

# Cyber Resilience: Strengthening Defences In An Increasingly Interconnected Digital Capital Market

October 2025



Thomas  
Murray | Cyber Risk

## UNDER CYBER ATTACK?



Call our incident response  
team 24/7 on [+44 \(0\) 207 459 4888](tel:+442074594888)  
for immediate help from our experts

## About me



Edward Starkie

Director, GRC at Thomas Murray.

- Consultant specialising in business focused cyber security, compliance and resilience.
- Heavily focused on leveraging threat intelligence and providing pragmatic advice for business leaders on how to achieve long term objectives.
- A full member of the Chartered Institute of Information Security (CIIISec).
- A certified Information Security Manager (CISM).
- Previous experience includes Kroll, PwC, Shell, Ds Smith, Royal Mail.
- London based but with a global portfolio of clients.

## A global partner

For 30 years, leaders of the world's **top financial institutions** have turned to Thomas Murray for its independent advice, global coverage and leading technologies.

### 01

With clients in 15+ countries, TM Cyber Risk has the global reach to support the most complex and geographically demanding challenges through threat- intelligence-first services that deliver actionable outcomes for our clients and their communities.



### 02

Our services are delivered by an in-house team of experienced professionals drawn from a range of backgrounds including banking, government, industry, consultancy, military, and law enforcement.



### 03

Few other businesses place as much value on combining deep industry expertise with long-standing relationships, to become our clients' trusted advisors.



## Full service offering

Bringing the best of our collective experience, energy and creative power to safeguard our clients and their communities.

### ➤ Respond

Respond to unexpected events, preserving reputation and value

### ➤ Improve

Understand your risk profile based on real world factors

### ➤ Secure

Defend against known and unknown threats

### ➤ Quantify

Plan continuous improvement using our knowledge of real-world events





## Why Thomas Murray?



**Visibility at Scale:**  
New CTI observables per day

**Up to 100,000**

---



**Excellence:**  
Years of cyber security experience

**170+ years**

---



**Experience:**  
Previous client engagements

**Over 5,000**

---



**Speed:**  
Quicker incident response processes

**Up to 45%**

---

# Session overview

---

## ➤ My Objectives

- Give an overview of resilience.
- Outline factors impacting operational resilience.
- Outline challenges in this space.
- Present a potential solution.
- Hold your attention.

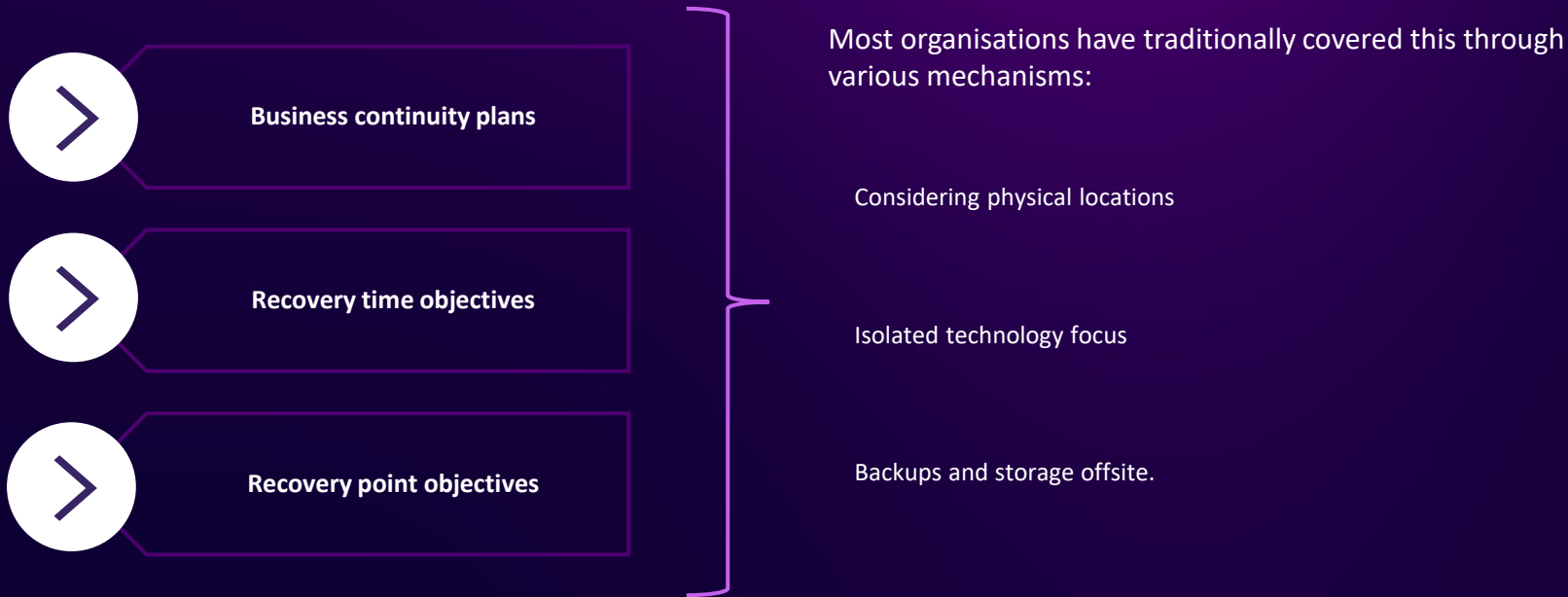
## ➤ Your Objectives

- Stay sat down (or at least don't run away).\*
- Answer some of the questions.

Disclaimers:

\*Exceptions do apply.

## Traditional resilience on a page







## Factors driving change in this space

---

### Digitalisation

Shift to a digitally enabled FS world.

Introduction of new technologies.

### Cyber security Implications

Changing threat landscape.

Impact of geopolitics.

### Counterparties and suppliers

Increased use of third-party providers.

# Factor One: Digitalisation

# What does this graph represent?

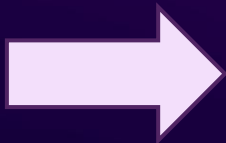


78%

companies that are using AI in at least one business function in 2025 (Gartner 2025)

## An additional complicating factor...

The most  
Googled AI  
related term  
in the UAE is:



1	free ai	100	<div><div></div></div>	⋮
2	ai generator	75	<div><div></div><div></div></div>	⋮
3	ai gemini	57	<div><div></div><div></div></div>	⋮
4	gemini	55	<div><div></div><div></div></div>	⋮
5	character ai	53	<div><div></div><div></div></div>	⋮

# Factor two: Cyber Security

## Traditional cyber security

Cyber security has traditionally focused on:



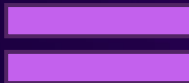
Deploying technology that hardens  
and secures the perimeter.



Prevention of incidents rather than  
curing.



Avoiding increasing cyber threats.



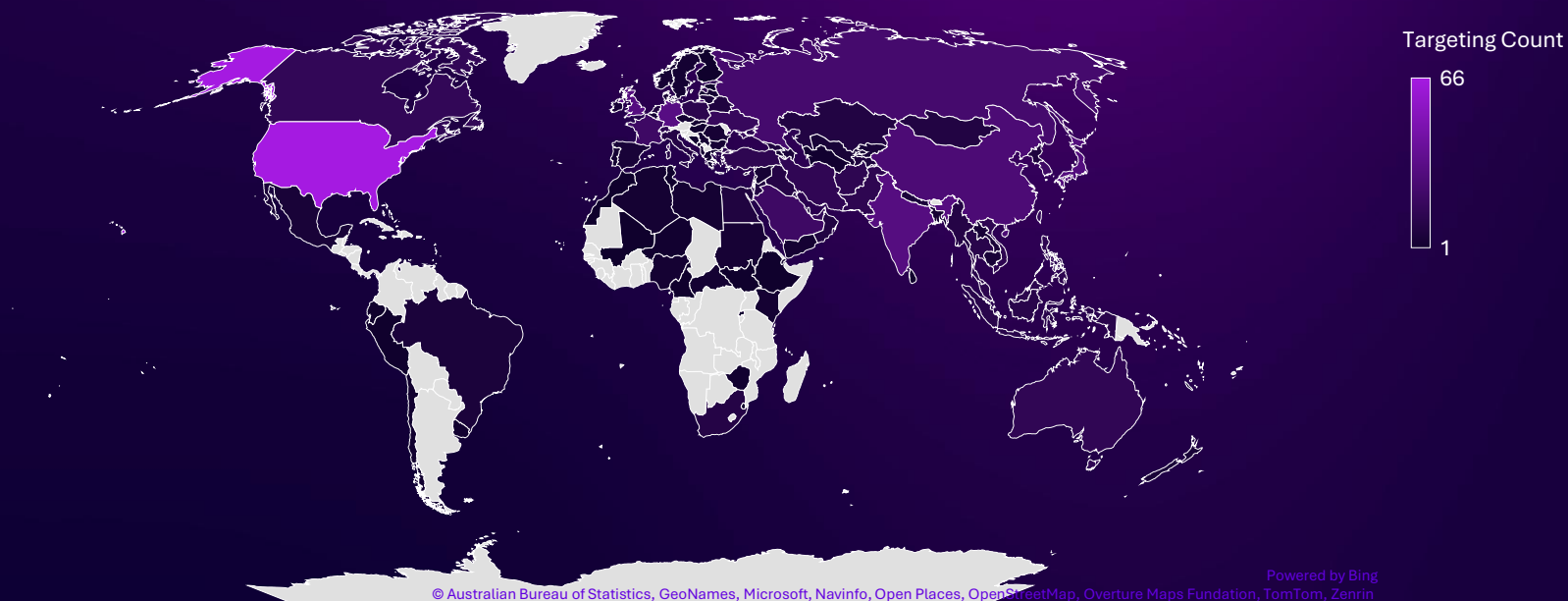
In 1990 we were overly confident...

## Global incidents (combined TM data) 2024-2025





# Global events shape the threat landscape



## The FS sector share common threats (ENISA)

NoName057	UserSec		Turk Hack Team
	Lockbit		Akira
	Cl0p		Anonym ous Russia
	NOES CAPE	ZulikG roup	Ano nym ous S...

Two Main motivations for threat actors here:

- Ideological
- Financial gain

To achieve their objectives these threat actors will typically use:

- Ransomware
- Distributed denial of service attacks.

Phishing remains the most common threat from a cyber security perspective, but why?



1 All of your files are currently encrypted by no\_name\_software.

2  
3 These files cannot be recovered by any means without contacting our team directly.

4  
5 DON'T TRY TO RECOVER your data by yourselves. Any attempt to recover your data (including the usage of the additional recovery s  
6 if you want to try - we recommend choosing the data of the lowest value.

7  
8 DON'T TRY TO IGNORE us. We've downloaded a pack of your internal data and are ready to publish it on our news website if you do  
9 So it will be better for both sides if you contact us as soon as possible.

10  
11 DON'T TRY TO CONTACT feds or any recovery companies.

12 We have our informants in these structures, so any of your complaints will be immediately directed to us.

13 So if you will hire any recovery company for negotiations or send requests to the police/FBI/investigators, we will consider thi  
14

15 DON'T move or rename your files. These parameters can be used for encryption/decryption process.

16  
17 To prove that we REALLY CAN get your data back - we offer you to decrypt two random files completely free of charge.

18  
19 You can contact our team directly for further instructions through our website :

20  
21 TOR VERSION :

22 (you should download and install TOR browser first <https://torproject.org>)

23  
24 <https://aazsbsgya565vlu2c6bzy6yfiebkcbtvvcyvtvolt33s77xypi7nypxyd.onion:80/>

25  
26 Your company id for log in: [snip]

27 Your company key: 3 of any of your dc through comma. Example: "DC1, DC2, DC3". You can type less if you have no enough  
28

29 YOU SHOULD BE AWARE!

30 We will speak only with an authorized person. It can be the CEO, top management, etc.

31 In case you are not such a person - DON'T CONTACT US! Your decisions and action can result in serious harm to your company!

32 Inform your supervisors and stay calm!

# How is ransomware doing?

Cumulative Victims per Month (2023–2025)



... It's a good business to be in

## A recent incident...

---

*“At £1.9 billion of financial loss, this incident appears to be the most economically damaging cyber event to hit the UK”*



<https://cybermonitoringcentre.com/2025/10/22/cyber-monitoring-centre-statement-on-the-jaguar-land-rovercyber-incident-october-2025/>

# Factor Three: Counterparties and suppliers







## According to a recent ECB reports of the 109 SIs surveyed....



17,051 service providers were identified, of which 5,929 supported critical functions and 4,747 were external providers

57

Average number of external providers of critical functions per SI  
(minimum of one, maximum of 936)

98

Average number of contracts with external providers for critical functions  
(minimum of two, max 1,512 contracts)

[https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.outsourcing\\_horizontal\\_analysis\\_202402~2b85022be5.en.pdf](https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.outsourcing_horizontal_analysis_202402~2b85022be5.en.pdf)

## Additional insights

Of the 109 Sis surveyed..

88

Outsource payment services

102

Outsource ICT Services (not cloud)

Critical and external contracts that

Support time-critical operations

51%

Are either impossible to reintegrate or substitute.

25%

## Or, to put it another way

---

**€25.1 Billion**

**(the total) budget for critical external  
service providers.**

## And across Europe more widely....

---

**15,000**

ICT Third Party Providers directly serve **1,600** EU financial entities

**9,000** ICT Third Party Providers supported critical or important functions

[https://www.esma.europa.eu/sites/default/files/2023-09/ESA\\_2023\\_22\\_-\\_ESAs\\_report\\_on\\_the\\_landscape\\_of\\_ICT\\_TPPs.pdf](https://www.esma.europa.eu/sites/default/files/2023-09/ESA_2023_22_-_ESAs_report_on_the_landscape_of_ICT_TPPs.pdf)



**So, considering everything we have just covered...**

**do we need a new approach?**

# The proposed solution

*Community-driven outsourced risk management is a collaborative approach where a community, rather than single entities, take an active role in identifying and assessing issues that can introduce risk.*

*The core idea is to leverage the collective knowledge, expertise, and resources of a group of organizations rather than individual organisations.*



Or, to put it another way

Assessed once, leveraged by many.



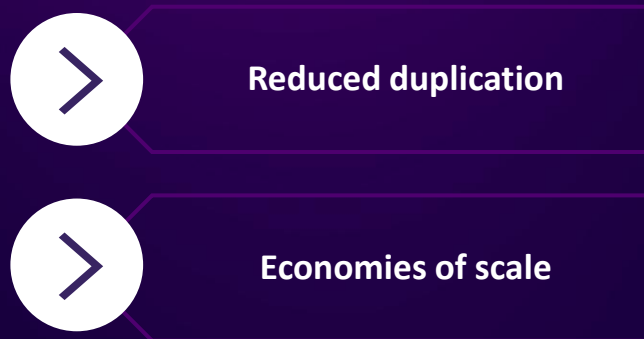
# Benefits of a community led approach

---

## Increased effectiveness



## Increased efficiency



[An example of a community in operation?](#)

## Existing community driven approaches to risk management



Limitations :

SWIFT network users.

Assessment of the SWIFT infrastructure.

Automotive Industry.

Leverages ISO27001

Geographic.

Only useful for financial entities in a supply chain.

No certification for compliance.

# But it's not that simple...

# An extra consideration

- Who might want to attack your organisation?
- How might they do it?
- Which attacks are most relevant to your organisation?
- Which attacks will cause the biggest impact?



# Effective cyber security in three statements

---

The “What”

The “So what”

The “Now  
what”

# A recent case study

# Marks and Spencer's

Who

- A FTSE 100 retailer.

What

- Ransomware incident.

When

- Initial incident on 19<sup>th</sup> April 2025.

Where


- Impacted major parts of the business, front and back office.

How

- Potentially via a trusted third party.






The logo consists of the letters 'M&S' in a large, black, serif font, set against a white rectangular background.

M&S

EST. 1884

A close-up of Frodo Baggins from 'The Lord of the Rings: The Two Towers', looking distressed with a tearful expression.

**There is some good  
in this world, Mr. Frodo.  
And it's worth fighting for.**

# Final thoughts

# Key questions

---

1. Are financial services similar enough to be targeted by the same threat actors?
2. Do the control requirements vary significantly for each individual financial entity?
3. Does every organisation need a different control assessment methodology to assess operational resilience?
4. Is there a need for every entity in the value chain or the suppliers to send/ complete different questionnaires for operational resilience?



## To succeed, any assessments:

- Must be detailed
- Based on threat intelligence
- Conducted in a way that can be shared.

# Conclusion

---

Businesses demand new technology, but to do so securely requires an understanding of the threats facing organisations, and appropriately robust assurance. The current approach of individual assessments is unsustainable:

Organisations are facing the same challenges.

This is not a technology problem, and technology alone will not solve this.

A community led approach built on strong relationships and based on trust will.

# Thank You



Thomas  
Murray

Cyber Risk

For more information:

Ed Starkie

[estarkie@thomasmurray.com](mailto:estarkie@thomasmurray.com)

Disclaimer: This proposal is meant for discussion only and should not be treated as a final contract. If you agree with the contents of this draft and non-binding offer, especially the proposed scope of service and the fees for the services, we will complete our internal due diligence checks and then send you a binding offer incorporating changes and amendments we agree, including our General Terms and Conditions to validly engage us.

# Example of key controls

---



## Technical

- Multi-factor authentication
- Endpoint Detection and Response
- Patching and vulnerability Management
- Encryption, rest, transit, use
- Segmentation of networks



## Human

- Engaging and topical training
- Policies, procedures (SoPs)
- 4eyes
- Employee vetting



## Information Sharing

- Latest tactics, techniques and procedures (TTPs)
- Within an organisation, industry, or wider body of trust.
- Ability to ingest, information as well as share appropriately.