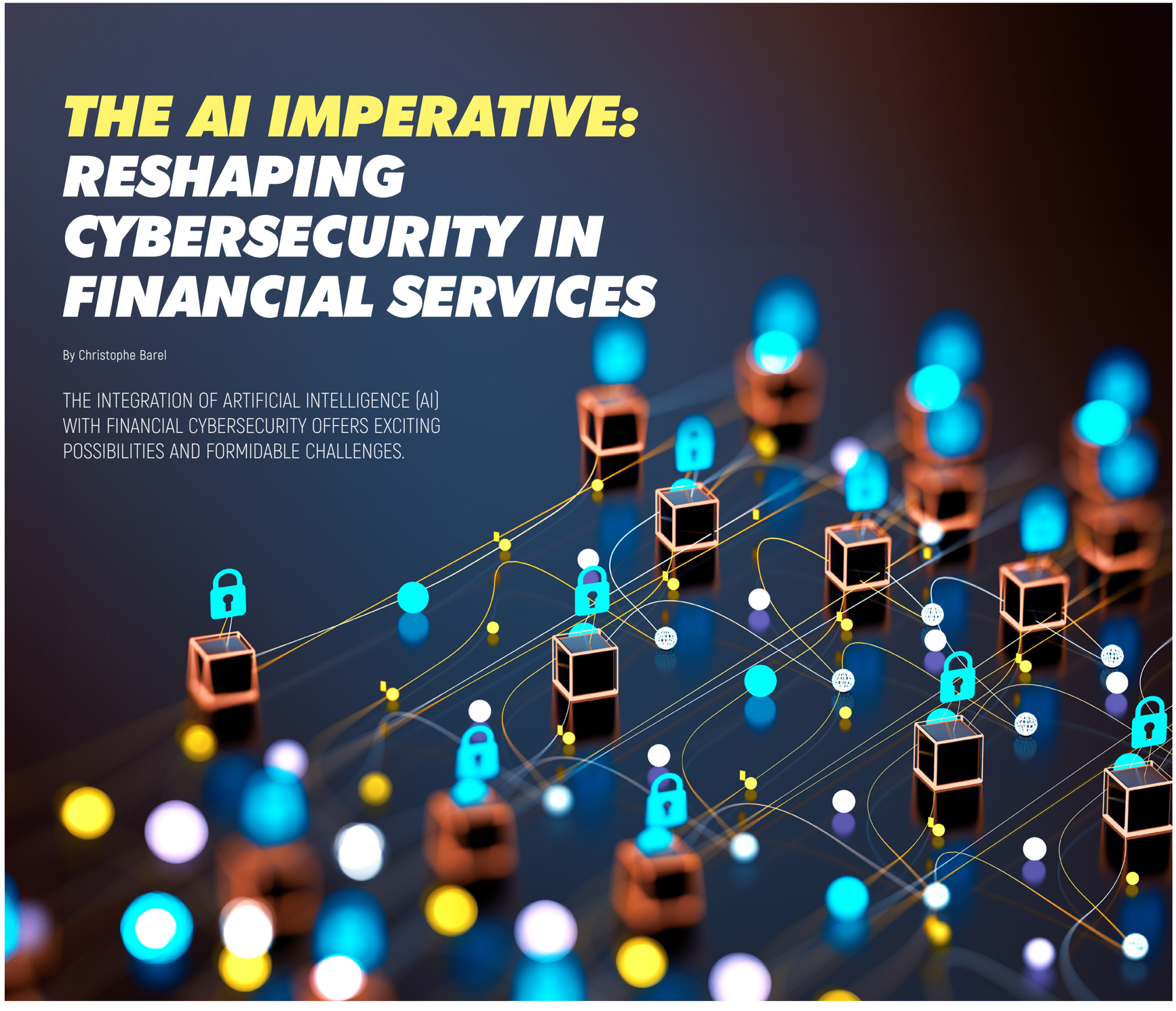
THE AI IMPERATIVE: RESHAPING CYBERSECURITY IN FINANCIAL SERVICES

By Christophe Barel

THE INTEGRATION OF ARTIFICIAL INTELLIGENCE (AI) WITH FINANCIAL CYBERSECURITY OFFERS EXCITING POSSIBILITIES AND FORMIDABLE CHALLENGES.



We can revolutionise how financial systems are safeguarded using AI to automate processes, analyse data, and make more informed decisions. But AI brings concerns around transparency, interpretability, and accountability as well. Organisations must constantly define the boundaries of acceptable AI use while tackling security, ethical, and regulatory concerns equally often.

One significant concern for financial institutions (FIs), in particular, is the impact of AI on their clients' trust. They'll have to strike a delicate balance between harnessing the advantages of AI and mitigating its inherent risks. That has become a paramount issue for the financial sector and will continue to be.

AI-DRIVEN INSIGHTS FOR PROACTIVE CYBERSECURITY

The fusion of AI and human expertise – dubbed 'collaborative intelligence' – is ushering in a new era of proactive security. AI's remarkable ability to quickly process vast volumes of data, identify patterns, minimise errors, and offer real-time insights has fundamentally transformed threat intelligence. Operating at a pace far beyond human analysts, AI enables organisations to swiftly detect, mitigate, and respond to threats.

Nonetheless, it is the human expertise that makes the impact transformative. Adding critical thinking, contextual understanding, and strategic decision-making, creates a collaborative dynamic between human operators and AI tools. In this way, AI assumes the role of a vigilant guardian, promptly informing humans of potential threats. This symbiotic partnership improves the overall efficacy of threat detection and response, thereby ensuring heightened safety and operational efficiency.

AI's ability to analyse extensive datasets helps security professionals evaluate the vulnerability of corporate assets to specific threats by expediting threat detection and facilitating efficient risk prioritisation. Moreover, AI models continually adapt through machine learning (ML), which can swiftly recognise emerging malicious patterns. In a notable example, Google deployed a cutting-edge ML model in 2023 that effectively thwarted emerging attack methods, demonstrating the power of AI in proactive security.

The advancing capacity of AI to generate synthetic data could bolster fraud management as well. AI can mimic real scenarios and improve core machine learning tools, potentially transforming cybercrime prevention in our digital world. For instance, Mastercard has rolled out Decision Intelligence™ across its global network, an AI system powered by ML that enhances approval rates for valid transactions by analysing cardholders' past spending patterns when assessing new transactions.

AI's potential in financial services extends beyond threat detection. Generative AI – AI that creates text, images, and other content – can deepen board engagement by providing clearer and more easily understandable reports written in less technical language. That helps C-suite executives and board members better identify the organisation's cybersecurity infrastructure's strengths and weaknesses.

This clarity and comprehensibility facilitates more informed decision-making at the executive level and contributes to a more effective allocation of resources to bolster cybersecurity measures, safeguarding the organisation's digital assets and reputation.

AI AS A TOOL TO ADDRESS THE CYBER TALENT SHORTAGE

AI-driven automation is a powerful ally where skilled cybersecurity professionals are in short supply. AI liberates cybersecurity experts from routine, time-consuming tasks – such as monitoring and analysing security logs or responding to routine security incidents – allowing professionals to focus on more valuable activities, like advanced threat analysis, incident response, and strategic cybersecurity decision-making.

Indeed, AI plays an increasingly significant role in mitigating the cyber talent shortage in financial services across APAC, in both the public and private domains. In May 2023, for instance, the Monetary Authority of Singapore (MAS) announced the Financial Sector Artificial Intelligence and Data Analytics (AIDA) Talent Development Programme, part of the National AI Programme in Finance, which aims to bolster the supply of AIDA talent. Similar programmes have been implemented in Taiwan and Korea.

Generative AI, in particular, is increasingly being used by threat actors, **ESPECIALLY IN FRAUDULENT ACTIVITIES LIKE CYBERATTACKS AND DECEPTION.** Threat actors exploit generative AI's capacity for complexity to lend sophistication to fraudulent impersonation, driving FIs to respond with multi-layered security measures, such as biometric authentication and stringent verification processes.

RISKS OF AI IN THE FINANCIAL SECTOR

Nonetheless, the rising adoption of artificial intelligence in finance has not been without risk. A recent paper issued by the International Monetary Fund warns of biased results, privacy concerns, unclear outcomes, reliability problems, and the potential for new systemic risks, among other challenges – including AI's potential to be harnessed as a weapon by malicious actors.

Generative AI, in particular, is increasingly being used by threat actors, especially in fraudulent activities like cyberattacks and deception. Threat actors exploit generative AI's capacity for complexity to lend sophistication to fraudulent impersonation, driving FIs to respond with multi-layered security measures, such as biometric authentication and stringent verification processes.

The surge in phishing content designed by generative AI further complicates the cybersecurity landscape, necessitating continuous employee training to thwart phishing attempts. Threat actors also use generative AI for reconnaissance and target selection, enabling state-sponsored cybercriminals to process stolen and open-source data more efficiently. These tools can identify patterns that enhance espionage tradecraft, aid social engineering campaigns, and create more effective lure materials for successful compromises, according to current open-source reports. A recent article describes using AI-powered chatbots in scams, a new level of sophistication in cybercriminals' tactics, techniques and procedures or TTPs.

Meanwhile, threat actors use AI-enabled large language models to create and improve malware. While AI-generated malware has limitations, AI greatly assists skilled and less-skilled developers, which marks a concerning trend in the evolving cyber threat landscape.

DATA SECURITY IN THE ERA OF AI

As AI usage grows, financial institutions must focus on bolstering their resilience. Generative AI in particular, has reduced the barriers for cyber threat actors, granting them access to potent tools.

Financial institutions must sustain digital trust by prioritising resilience, reducing risks, and adhering to thoughtful internal policies and government regulations concerning AI usage. This involves implementing a transparent, responsible AI use policy that empowers employees to make informed decisions. AI considerations should be built into resilience programs. These strategies may include simulating AI-driven cyber threats, enforcing stringent controls on data access, and fostering collaborative efforts with other sectors to enhance collective defence against emerging threats.

Singapore has been a leader in AI governance in financial services. MAS provides guiding principles on using AI in the financial sector and, in June 2023, released a toolkit for responsible AI use. In September 2023, FS-ISAC released their Framework of an Acceptable Use Policy for External Generative AI, emphasising fairness, ethics, accountability, and transparency in the financial sector's AI endeavours.

BUILDING RESILIENCE WITH AI IN CYBERSECURITY IN THE FINANCIAL SECTOR

The evolving relationship between AI and cybersecurity in our sector holds immense potential. By thoughtfully integrating AI into our programmes, institutions gain powerful tools for rapidly analysing data, detecting anomalies, and predicting potential threats.

However, FIs must balance AI's capabilities with human oversight for a truly resilient and adaptive financial ecosystem. Ethical considerations and proactive security measures should guide the use of AI to align with ethical standards and regulatory requirements. This blend of AI and human expertise equips financial institutions to respond effectively to emerging threats, adapt to evolving tactics, and maintain high ethical standards in their operations, thereby enhancing their overall cybersecurity resilience.

Financial institutions must, therefore, prioritise knowledge sharing and implement resilience-building measures within a robust ethical and governance framework. That vigilant approach harnesses AI's potential in the financial sector while preserving stakeholder trust. ✱

■ *Christophe Barel is the Managing Director for Asia Pacific at FS-ISAC, the member-driven, not-for profit organisation that advances cybersecurity and resilience in the global financial system, protecting financial institutions and the people they serve. Founded in 1999, the organisation's real-time information sharing network amplifies the intelligence, knowledge, and practices of its members for the financial sector's collective security and defence. Member financial firms represent more than 100 trillion in assets in more than 70 countries. Prior to joining FS-ISAC, Christophe was Managing Director at data and intelligence provider Acuris Group where he has set up their Risk & Compliance business for Asia Pacific, focusing on areas such as AML/KYC screening, cybersecurity and enhanced due diligence. Christophe has been based in Asia for about a decade, starting off in Hong Kong before moving to Singapore in 2015. Previously, he worked for a variety of consulting and tech companies.*