PROACT COMMVAULT

NIS2 and DORA - Cyber Recovery

“By Failing to prepare, you are preparing to fail” – B. Franklin

“Proper preparation and planning prevents poor performance” – British Army

Proact.co.uk/security

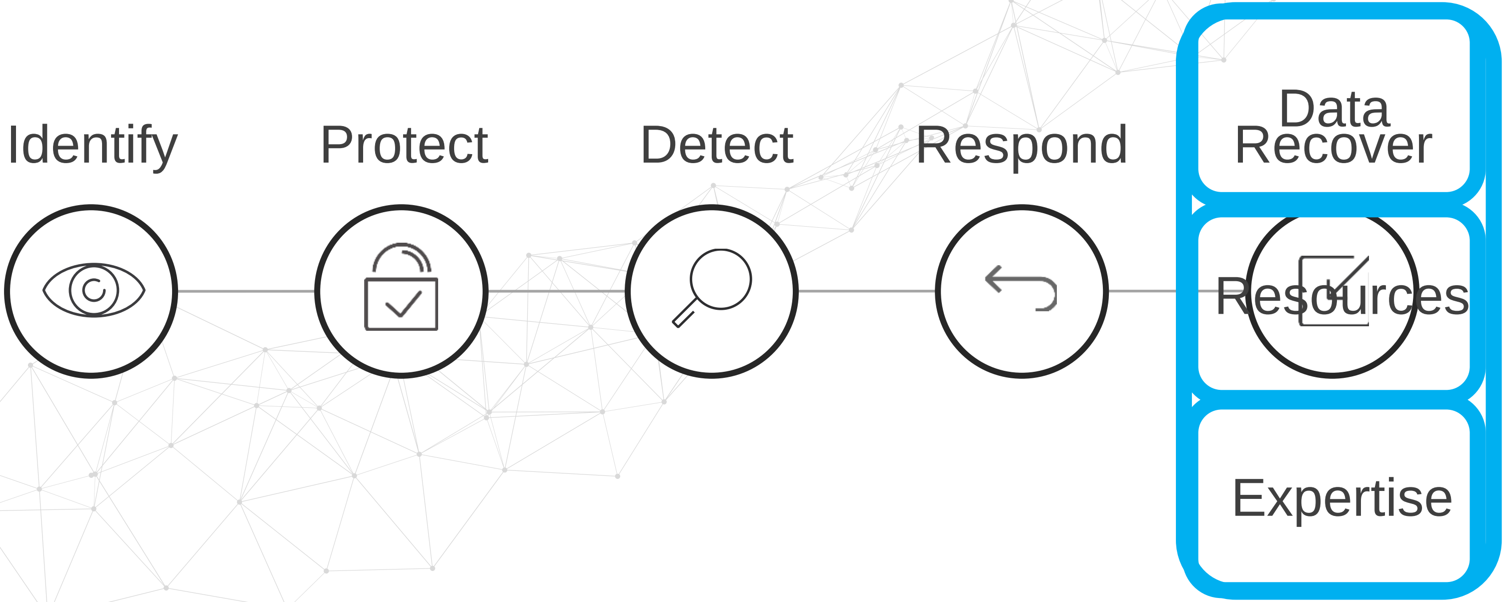
Shane Wallace

Managed Service Architect
(DRaaS & Cyber Recovery)

PROACT

COMMVAULT

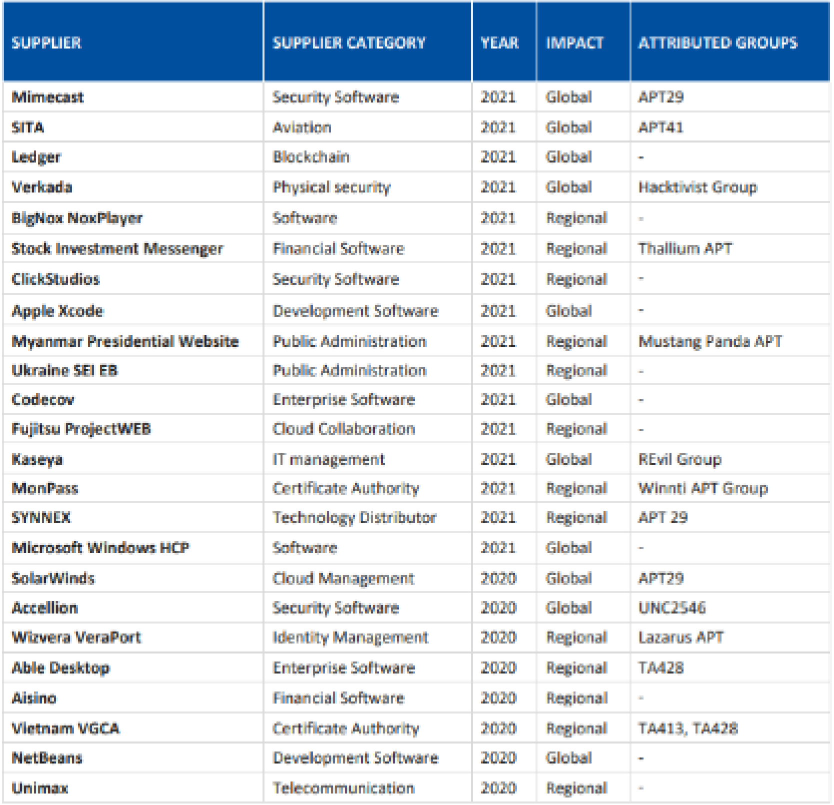
NIST Cyber Security Framework



PROACT

COMMVAULT

Nation State Attack’s 2021



SUPPLIER	SUPPLIER CATEGORY	YEAR	IMPACT	ATTRIBUTED GROUPS
Mimecast	Security Software	2021	Global	APT29
SITA	Aviation	2021	Global	APT41
Ledger	Blockchain	2021	Global	-
Verkada	Physical security	2021	Global	Hacktivist Group
BigNox NoxPlayer	Software	2021	Regional	-
Stock Investment Messenger	Financial Software	2021	Regional	Thallium APT
ClickStudios	Security Software	2021	Regional	-
Apple Xcode	Development Software	2021	Global	-
Myanmar Presidential Website	Public Administration	2021	Regional	Mustang Panda APT
Ukraine SEI EB	Public Administration	2021	Regional	-
Codecov	Enterprise Software	2021	Global	-
Fujitsu ProjectWEB	Cloud Collaboration	2021	Regional	-
Kaseya	IT management	2021	Global	REvil Group
MonPass	Certificate Authority	2021	Regional	Winnti APT Group
SYNNEX	Technology Distributor	2021	Regional	APT 29
Microsoft Windows HCP	Software	2021	Global	-
SolarWinds	Cloud Management	2020	Global	APT29
Accellion	Security Software	2020	Global	UNC2546
Wizvera VeraPort	Identity Management	2020	Regional	Lazarus APT
Able Desktop	Enterprise Software	2020	Regional	TA428
Aisino	Financial Software	2020	Regional	-
Vietnam VGCA	Certificate Authority	2020	Regional	TA413, TA428
NetBeans	Development Software	2020	Global	-
Unimax	Telecommunication	2020	Regional	-

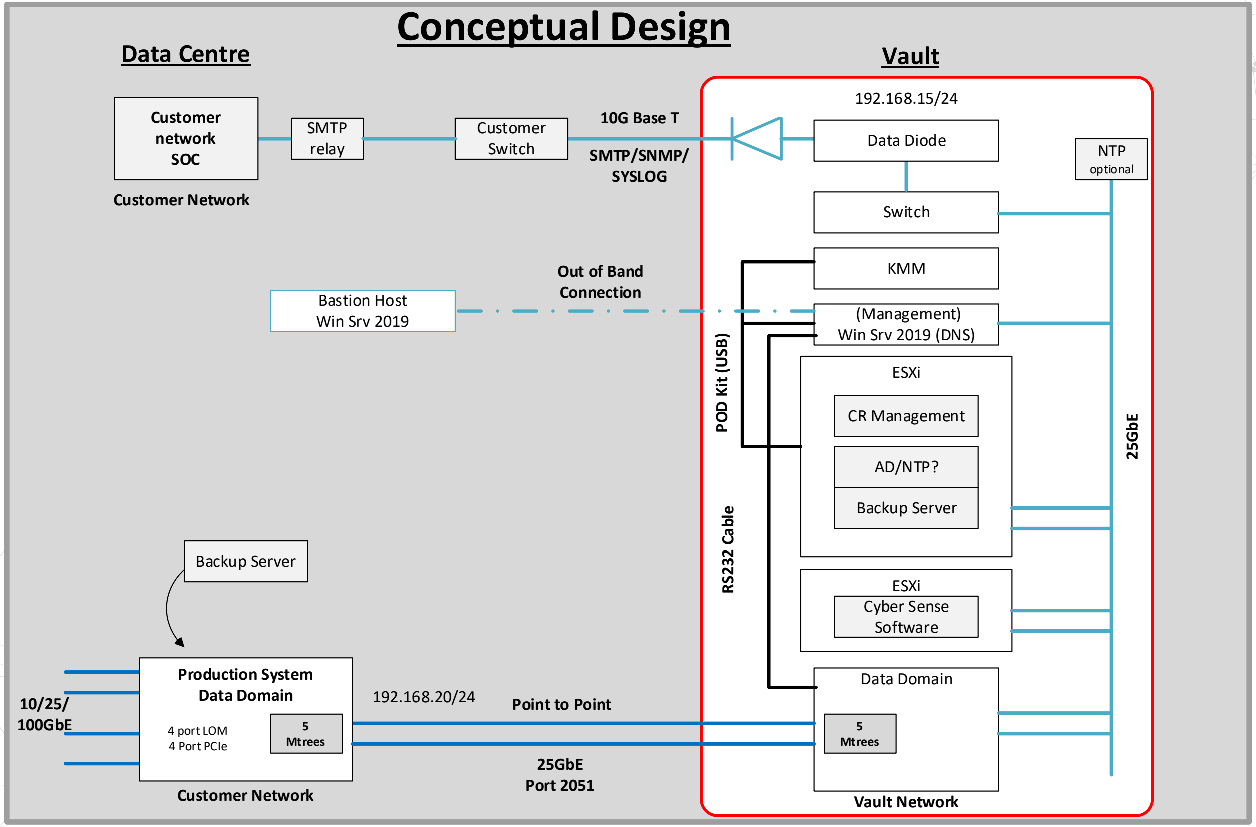
enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS

JULY 2021

Conceptual design of a Vault



Features

- At least 2 x Data Domains required
- Preferably in the same Data Centre

- Separate cabinet
- No Shared infrastructure
- No external Media allowed in the vault.
- All Management internal to the vault.

- Smallest attack surface
- Backup Software agnostic
- Safe area for restore testing
- Analytics internal to vault

Regulations and future guidance

USA

- Cyber Incident Reporting for Critical Infrastructure (CIRCIA)

European Union

- Network and Information systems 2.0 (NIS)
- Digital operations Resiliency ACT (DORA)
- Cyber Resiliency ACT

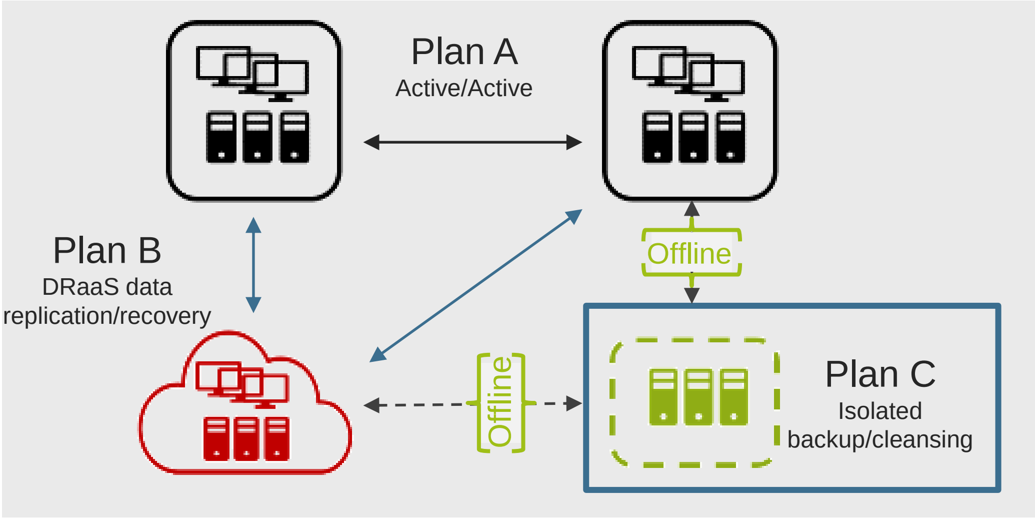
United Kingdom

- National Cyber Strategy 2022
- Financial Services and Markets Bill 2022

Requirements from the Industry

1. Supply Chain Inspection
2. Separation of Duty
3. Run Book Creation
4. Data Isolation (offline)
5. Rapid Recovery in the event of a Cyber Attack
6. Auditability
7. Ability to Test Recoveries / Recover back quickly

When plan A and plan B fail ?



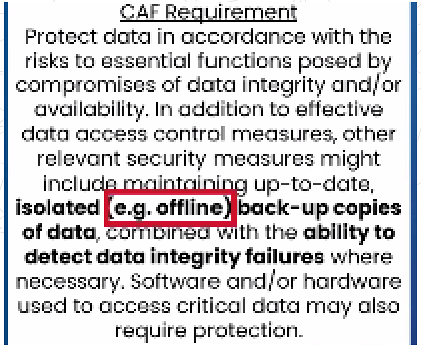
Ransomware and other Cyberattacks can remain undetected on average **up to 99 days**, raising the threat of having **no 'clean' back-up available**

- Plan A and Plan B are infected and unusable
- Retention? No clean data and cannot recover
- Recovery Solution needs to be disconnected from network / Offline network
- Finding an isolated environment to recover clean data / cleanse the data (Clean Room)

UK Guidelines

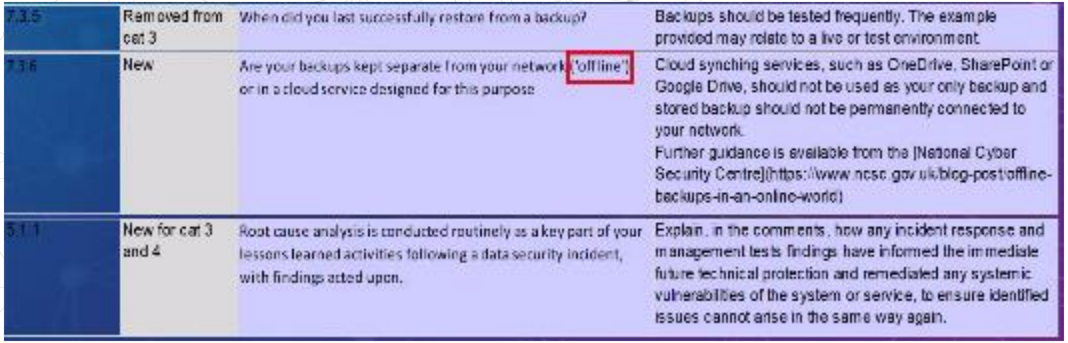
- NCSC – National Cyber Security Centre
- Cyber Essentials Framework – Data Security Protection Toolkit
- Cyber Assessment Framework
- HSE Report Recommendations page 13:

“**Offline Backups** (or backups that are verified as inaccessible to attackers with full control of Production IT)”

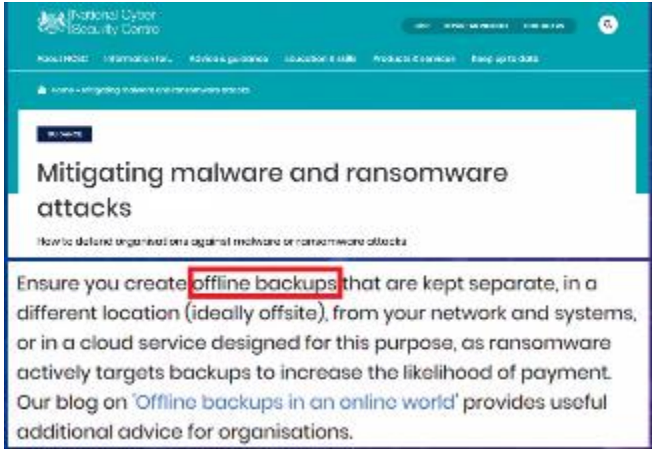


CAF Requirement

Protect data in accordance with the risks to essential functions posed by compromises of data integrity and/or availability. In addition to effective data access control measures, other relevant security measures might include maintaining up-to-date, **isolated (e.g. offline) back-up copies of data**, combined with the **ability to detect data integrity failures** where necessary. Software and/or hardware used to access critical data may also require protection.



7.3.5	Removed from cat 3	When did you last successfully restore from a backup?	Backups should be tested frequently. The example provided may relate to a live or test environment.
7.3.6	New	Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose	Cloud synching services, such as OneDrive, SharePoint or Google Drive, should not be used as your only backup and stored backup should not be permanently connected to your network. Further guidance is available from the [National Cyber Security Centre](https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world)
5.1.1	New for cat 3 and 4	Root cause analysis is conducted routinely as a key part of your lessons learned activities following a data security incident, with findings acted upon.	Explain, in the comments, how any incident response and management tests findings have informed the immediate future technical protection and remediated any systemic vulnerabilities of the system or service, to ensure identified issues cannot arise in the same way again.



Mitigating malware and ransomware attacks

How to defend organisations against malware or ransomware attacks

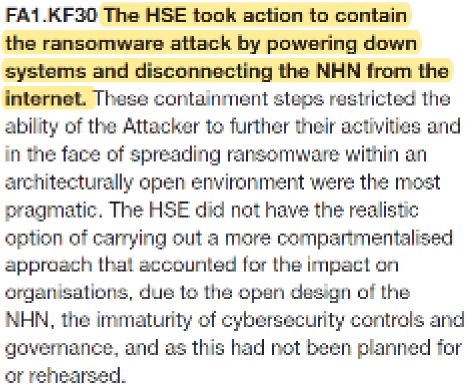
Ensure you create offline backups that are kept separate, in a different location (ideally offsite), from your network and systems, or in a cloud service designed for this purpose, as ransomware actively targets backups to increase the likelihood of payment. Our blog on 'Offline backups in an online world' provides useful additional advice for organisations.

HSE: Response to Cyber Attack

Conti cyber attack on the HSE

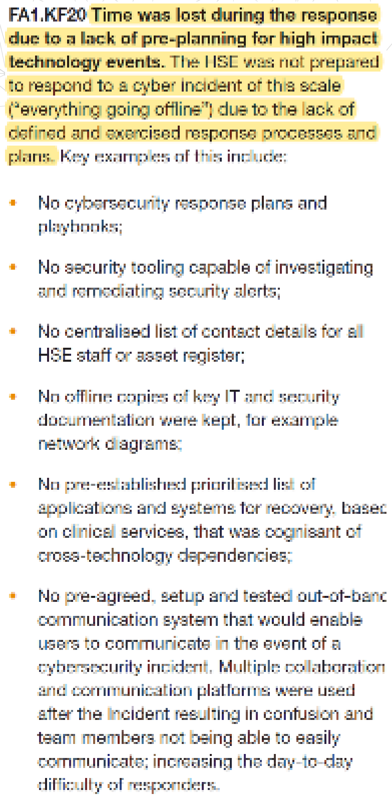
Independent Post Incident Review

Organisations’ IT disaster recovery plans should be based on a prioritised list of applications and systems to recover, should the technology base of the organisation have to be rebuilt or recovered, informed by an up-to-date asset register and mapping of critical operations to technology. Offline backups (or backups that are verified as inaccessible to attackers with full control of production IT) must be available for all critical systems, data and infrastructure, including core IT infrastructure such as Active Directory (“AD”), with a well-defined and tested restore procedure that includes verification of ability to recover all systems to a common point-in-time.



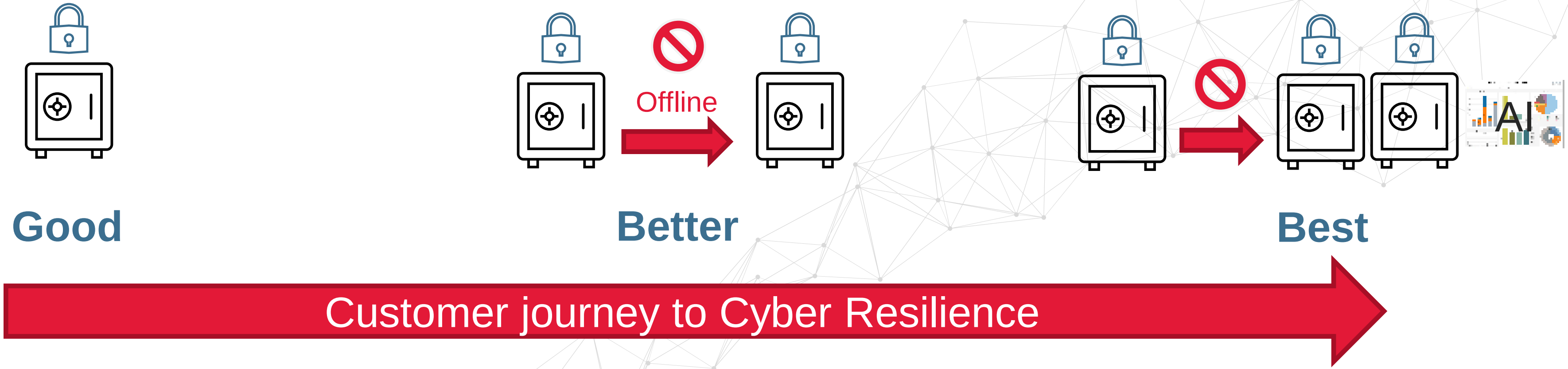
FA1.KF30 **The HSE took action to contain the ransomware attack by powering down systems and disconnecting the NHN from the internet.** These containment steps restricted the ability of the Attacker to further their activities and in the face of spreading ransomware within an architecturally open environment were the most pragmatic. The HSE did not have the realistic option of carrying out a more compartmentalised approach that accounted for the impact on organisations, due to the open design of the NHN, the immaturity of cybersecurity controls and governance, and as this had not been planned for or rehearsed.

The HSE took action to contain the ransomware attack by powering down systems and disconnecting the NHN from the internet.



FA1.KF20 **Time was lost during the response due to a lack of pre-planning for high impact technology events.** The HSE was not prepared to respond to a cyber incident of this scale (“everything going offline”) due to the lack of defined and exercised response processes and plans. Key examples of this include:

- No cybersecurity response plans and playbooks;
- No security tooling capable of investigating and remediating security alerts;
- No centralised list of contact details for all HSE staff or asset register;
- No offline copies of key IT and security documentation were kept, for example network diagrams;
- No pre-established prioritised list of applications and systems for recovery, basec on clinical services, that was cognisant of cross-technology dependencies;
- No pre-agreed, setup and tested out-of-banc communication system that would enable users to communicate in the event of a cybersecurity incident. Multiple collaboration and communication platforms were used after the Incident resulting in confusion and team members not being able to easily communicate; increasing the day-to-day difficulty of responders.



Offline

Good

Better

Best

Customer journey to Cyber Resilience

Lower Cost increased risk

- Retention – Locked copies of backup data
- Separate security credentials
- Worm / Immutable
- Elevated and reviewed security credentials

Less risk but longer recovery

- IT Admins can't access, override security credentials or retention policy's
- Supports multi vendor backup software
- Data is isolated from production
- Protection from internal threats
- Multi backup vendor support

Higher costs shorter recovery

- Offline Technology
- Full content Analytics and machine learning
- In-Vault recovery and clean room
- Vaulted and Offline
- Full depth Analytics
- Enhanced recovery tools and capabilities

PROACT

COMMVAULT

	Step 1	Step 2	Step 3	Step 4	Step 5
Cyber Impact	Contain the Breach	Incident Response	Identify type of attack	Assess and plan	Repair and Recover
Average downtime from a cyber attack is **21 days**	Disconnect: • **Internet** • **LAN** Re-route traffic Change Passwords	Activate the Incident Response Unit.	Sophos estimate there are 650,000 new variants, 75% are seen only once. There will be multiple variants of Malware in the environment and various tools used to deliver the attack	**Environment is treated like a crime scene.** Estimate the blast radius. Assess recovery Options Estimate options for Quickest Time to Recovery Assess backups quality. Plan Recovery	Obtain resources (servers, switches, storage) to execute plan. Execute

Recovery of Critical Materials Measured in Days

Recovery

Proact Cyber Recovery Approach

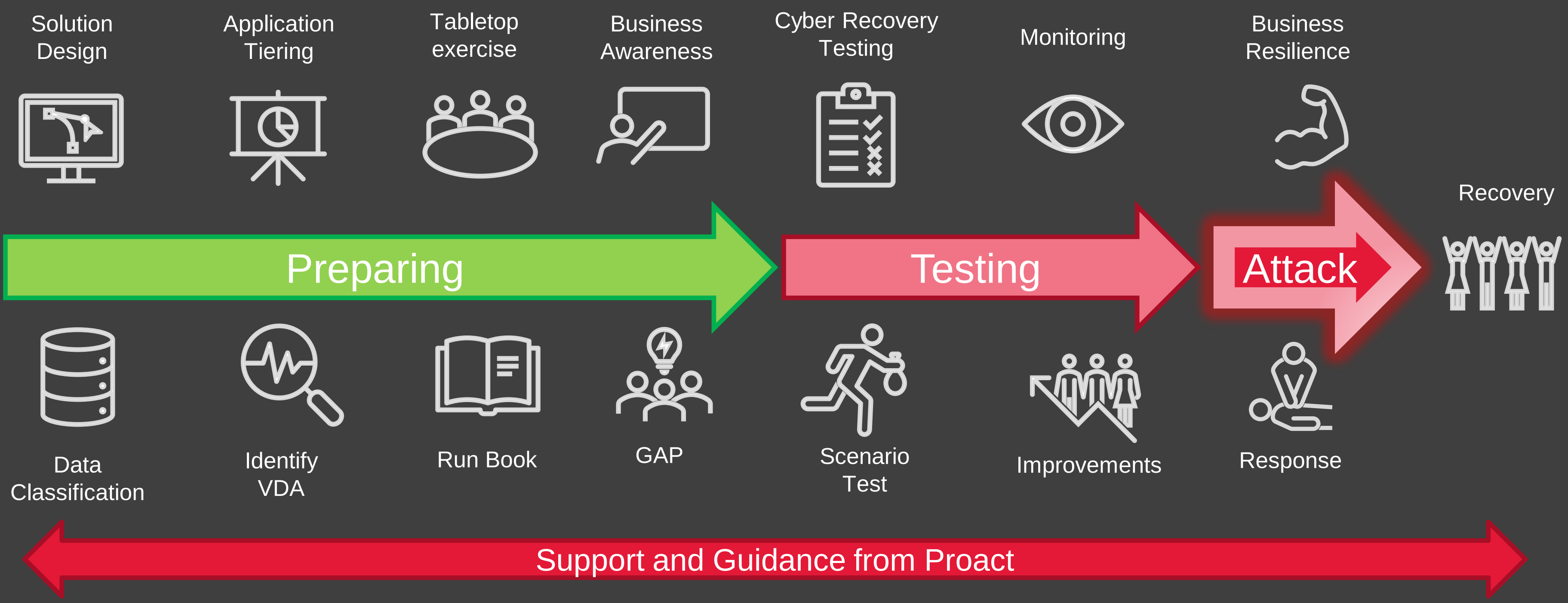
1. Preparation
2. Backup
3. Detection and Notification
4. Containment and Recovery
5. Investigation
6. Remediation
7. Recovery

Proact Cyber Recovery Approach

PROACT

COMMVAULT

Proact Team will guide you through the process of being Cyber Recovery ready



Solution Design

Application Tiering

Tabletop exercise

Business Awareness

Cyber Recovery Testing

Monitoring

Business Resilience

Recovery

Preparing

Testing

Attack

Data Classification

Identify VDA

Run Book

GAP

Scenario Test

Improvements

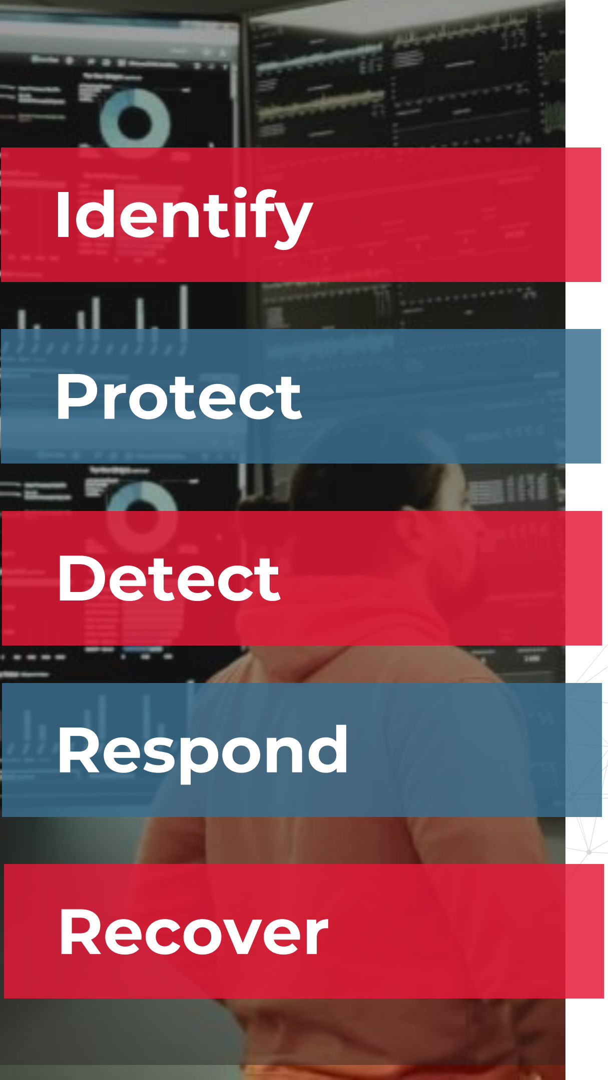
Response

Support and Guidance from Proact

Proact Security Portfolio

PROACT

COMMVAULT



Identify

Vulnerability Management, Threat Intelligence, Attack Surface Monitoring

Protect

Firewalls, Endpoint Protection, Phishing Defences, Web Proxies, ZeroTrust Access, Authentication (MFA), Staff awareness, Cyber Training/Education

Detect

Security Logging and Detection / 24/7 SOC services

Respond

MDR/XDR Services, Containment, Eradication, Incident Response Planning and Execution

Recover

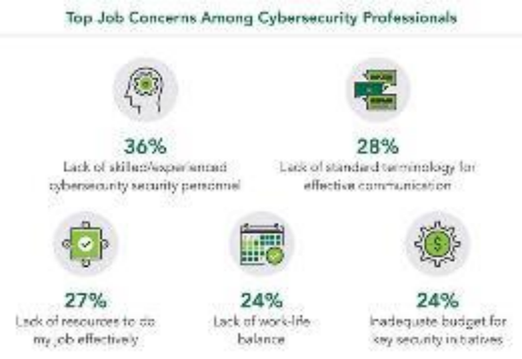
Cyber Recovery and Disaster Recovery

PROACT

COMMVAULT

Why Proact?

- 10+ years SOC services
- Mature BaaS service and skillsets
- Mature DRaaS and skillsets
- 25+ years Cloud offerings
- Mature Managed Services



Top Job Concerns Among Cybersecurity Professionals

36% Lack of skilled/experienced cybersecurity security personnel

28% Lack of standard terminology for effective communication

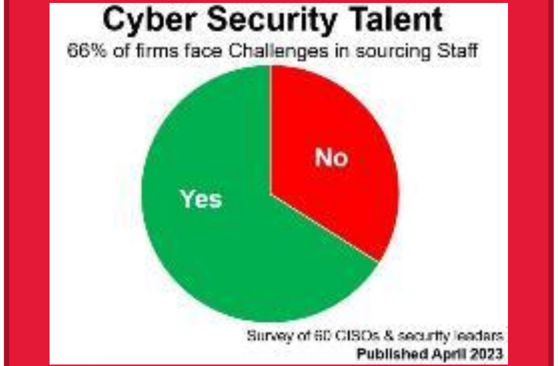
27% Lack of resources to do my job effectively

24% Lack of work-life balance

24% Inadequate budget for key security initiatives

ComputerWeekly.com

Hiring and retention challenges in cyber security persist



Cyber Security Talent

66% of firms face Challenges in sourcing Staff

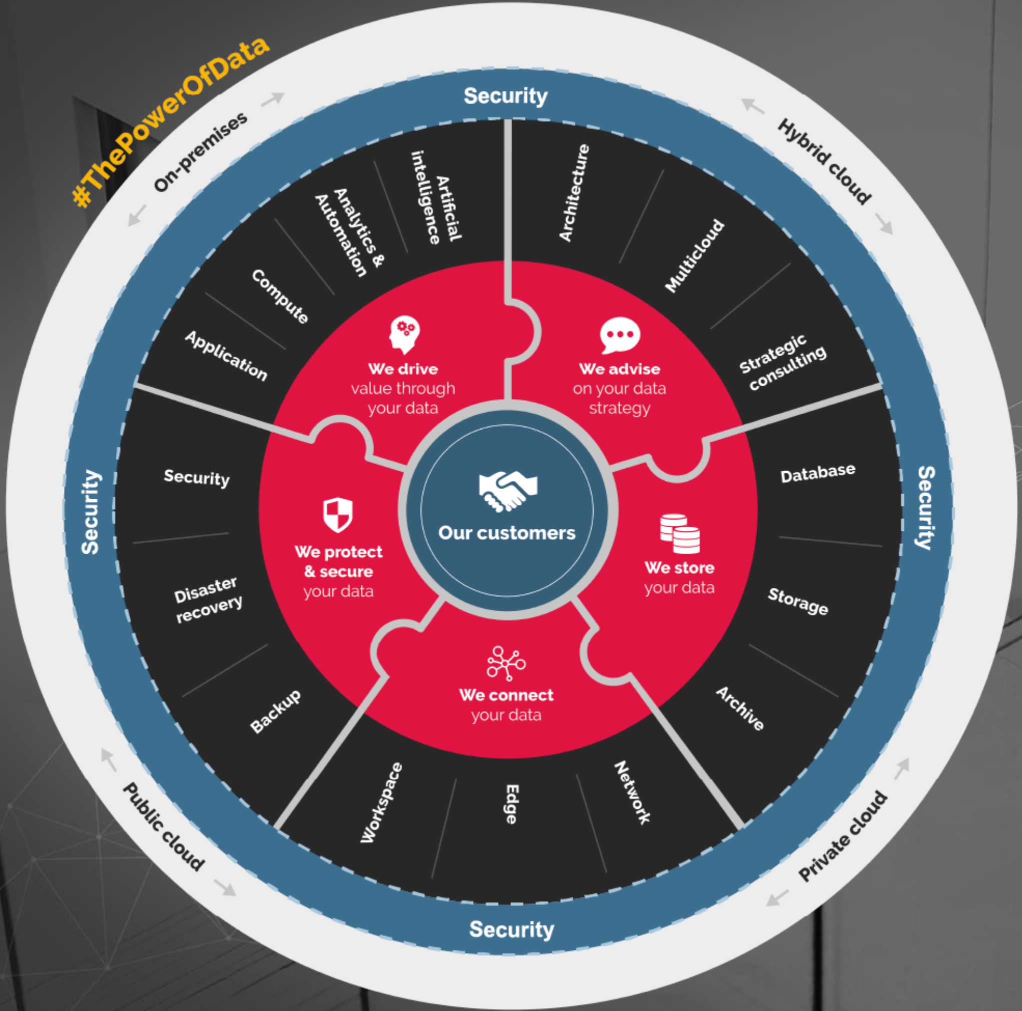
Survey of 60 CISOs & security leaders

Published April 2023

Proact UK in numbers

FI
NO
EE
LV
DE
CZ
SK

- Established in 2000
- £65m turnover
- 250 UK Staff
- 1,000+ customers
- ISO9001, ISO27001, PCI DSS
- 24x7 UK NOC & SOC
- 100+PB under management



Value through **our portfolio**

Thoughts

Cyber Security is ever increasing in its complexity so a recoverable position may be the only reliable choice to offer your business.

The technology alone will not be enough to make you Cyber resilient you need a plan that’s tested

“Offline Backup” is now considered the best option if you need to fully recover as recommended by independent auditors

Employing people capable of delivering is difficult

Having a trusted partner can allow you to skip the learning curve

Got a question?

Shane Wallace

Managed Service Architect
(DRaaS & Cyber Recovery)
swallace@proact.co.uk
07713 311 300

Tim Simons

Head of Security Services
tsimons@proact.co.uk
07824 505 462

Andrew Ward

Client Director
award@proact.co.uk
07973 627 727

PROACT

Thank you

www.Proact.co.uk

National Cyber Security Centre
a part of GCHQ

10 Steps to Cyber Security

This collection is designed for security professionals and technical staff as a summary of NCSC advice for medium to large organisations. We recommend you start by reviewing your approach to risk management, along with the other nine areas of cyber security below, to ensure that technology, systems and information in your organisation are protected appropriately against the majority of cyber attacks and enable your organisation to best deliver its business objectives.

Risk management
Take a risk-based approach to securing your data and systems.

PROACT
COMMVAULT

Engagement and training
Collaboratively build security that works for people in your organisation.

PROACT

Asset management
Know what data and systems you have and what business need they support.

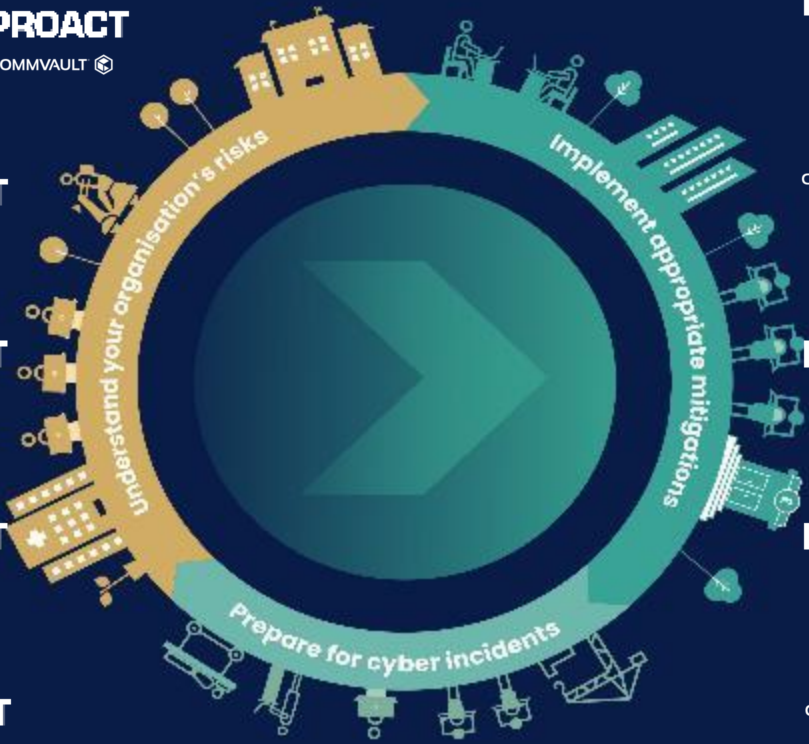
PROACT
COMMVAULT

Architecture and configuration
Design, build, maintain and manage systems securely.

PROACT
COMMVAULT

Vulnerability management
Keep your systems protected throughout their lifecycle.

PROACT


Understand your organisation's risks
Implement appropriate mitigations
Prepare for cyber incidents

PROACT

Identity and access management
Control who and what can access your systems and data.

COMMVAULT

Data security
Protect data where it is vulnerable.

PROACT

Logging and monitoring
Design your systems to be able to detect and investigate incidents.

PROACT
COMMVAULT

Incident management
Plan your response to cyber incidents in advance.

COMMVAULT

Supply chain security
Collaborate with your suppliers and partners.