Recovering Your Organization After a Ransomware Attack

PowerProtect Cyber Recovery

Yiannis Psichas
DPS Advisory SE
yiannis.psichas@dell.com

DELL Technologies

Cyber threats 2021: the facts

Every 11 seconds

A cyber or ransomware attacks occur[1]

$6T

Total global impact of cyber crime in 2021[2]

$13M

Average cost of cybercrime for an organization[3]

Banking	$18.4M
Utilities	$17.8M
Software	$16.0M
Automotive	$15.8M
Insurance	$15.8M
High Tech	$14.7M
Capital Markets	$13.9M
Energy	$13.8M
US Federal	$13.7M
Consumer Goods	$11.9M
Health	$11.9M
Retail	$11.4M
Life Sciences	$10.9M
Media	$9.2M
Travel	$8.2M
Public Sector	$7.9M

*[1]Cybersecurity Ventures: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021 https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021

[2]Cybersecurity Ventures: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021

[3]Accenture Insights, Ninth Annual Cost of Cyber crime Study March , 2019 - https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

DELL Technologies

Threat vectors are increasing

* By cartoonist John Klossner – May 2016

156 million phishing emails sent W
every day

16 million make it through filters

8 million are opened

800,000 LINKs are click'd

IF 12% click on phishing emails

All it takes is **ONE**

Cyber Events are Increasing

Both in frequency & sophistication

Microsoft Exchange

Exchange

According to Volexity, attacks using the four zero-days may have started as early as January 6, 2021. Dubex reported suspicious activity on servers in the same month.

https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/

Solarwinds

solarwinds
The Power to Manage IT

In March 2020, nation-state hackers, compromised a DLL file linked to software update for the Orion platform by SolarWinds.

https://www.upguard.com/blog/biggest-data-breaches

Kaseya

Kaseya Automating IT

In this latest incident the hackers showed that by going after the software supplier of multiple organizations they can pop dozens, perhaps hundreds of victims in one go.

https://www.bbc.com/news/world-us-canada-57202826

Ransomware

…big-game hunting ransomware families (are) continuing to refine and change their tactics, techniques and procedures to become more evasive and nation state-like in sophistication

https://www.infosecurity-magazine.com/news/ransomware-legacy-malware-2021/

Worldwide Guidance

One common theme sticks out

Gartner	THE WHITE HOUSE	Hong Kong Monetary Authority	SingCERT Singapore Computer Emergency Response Team
"Create an **isolated recovery environment**:."	"Ensure that backups are **not connected to the business network**"	"Secure tertiary data backup should be **disconnected** … [to] withstand targeted cyber attacks … or … malicious insiders."	"It is important that the backup data is stored **offline** and not connected to your network."
CISA Cybersecurity & Infrastructure Security Agency	SHELTERED HARBOR	Department of Justice Federal Bureau of Investigation	ACSC Australian Cyber Security Centre
"It is critical to maintain **offline**, encrypted backups of data"	"Data Vault requirement: '**Air gapped**'"	"Ensure backups are **not connected** to the networks they back up."	"Daily backups of important data, software and settings, **stored disconnected**…."

enisa

Have a good and verified backup of all your business-critical files and personal data and keep it updated, and isolated from the network (July 2022)

DELL Technologies

Cyber Resilience is a Strategy

Cyber Recovery is a Solution

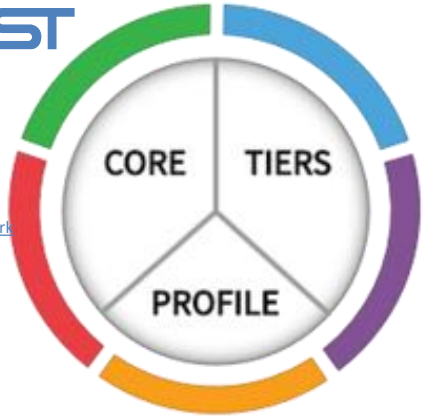
"Resilience" means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. This includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

Cyber Resilience is a **STRATEGY** that incorporates people, process and technology into a holistic framework that protects an entire business, organization or entity.

https://www.nist.gov/cyberframework/framework

NIST

https://www.nist.gov/cyberframework/new-framework



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

https://www.gartner.com/doc/reprints?id=1-28YE33CH&ct=220131&st=sb%20%5bgartner.com%5d

Disaster Recovery Is Not Cyber Recovery

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

Category	Disaster Recovery	Cyber Resilience
Probability	Low	High
Data to Recovery	Impact known	Impact unknown
Recovery Point	Typically known	Typically unknown
Recovery Time	Close to instant	Trusted, verified, reliable & fast
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

3 I's of Cyber Recovery

Modern threats require modern solutions

Isolation

Physical & logical separation of data

PowerProtect Cyber Recovery vault is protected with operational air gap either on-premises or in cloud and multi-cloud offers

Immutability

Preserve original integrity of data

Multiple layers of security and controls protect against destruction, deletion and alteration of vaulted data

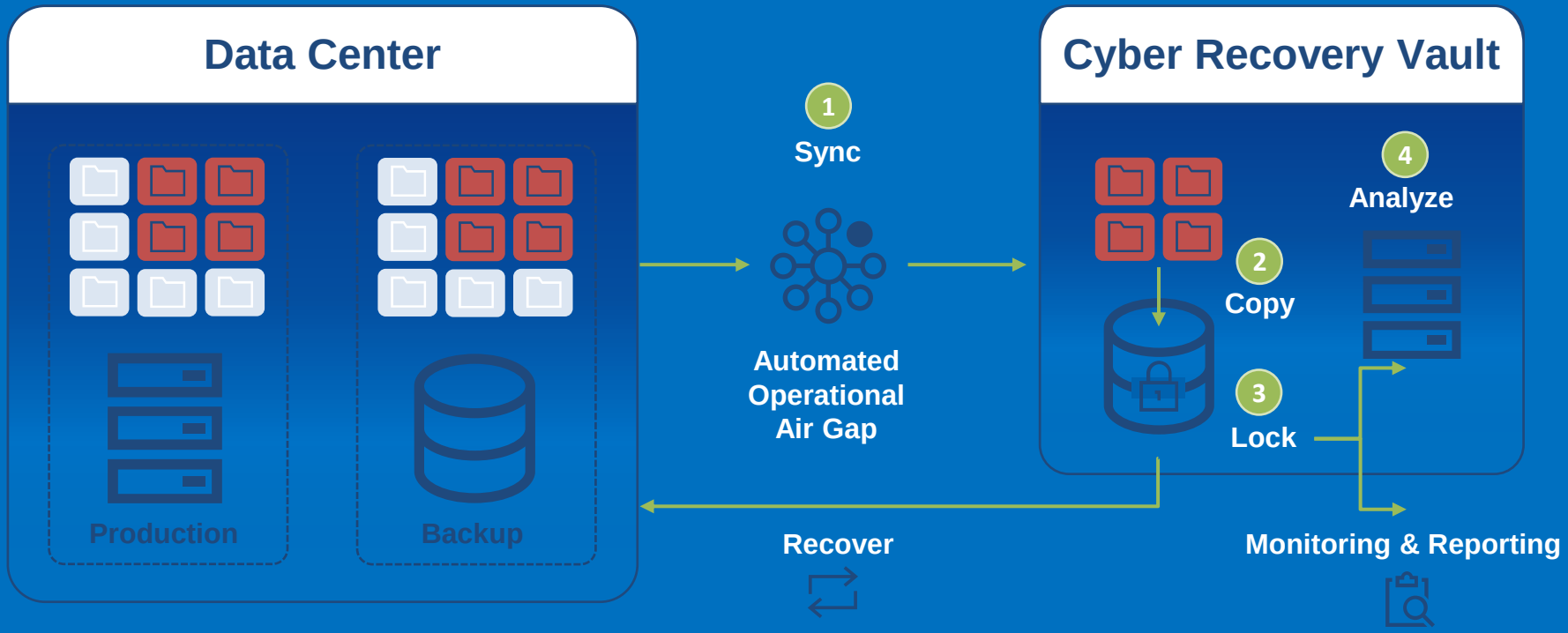
Intelligence

ML & analytics identify threats

CyberSense enables assured recovery of good data and offers insight into attack vectors from within the Cyber Recovery vault

PowerProtect Cyber Recovery

Data Vaulting and Recovery Processes



DELL Technologies

Cyber Recovery Solution Differentiators

- Retention-locked copies of backup data & catalog
- Separate security officer credentials

- IT or Backup admins can't access, override security credentials, or retention policies in the vault
- Architecture supports multi-vendor backup software

- Network isolation & removal from management network
- Advanced HW NTP Clock Tampering
- Meets stringent Sheltered Harbor vault requirements
- Full file content analytics & machine learning trained for attack vectors to identify possible compromise
- In-vault intelligence tools to accelerate recovery of "clean" copies

Sheltered Harbor Data Vaulting

Data Vault Requirements

- ✓ *"Unchangeable"*
- ✓ *"Separated"*
- ✓ *"Survivable"*
- ✓ *"Accessible"*
- ✓ *"Decentralized"*
- ✓ *"Owned & managed by institution or service provider"*

PowerProtect Cyber Recovery

is the only turnkey data vaulting solution endorsed by Sheltered Harbor

DELL Technologies

DELL Technologies

Cyber recovery & data protection leadership

2015	First “Isolated” recovery solution with custom deployment
2018	Introduced PowerProtect Cyber Recovery solution
2019	First technology vendor in Sheltered Harbor Alliance Partner Program
2020	First Endorsed Sheltered Harbor Solution – PowerProtect Cyber Recovery
2021	Introduced PowerProtect Cyber Recovery for Multi-Cloud & AWS
2022	Introduced PowerProtect Cyber Recovery for Azure

2000+ **Cyber Recovery Customers**

#1

Data Protection Appliances & Software*

[1] Based on combined revenue from the IDC 3Q20 Purpose-Built Backup Appliance (PBBA) Tracker, with select Storage Software segments from the 3Q20 Storage Software and Cloud Services Qview.
[2] IDC 3Q20 Storage Software and Cloud Services Qview

DELL Technologies


DELL Technologies

Dell Data Protection Portfolio Ecosystem