PIMFA WEALTHTECH

SPRING 2025

TECH SPRINT FINDINGS: STRENGTHENING THE INDUSTRY'S CYBER SECURITY DEFENCES

PIMFA WealthTech is a marketplace that drives networking and engagement around the adoption of new technologies in the wealth management and advice sector. It is led by an Advisory Council made up of senior leaders from across our industry, over the year it runs a series of 'tech sprints' to explore how and where new technology can help address specific areas of industry challenge and opportunity.

The latest in the series focused on cyber security and asked specifically how fintech solutions could support the wealth management and financial advice industry in its efforts in preventing, detecting, responding to and recovering from cyber-attacks.

Business continuity and protection for both the organisation and their clients is paramount and specialist Fintechs and new technology solutions play a pivotal role in empowering wealth managers and advisers to strengthen their cybersecurity practices.

These advanced tools and automated systems are specifically designed to enhance their capacity to prevent, detect, respond to, and recover from cyber security attacks by providing streamlined, user-friendly platforms that enhance their ability to detect and respond to threats in real time, ensuring rapid intervention before potential damage occurs. With improved threat detection capabilities, continuous monitoring, and sophisticated risk management tools, Fintechs make cyber security more accessible and manageable. This reduces the complexity typically associated with traditional security measures while enhancing operational efficiency, ultimately minimising time, resources, and costs that would otherwise be spent on manual security processes.

When responding to incidents, specialist cyber security Fintechs provide coordinated, expert-led intervention to contain and mitigate the impact of cyber threats. Their teams are equipped to manage security breaches, investigate root causes, and ensure minimal operational disruption.

WHY CYBER SECURITY?

In the face of ever increasing sophistication of financial criminals and the cost it brings to customers and firms alike, this topic was chosen as the statistics surrounding it are genuinely alarming, with latest research showing that the number of cyber-attacks rising by over 200% since the pandemic and, on average, the cost of cybercrime to financial services is 40% higher than other industries. The average cost of a data breach stands at $5.9M against a global average of $4.45M *.

Apart from cost, the consequences of service disruption and reputational damage following an attack can be severe and the effect on clients can, in some cases, be devastating.

THE PROBLEM STATEMENT

Fintechs that participated in this tech sprint were asked to answer the following problem statement:

"How can a specialist cyber security Fintech provide unique and additional value to support wealth managers in preventing, detecting, responding and recovering from cyber security attacks?"

*https://www.beyondencryption.com/blog/cybersecurity-statistics-financial-services

THE FINDINGS

Two Fintech firms were particularly successful and presented their solutions to a panel of members of PIMFA WealthTech and its Advisory Council. Below is a summary of some their key findings and proposed solutions:

NAVOS TECHNOLOGIES https://navos.co.uk/

Offered a full-service solution that could assist firms across 6 pillars, namely:

1. **Audit –** reviewing what cyber security measures are already in place, reporting back on what next steps are required to keep clients secure
2. **Advisory -** on best practice and the continuously evolving threat levels and characteristics
3. **Testing -** right across the business, both internal and external and with a Focus on backup data, which is predominantly less protected than live, and is now more commonplace for attack. Also look at other tech like the mobile phones used by staff
4. **Detection -** cyber security as a managed service in conjunction with their technology partners, offering increased and proactive ability to identify a cyber threat
5. **Recovery -** managed backup with an immutable file system that can't be modified, deleted, or encrypted. Allows recovery of data in minutes and hours, rather than weeks
6. **Education -** ensuring that staff understand the cyber threat landscape and educating them on the business risks

MYCENA UNPHISHABLE ACCESS https://mycena.co/pimfa/

Offered a preventative solution that worked to eliminate password-related vulnerabilities as they reported '90% of breaches are caused by criminals stealing login credentials (passwords and two-factor authentication tokens)' and AI-powered phishing and deepfake attacks make it almost impossible for employees to distinguish legitimate requests from fraudulent ones.

Their solution tackles credential-based risks at the root by separating the identity layer (who you are) from the authentication layer (what you're allowed to access):

1. **No Stored or Known Credentials:** their technology generates and distributes encrypted credentials that employees never see or know, removing the risk of password reuse, phishing, and theft.
2. **Multi-Layered Security Model:** technology that applies multiple security layers, ensuring that even if an attacker breaches one level, they cannot access critical systems.
3. **Eliminates Single Point of Failure:** Unlike traditional password managers or SSO solutions, Mycena ensures that each system has unique credentials, preventing an attack on one system from compromising others.