Recap of: Defending Your Data

Thank you for attending!

From Prevention to Resilience

The core message from the session was a necessary shift in thinking:

> ***Security is no longer just about stopping attacks, it's about remaining operational when they happen***

From Syscomm's experience across 200+ ransomware recoveries:

-Every organisation had security controls in place

-Attacks still succeeded due to gaps (configuration, visibility, process)

-Average recovery time was 9 weeks

The reality is clear: You cannot rely on prevention alone, resilience is now critical to survival.

Why Syscomm Took a Different Approach

As explained by Chris Tyler, Syscomm's decision to adopt FlashSystem internally was not theoretical, it was driven by real-world experience.

Unlike many MSPs, Syscomm does not simply resell or host platforms based on cost or vendor alignment.
We design and operate infrastructure based on one principle:

> ***Would we trust this to recover our own business?***

That has led to a number of key differentiators:

-We use the same platforms we recommend

-Resilience is engineered into the core, not bolted on

-We design for failure scenarios, not steady-state operation

-We maintain control of the platform

-We prioritise recovery speed and certainty

IBM FlashSystem – Built for Cyber Resilience

Protect: Quantum-safe encryption & Immutable, tamper-proof snapshots

Detect: AI-driven anomaly detection at disk level (100% data inspection) & Detection in seconds, not days

Recover: Known clean recovery points & Recovery capability measured in seconds

This is about minimising impact, not just trying to stop it.

The Cyber Landscape - IBM Perspective

Neil McGovern reinforced the scale of the risk:

95% likelihood of a cyber incident within 3 years

94% of backups are targeted during attacks

Average financial impact in the millions, often far higher when reputation is considered

The key issue: Traditional disaster recovery was never designed for cyber events.

"This is the difference between weeks of disruption and a controlled, rapid recovery"

The live demonstration showed:

Ransomware detection within seconds	Automatic preservation of clean recovery points	Instant restoration of systems from immutable snapshots

Alongside the demonstration, the day featured a range of other highlights, including the Ferrari driving simulator, 360° theatre experiance and a tour of the IBM innovation studio.

Key Risks Identified Across IBM and Syscomm insights:

NO IMMUTABILITY
Backups without immutability are routinely compromised.

SLOW RECOVERY
Recovery processes **are rarely tested** under real **conditions.**

EXPOSED STORAGE
Storage platforms are often accessible to **attackers.**

FALSE SECURITY
Cloud environments are assumed secure without validation.

Final Thoughts

The organisations that recover successfully are not those with the most tools but those with proven, tested, and controlled recovery capability.

If you would like to review your current position, validate your platform, or explore how this approach could apply to your environment, get in touch with the team today!

A Critical Challenge to Consider

One of the most important messages from the session was this:

If you are using a cloud provider or MSP, you must ask:

- What platform is my data actually sitting on?
- Are backups immutable, or can they be deleted?
- How quickly can I recover and has it been tested?
- Is detection happening at the right layer, or only after impact?
- Who is responsible when recovery fails?

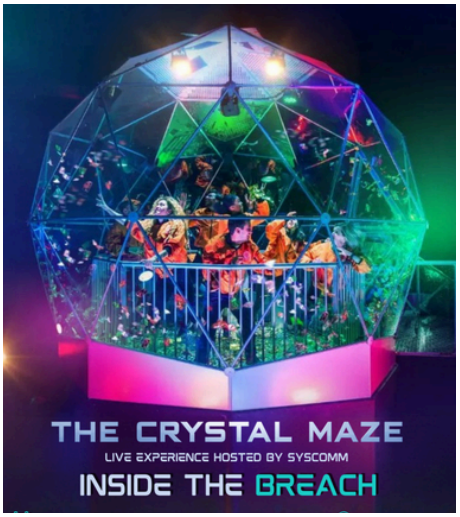
Because the reality we continue to see is: Data hosted in cloud or MSP environments is still being encrypted, deleted, and unrecoverable. There is often a false assumption of resilience simply because the infrastructure is outsourced.

Recommended Next Steps

To assess your own position:

- Complete the Cyber Resilience Assessment
  Identify critical systems and minimum viable operations
- Validate recovery capability (not just backup presence)
- Test recovery under realistic conditions
- Review whether your current platform genuinely supports resilience

Scan for assessment



Enjoyed this Event? Don't Miss Our Next One.

Our upcoming event at the Crystal Maze Experience in London takes things up a level, giving you rare, behind-the-scenes insight into how cyber breaches actually happen not just in theory, but in practice. Expect an immersive experience that brings real-world attack scenarios to life, showing where organisations are most vulnerable and how to stay resilient when it matters most. For more information visit our Events page at www.syscomm.co.uk