Cyber Resilience –
Why The Next Evolution of Security is a Bigger Leap Than You Suspect!
(and what it has to do with car tires!)

EVOLUTION OF CONTROL

IT SECURITY

"Stop those computers getting viruses"

INFORMATION SECURITY

"Information is an asset, how can we protect it?"

CYBER SECURITY

"Protect digital systems to prevent real world impact"

CYBER RESILIENCE

???

proofpoint.

‘CYBER RESILIENCE’ – ANOTHER BUZZ WORD?

proofpoint.

LIKE CYBER-SEC, IT'S CAUGHT THE ATTENTION OF EXECS

- 84% of respondents say cyber resilience is considered a business priority in their organization
- 92% of business executives surveyed agree that cyber resilience is integrated into enterprise risk management strategies, however only 55% of security-focused executives surveyed agreed
- 87% of executives are planning to progress cyber resilience by strengthening resilience policies and standards
- 88% of respondents indicated that they are concerned about the cyber resilience of their supplier ecosystem

58%
of surveyed CISOs in Sweden feel their organization is at risk of suffering a material cyber attack in the next 12 months

WORLD ECONOMIC FORUM
Global Cybersecurity Outlook 2022

proofpoint.

HOW IS CYBER RESILIENCE ARRIVING IN OUR LIVES?

proofpoint.

HOW IS CYBER RESILIENCE ARRIVING IN OUR LIVES?

HOW IS CYBER RESILIENCE ARRIVING IN OUR LIVES?

proofpoint.

HOW IS CYBER RESILIENCE ARRIVING IN OUR LIVES?

- The contents of these papers do not sound new.
- They are the same security good practices we have pursued for years, repackaged..

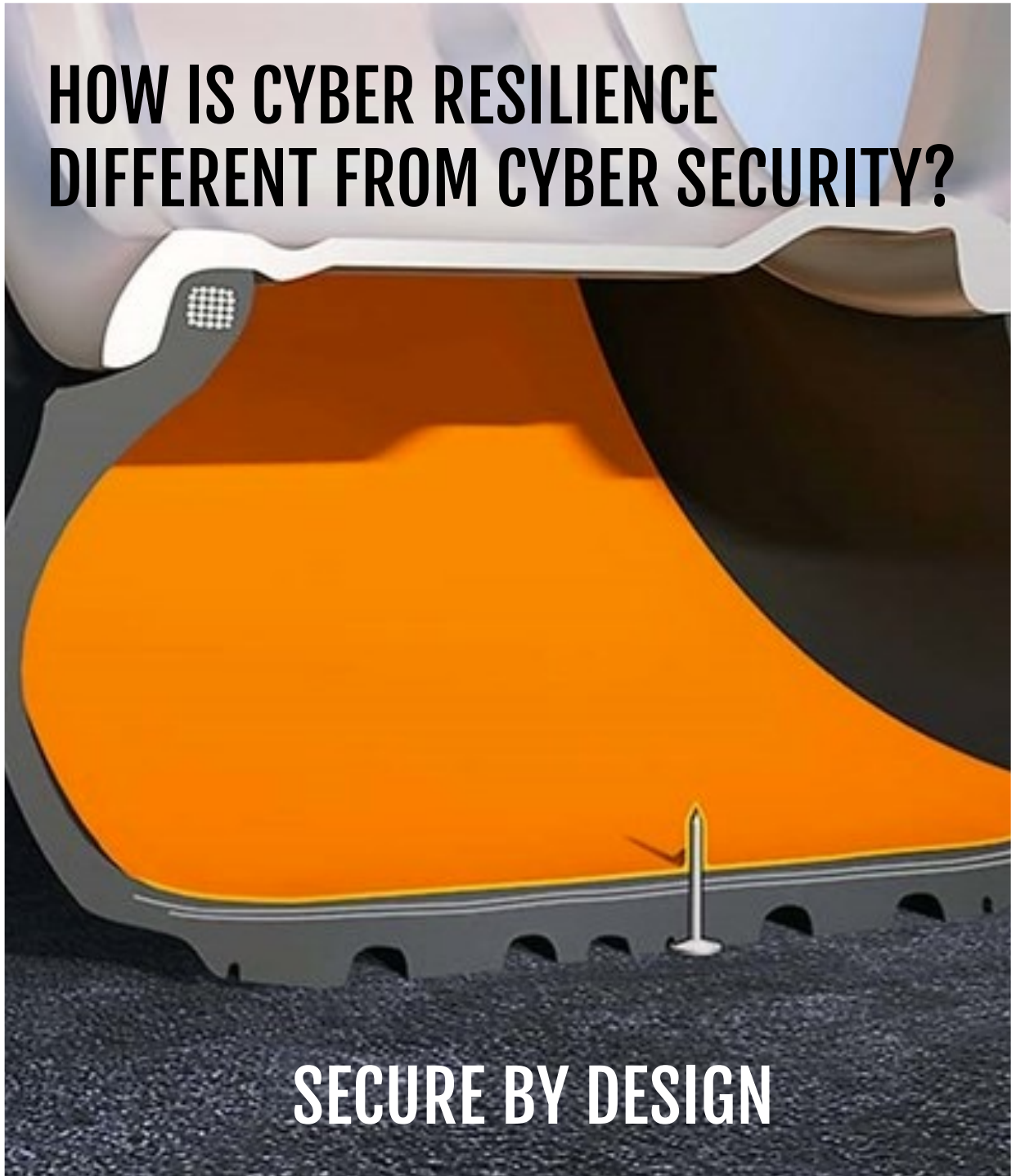
"there should be nothing new or additional in the Framework"

'Cyber Resilience Framework' – Scottish Govt

The Scottish Government

proofpoint.

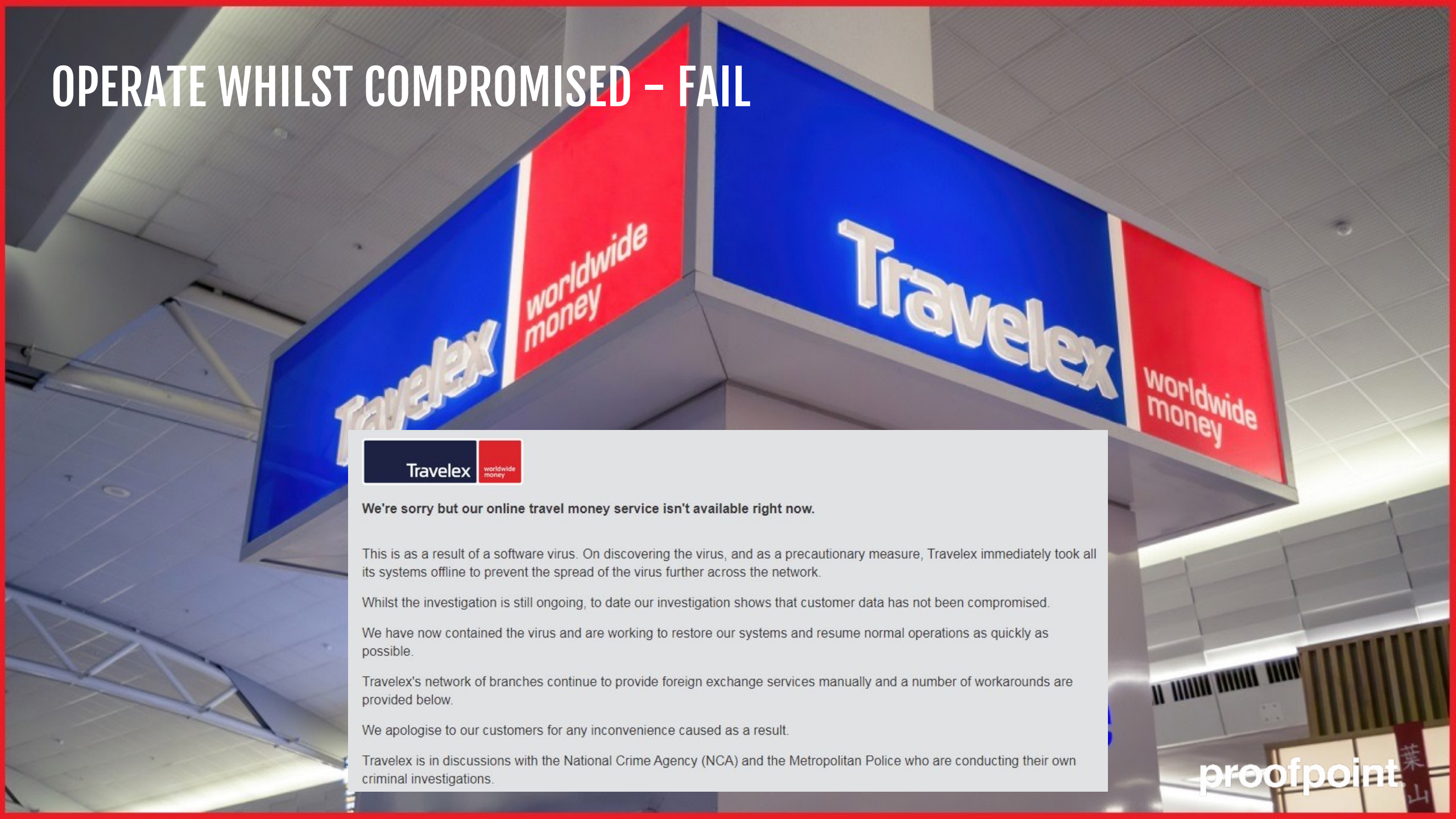
HOW IS CYBER RESILIENCE DIFFERENT FROM CYBER SECURITY?



SECURE BY DESIGN

OPERATE WHILE COMPROMISED

OPERATE WHILST COMPROMISED – FAIL



Travelex worldwide money

We're sorry but our online travel money service isn't available right now.

This is as a result of a software virus. On discovering the virus, and as a precautionary measure, Travelex immediately took all its systems offline to prevent the spread of the virus further across the network.

Whilst the investigation is still ongoing, to date our investigation shows that customer data has not been compromised.

We have now contained the virus and are working to restore our systems and resume normal operations as quickly as possible.

Travelex's network of branches continue to provide foreign exchange services manually and a number of workarounds are provided below.

We apologise to our customers for any inconvenience caused as a result.

Travelex is in discussions with the National Crime Agency (NCA) and the Metropolitan Police who are conducting their own criminal investigations.

OPERATE WHILST COMPROMISED – FAIL

proofpoint.

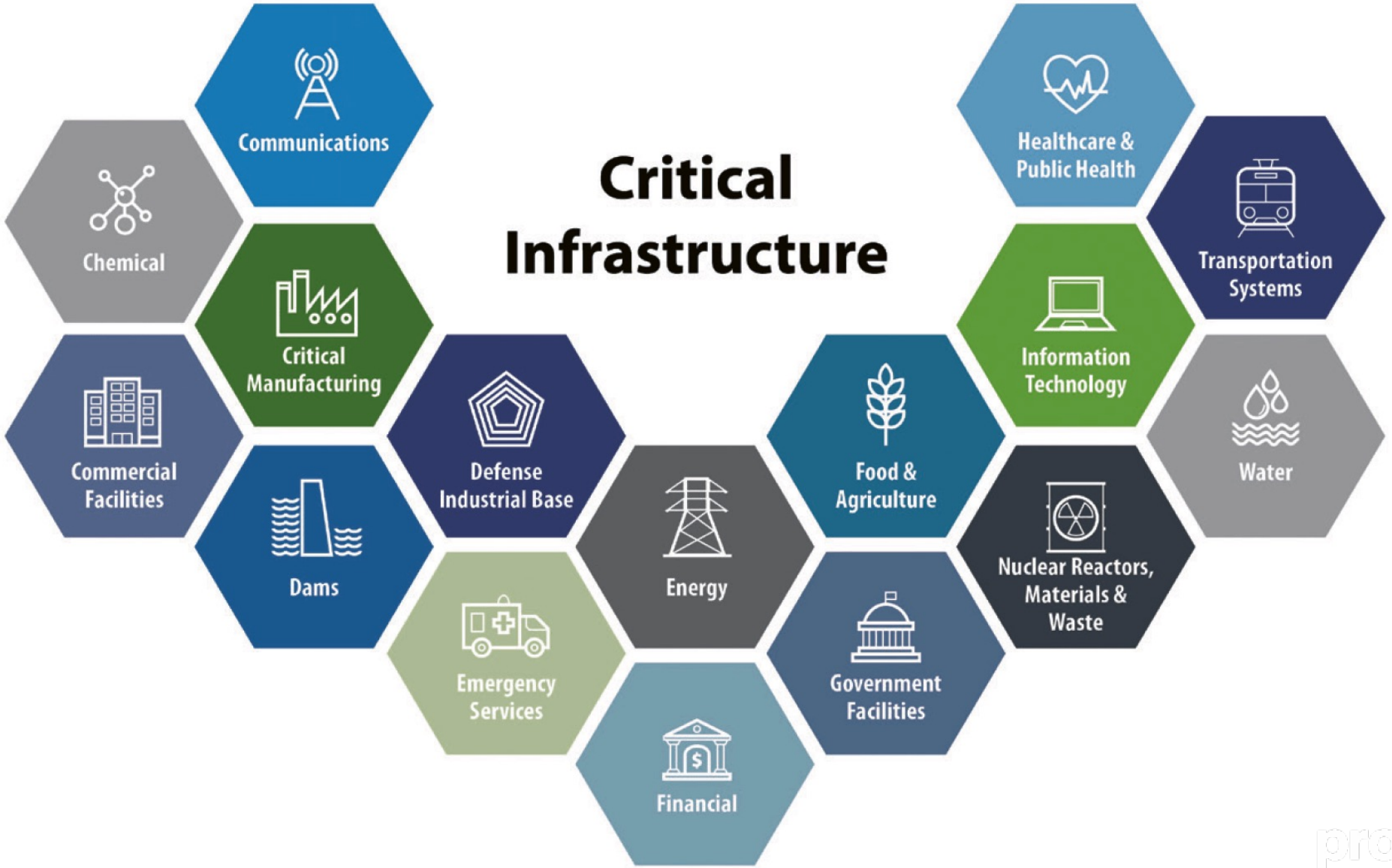
OPERATE WHILST COMPROMISED – FAIL

proofpoint.

OPERATE WHILST COMPROMISED – PARTIAL SUCCESS

proofpoint.

“48 HOURS FROM ANARCHY”



CHALLENGES TO CYBER RESILIENCE

TECHNOLOGY

- Increasing opacity of systems
- Both very old and very new technology expect constant connectivity
- Simple designs are more ‘supportable’ but can be less resilient (e.g. flat networks)

BUSINESS

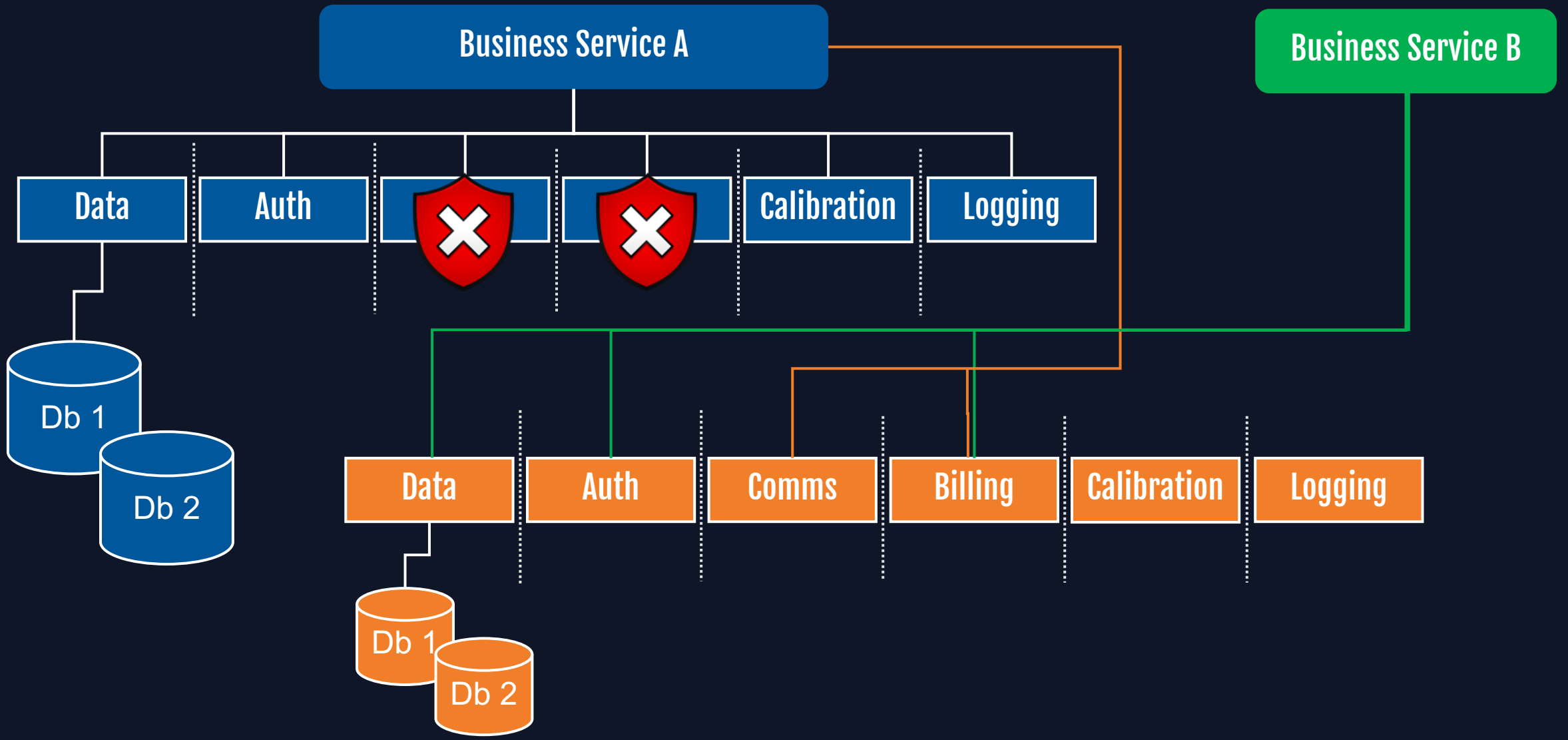
- Resilience is often enabled by spare capacity, which contradicts ‘lean’ culture
- Business units are loathe to test resilience for fear of disruption
- Business units are rarely clear on the criticality of systems

ACHIEVING CYBER RESILIENCE?

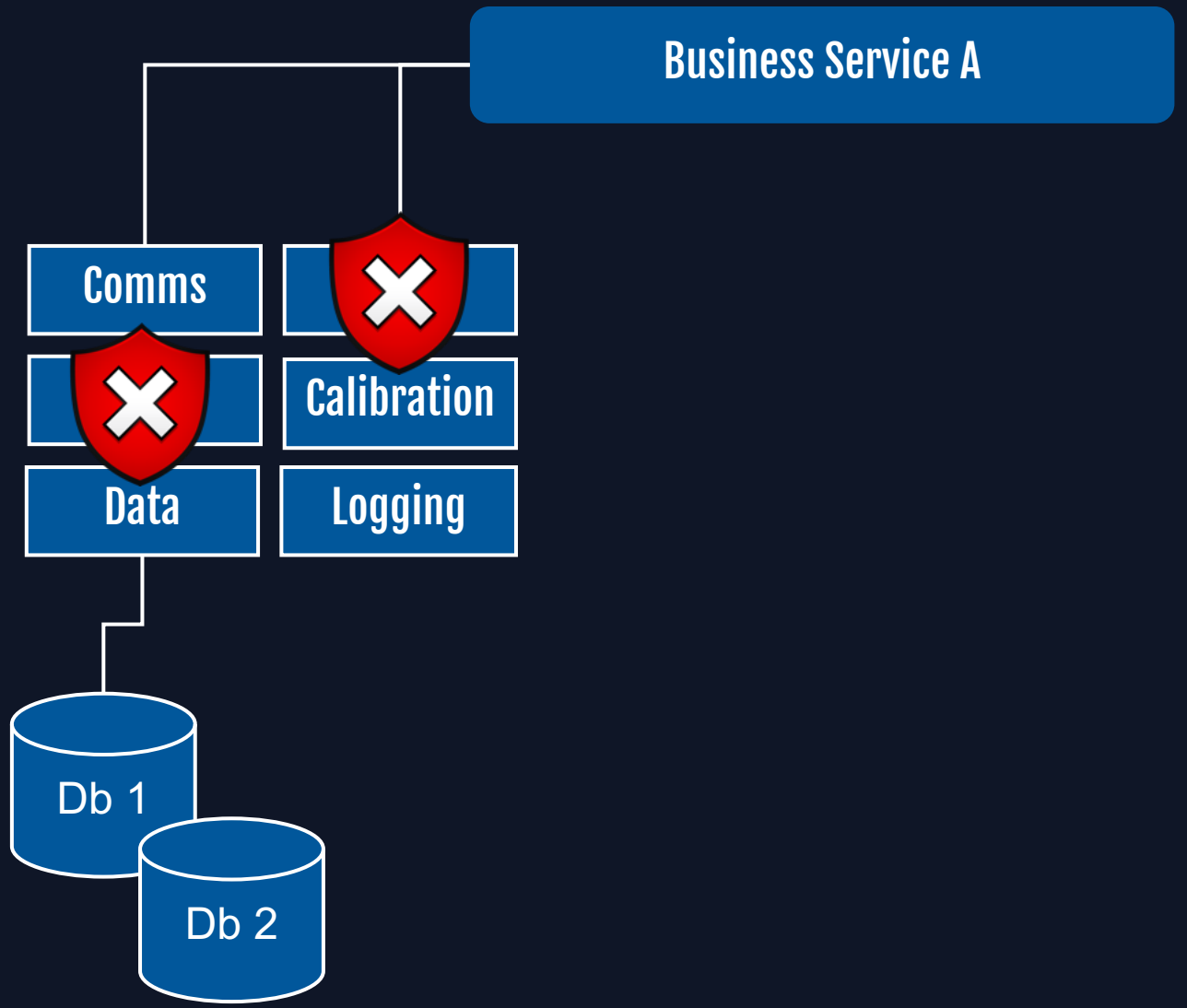
Service Component Architecture

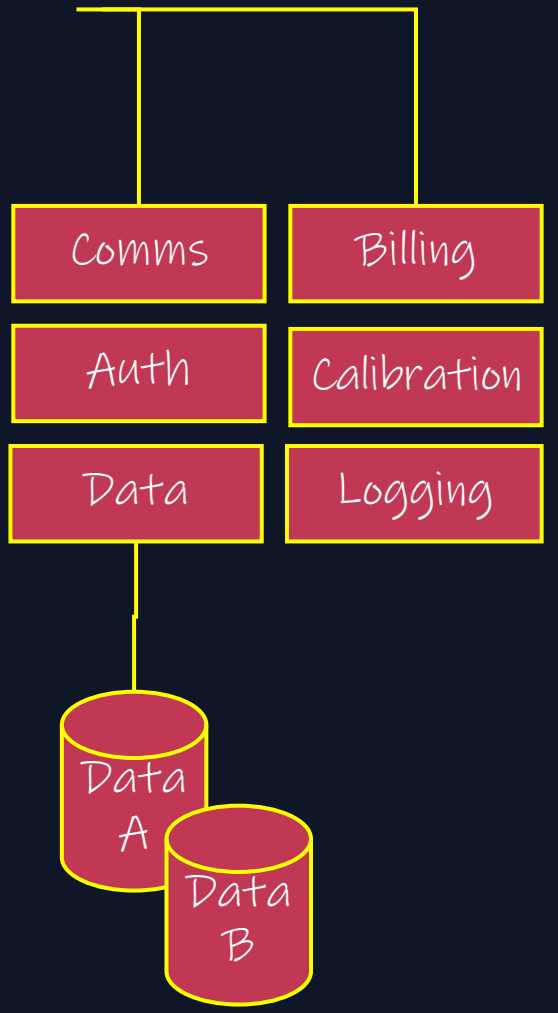
System B

SERVICE COMPONENT ARCHITECTURE



SYSTEM B


Business Service A
Comms
Calibration
Data
Logging
Db 1
Db 2


Comms
Billing
Auth
Calibration
Data
Logging
Data A
Data B

ACHIEVING CYBER RESILIENCE?

Service Component Architecture

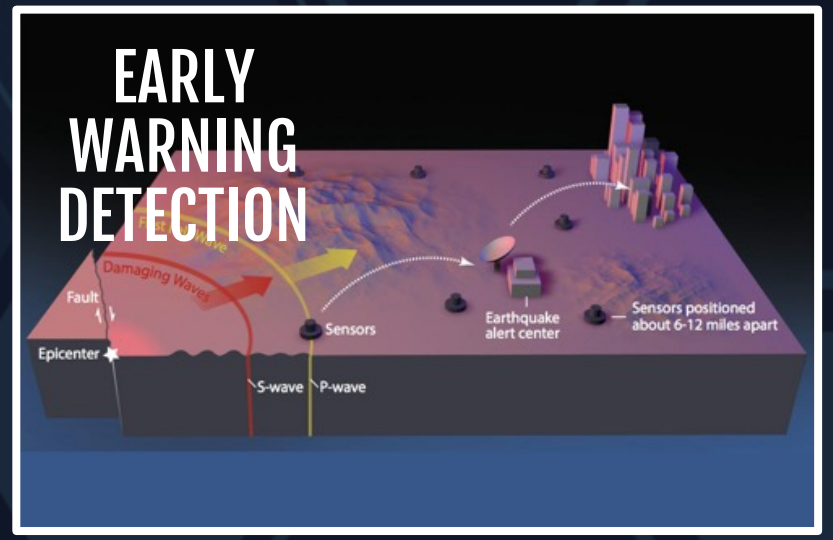
- Break down essential services into components, and create multiple instances of logically separated components

System B

- Create an entirely separate system to deliver the same service, based on different technology selections and architectural principles

	SCA Design	System B
Resilience	****	*****
Flexibility	****	*
Simplicity	*	***
Cost	$$$$	$$$$$

PRAGMATICALLY ACHIEVING CYBER RESILIENCE?



proofpoint.

WHAT DOES THIS MEAN FOR CISOS?

Growing Scope & Seniority

- Cyber-resilience places the CISO at the heart of the successful enterprise
- The scope & importance of the CISO role increases
- We gain ‘Big C’ status, at last...
  ....but be careful what you wish for!

Burnout

- 65% of Swedish CISOs feel that their role places ‘excessive expectations’ on them currently
- Expanding the accountabilities further will amplify this problem

RESIST

PREVENT INCIDENTS

I. People are your primary attack surface & at the root of 90%+ of incidents
II. Email is the primary attack tool
III. Almost every attack has an ‘insider threat’ aspect

proofpoint.

ROBUST

FOCUS ON THE KEY COMPONENTS

I. Network Layering
II. Segmentation Analysis & Assurance
III. Pre-Agreed Disconnection Processes
IV. Early Warning Indicators
V. Fusion Centre
VI. Chaos Engineering

REBOUND

REVISIT BUSINESS CONTINUITY PLANS

I. Map out critical business processes, not every supplier
II. Identify how you can keep that process running, even if it means paper based!
III. Rehearse the fallback process model


proofpoint
Thank you!
proofpoint