linx

LINX Security Update

Operational Resiliency in the Face of Ransomware Threats

Julian Salter
Cyber Security Architect

20th November

LINX 125

Your Worst Nightmare

How it typically plays out

- System Unavailable
- Request for payment
- Dialogue
- Stalling
- Impatience
- Embarrassment
- Sale of Data

```
>>> CHANGES LOCKED OUT <<<

** IMPROPER REQUEST **

** ACCESS DENIED **
```

Could it get any worse?

(Yes)

(It can always get worse)

Virtually Trash the Infrastructure

How quickly could you **rehydrate** your systems from nothing?

The damage isn't only the loss of data, what about the infrastructure?

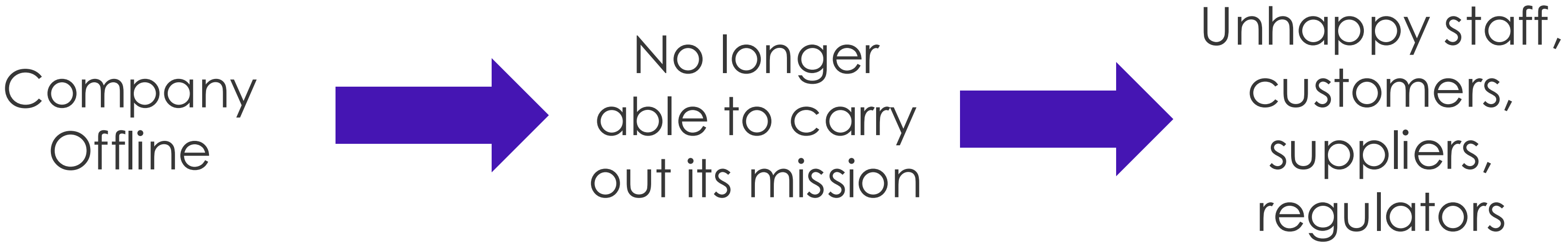
- Erasing disks
- Trashing Hypervisors
- Corrupting bootloaders
- Wiping firmware
- Resetting TPMs

Virtually Trash the Infrastructure

How quickly could you **rehydrate** your systems from nothing?

<u>This is not a theoretical scenario</u>

Results?

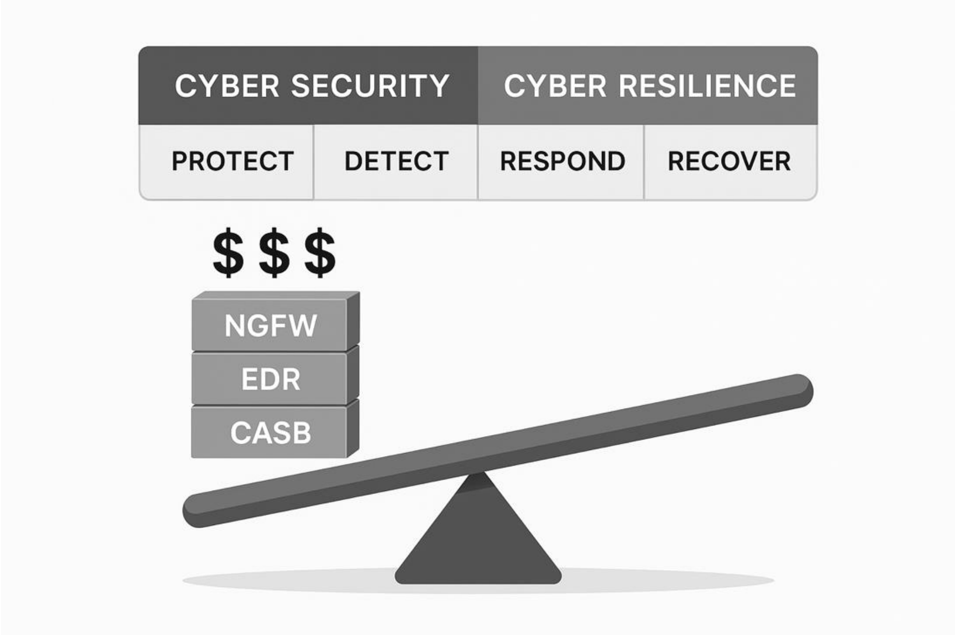


Company Offline → No longer able to carry out its mission → Unhappy staff, customers, suppliers, regulators

Cyber Security

Ransomware! We did a table-top exercise, assessed the risks, have recovery plans

- Ransomware is just another kind of cyber threat to manage
- Too much focus on Preventive and Detective controls
- Are we getting good ROSI?
- What about **resiliency?**



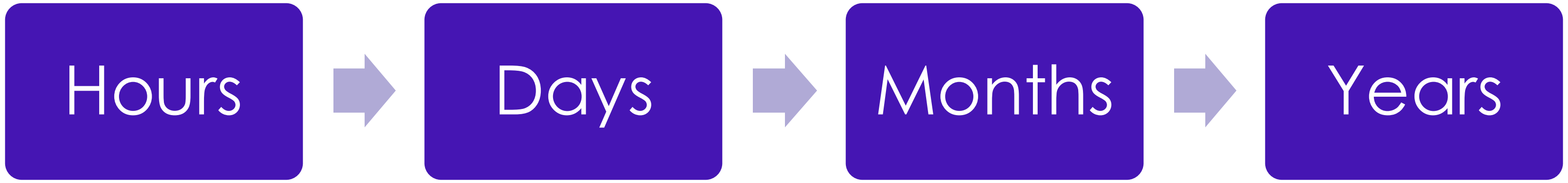
CYBER SECURITY		CYBER RESILIENCE	
PROTECT	DETECT	RESPOND	RECOVER

Minimum Viable Company

GRF - Operational Resilience Framework

- What are our critical external services?
- What are the Minimum Viable Service Levels (MVSL) we need to deliver our critical service?
- What are the minimum Viable Service Delivery Objectives (MVDO) to reach the MVSL?

How quicky could YOU rehydrate your network/system to reach the MVSL?



Hours

Days

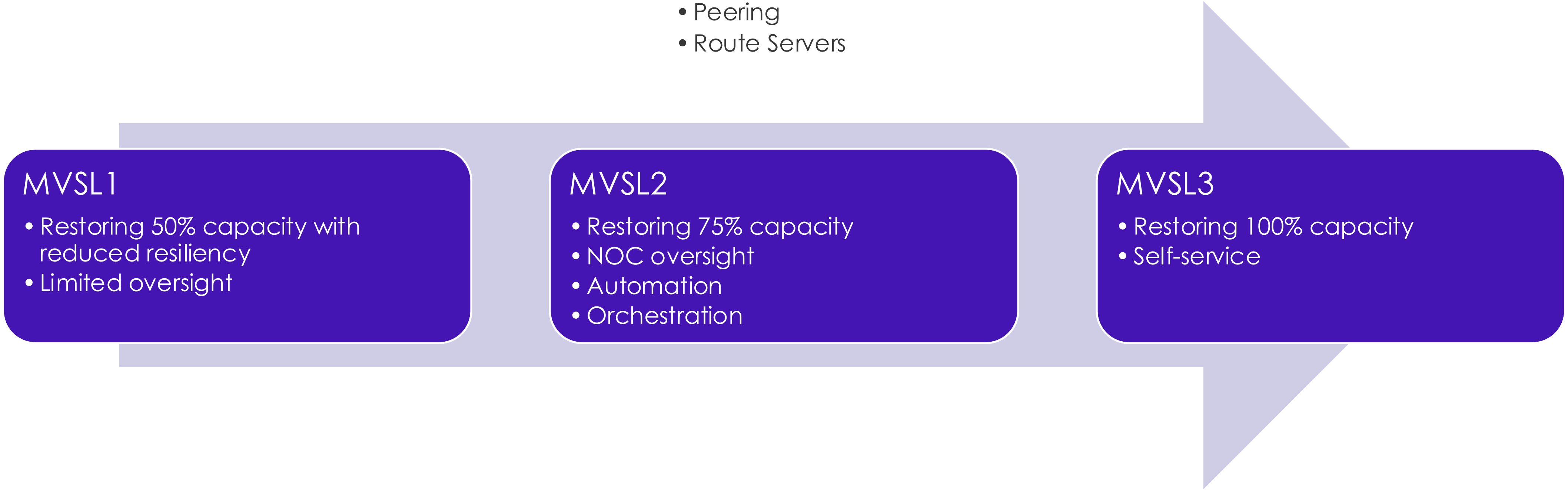
Months

Years

How Could this Look in Practice?

Critical Services

- Peering
- Route Servers



MVSL1

- Restoring 50% capacity with reduced resiliency
- Limited oversight

MVSL2

- Restoring 75% capacity
- NOC oversight
- Automation
- Orchestration

MVSL3

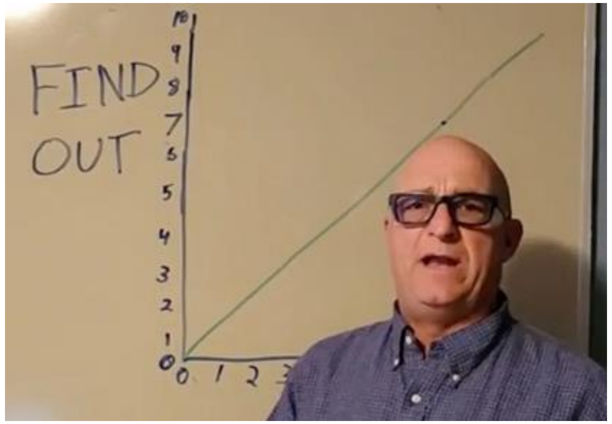
- Restoring 100% capacity
- Self-service

Each MVSL has a MVDO

Where Are We Now?

Investigation and Research

- Network capacity planning informs recovery planning
- Resiliency mindset is being promoted across teams
- Building resiliency across the entire application stack
- Critical datasets are being identified and moved to offsite immutable storage
- Recovery processes will become part of Acceptance Criteria
- Active Testing and Stress Testing (utilising our lab)
- Complex Dependencies better understood
- Reducing Technical Debt



Strategic KPI

How quickly could we rehydrate our critical systems?

- Design for resilience
- Reduce Complexity
- Improve Documentation
- Recovery Processes
- Lab testing
- Increase Automation and Orchestration
- (IaaC) Infrastructure as Code
- Immutable backups

Security are in the Room!
Come and Talk to Us!