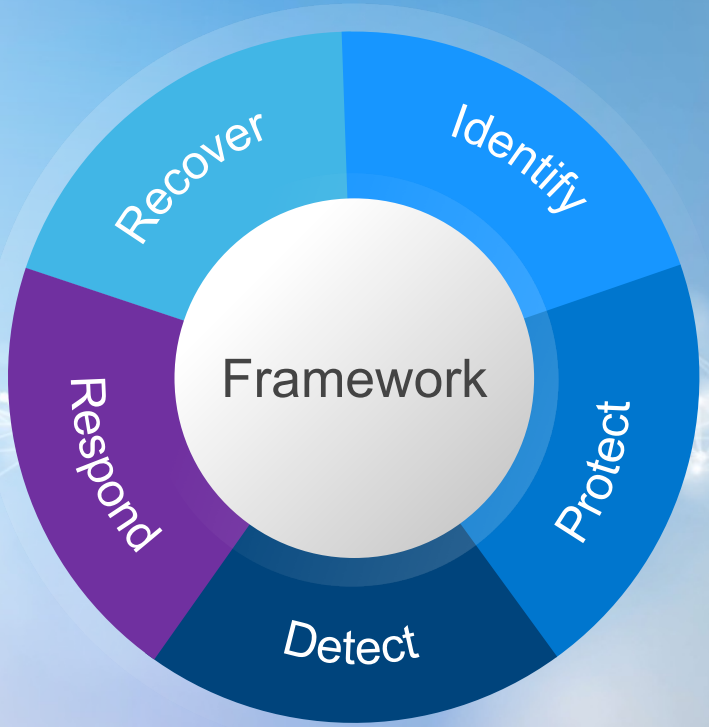
Fabio Zezza
DPS Sales Lead - Italy

DELL Technologies

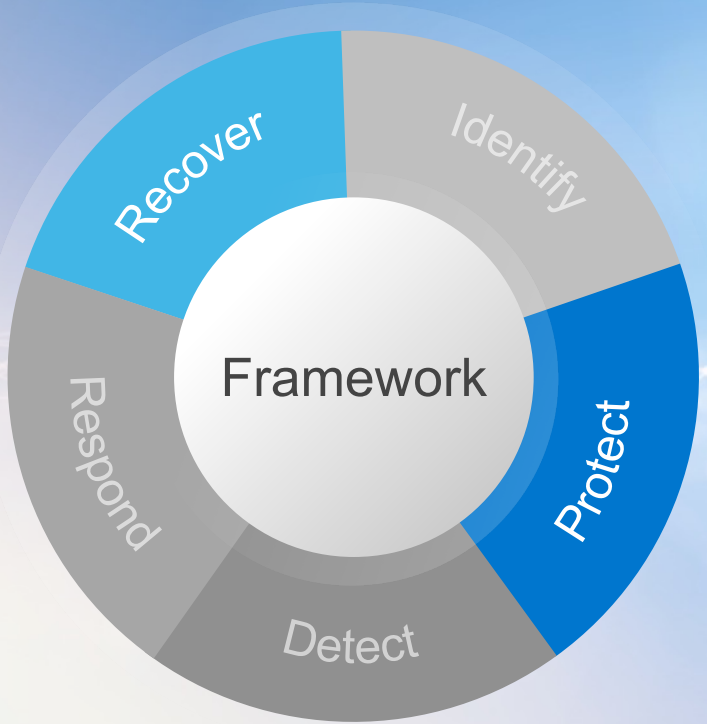
Cyber resilience is a strategy.

A high-level holistic strategy that includes cyber security standards, guidelines, people, business processes and technology solutions.

Example: NIST Cybersecurity Framework



Source: https://en.wikipedia.org/wiki/Cyber_resilience



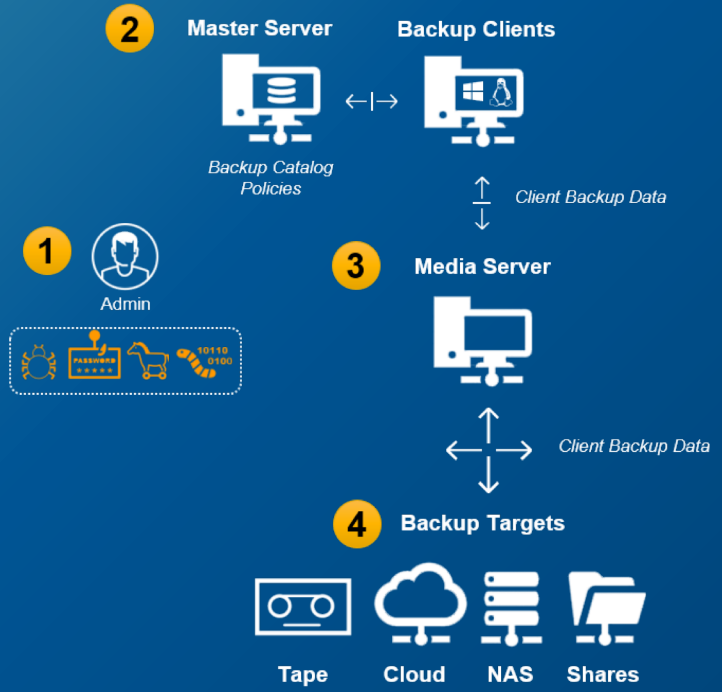
Cyber recovery is a solution.

A data protection solution that isolates business-critical data away from attack surfaces.

Critical data is stored immutably in a hardened vault enabling recovery with assured data availability, integrity and confidentiality.

Source: https://en.wikipedia.org/wiki/Cyber_resilience

Ransomware Increasingly Targeting Backups



1. **IT and Backup admins are main targets for compromise**

2. **Master Server (Backup Catalog):** Backup master server is targeted and infected resulting in encrypted/wiped backup catalog, or pre-mature policy expiration

3. **Media Server:** All mounted filesystems on the media server are targeted and encrypted/wiped

4. **Backup Targets:**

   Disk / NAS: Filesystems on the media server are targeted and encrypted/wiped. **Backup repositories can become encrypted/wiped** from ransomware crawling network file shares

   Tape: Provides a better chance to recover from the destructive event if threat was removed from the environment prior to attack. However, **if backup catalog is held hostage or destroyed, recovering from the tape will be increasingly difficult**

   Cloud: General-purpose or Public Cloud offer the advantage of remote protection but are inherently less secure due to reliance on internet (always on) or unsecure networks, leaving data, backups and catalogs exposed

What are the Experts Saying?

*"Maintaining current backups **offline** is critical because, if your network data is encrypted with ransomware, your organization can restore systems"* Anne Neuberger, Open letter to business leaders, June 2, 2021

*"Ensure backups are **not connected** to the networks they back up."*

Gartner

*"Create an **isolated recovery environment***

*"Maintain **offline**, encrypted backups"*
*"Gold images of **critical systems** + source code or executables"*

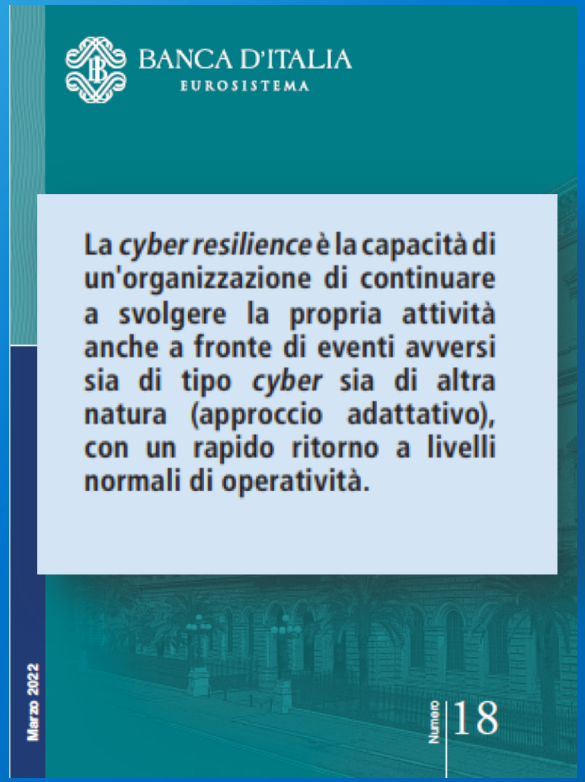
https://www.cisa.gov/publication/ransomware-guide

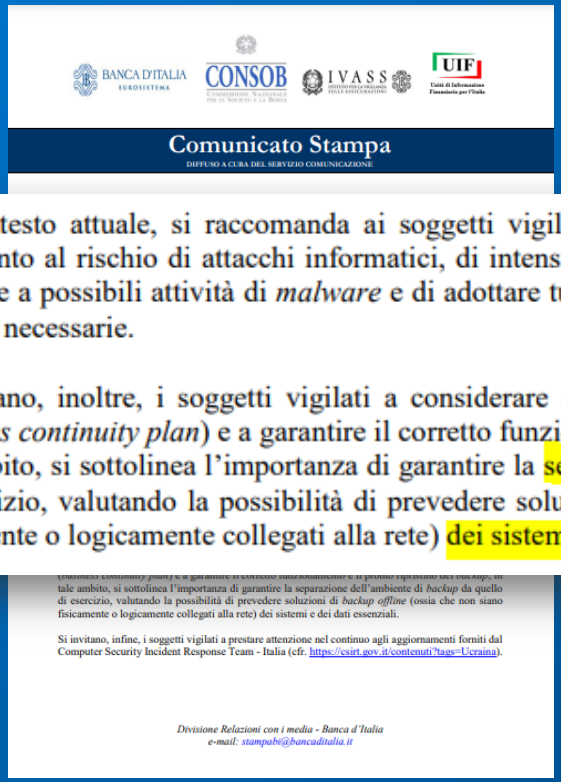
enisa

*3-2-1 rule. Keep 3 copies of any important files. Store those copies on **2 different storage** media to protect them against different risks. Have at least 1 off-site backup, **outside** of the SME core ICT environment"*

DELL Technologies

Local Institutions adopting similar recommendations





Disaster recovery is not cyber recovery

Disaster Recovery / Business Continuity is not enough to address modern cyber threats

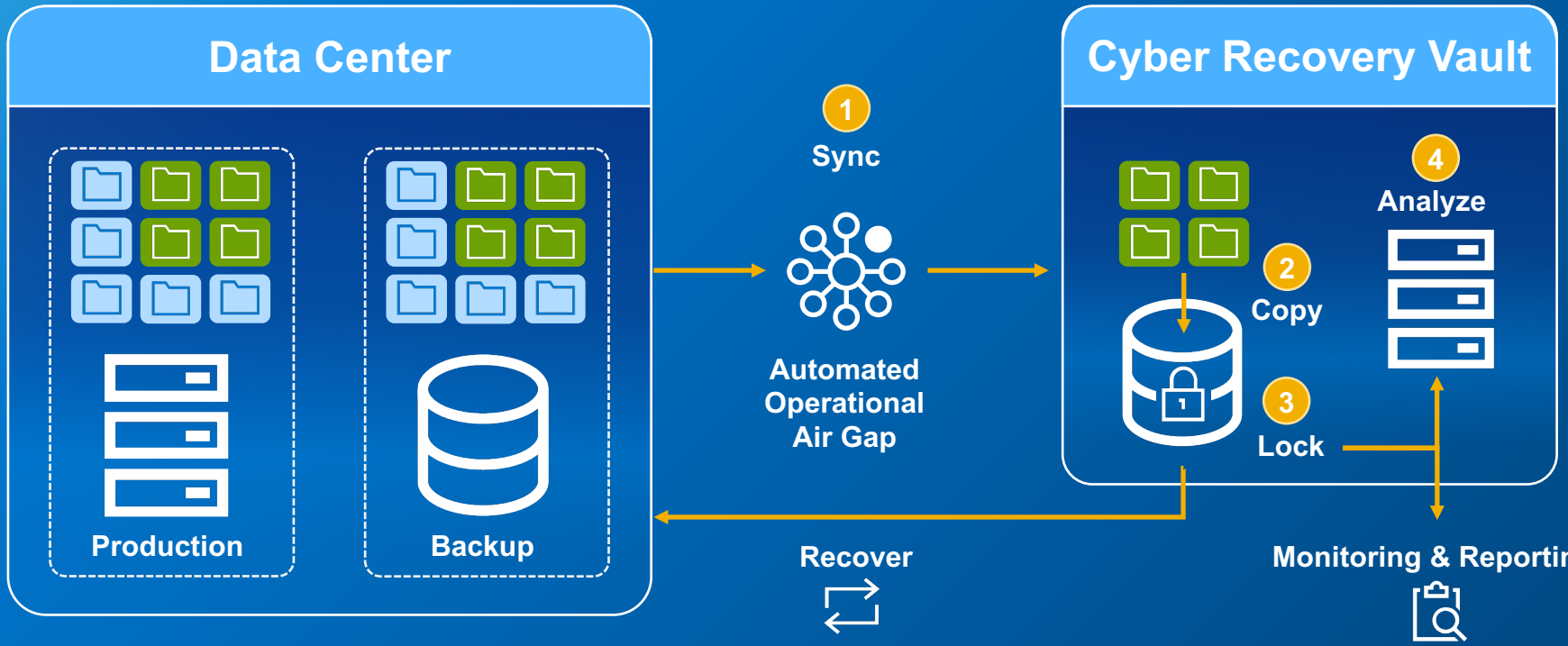
CATEGORY	DISASTER RECOVERY	CYBER RECOVERY
Recovery Time	Close to instant	Reliable & fast
Recovery Point	Ideally continuous	1 day average
Nature of Disaster	Flood, power outage, weather	Cyber attack, targeted
Impact of Disaster	Regional; typically contained	Global; spreads quickly
Topology	Connected, multiple targets	Isolated, in addition to DR
Data Volume	Comprehensive, all data	Selective, includes foundational services
Recovery	Standard DR (e.g., failback)	Iterative, selective recovery; part of CR

Cyber Recovery Requirements

Modern threats require modern solutions

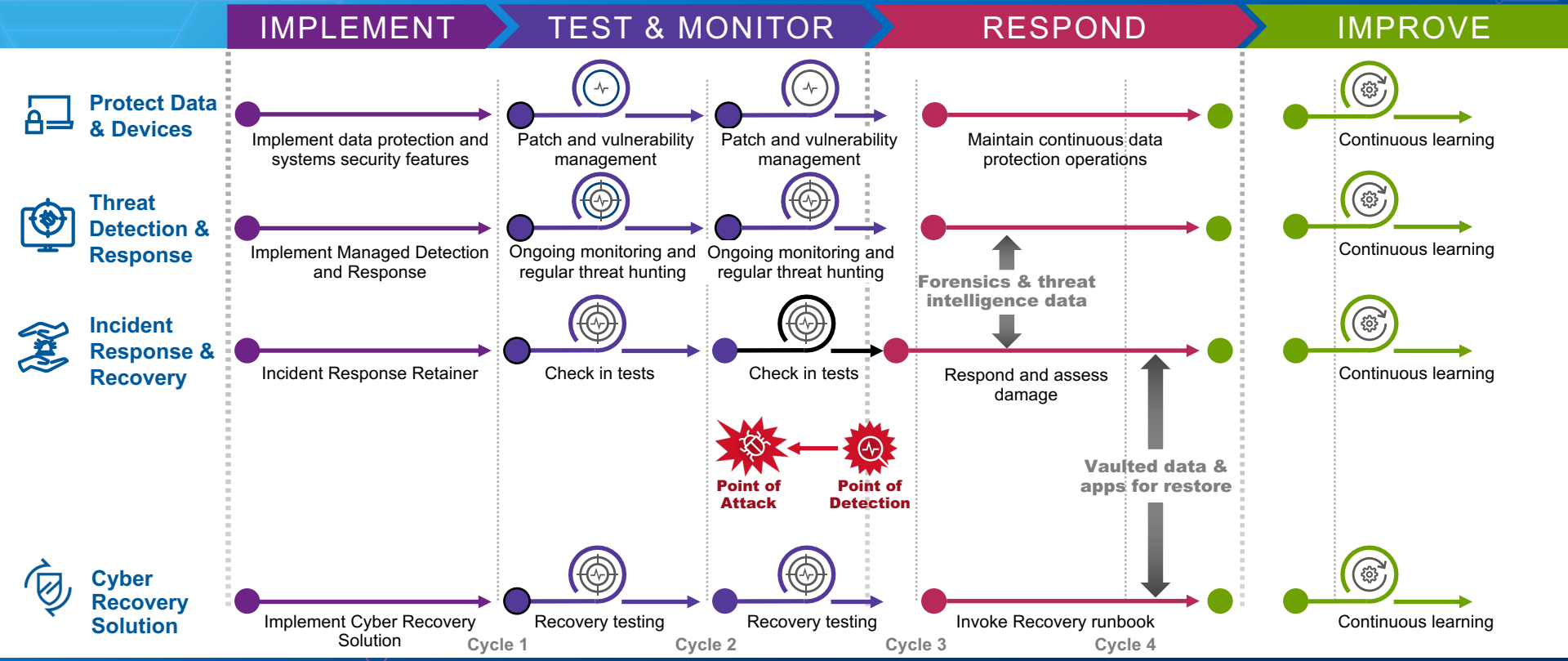
Implementing a Cyber Recovery Solution

Data Vaulting and Recovery Processes



Connecting protection, detection, response and recovery

Tie together key capabilities to reduce recovery and keep the business up and running



Next steps

Assess

Assess your current cyber resiliency to determine your readiness and program maturity.

Explore

Explore the breadth of advanced solutions, services and intrinsic security innovations from market Leaders.

Plan

Work with trusted security experts to build your strategy for enhancing cyber resiliency.

Implement

Modernize your security posture to help build your breakthrough with confidence.


DELL Technologies