Managing Systemic Cyber and Cloud **Outage Risks**

Artex

Events in the first half of 2025, from the Heathrow power outage in March to a series of high-profile ransomware attacks on UK businesses, have highlighted businesses' increasing vulnerability to systemic risks associated with critical infrastructure.

At the Artex Annual Roundtable in December, hosted in association with AIRMIC, Dr Ioannis Agrafiotis of the University of Oxford shared the results of his research into systemic cyber risks. He compared the findings with real-world scenarios and shared insights on strengthening businesses' resilience to cloud and software provider outages.

Alongside the Global Cyber Security Capacity Centre at Oxford, simulations were run over a six-year period covering cyber attacks and supplier failures within digital ecosystems.

The team based their simulations on three key assumptions:

- Key suppliers whose services were core to the business operations of multiple organisations and whose failure could represent a systemic risk for clients;
- Businesses' level of dependency on specific technologies such as cloud platforms and ISPs; and
- Widespread dependency among organisations on the same software solutions.

Two specific series of simulations were developed:

- The first, based on a '**Predator-Prey**' model, created a dynamic environment involving populations of cyber criminals (Predators) and target companies (Prey).
- The second simulation modelled the **impact of services failures among cloud service providers (CSPs),** with reference to three tiers of organisations: the 'big three CSPs' (AWS, Azure and GCP); resellers, such as managing service providers; and corporate and SME organisations using both services.

LESSONS LEARNED

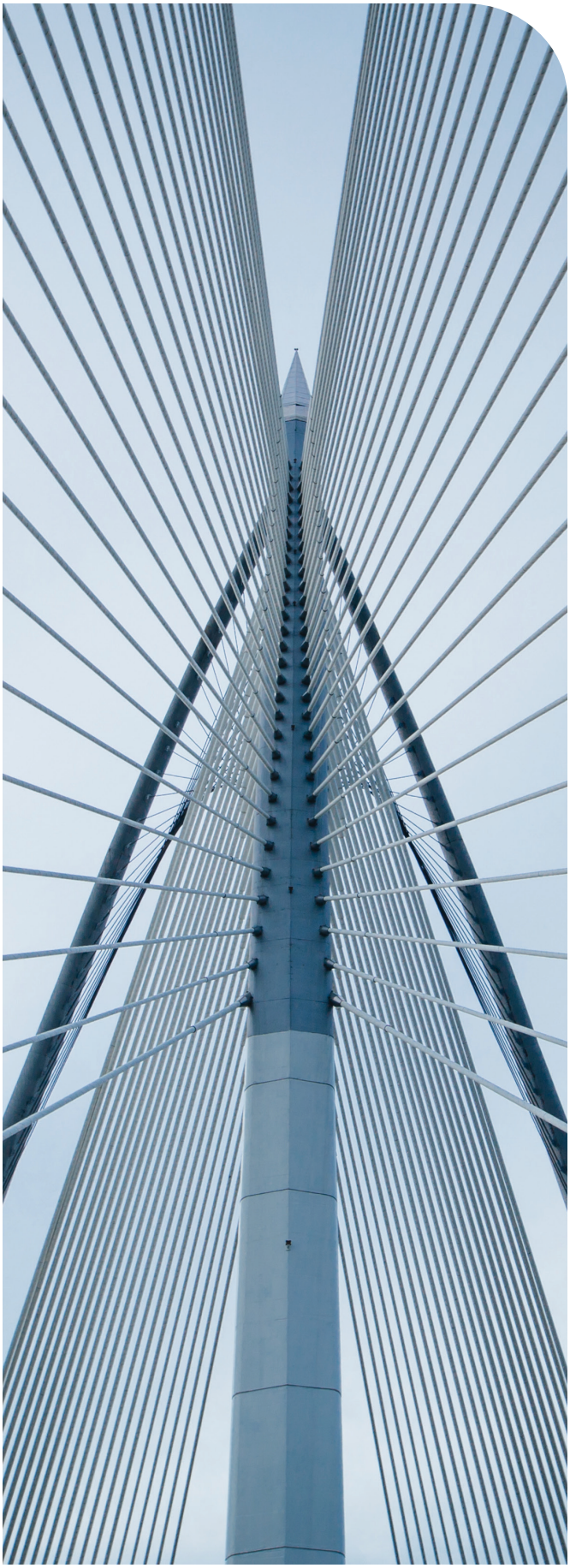
One of the key lessons for risk managers and cybersecurity professionals from the **Predator/Prey simulations** was that the most significant 'black swan' cyber events were commonly due to a single point of failure, where the vulnerability was exploited by attackers prior to software patching.

The simulations also revealed that systemic risk was increased by:

- More sophisticated threat actors
- Weak defensive practices among target companies
- The willingness of insureds to pay ransoms
- Insureds' reluctance to share data on common vulnerabilities and improve cyber hygiene

In the **cloud service simulations,** researchers found that increasing the number of connections between tiers increased the impact of systemic failure from the outage of a single CSP. The impact also worsened significantly with an increase in 'cyclic' connections — where CSP users provide CSPs with essential services in return.

The level of harm experienced by cloud service users was influenced by the level of co-dependency among clients, the likelihood of simultaneous failure of multiple service providers, the cyclical connections between the three tiers and whether businesses had redundancy with alternative cloud providers.



SYSTEMIC CYBER RISK OUTLOOK

Following the conclusion of the research project in 2023, two major events caused by single points of failure significantly impacted business operations globally:

- ***July 2024 CrowdStrike software update*** that crashed Microsoft Windows systems; and
- ***Amazon Web Services outage*** in October 2025.

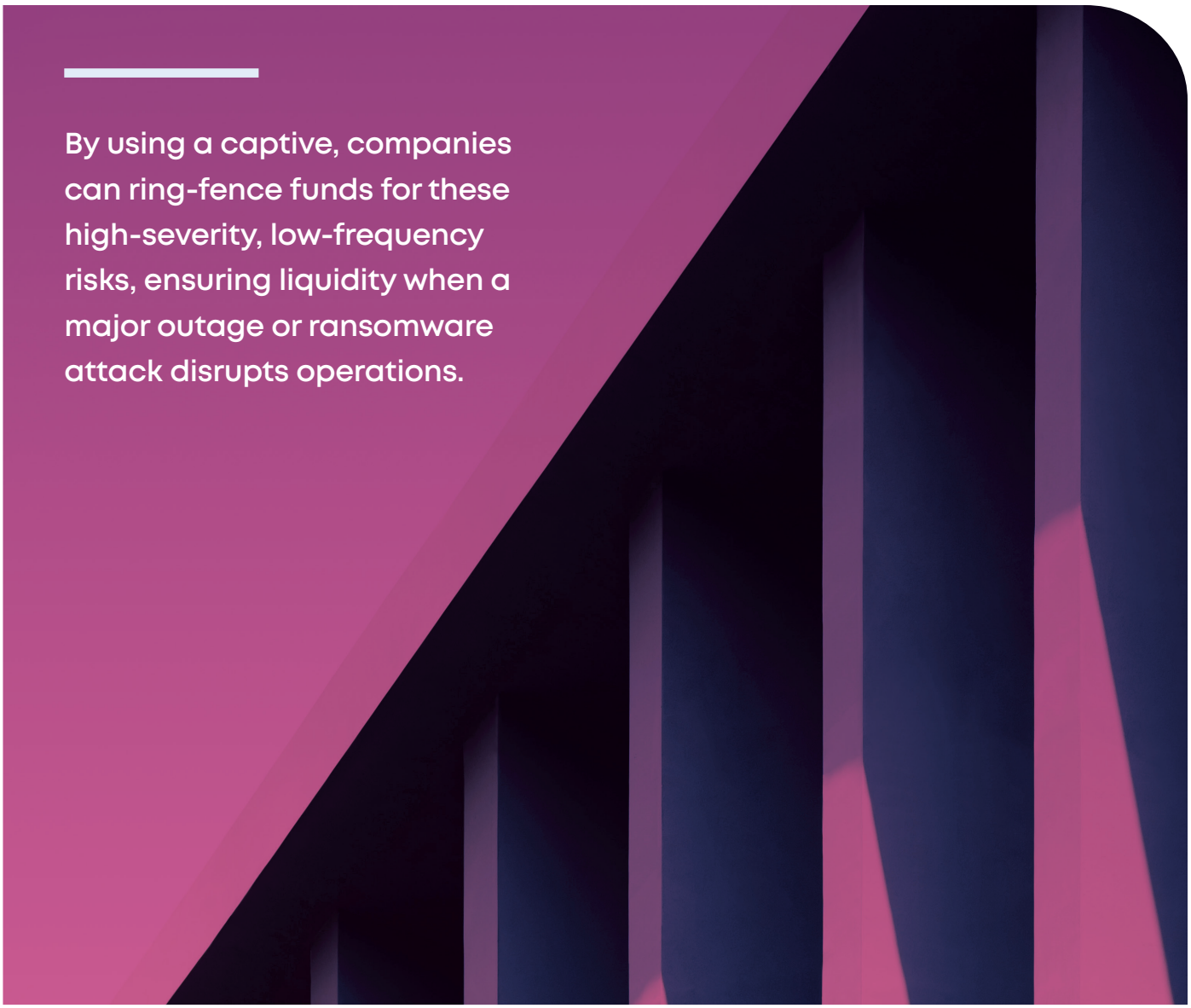
Both events focused minds in the risk management and cybersecurity communities on potential exposures in businesses' digital supply chains.

Both Dr Agrafiotis' research and these real-life events emphasise the pressing need for businesses and their insurers to have the following:

- Better understanding of core business dependencies within digital supply chains
- Greater visibility of supply chain vulnerabilities
- Knowledge of mitigations that could reduce the impact of supplier outages

They also point to the need for better board-level understanding of potential risks, closer communication between boards and their IT and risk management functions and, where possible, greater sharing of cyberthreat intelligence to reduce the number of businesses disrupted by common vulnerabilities.

The Global Cyber Security Capacity Centre at Oxford focuses its attention now on simulating systemic risk for the AI supply chain, an emerging technology that can significantly alter the risk landscape for organisations.



By using a captive, companies can ring-fence funds for these high-severity, low-frequency risks, ensuring liquidity when a major outage or ransomware attack disrupts operations.

INTEGRATING CAPTIVE INSURANCE INTO CYBER RESILIENCE STRATEGIES

Artex recommends that one way businesses can strengthen their resilience against systemic cyber and cloud outage risks is by leveraging captive insurance structures. Captives allow organisations to retain and finance their own risk, providing flexibility to design bespoke coverage for exposures that may be difficult or costly to insure in the traditional market — such as systemic failures across cloud service providers or cascading cyber events. By using a captive, companies can ring-fence funds for these high-severity, low-frequency risks, ensuring liquidity when a major outage or ransomware attack disrupts operations.

Captives can also serve as a platform for pooling risk across multiple entities within a group or even among industry peers, creating a shared buffer against systemic events. This approach not only improves financial resilience but also incentivises better risk management practices, such as enhanced cyber hygiene and investment in redundancy measures. In addition, captives can be structured to access reinsurance markets, providing an extra layer of protection while maintaining control over coverage terms and claims handling.

At Artex, we believe there is more to alternative risk management. As a trusted leader and provider of diverse (re)insurance and ILS solutions, our global team operates at the intersection of art and science — where creative thinking meets expertise and superior outcomes are made. That's how we're able to fully understand our clients' needs and deliver the most comprehensive solutions available.

Established in more than 35 domiciles internationally, we're here to help you make empowered decisions with confidence, reduce your total cost of risk and improve your return on capital. At Artex, we believe in finding you a better way.

Artex

artexinfo@artexrisk.com
+1 630 694 5050
artexrisk.com