



ORPHEUS

Hidden Dependencies

Supply-chain cyber risk across
healthcare and the public sector

Tim West
Director of Intelligence Services

The Shift

Cyber risk now moves across organisational boundaries

- ❑ Digital transformation expands the attack surface exponentially
- ❑ Suppliers, platforms and cloud services create hidden dependencies
- ❑ A single point of failure can cascade downstream
- ❑ Traditional perimeter controls cannot contain ecosystem risk



Who targets Healthcare?

Shared infrastructure attracts multiple threat actors

State actors

- Strategic disruption and long-term access
- Targeting of research, IP and sensitive patient data
- Pre-positioning within critical national infrastructure
- Exploiting concentration risk in shared providers

Cybercriminals

- Financial gain and data monetisation
- Ransomware targeting operational downtime
- Credential harvesting across healthcare ecosystems
- Leveraging third-party access for lateral movement

Hacktivists

- Ideological disruption and visibility
- DDoS and defacement of public-facing systems
- Targeting policy-sensitive institutions
- Amplifying reputational impact through public exposure

Different motives – Same path

All exploit interconnected digital environments

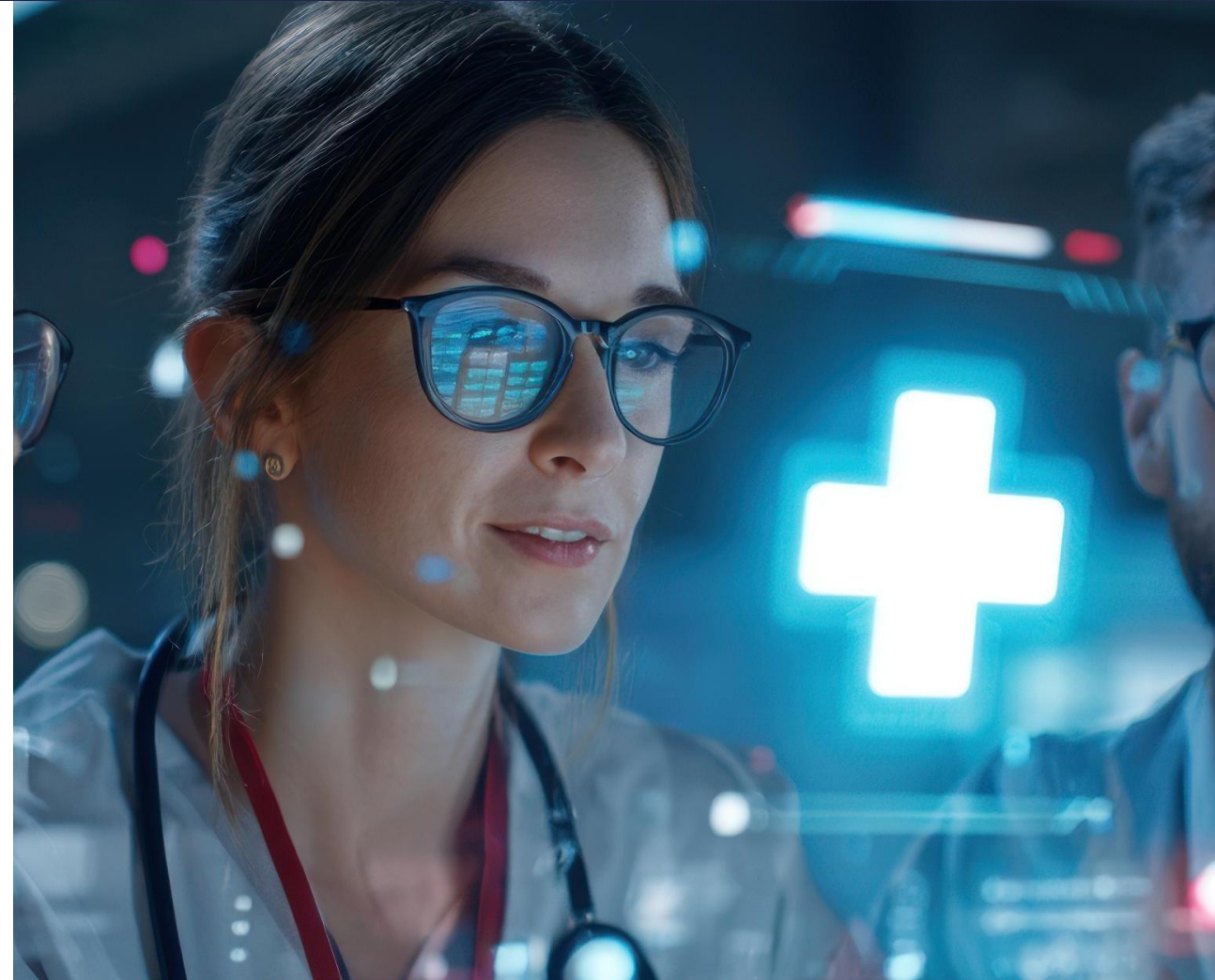
- State actors seek persistent access and strategic positioning
- Cybercriminals pursue scale, monetisation and operational leverage
- Hacktivists aim for visibility and reputational impact
- All move through shared suppliers, identity systems and cloud platforms



Healthcare's risk is systemic

Operational pressure amplifies impact

- Modern healthcare depends on dense, shared digital infrastructure – cloud platforms, diagnostics systems, logistics and outsourced services
- An incident affecting one supplier can cascade across hospitals, GP networks, laboratories and national services
- The impact is not just data loss – it is operational disruption and patient care risk
- Shared platforms create concentration risk. One compromise can affect many organisations at once



The real attack surface is the supply chain

Compromise one supplier, impact many organisations

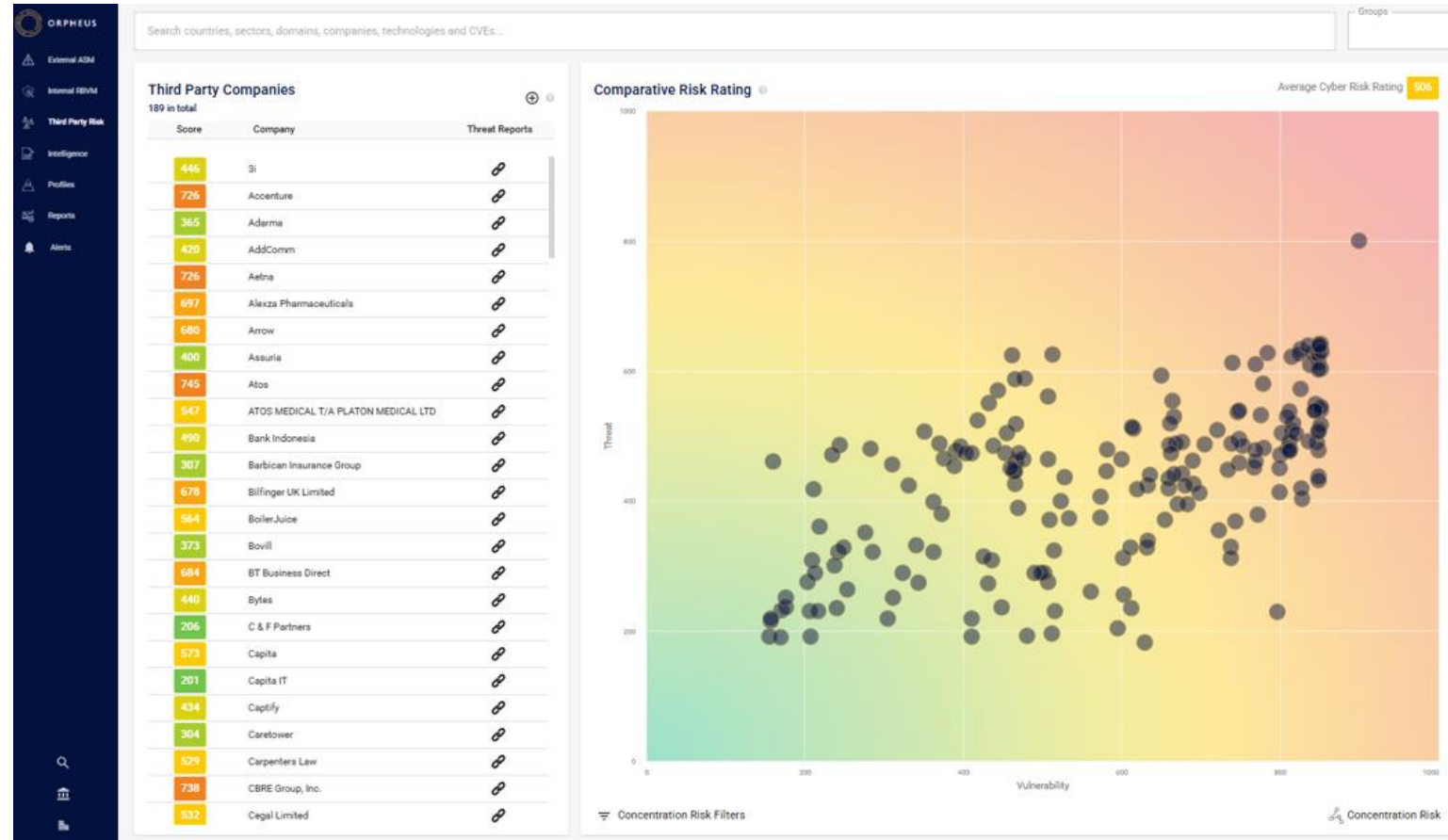
- Healthcare relies on shared suppliers – cloud, diagnostics managed platforms
- Attackers scale by compromising a single provider
- Identity reuse and shared infrastructure amplify impact
- Risk now extends beyond organisational borders



December snapshot – what Orpheus is seeing

Concentration & downstream exposure at scale

- Third-party exposure clustered across shared providers
- Higher vulnerability correlating with higher concentration
- One compromised supplier creating downstream impact
- Systemic exposure visible across the ecosystem



What does this mean for Leadership?

Under the UK Cyber Security and Resilience Act, supply-chain cyber resilience becomes a legal duty – not a discretionary control



Leaders must evidence compliance with the UK Cyber Security and Resilience Act across their supply chains

- Leaders must know which third parties they rely on – and quantify exposure
- Risk now sits beyond internal systems – across shared and regulated infrastructure
- Concentration risk can trigger systemic failure and regulatory intervention
- Governance must be continuous, measurable and defensible – not static and questionnaire-based



ORPHEUS

From visibility to control

Static questionnaires cannot keep pace with a live, interconnected supplier ecosystem

From exposure to strategic control

Real-time control of interconnected supply-chain risk

- Continuous monitoring across third-party ecosystems
- Live attack surface and vulnerability intelligence
- Concentration and systemic risk visibility
- Prioritised remediation aligned to operational impact

ORPHEUS

Company View
RBVM
Portfolio View
Intelligence
Threat Analysis
Profiles
Reports
Alerts

Acme Ltd

Cyber Risk Report | Attack Surface Highlights | Relevant Intelligence Reports

Sectors: Retail
Countries: United Kingdom

Cyber Risk Rating
622 High
Threat Score 394
Vulnerability Score 849

The cyber risk score is made up of distinct threat and vulnerability scores. Orpheus replicates the methods used by threat actors to uncover intelligence that would be useful to malicious parties looking to target Acme Ltd. The scores suggest more of Acme Ltd's cyber risk stems from its vulnerabilities than its threat. As a result, mitigating the vulnerabilities we have identified will have the biggest effect on reducing Acme Ltd's overall risk level. Acme Ltd has a higher risk score than average in its sector. Sector Average 388

Vulnerabilities
849 Very High
The vulnerability score is a comparative score against peers both within sector and globally. This score takes into account a combination of infrastructure and technology, detected known vulnerabilities, and breached credentials. Acme Ltd's score indicates that it is performing worse than 85% of companies currently on record.

Vulnerabilities 243 High Risk 2
We recommend that organisations perform regular software vulnerability assessments across their entire estate, prioritising issues based on CVSS scores, starting with the highest. High risk software vulnerabilities include those known to be exploited, those with a high likelihood of exploitation in the future, and those known to be used by ransomware gangs.

Breached Credentials 7
Breached credentials can be valuable for credential stuffing attacks, and their proportion relative to the total number of employees can serve as an indicator of a company's overall cybersecurity standards. Enforcing multi-factor authentication is recommended to mitigate this risk.

Exposed Remote Access Services 0
It is discouraged to directly expose remote desktop applications and other similar remote access services to the internet. These represent attractive targets for threat actors using breached credentials and brute force attacks.

Attack Surface Size 15
Organisations can mitigate against open port discovery by closing unnecessary services on hosts, and by configuring TCP Wrappers that limit IPs or domains that are allowed to probe or connect to the service. A higher number of distinct services increases the organisation's potential attack surface and therefore increases its chances of being targeted and compromised by threat actors.

Exposed Databases 1
We recommend that organisations find alternative ways to connect to database services and avoid making them publicly accessible. Solutions can include SSH tunneling and port forwarding for users.

Expired Certificates 0
Organisations should implement an SSL certificate lifecycle management process to prevent certificate expiration. To mitigate the risk of expired certificates, organisations should set

Threats
Sector Score 388
Country Score 624
Related Intelligence Reports 94
Recent Dark Web Mentions 552

The threat score is based on intelligence reports written by our expert analysts on an ongoing basis, which provide unique insights into the global threat landscape. This score is calculated from an aggregated severity of intelligence reports that are relevant to Acme Ltd based on threats to its sector, countries of operation and the identified technologies that it operates. Acme Ltd's sector has a threat rating of 388. The countries in which it operates have a combined threat rating of 624. Orpheus has identified a number of deep and dark web discussions that may be relevant to Acme Ltd's brand, products or technologies it operates.

Comparison to similar organisations
Worse Better Similar
Vulnerabilities Email Security Attack Surface Size
Certificate Health Remote Access Breached Credentials

To effectively reduce risk, we recommend starting with the following:

Next Steps

1. Restrict public access to operational technology (OT)
2. Restrict public access to databases
3. Patch high risk vulnerabilities

Thank you
Any questions?

Explore
TPRM



Speak to
Orpheus



ORPHEUS

CONTACT US:

Sales@orpheus-cyber.com

orpheus-cyber.com