COMMVAULT® | Be ready™

The Implications of Ransomware on Data Governance

And the business integrity gap

Nigel Tozer, Director WW GSI Marketing

3rd June 2021

Today's Session

Ransomware & Data Governance

We'll be looking at:

- Preparing your backup & Business Continuance/Disaster Recovery (BCDR) systems for cyber recovery

- The role of data governance in reducing your attack surface

- Why data visibility is a critical factor in preventing & dealing with a data breach

COMMVAULT

Preparing Your Backup, BCDR & Cyber Recovery

- Ransomware outages can be unlike any other kind of outage

- Core systems can be lost: Active Directory, DNS, comms, etc. (oh, and you might not be able to recover to your own DC)

- Cloud disaster recovery should be very strongly considered

COMMVAULT®
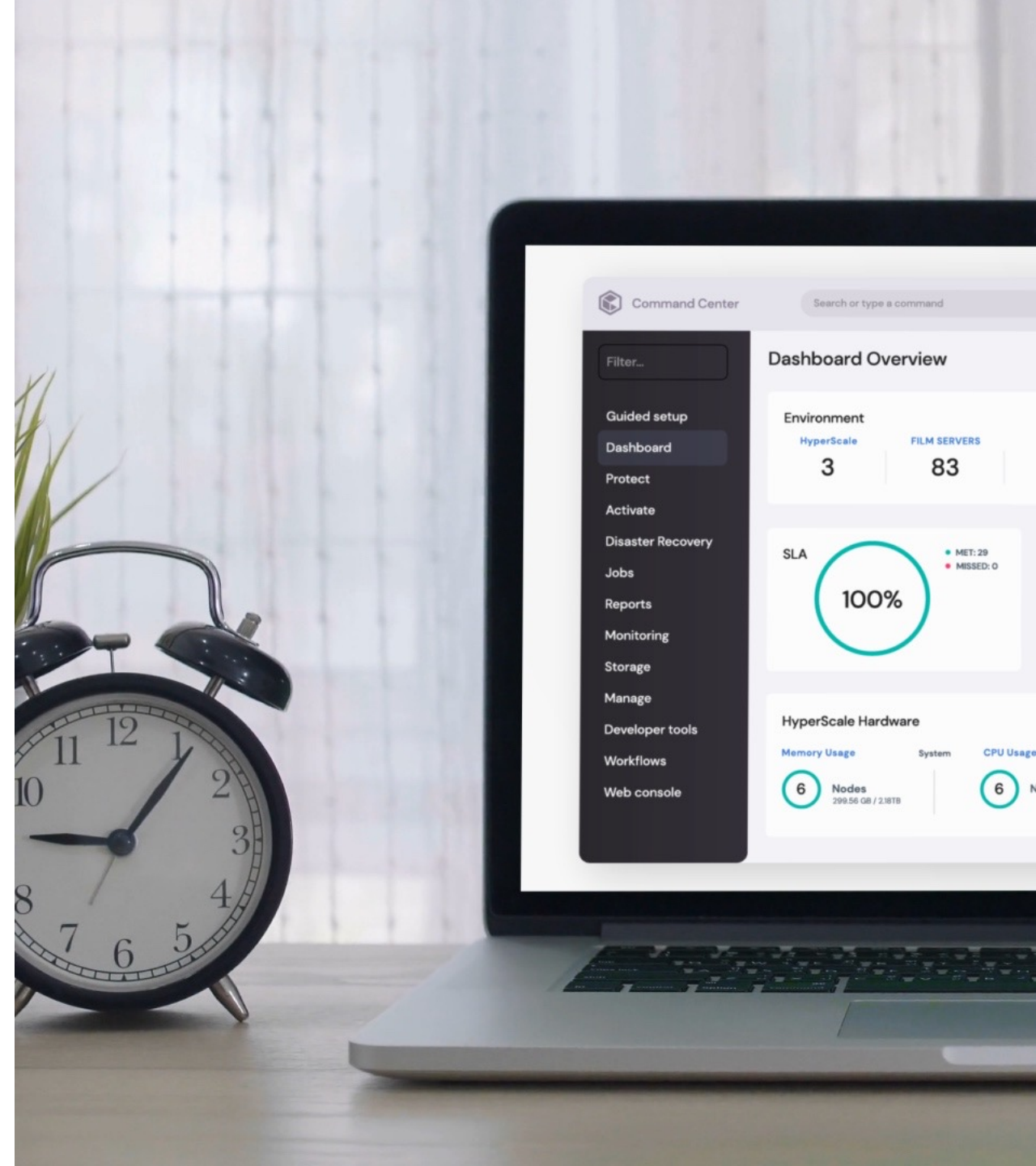
Backup: it's not BC or DR

But it could be your cyber recovery command centre

- Achieve/maintain ISO27001/2 & SOC-2 standards
- Harden recovery systems (to NIST & CIS Benchmarks)
- Apply a Zero Trust, AAA security model, end-to-end
- Use FIPS 149-2 Certified encryption (inc. for networks)
- AI powered ransomware detection & automation
- Use multiple immutable storage targets & air-gapped cloud storage
- Leverage the Security Assessment Dashboard

COMMVAULT

Recovery Processes

Careful planning is required

- Disaster Recovery Planning: it's a scheduled process, not a timeline!

- It can feel like a war – with the first casualty being the actual recovery plan

- You're up against: conflicting priorities, dependencies, malware scans before recovery, IT staff fatigue, supplier logistics, vendor support… and much more

COMMVAULT®

Data Governance: is it Hurting Your Cyber Resilience?

Data visibility

40%-80%

of files in a typical enterprise are redundant, outdated or trivial (ROT), or do not have an assigned owner in the directory service[1]

Automation & governance

55%

of a typical organization's data is "dark" – ungoverned, unquantified and untapped[2]

Attack surface

Over 54%

of organisations have experienced a significant cyber-attack in the past year[3]

COMMVAULT®

1: https://www.enterprisetimes.co.uk/2020/02/11/three-ways-to-build-a-data-driven-culture-in-your-organisation/
2: Splunk – The State of Dark Data, 2019
3: IBM - https://www.ibm.com/security/data-breach

Data Visibility

It's critically important before & after a breach

- If you don't have data visibility, you don't know what your actual exposure is – or was

- Having a global index & entity profile will help you meet the 72hr breach notification deadline

- There's a business benefit of a data index/entity profile: data access and increased data quality for AI & analytics projects

COMMVAULT®

Next steps

Additional resources

- Find out more about ransomware protection at commvault.com/ransomware

- Learn more about Commvault File Storage Optimisation, Data Governance and eDiscovery & Compliance at commvault.com/activate

- If you want a fast follow-up, please get in touch with the host and we can arrange a round table

Follow us on social media

Contact Info

And Social

Paul Hammond, insurance vertical lead:

phammond@Commvault.com

General information:

Commvault_team@Commvault.com

Social:

https://twitter.com/Commvault

https://www.linkedin.com/company/commvault/mycompany/

COMMVAULT®