L’importanza della protezione dei dati ai tempi del ransomware

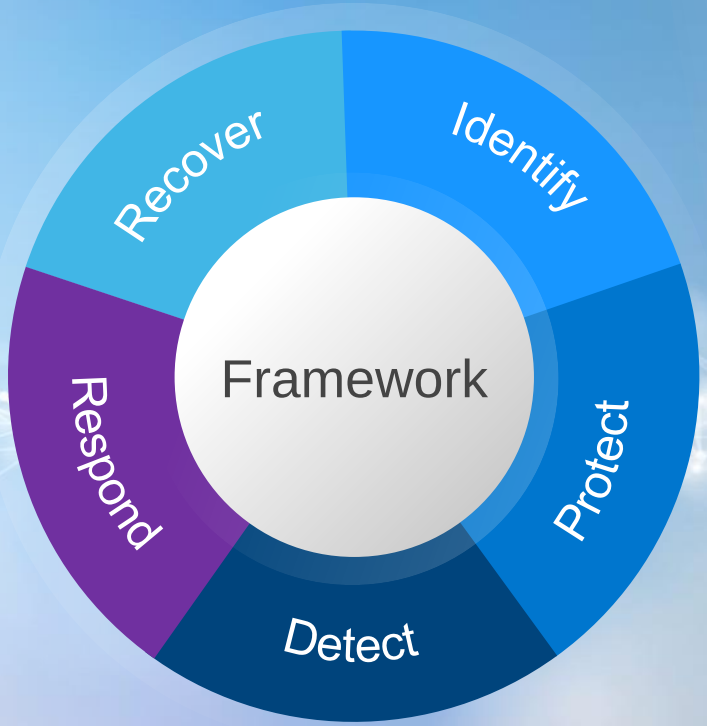
Fabio Zezza
DPS Sales Lead - Italy

DELL Technologies

Cyber resilience is a strategy.

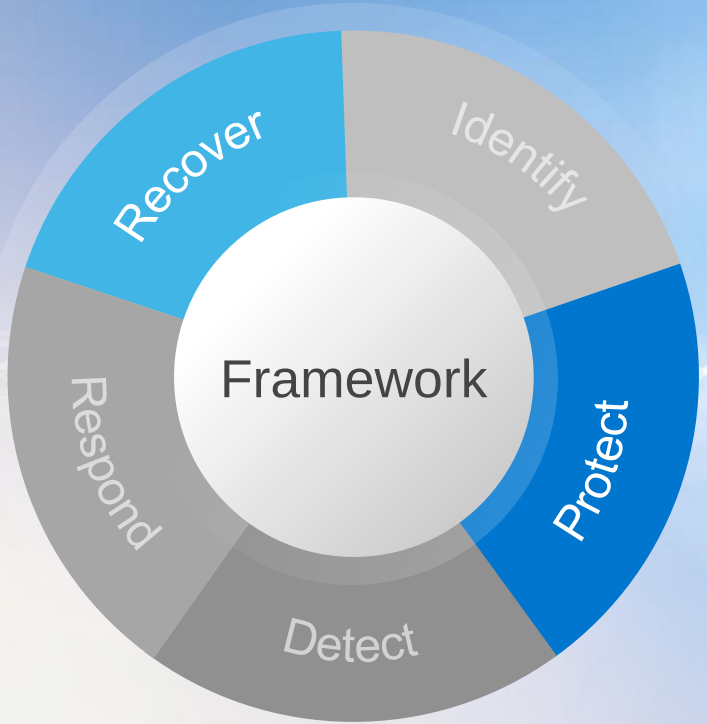
A high-level holistic strategy that includes cyber security standards, guidelines, people, business processes and technology solutions.

Example: NIST Cybersecurity Framework



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

© Copyright 2021 Dell Inc.



Cyber recovery is a solution.

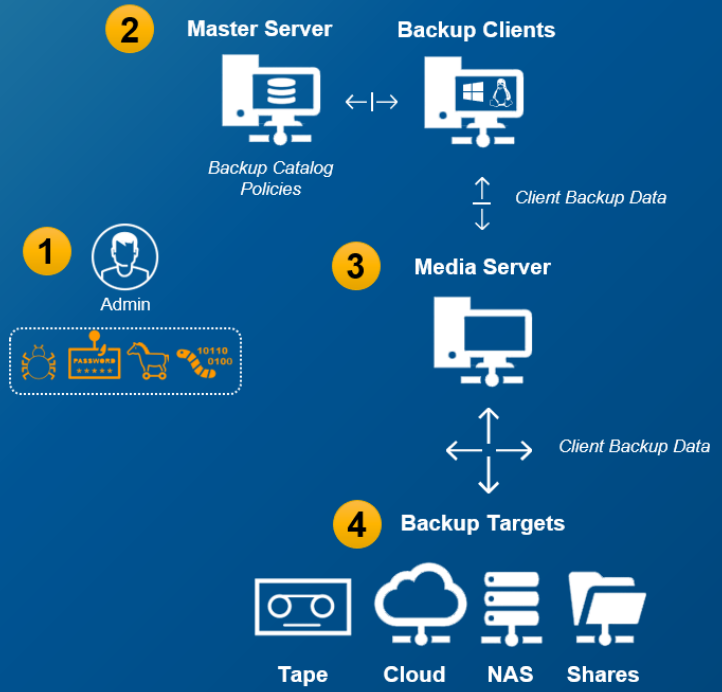
A data protection solution that isolates business-critical data away from attack surfaces.

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

© Copyright 2021 Dell Inc.

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:**

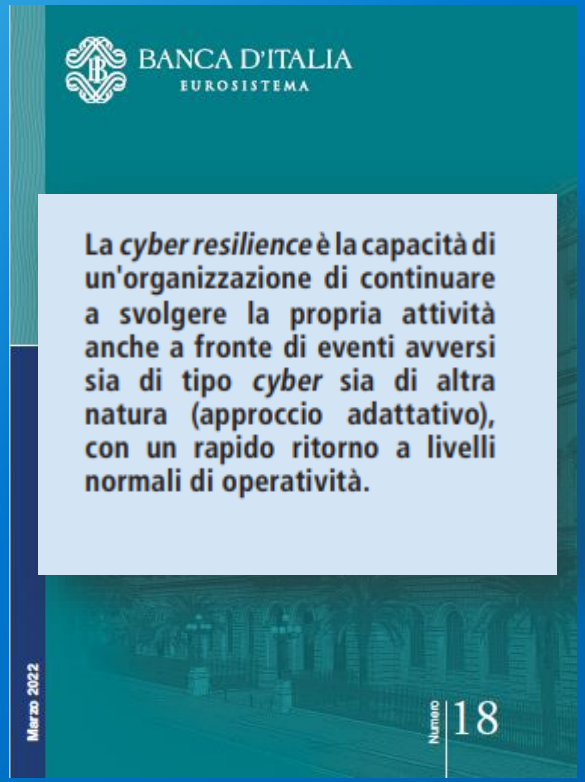
   Disk / NAS: Filesystems on the media server are targeted and encrypted/wiped. **Backup repositories can become encrypted/wiped** from ransomware crawling network file shares

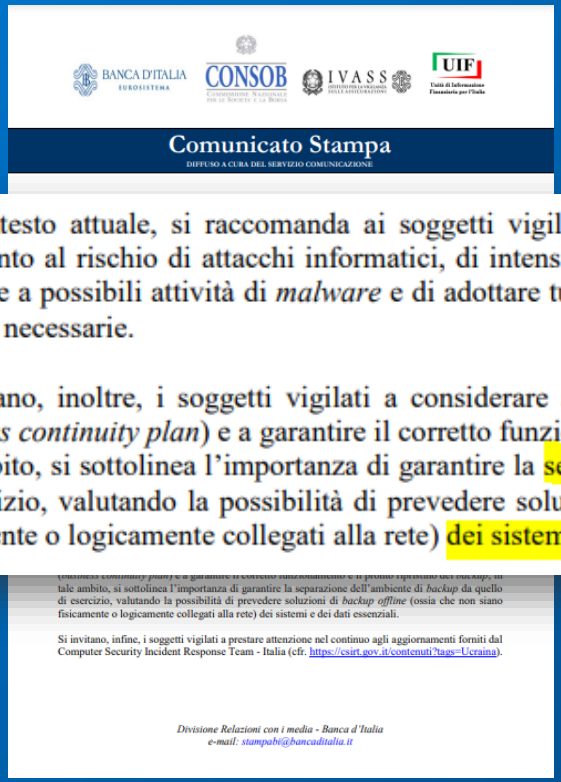
   Tape: Provides a better chance to recover from the destructive event if threat was removed from the environment prior to attack. However, **if backup catalog is held hostage or destroyed, recovering from the tape will be increasingly difficult**

   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

© Copyright 2021 Dell Inc.

Institutions are adopting similar recommendations





Nel contesto attuale, si raccomanda ai soggetti vigilati di esercitare la massima attenzione con riferimento al rischio di attacchi informatici, di intensificare le attività di monitoraggio e difesa in relazione a possibili attività di *malware* e di adottare tutte le misure di mitigazione dei rischi che si rendano necessarie.

Si invitano, inoltre, i soggetti vigilati a considerare attentamente i piani di continuità aziendale (*business continuity plan*) e a garantire il corretto funzionamento e il pronto ripristino dei *backup*; in tale ambito, si sottolinea l'importanza di garantire la separazione dell'ambiente di *backup* da quello di esercizio, valutando la possibilità di prevedere soluzioni di *backup offline* (ossia che non siano fisicamente o logicamente collegati alla rete) dei sistemi e dei dati essenziali.

© Copyright 2021 Dell Inc.

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

© Copyright 2021 Dell Inc.

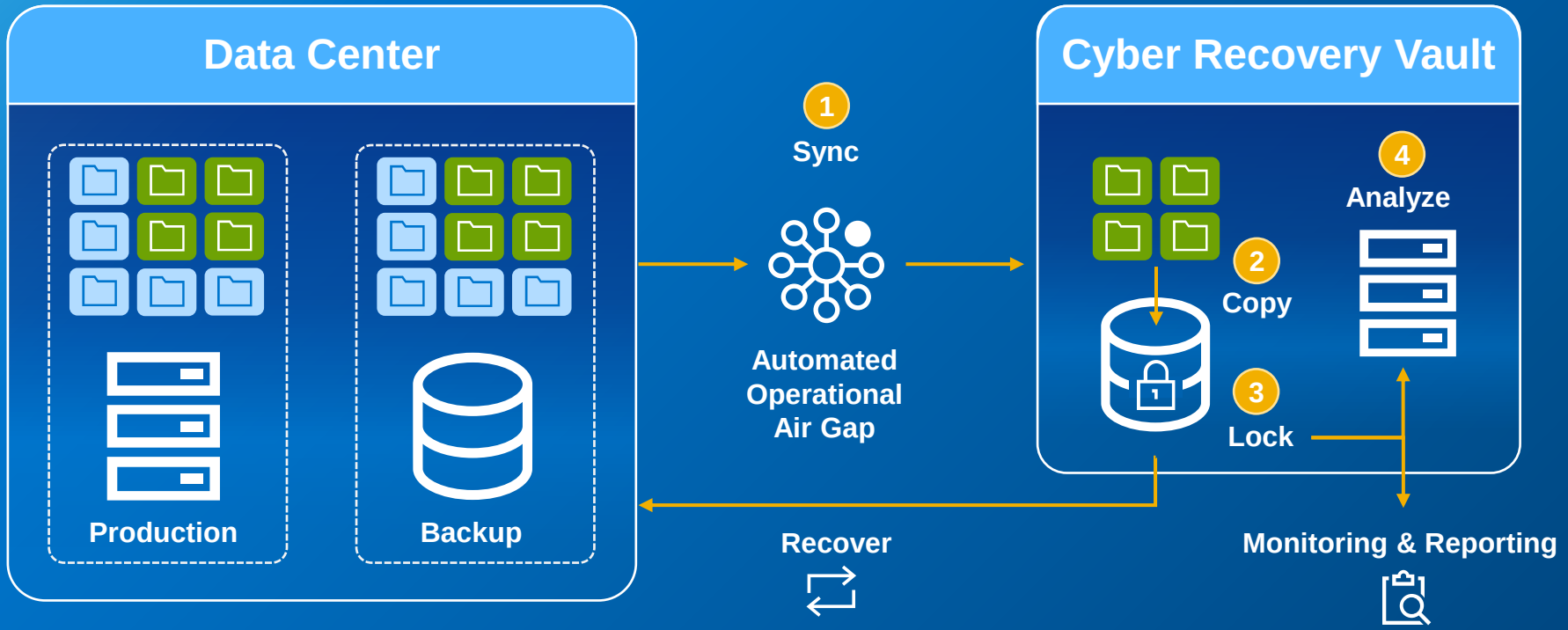
Cyber Recovery Requirements

Modern threats require modern solutions

© Copyright 2021 Dell Inc.

Implementing a Cyber Recovery Solution

Data Vaulting and Recovery Processes



© Copyright 2021 Dell Inc.


DELL Technologies