RACHEL HAYES
PARTNER
Technology

Cybersecurity: the biggest business risk

The biggest perceived technology risk for Irish businesses remains cybersecurity and the related data protection liability exposure. Only 17% of businesses feel very or extremely confident that their cybersecurity posture is keeping pace with AI-driven threats and, worryingly, 20% report no confidence at all. There is also a clear gap between the AI-driven threats that have started to emerge across European markets and the cyber resilience of most Irish businesses.

That concern sits within a hardening regulatory framework in an effort to tackle it. NIS 2 imposes enforceable cyber resilience obligations on a substantially expanded set of entities and their supply chains, with personal liability exposure for senior management that has reset how many boards now think about their own role in oversight. DORA places parallel operational resilience obligations on financial services firms and brings their critical ICT third-party providers within the scope of the European competent authorities. Cybersecurity has ceased to be a discretionary technology investment. It is a legal obligation to ensure baseline operational resilience across EU organisations, making the consequences for non-compliance an increasing board agenda item.

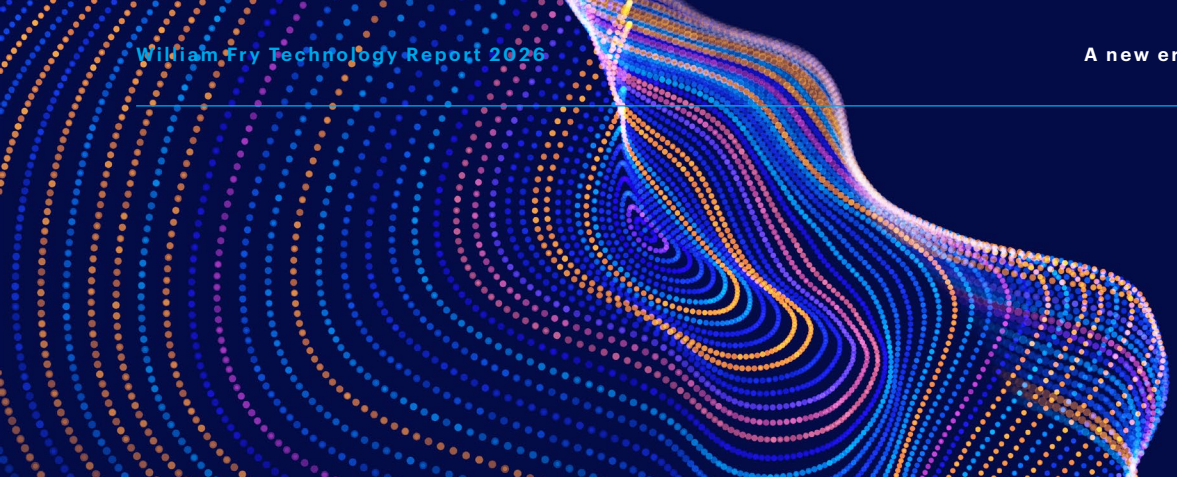
Recent events have reinforced this posture at national level. Over the past five years, Ireland has experienced a significant increase in cyber incidents, including the Health Service Executive ransomware attack in 2021. This landscape has emerged alongside a wave of AI-driven threats and geo-political rivalries including advanced phishing, social engineering and ransomware attacks. Officials at the Irish National Cyber Security Centre have warned that the malevolent use of advanced AI through state-linked tools could enable widespread automated attacks at scale. Reports earlier this year of Anthropic's Mythos model being used to power autonomous cyber operations have reinforced the wider concern that offensive capability is outpacing defensive maturity in many nation states (including, Ireland) and, as a result, organisations.

Thomas Kinsella of Tines frames these cybersecurity concerns into the practical operational response that boards now need to put in place:

> *You can significantly mitigate cybersecurity risk by implementing smart guardrails, using the principle of least privilege and pursuing a reasonable approach with smart automation platforms. You should not be giving AI access to your entire CRM, or everything in your AWS account. Allowing AI to make recommendations, suggest actions and possibly take some non-destructive actions is very safe, and with the right guardrails in place, massively beneficial to almost every company.*
>
> **Thomas Kinsella**, Co-Founder and CCO, Tines

Sasha Rubel of AWS gives context to the same issue more broadly, connecting cybersecurity concerns directly to the wider procurement decision:

> *Issues around cybersecurity and privacy are central when it comes to AI. The question of cybersecurity being a top priority is linked directly to the question of choice of technology - because if you limit choice, you also limit a lot of cybersecurity innovations.*
>
> **Sasha Rubel,** Head of AI and Generative AI Policy, EMEA, Amazon Web Services



The Mythos moment: AI outpacing cyber

The reported capabilities of new models like Anthropic's Mythos will significantly change the cybersecurity dial going forward. Announced by Anthropic on 7 April 2026 and withheld from general release on cybersecurity grounds, Mythos has reportedly identified thousands of high-severity vulnerabilities across every major operating system and web browser. The UK AI Security Institute has independently confirmed that the model can execute multi-stage attacks and discover and exploit vulnerabilities autonomously, completing tasks that would otherwise take human professionals days of work. Critically, Anthropic confirms these capabilities were not the product of dedicated security training but emerged as a downstream consequence of general improvements in code, reasoning and autonomy. This signals that comparable capability will appear across the frontier, including in open-weight releases that cannot be access-controlled.

Measured decision-making needs to prevail in the face of such extraordinary claims, but there is no doubt that models like Mythos, which demonstrate what is possible, could pose problems for organisations. Anthropic has acted responsibly in withholding the model. However, it is only a matter of time before other entities, and perhaps even nation states, make similarly powerful models available to the world at large via open source.

EU rules increasingly seen as a source of certainty and uniformity

The figure that should give the greatest comfort to organisations operating in Ireland and across the EU is that 47% of respondents agree that an EU-wide approach to digital and technology regulation enhances business certainty compared to decentralised regimes in other global markets. The figure is not a majority, but the direction of travel is clear.

The EU's AI Digital Omnibus deal which was provisionally agreed on 7 May 2026 sets to simplify EU Regulation in this area. The Council and Parliament agreed to delay application of the AI Act to 2 December 2027 for Annex III systems (being High-Risk AI Systems) and to 2 August 2028 for AI embedded in regulated products. The Article 50 provision on watermarking on synthetic content now has a grace period of four months now kicking in from 2 December 2026. Interestingly, it was also agreed that the EU AI Act would no longer apply to AI in machinery covered by the EU's machinery regulations, and such AI systems will now be subject to horizontal regulation under their existing rules. The text of the Omnibus remains subject to formal endorsement at the time of writing.

The practical effect for businesses is fixed dates against which to plan procurement, contract renegotiation and compliance investment, with the underlying obligations unchanged in scope. The insight to be gleaned from these changes is that there is a clear intent in Europe to move to a more pro-business and innovation-friendly footing with our regulations.