



**ORPHEUS**

Predict. Act. Prevent.

# Concentration Risk and The Evolution of Third-Party Cyber Risk Management

 **UK  
CYBERWEEK**  
EXPO & CONFERENCE  
23-24 APRIL 2025 OLYMPIA LONDON

Stuart Barnett - Director Cyber Threat Intelligence

[sales@orpheus-cyber.com](mailto:sales@orpheus-cyber.com)

# What's at Stake?

- **Third Party Cyber Risk Management and Concentration Risk** – why over-reliance on a single vendor, region, or technology creates systemic vulnerability.
- **The Real Cost of Third-Party Breaches** – lessons learned from recent incidents.
- **The Regulatory Shift** – how DORA, NIST, and other frameworks are redefining third-party risk management.
- **Why continuous third-party risk monitoring is no longer optional** – it's essential.

# Orpheus: Intelligence that Powers Security & Resilience



- **Accredited** → One of only six companies accredited for Cyber Threat Intelligence by both the FCA & Bank of England.
- **Predictive** → Deploying Machine Learning & AI for predictive risk insights. Insurance sector proof of predicting claims.
- **Technical Innovation** → UK Ministry of Defence proving 94% accuracy in predicting future exploitation of vulnerabilities.
- **Actionable** → Monitoring the attack surface of companies and prioritizing issues based on intelligence, which drives action.
- **Trusted by Global Organisations** → Supporting financial services, critical national infrastructure, and regulated industries.



# July 2024

## Were you ready?

- Major IT incident as a result of a faulty configuration update
- 8.5 million systems affected worldwide
- Significant disruption across multiple sectors
- Extraordinary financial losses estimates - US\$10 billion

# Third Party Cyber Risk

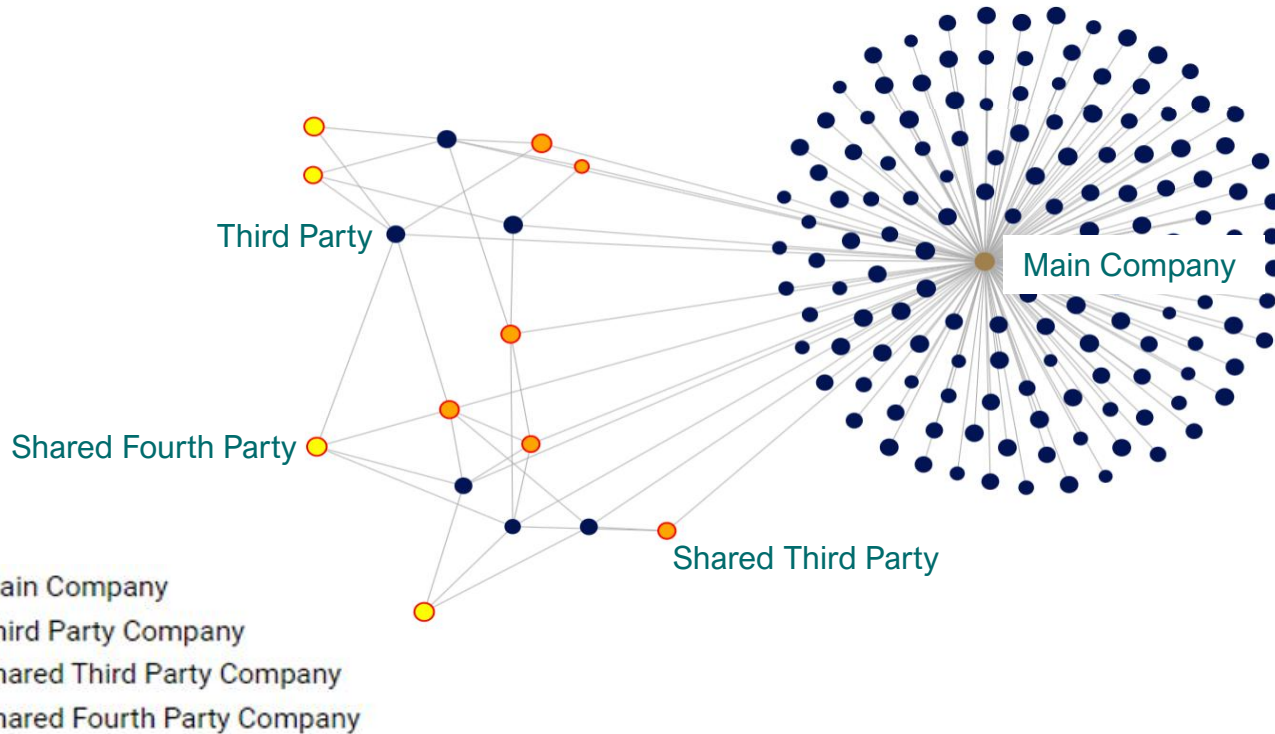
## The Perils of Over-Reliance

Diversification is no longer optional  
– it's a resilience strategy



- **Supply chains are designed for efficiency** but efficiency often comes at the cost of resilience.
- **What is Concentration risk?** Over-reliance on certain critical vendors or suppliers. Systemic vulnerabilities.
- **Why is this a problem?** Lack of diversification in critical vendors and/or suppliers leaves organisations more vulnerable to disruption, failures or targeted attacks.
- **Increasing regulatory requirements** surrounding third party cyber risk management and critical service providers.
- **A strategic business risk** not just a cyber security issue. Third party and concentration risks affect business resilience and continuity.

# Concentration Risk Example



# The Real Costs of Third-Party Breaches

**CHANGE**  
HEALTHCARE



## Financial Impact

- Direct losses - Fraud, ransomware payment, theft of funds
- Regulatory fines
- Legal fees
- Incident response costs
- Increased insurance premiums
- Restorative cyber security enhancements

**Progress**® MOVEit®



## Operational Disruption

- Downtime and business interruption
- Incident response & recovery
- Reliance on 3<sup>rd</sup> Party on restoration of services
- Loss of intellectual property via a 3<sup>rd</sup> Party and subsequent competitive advantage

solarwinds



## Reputational Damage

- Customer trust
- Brand damage
- Stock price impact
- Loss of business
- Increased compliance burdens and focus



# Orpheus Insights: Navigating the Regulatory Shift

- **Proactive and collaborative approaches** are being actively encouraged.
- Requirement for **continuous oversight** and real-time monitoring.
- **Critical service providers** have greater scrutiny.
- **Threat led penetration testing frameworks** have increasing consideration of third-party elements and concentration risk.
- Highly regulated industries require **diversification strategies** for risk mitigation.

# Continuous Monitoring Isn't Optional

Cyber threats move fast. Periodic assessments won't keep up.

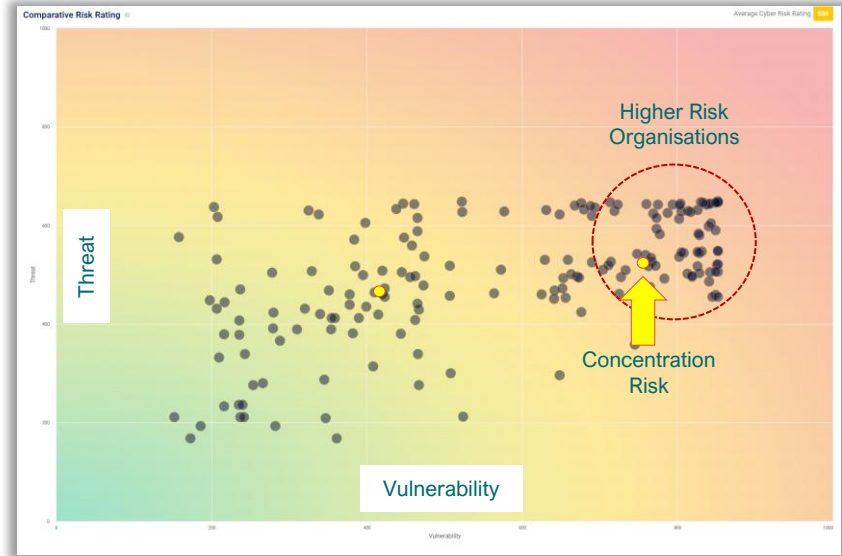
- **Detect vulnerabilities before they're exploited within your third parties.**  
New vulnerabilities emerge daily. Static assessments don't capture real-time threats.
- **Prioritise critical risks in the third-party ecosystem.**  
Regulatory pressure demands ongoing oversight; not just a once-a-year audit.
- **Provide actionable insights that allow security teams to mitigate threats proactively.**  
Threat actors exploit blind spots; if you're not continuously monitoring third-party risk, you're operating in the dark.
- **Leverage third party monitoring platforms and expertise.**  
Mapping third parties and identifying concentration risk can be difficult.

# Resilience Starts Here:

## Lead with Orpheus

- Understand your 3rd party risks - map your suppliers and assess threat and vulnerability.
- Assess, identify and mitigate concentration risk - build resilience through diversification.
- Monitor how this risk (threat and vulnerability) changes over time.

What is the cyber risk across my Third Parties?



How does the cyber risk change over time?



# Orpheus: Your Cyber Risk Command Centre

Orpheus gives you the visibility, context and prioritisation to stay ahead of threats:

- **Adopt a proactive compliance mindset** - Regulation through mechanisms such as DORA, NIST, and UK legislation rules are only getting stricter.
- **Move beyond one-off assessments** - continuous third-party risk monitoring is essential. Platforms such as Orpheus can map your Organisations supply chain, identify 'concentration risk' and help you manage 3<sup>rd</sup> party risk.



**TAKE CONTROL. PROTECT  
YOUR CRITICAL ASSETS AND  
THIRD-PARTY SUPPLY CHAIN.**



Request a  
Third-Party  
Risk  
Assessment



Contact  
our Lead  
team

**Thank you**  
Any questions?



**ORPHEUS**

CONTACT US:

[stuart.barnett@orpheus-cyber.com](mailto:stuart.barnett@orpheus-cyber.com)

[orpheus-cyber.com](http://orpheus-cyber.com)

