



proofpoint®

Cyber Resilience —

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

proofpoint

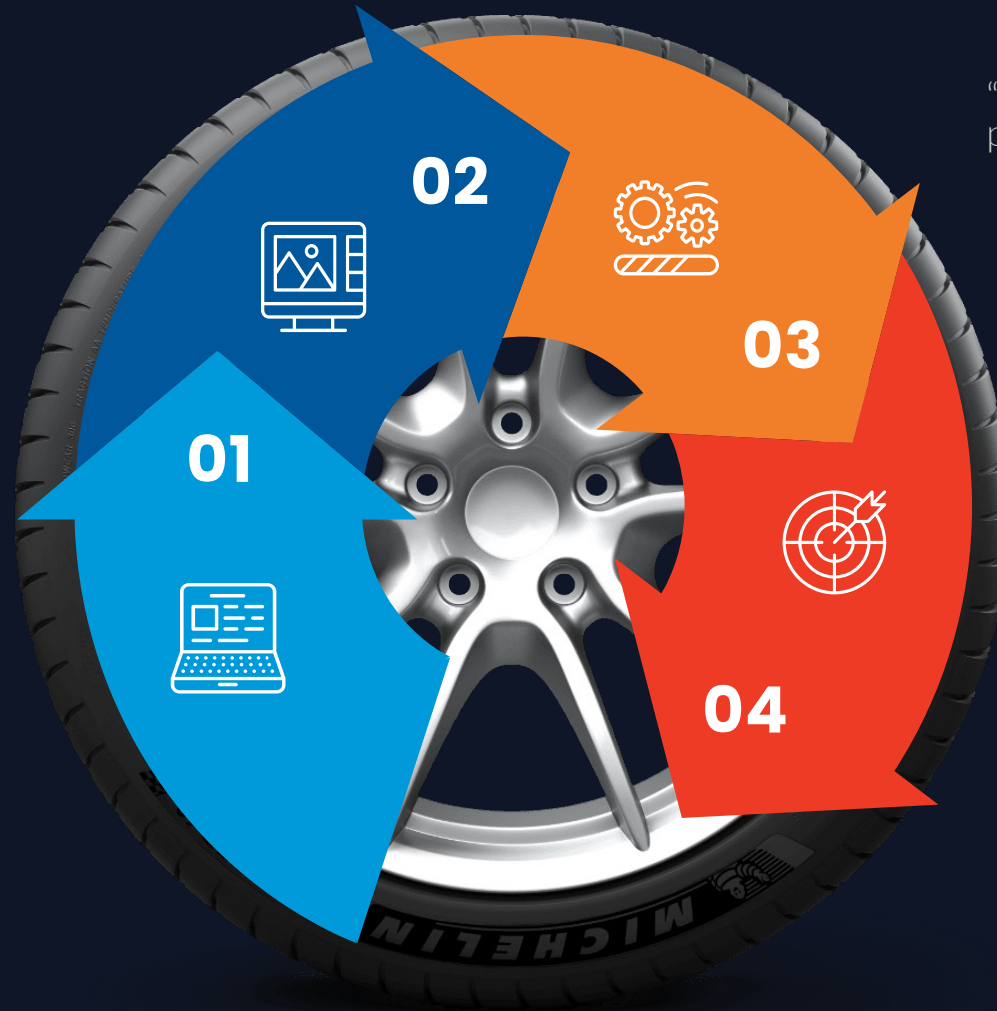
EVOLUTION OF CONTROL

INFORMATION SECURITY

“Information is an asset, how can we protect it?”

IT SECURITY

“Stop those computers getting viruses”



CYBER SECURITY

“Protect digital systems to prevent real world impact”

CYBER RESILIENCE

???

'CYBER RESILIENCE' – ANOTHER BUZZ WORD?

Cyber Resilience Act
Loi sur la cybersécurité



Commission européenne |
European Commission

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



HOW IS CYBER RESILIENCE ARRIVING IN OUR LIVES?

NIS2 DIRECTIVE

HOW IS CYBER RESILIENCE ARRIVING IN OUR LIVES?

The logo for the Digital Operational Resilience Act (DORA) features the word "DORA" in a bold, yellow, sans-serif font. It is surrounded by twelve yellow five-pointed stars arranged in a circular pattern, similar to the flag of the European Union. The background is a dark blue with a subtle pattern of diagonal lines.

DORA

**Digital
Operational
Resilience
Act**

HOW IS CYBER RESILIENCE ARRIVING IN OUR LIVES?

EU Cyber Resilience Act

Rules for
digital products



#DigitalEU #CyberSecEU

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

HOW IS CYBER RESILIENCE DIFFERENT FROM CYBER SECURITY?

SECURE BY DESIGN



**OPERATE WHILE
COMPROMISED**

OPERATE WHILST COMPROMISED – FAIL

Travelex

worldwide
money

Travelex

worldwide
money

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.

proofpoint

OPERATE WHILST COMPROMISED – FAIL



The screenshot shows the BBC News website interface. At the top, the BBC logo is on the left, followed by a user profile 'Andy' with a notification bell icon. Navigation links for 'Home', 'News', 'Sport', and 'Weather' are visible. A red banner with the word 'NEWS' in white is prominent. Below this, a horizontal menu lists various news categories: Home, Cost of Living, War in Ukraine, Climate, UK, World, Business, Politics, and Scotland. Under the Scotland category, sub-links include Scotland Politics, Scotland Business, Edinburgh, Fife & East, Glasgow & NE, Orkney & Shetland, South, Tayside & Central, Alba, and Local News. The main headline reads 'Sepa cyber attack recovery could take years' in large, bold black text. Below the headline, the date '© 24 June 2021' is displayed.



OPERATE WHILST COMPROMISED – FAIL



COLONIAL PIPELINE CO

213

NO SMOKING

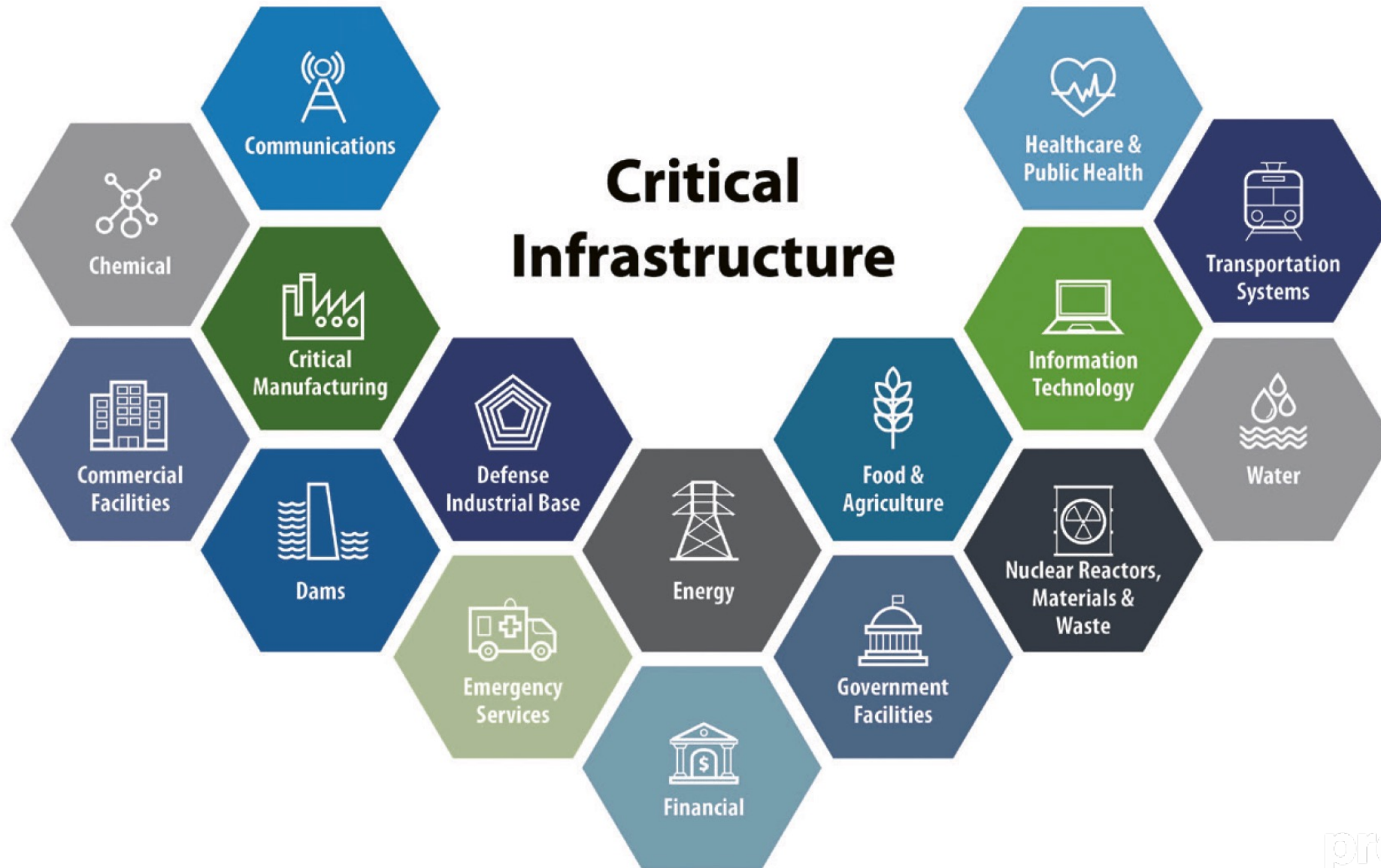
proofpoint.

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?

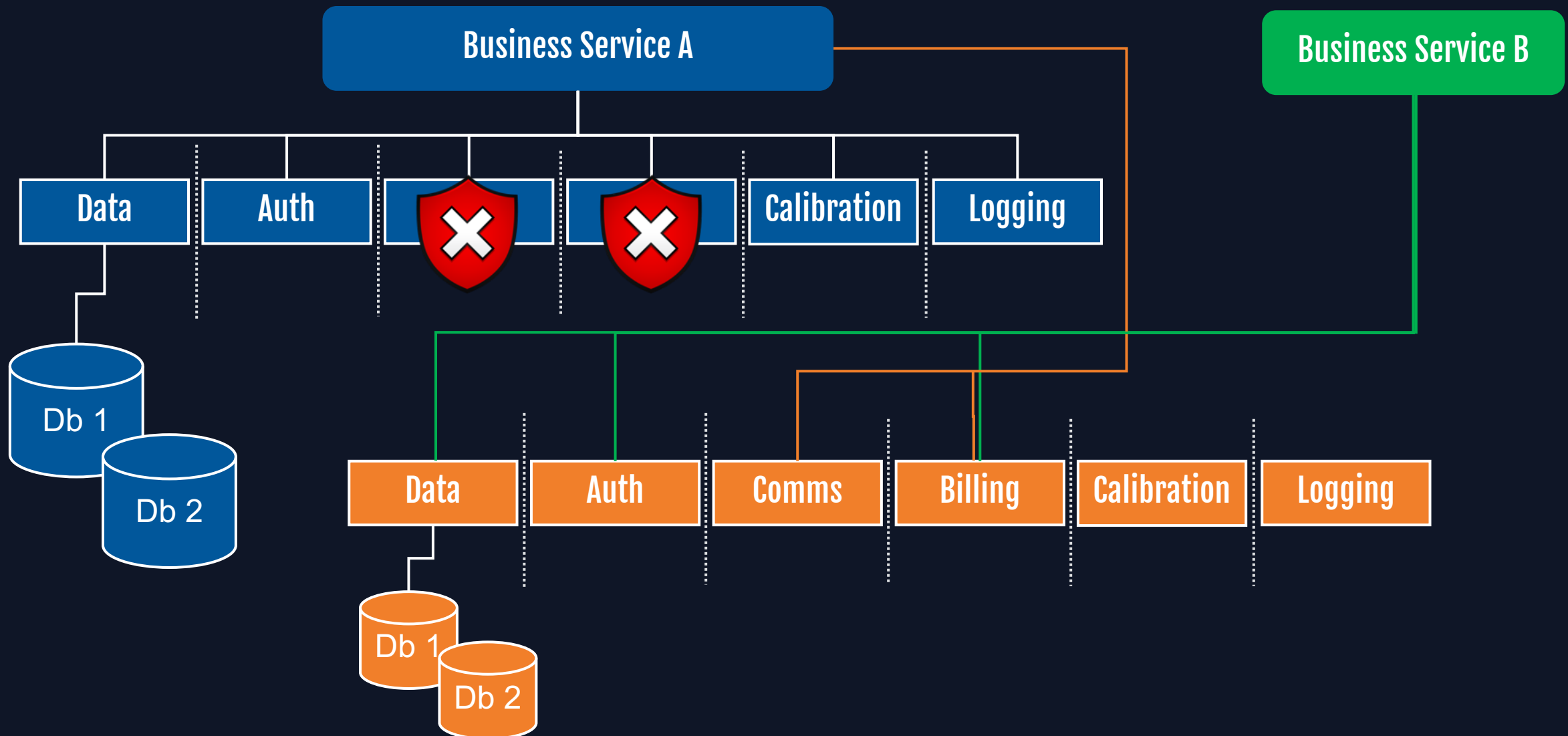
Service Component Architecture



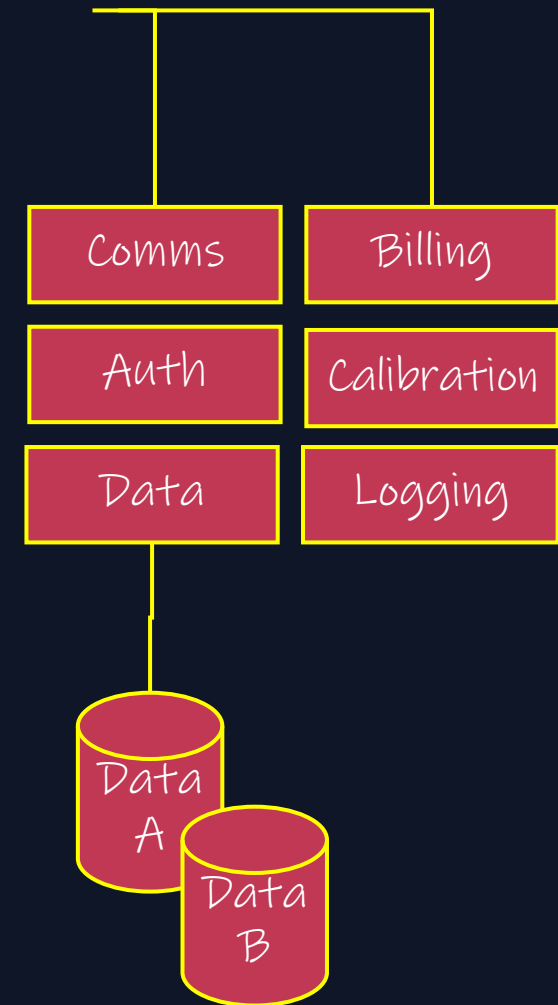
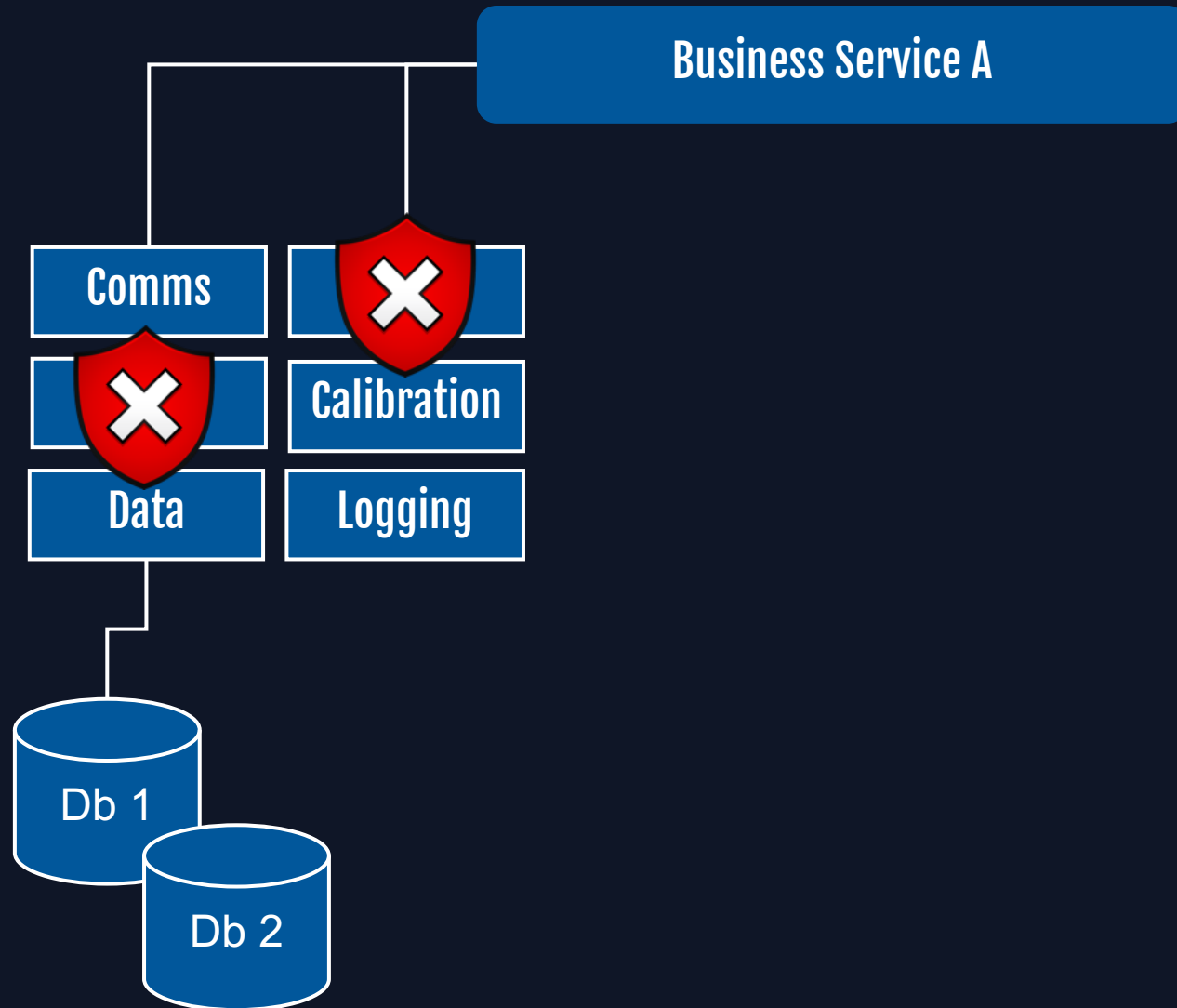
System B



SERVICE COMPONENT ARCHITECTURE



SYSTEM B



ACHIEVING CYBER RESILIENCE?

Service Component Architecture

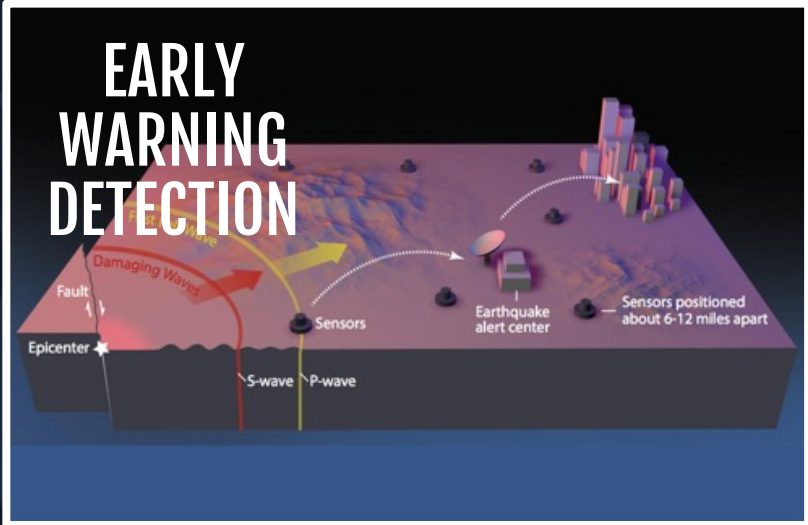
- Break down essential services into components, and create multiple instances of logically separated components

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?



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

```
operation == "MIRROR_X":
    mirror_mod.use_x = True
    mirror_mod.use_y = False
    mirror_mod.use_z = False
operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True
```

```
selection at the end -add
mirror_ob.select=1
mirror_ob.select=1
context.scene.objects.active
("Selected" + str(modifier
mirror_ob.select = 0
 bpy.context.selected_obj
 data.objects[one.name].sel
```

```
types.Operator):
    X mirror to the selected
    object.mirror_mirror_x"
    mirror X"
```

proofpoint

Thank you!

proofpoint.