

The future of cybersecurity in the financial services sector



Cyber threats are greater than ever before. They are impacting all services and all industries, but none quite as much as the financial services sector. As data becomes more accessible and the digital landscape becomes more complex, so too are the threats they face. The financial services sector has a responsibility to safeguard the financial and personal information of its clients and ensure it keeps ahead of evolving threats. Northern Ireland is the fastest-growing region in the UK for financial and related professional services. With cutting-edge research institutions and a strong technology ecosystem, Northern Ireland is well-positioned to help other businesses innovate, adapt, and safeguard digital infrastructure. Invest Northern Ireland's JENNY SANTIAGO YOUNG explains what future cyber threats might look like, and how Northern Ireland can help businesses mitigate risk.

As AI becomes more embedded in infrastructure, securing AI itself is paramount. AI and learning language model (LLM) systems are vulnerable to emerging threats such as Prompt Injection (malicious prompts that manipulate AI behaviour) and Data Poisoning (corrupted training data that skews outputs). Cybersecurity must be integrated throughout the AI lifecycle, from design and development to deployment and maintenance. But there is also an opportunity for AI to be a cybersecurity enabler.

“The launch of the UK’s first Cyber-AI Hub, hosted by CSIT, marks a significant milestone by integrating AI into cyber-defence strategies. This will develop a talent pipeline of AI-cyber professionals and encourage further sectoral development.”

AI enhances cybersecurity by automating threat detection, analysing anomalies, and accelerating incident response. Machine learning algorithms can process vast datasets to identify patterns that signal potential breaches more efficiently than traditional methods. AI systems can detect malicious code, prevent fraud, monitor network behaviour, and generate reports for stakeholders. These capabilities are already being deployed across Northern Ireland’s finance, healthcare, and public service sectors, helping protect critical infrastructure.

Northern Ireland’s cyber security sector generates over £258 million in Gross Value Added (GVA) and supports



Jenny Santiago Young: Northern Ireland is positioning itself as a leader in responsible AI adoption.

more than 2,750 jobs. The region has become a hub for innovation, anchored by institutions like Queen’s University Belfast’s Centre for Secure Information Technologies (CSIT). The launch of the UK’s first Cyber-AI Hub, hosted by CSIT, marks a significant milestone by integrating AI into cyber-defence strategies. This will develop a talent pipeline of AI-cyber professionals and encourage further sectoral development. The Cyber-AI Hub is developing secure data analytics pipelines, robust training paradigms and monitoring systems to ensure AI technologies remain secure, robust and resilient.

Northern Ireland is also investing in the future of cybersecurity and AI capabilities through the £1.3 billion

investment City and Growth Deal projects, supported by Invest Northern Ireland. Initiatives such as Momentum One Zero, the Cognitive Analytics Research Laboratory, and the Artificial Intelligence Collaboration Centre empower businesses to integrate AI into their cybersecurity programmes while safeguarding from emerging vulnerabilities.

“Financial services are increasingly data-driven, and Northern Ireland is positioning itself as a leader in responsible AI adoption. The Artificial Intelligence Collaboration Centre (AICC) is a government-backed initiative, supported by Invest Northern Ireland, is designed to accelerate AI integration across industries, including banking, insurance, and asset management.”

Financial services are increasingly data-driven, and Northern Ireland is positioning itself as a leader in responsible AI adoption. The Artificial Intelligence Collaboration Centre (AICC) is a government-backed initiative, supported by Invest Northern Ireland, is designed to accelerate AI integration across industries, including banking, insurance, and asset management. For FinTechs and established institutions alike, AICC provides hands-on expertise, collaborative R&D opportunities, and a trusted environment for deploying AI responsibly.

In addition to academic and research-led sectoral development, Northern Ireland’s industry experts are leveraging

AI to counter increasingly sophisticated cyber threats. FinTrU, for example, works with the world's largest banks for know-your-customer (KYC) and legal and compliance services. FinTrU has forged ahead with its technology-led solutions by using AI for client lifecycle management and automated extraction of critical business information.

“The financial services sector is becoming more reliant on cloud, edge, and applied AI, but heavy reliance on third-party providers can have severe consequences. This is why third-party management capabilities are critical for mitigating associated risks, such as data privacy reaches, data loss and misconfiguration.”

ISX4, based in Belfast, Newry, Dublin, London, and New York, works with global financial services industry leaders, such as JP Morgan, AIB, HSBC, Bank of Ireland, and Credit Agricole. Its AI agents handle inquiries from both customers and staff, and it can also offer live call scam detection, cloud hosting, and a whole host of AI led solutions.

Third-party risk management and supply chain

The financial services sector is becoming more reliant on cloud, edge, and applied AI, but heavy reliance on third-party providers can have severe consequences. This is why third-party management capabilities are critical for mitigating associated risks, such as data privacy breaches, data loss and misconfiguration.

According to McKinsey's emerging technology in financial services report, third-party and supply chain management were the greatest capability weaknesses for businesses. It's essential that financial services providers can prove to clients that their information is secure through efficient risk management practices. Such practices also empower management to hold third-party providers accountable.

Northern Ireland-based cybersecurity firm Rapid7 partnered with CSIT to advance cloud security using AI and machine learning. Their joint research focuses on identifying active threats in cloud environments, particularly

the exposure of sensitive data. CSIT embedded researchers within Rapid7 to co-develop solutions that enhance threat detection. Raj Samani, Rapid7's Chief Scientist, noted: “This partnership comes at a time when there is a defender advantage surrounding AI. That window will close, so industry-academia collaboration is critical to expedite security advancements.” This collaboration between industry and academia can help financial services businesses stay on top of new cyber threats, enhancing third-party and supply chain risk management.

Regulatory compliance

In an already complicated global regulatory environment, cyber regulation is becoming more complex. Firms need to stay on top of regulatory expectations and demonstrate strategies to adapt to future regulatory changes. Developing cyber risk reporting is key, and building frameworks can encourage a better understanding of areas within digital architecture that are susceptible to risk.

The regulatory technology (RegTech) ecosystem in Northern Ireland is vibrant with a well-connected community and a mix of indigenous and externally owned investors. RegTech companies located in the region, such as Arkk Consulting, Datactics, Funds Axis, Netrio and Pytilia, deliver general compliance, regulatory and compliance management, and regulatory reporting, as well as cyber, identity, and privacy solutions.

Northern Ireland is also home to global financial institutions such as Aflac, Allstate, Citi and Danske Bank, and professional services firms like EY and PwC, that have significant expertise in financial crime. All are developing and delivering compliance solutions for their global networks and the global banking industry in anti-money laundering (AML), fraud detection and counter-terrorism funding regulations.

In addition, the FinTech Corridor and RegTech Supercluster were established as cross-border collaborations to take advantage of the region's expertise in FinTech and RegTech. Northern Ireland's unique location within the UK combines the UK's regulatory framework with close proximity to European and local Irish financial services markets.

Talent management and skills

Not all cyber risks are related to software and technology. One of the

biggest challenges currently being faced by financial services providers is finding the right talent and managing that talent. Northern Ireland aims to expand its cybersecurity workforce to 5,000 professionals by 2030, and AI will play a central role in this. Educational programmes, industry partnerships, and government initiatives are aligning to equip talent with skills to tackle both AI-driven threats and the protection of AI systems.

“Firms need to stay on top of regulatory expectations and demonstrate strategies to adapt to future regulatory changes. Developing cyber risk reporting is key, and building frameworks can encourage a better understanding of areas within digital architecture that are susceptible to risk.”

Northern Ireland's financial services sector is being strengthened by a growing artificial intelligence research capability that brings together expertise in law, finance and technology. Across Ulster University and Queen's University Belfast, centres such as the Centre for Legal Technology, the Finance and Artificial Intelligence Research Lab, and the Centre for Finance and Responsible Technology are shaping how AI is developed and applied across financial and professional services.

These centres help translate cutting-edge AI research into real-world financial services applications — from improving regulatory compliance and risk assessment to supporting innovation in FinTech and legal technology. Their research spans areas such as advanced data analytics, algorithmic decision-making, AI safety, financial risk management, and the responsible use of machine learning and emerging foundation models. Alongside technical innovation, there is a strong emphasis on ethics, accountability and public trust, ensuring AI-enabled services remain fair, explainable and robust.

Recent investments such as Allstate's £16 million commitment to [reskill its workforce](#) in Northern Ireland in areas like cybersecurity, AI, and cloud computing highlight how public-private collaboration is fuelling innovation across the region.

In addition to dedicated Finance and FinTech courses, both Northern Ireland universities offer programs across the full spectrum of cross-cutting skills in areas including Business and Economics; Computer Science; Engineering and Technology; and Law. This supply of skills, combined with a strong talent pipeline in product development and implementation, technology research and development, and regulatory compliance and significant domain expertise in finance, cyber security and legal services, makes NI a compelling location for future investment in financial services.

All you need in one place

Financial services is a highly regulated industry that requires talent with a strong understanding of regulatory standards, technical capabilities within technology and data domains, and business knowledge. Operating costs in Northern Ireland are significantly lower than those in Dublin, and nearly 46,000 people are employed in financial and professional services, supported by strong graduate pipelines from Queen's University Belfast and Ulster University.

Many Irish businesses have already invested in Northern Ireland for its available talent and business ecosystem

“Northern Ireland aims to expand its cybersecurity workforce to 5,000 professionals by 2030, and AI will play a central role in this. Educational programmes, industry partnerships, and government initiatives are aligning to equip talent with skills to tackle both AI-driven threats and the protection of AI systems.”

that combines the essential and evolving skills needed for the financial services sector. For example, Ergo, the Irish IT solutions provider announced a £4.5 million investment to establish a new office in Northern Ireland that will bolster its digital practice, and build out its wider managed services proposition, incorporating IT solutions covering cloud and infrastructure, data and AI, as well as cyber security for organisations across both the public and private sectors. Furthermore, in July last year, ControlSoft Automation

Systems announced it was establishing a software engineering, mechanical and electrical hub in Belfast.

Northern Ireland offers a strategic extension for financial services firms based in Ireland, combining cost efficiency, talent availability, and innovation support within the UK market.

Jenny Santiago Young is Regional Director, Republic of Ireland at Invest Northern Ireland. Invest Northern Ireland's Dublin based team supports Irish-based companies who wish to establish and expand successful operations in Northern Ireland. The team can help with initial fact-finding, bespoke discovery visits, property and talent sourcing, business, and sector network introductions through to tailored packages of financial assistance.

Invest NI can help your company grow in Northern Ireland.

To find out more, visit:

<http://investni.com/financialservices> or contact Jenny Santiago Young: jenny.santiago-young@investni.com or Eoin Storan, Business Development Manager, Invest NI Dublin: Eoin.Storan@investni.com