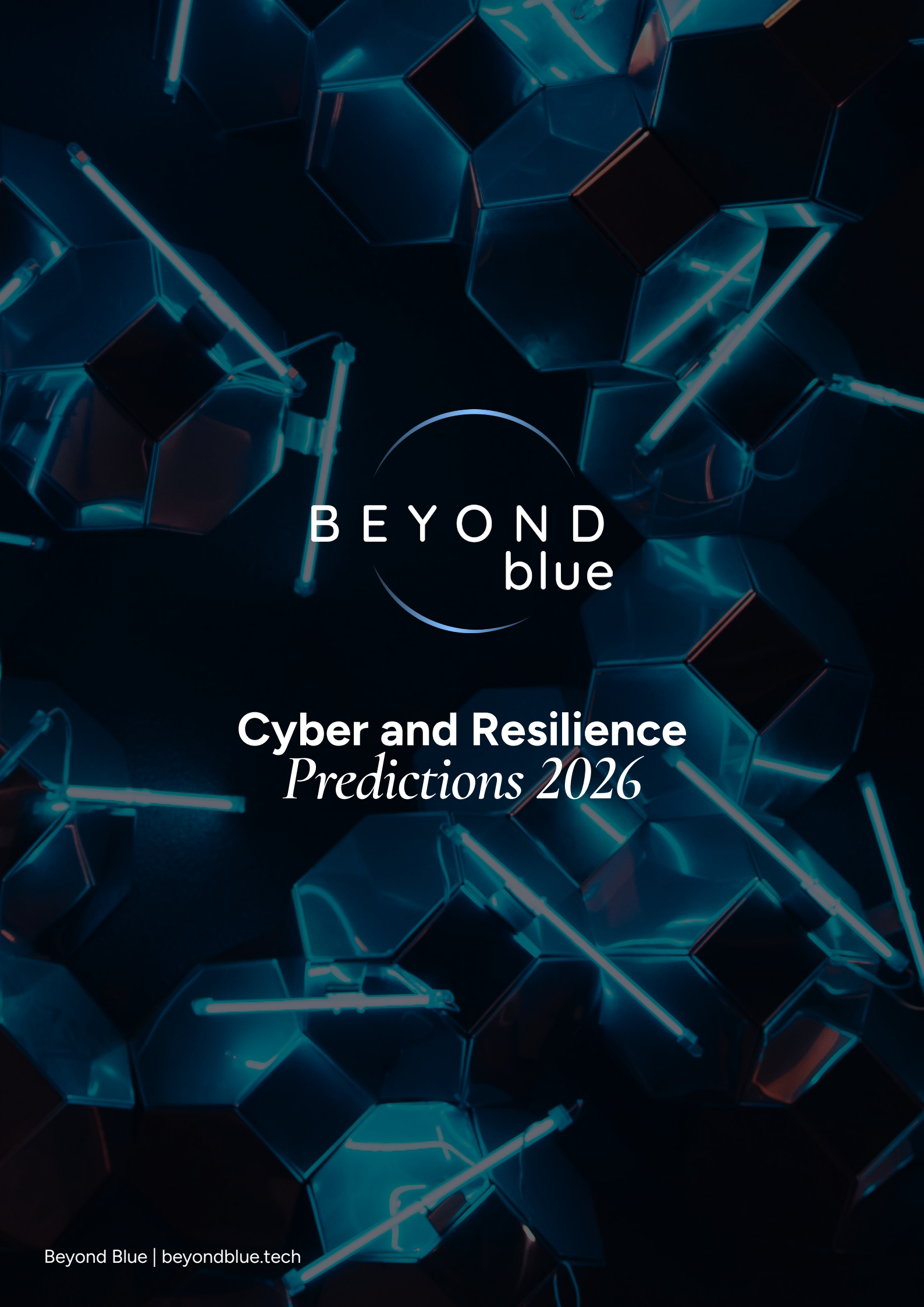
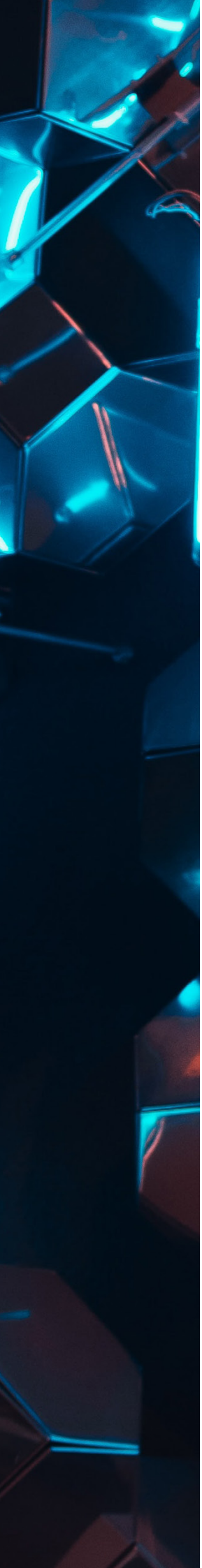


Cyber and Resilience
Predictions 2026



It's that time of year again, when the cyber and resilience community dust off their crystal ball and forecast what may lie ahead for the industry in the year ahead.

But before we look to the future, what lessons can be learned from the past?

If 2025 taught us anything, it's that the attack landscape is evolving with a complex mix of state and non-state attackers causing security and economic disruption.

The perimeters of our organisations are more secure - but this means attacker tactics are changing.

Supply chain attacks have been in ascendancy for a while, but now so too is sophisticated social engineering of IT help desks and service providers. There is also a disturbing move towards overseas cyber criminals recruiting insiders to gain access to organisations, or in the case of North Korea placing IT workers directly inside target firms.

This year, the UK witnessed its largest cyber event in history, which rippled from a major automotive manufacturer across to small family owned businesses, putting their welfare and future at risk. It was an event few will forget, with the UK's economy projected to suffer a £2 billion loss, and the government stepping in to protect thousands of small businesses, who were at risk of collapse after Jaguar Land Rover's production lines were temporarily halted.

The attack landscape also diversified, with Western groups, like Scattered Spider, being responsible for the most publicised incidents. While Russian actors exploited Zero Day flaws to attack major institutions and put their sensitive data at risk. This happened in parallel with threat actors more frequently turning to AI and insiders to speed up their exploits and execute larger-scale attacks.

But technology failures weren't limited to malicious activity.

2025 was also the year of surprising dependencies.

It was a year when the Iberian power grid collapsed plunging Spain and Portugal into darkness, while a failure of a single high voltage transformer bushing at North Hyde substation closed the UK's busiest airport for a day. AWS and Microsoft also had cloud outages, which unearthed surprising consequences and dependencies.

All of these very different events underlined the interconnectedness of our modern world - and perhaps it's fragility too.

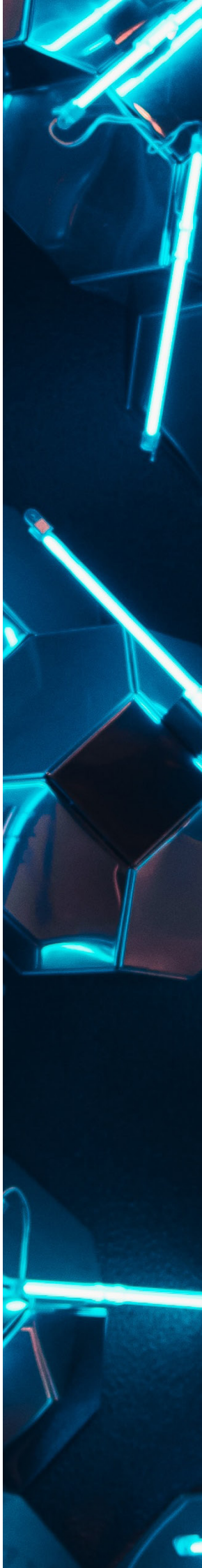
These events also reinforce that resilience will be the theme for 2026, perhaps demanding greater regulatory attention than our historic focus on privacy and confidentiality.

The government released its own government resilience action plan last year - but hidden in there are hard (and unfunded) choices over how we reengineer our national infrastructure to be more resilient. Expect more of these disruptions in 2026... and resilience to stay on the national agenda.

But this requires security and digital teams to work more closely with business continuity and safety professions to achieve a more holistic approach to resilience – and to be ready to exercise and test how effective that approach really is.

Perhaps we ought to stop thinking of the traditional triad of Confidential, Integrity and Availability - and start thinking about a new trinity of Security, Safety and Resilience.

So, how can the events of the last twelve months prepare us for the future? **Here are Beyond Blue's predictions for 2026...**



Regulatory compliance will advance, but resilience oversight will remain a challenge

The Cyber Security and Resilience Bill (CSRB) will work its way through parliament and a ban on ransomware payments for critical infrastructure providers could be introduced as well.

However, as a bill there is much on cyber security in the CSRB, but rather less on resilience.

The EU is pressing on with its Critical Entities Resilience Directive, which is designed to improve the resilience of key services and isn't confined only to digital, but we don't have a comparable framework in the UK. Perhaps we should?

It will be interesting to see how the government navigates this challenge.

Managed Service Providers can expect much greater attention from regulators, and their clients that qualify as Operators of Essential Services.

However, we really do need a better approach to providing independent assurance of the resilience of these providers, otherwise, we risk overlapping regulations and many hundreds of clients demanding evidence and assurance from them in different ways and at different times.

Another key issue for regulation is effective supervision and enforcement. This will be hard to achieve, placing some challenging demands on information commissioner John Edwards and his ICO team.

Geopolitics will drive a new era of information warfare

Geopolitics will remain febrile in 2026 - while we hope for peace in Ukraine - it seems likely that tensions between Russia and the West will continue to escalate and hybrid warfare will result in targeted attacks against the UK aimed at testing resolve, probing defences and disrupting support to Ukraine.

We can also expect US-Chinese tensions to impact supply chains and drive a scale up of cyber operations for economic gain.

Many European nations, particularly to the East, are increasingly concerned over Foreign Information Manipulation and Interference – FIMI.

We see more and more examples of attempts to sway public opinion, tilt elections, and sow discord by adversarial states. The scale and sophistication of these influence campaigns is growing using increasingly persuasive deep fakes. This will be the year where many lose the ability to differentiate truth from AI created fiction.

In the polarised and distrustful world of 2026 we will see examples of just how disruptive FIMI can be.

Minimum Viable Service (MVS) will become a strategic priority

Digital outages, whether innocent or malicious, are becoming more frequent in the interconnected digital world and we can expect these events to continue in 2026.

Organisations must accept these failures will happen, so the priority must shift from avoiding them entirely, to surviving through them.

Organisations must consider how they can restore a minimum level of service even when these outages occur.

It's not possible to make everything completely resilient, so organisations should focus on having the ability to bring up some of their core capabilities to keep them operational and protect their liquidity, customers and supply chain.

But it is vital they can do this securely.

Supply chain instability will continue to be a major concern

The events of 2025 made it clear that supply chains, both digital and physical, are far more brittle than organisations ever assumed.

Incidents, such as the Jaguar Land Rover shutdown, created a cascade of logistical failures because its suppliers had optimised themselves so tightly around just-in-time manufacturing that the shutdown severely impacted their own operations and liquidity.

Similarly, the AWS outage caught out many organisations that did not even realise they were dependent on the platform due to the complex layering of modern digital infrastructure.

Furthermore, the retail cyber attacks demonstrated how a single point of failure could affect something as basic as food supplies in remote regions, like the Outer Hebrides.

These examples showed how the risks with convoluted supply chains are unpredictable and should never be underestimated.

It's unmistakeable that 2026 will see heightened scrutiny of supply chains, with regulators, such as the Financial Conduct Authority, already making significant efforts to strengthen security and availability of Critical Third Parties to the UK's banking and finance industry.

AI will transform state and criminal cyber threats

Of course, no prediction would be complete without speculation over AI.

We will see AI find its role in transforming both state and criminal cyber threats.

Expect far more effective AI enabled social engineering, more effective targeting of vulnerable firms and more creative AI enabled exploitation of stolen data. Rapid and often shadow adoption of AI will find sensitive client data appearing in all too many large language models.

Improving the governance around AI (and managing the use of shadow AI within firms) will be on the agenda for many, although regulation in this space will be complicated by geopolitics. Expect ethical debates on the application of AI to lag technology development as society tries to play catch up and entrepreneurs' race ahead with highly leveraged investment.

These are Beyond Blue's cyber and resilience predictions for 2026.

The world of 2026 is *uncertain, messy and complex.*

Cyber resilience in the brave new world **isn't just about cyber security.**

It's about *organisations, people* and our *democratic societies* surviving in the face of changing threats and geopolitics.

Thank You