FStech

CyberSecurity Live 2024

6 November 2024
Hilton London Tower Bridge

CONFERENCE OVERVIEW

Sponsored by:

Bottomline

Metomic

THREATLOCKER

TRUSTMARQUE

CISCO Partner

www.fstech.co.uk/cybersecuritylive

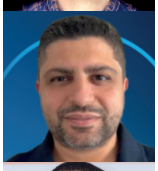
Follow the event on X: @FStechnology #CyberSecLive

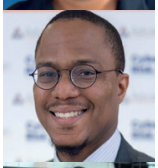
FStech

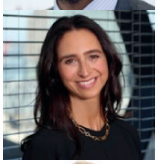
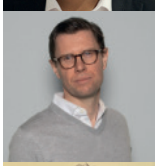
CONTENTS

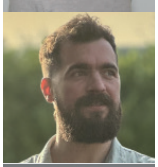
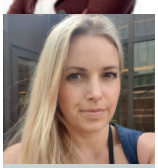







3 Introduction

4 Agenda

5 Keynote - BNP Paribas

6 Presentation - Bottomline

7 Panel - The AI security paradox

8 Presentation - Metomic

9 Presentation - University of Kent

10 Panel - Operational resilience under DORA and beyond

11 Presentation - Cisco

12 Presentation - The Payment Systems Regulator (PSR)

13 Fireside chat – sponsored by Trustmarque

14 Keynote - Financial Service Information Sharing and Analysis Centre

CyberSecurity Live 2024

INTRODUCTION

Jonathan Easton, editor, FStech conference chair

As the dust settles on another transformative CyberSecurity Live conference, it's a privilege to reflect on the key takeaways from this year's event; a gathering that has once again demonstrated the critical importance of staying ahead in an increasingly complex cyber threat landscape.

The 2024 conference underscored the financial services sector's pivotal role in maintaining global economic stability amidst rising cybersecurity challenges. From the revolutionary potential of AI in automating risk management to the relentless evolution of ransomware and insider fraud, our discussions revealed both the immense opportunities and sobering risks facing the industry.

Central to the dialogue was the importance of collaboration, resilience, and vigilance. The sector's ability to pre-empt and respond to emerging threats will hinge on its capacity to innovate, integrate robust frameworks like Zero Trust, and foster a culture of shared intelligence and adaptability.

Cybersecurity is not just a technical challenge—it is a business imperative and a moral responsibility. Cybersecurity Live 2024 highlighted the ingenuity and commitment across the sector, and showcased the industry's efforts in forging a safer, more resilient financial future. Thank you to all who contributed to this vital conversation, and I look forward to welcoming you to our future conferences.

FStech

AGENDA

08.30 – 09.00: Registration and refreshments

09.00 - 09.10: Chairman's welcome
Jonathan Easton, Editor, FStech

09.10 - 09.40: Keynote session: AI for Cyber Risk Automation
Sandip Wadje, Head of Emerging Tech Risks, BNP Paribas

09.40 - 10.10: In Under the Radar: How Can FSIs Mitigate the Risk of Insider Fraud?
Ruud Grotens, Head of Fraud & Financial Crime Solution Consulting, Bottomline

10.10 - 10.40: Panel discussion: The AI security paradox: How the tech is helping to fight cyber-crime and bolstering criminals
Panellists:
Deepak Bhandari, Director of Cyber Security, Oaknorth
Guy Morrell, Director of Information Security, British Business Bank
Mona Schroedel, Managing Associate, Freeths

10.40 - 11.10: Fireside chat: SaaS DLP in Action: Proactive Measures to Prevent Data Breaches
Ben van Enckevort, Co-founder and CTO, Metomic

11.10 - 11.40: Coffee break

11.40 - 12.10: Ransomware Harms and the Victim Experience
Dr Jason R.C. Nurse, Reader in Cyber Security, University of Kent

12.10 - 12.40: Panel discussion: Operational resilience under DORA and beyond: Strategic approaches to implementation
Panellists:
Adam Avards, Principal for Cyber and Third-Party Risk, UK Finance
Richard Breavington, Partner and Head of Cyber & Tech Insurance, RPC
Lorenzo Grillo, Managing Director – Europe & Middle East Cyber Risk Services Leader, Alvarez & Marsal
Sarah Pearce, Partner, Hunton Andrews Kurth (UK) LLP
Daniela Waugh, IT Security Manager, Markerstudy

12.40 - 13.10: Zero Trust Security: Reinventing Financial Services in a Digital-First Era
Mustafa Mustafa, Solutions Engineer Leader, Cisco

13.10 - 14.10: Lunch break

14.10 - 14.25: Leading the charge on APP fraud
Ben Woodside, APP Policy Manager, PSR

14.25 - 14.55: Fireside chat: Revolutionising financial security: Driving innovation and resilience with Zero Trust - (Sponsored by Trustmarque)
Elliott Morgan, Solutions Sales Specialist (Cyber Security), Trustmarque

14.55 - 15.25: Collaborative cybersecurity: Leveraging intelligence sharing in financial services
Teresa Walsh, Chief Intelligence Officer and Managing Director, EMEA, FS-ISAC

15.25 - 15.40: Chair's closing remarks, quiz and end of the conference

BNP Paribas

Keynote – AI for Cyber Risk Automation

In this keynote session Sandip Wadje, head of emerging tech risks at BNP Paribas focused on the opportunities that cyber risk automation can provide. He examined how the advances in adopting smaller models and agentic workflows are significantly changing approaches for delivering automation at scale.

Wadje started his presentation by highlighting that with so many AI models having been launched, it can be hard for financial institutions to keep up with the latest developments.

"We understand how we use the technology, but don't have a handle on where it is going, and models are now surpassing the imagination," Wadje said. "No one was able to tell their boards that everything was going to change and we haven't had time to fully appreciate the change."

In the future, Waje predicts that intelligence will be industrialised, while cyber-attacks may become more common and could affect investment decisions.

While there has been a lot of evolution in the cybersecurity space, Wadje said that there are essentially two types of defence. Firstly, there are enhancements of existing products, he explained. Secondly, he continued, there are plug-ins to existing systems.

"If you are a decision-maker in a cybersecurity company and you go to your boss and say 'I need money for an AI enhancement,' you are not going to be able to show the savings in the long term," Wadje explained.

He said that while generative AI (genAI) cyber agents are slowly appearing on the market, they are having little impact so far.

"Once you start to investigate genAI agents, and there are lots of them, you find out that they don't talk to others," Wadje said. "It gets the job done but can't integrate into other solutions and you often need three different agents to get the job done."

He pointed out that genAI is in the development stage and still uncertain. Many FSIs are unwilling to "burn their fingers" when they are unsure of where the technology is going, explained the head of emerging tech risks.

"Change will come one step at a time – there is no big bang," Wadje said. "You may have some plug-ins which do the job, but we are all going to implement AI eventually due to the cost savings."

Wadje explained that FSIs needed to "work backwards" to look at what enhancements they need and what could most benefit their business.

In Wadje's opinion, one of the best ways that FSIs can prepare themselves for the adoption of AI is through making their workforce more resilient. They need to ensure that their employees are upskilled properly to make full use of the technology.

"GenAI is so exciting that everyone wants to use it," Wadje said. "But if people are doing the same job they were doing yesterday with genAI – you are doing something fundamentally wrong."

He finished off his presentation by saying that AI is already good at providing summaries and advised FSIs to scan their last 10 years of reports on cybersecurity to provide insightful information in an easier format.

Bottomline

Under the Radar: How Can FSIs Mitigate the Risk of Insider Fraud?

Speaking at this year's Cybersecurity Conference, Ruud Grotens, head of fraud and financial crime consulting at Bottomline, presented findings from a survey conducted by FStech and Bottomline.

The survey, involving 100 global decision-makers, revealed ongoing issues with insider fraud driven by economic pressures and the cost-of-living crisis.

"Financial pressures have increasingly pushed individuals to commit fraud within their organisations," Grotens said, noting that the profile of insider fraudsters is evolving.

"A significant portion of cases now involve employees who have been with the organisation for less than a year," he added, attributing the shift to remote working conditions, reduced supervision in the physical workplace, and weaker loyalty among new hires.

Grotens said that banking and financial services industries have a much higher number of insider fraud cases compared to other sectors.

"Financial institutions manage higher-value assets and sensitive data, making them prime targets for insider threats," he continued.

According to the report, which surveyed 100 financial services professionals, 48 per cent of organisations face fewer than five incidents annually, indicating that while these cases may be infrequent, the risk remains constant. A further 24 per cent said that they lack sufficient data to assess frequency, a concerning indicator according to Grotens.

The survey found that six per cent of organisations reported more than 11 insider fraud incidents per year, suggesting larger vulnerabilities or more sophisticated methods are being used by insider threats.

"The key takeaway is that financial institutions need to close the visibility gaps in their insider fraud detection and monitoring," continued Grotens. "These hidden risks can be a bigger problem than they realise."

Looking ahead, he highlighted the upcoming "Failure to Prevent Fraud" law expected in the UK in 2025. The law will increase the accountability of organisations for fraud committed by their employees, even if management was unaware of it.

"This law will apply not only to UK-based organisations, but also to foreign organisations that conduct business activities in the UK," he said. "Under this law, financial institutions could be held liable for fraud committed by employees if the organisation benefited from it."

Grotens concluded his session by calling for a holistic approach to insider fraud prevention.

"A holistic approach is key to truly protecting against insider fraud," he told delegates. "Technology alone cannot solve the problem.

"Organisations need the right combination of evidence-based monitoring, empathy, education, and a strong organisational culture to effectively address insider fraud."

Panel

The AI security paradox: How the tech is helping to fight cyber-crime and bolstering criminals

Artificial Intelligence is revolutionising cybersecurity, offering new tools to defend against evolving threats. In this session, expert panellists explored the impact of AI on financial sector cybersecurity.

Speakers discussed key AI applications, including threat detection, anomaly identification, and automated response systems. The session examined how AI enhances traditional security measures and enables proactive defence strategies, as well as addressed the dual nature of AI in cybersecurity, exploring how threat actors leverage AI and how organisations can counter these emerging risks.

When asked whether UK financial institutions are prepared to defend against AI-powered cyber-attacks, Deepak Bhandari, director of cybersecurity at Oaknorth Bank said that AI makes it easier to access LLMs, which means there are new attacks cropping up, making things more complex. But he said that financial services institutions (FSIs) are reasonably prepared because of the strong regulatory frameworks driven by the Financial Conduct Authority (FCA).

Guy Morrell, director of information security at the British Business Bank said that one of the gaps for firms is that things such as cyber hygiene, patching, architecrual improvements, essentially things they have been doing for years, need to now be under even mot scrutiny.

"Focusing on making sure end-to-end processes are rigorous," he said. "Ensuring the cyber response plan is fast – things like that are where gaps can form."

Mona Schroedel, managing director at law firm Freeths, said that from a legal perspective, whether the product will help the company, its customers, and looking at if there is a negative impact is important, adding that firms can't just be "dazzled" by the technology.

"The law says automated decision making must have rigorous tests, it's not as straightforward as you think," she said. "The impact of 'system says no' is crucial, particularly when you're dealing with money."

When speaking about how the accessibility of AI can enable criminals to make attacks like Denial of Service even more damaging and the steps that FSIs can take to mitigate the associated risks, Bhandari said that from an internal perspective the focus is on architecture as well as looking at AI risk

automation and traffic monitoring.

"Those are critical," he continued.

British Business Bank's Guy Morrell said that there can be unexpected consequences of an attack, like employees being locked out of accounts.

"AI will only make it easier to write code, but the method is the same: bolt every door," he continued.

Schroedel told delegates that it's a matter of when not if.

"Anyone can fall for this now, the emails, the phone calls – from a legal perspective, minimising that risk is creating the right culture," she explained. "It's going to happen, we need that person to step up when they realise they shouldn't have clicked that link. Empowering people to come to the right people – that will go a long way."

When talking about the role of the regulators in setting standards for AI use in financial services cybersecurity, Schroedel said that the problem is that they are "lagging behind significantly".

"But even if you don't have regulation, it's not okay to be lax," she continued. "Firms should be running impact assessments. If something goes wrong, it will go a long way to show the regulators that you really tried."

Metomic

SaaS DLP in Action: Proactive Measures to Prevent Data Breaches

In this session Ben van Enckevort, chief technology officer and co-founder of Metomic, explored how Data Loss Prevention (DLP) solutions for SaaS environments can help businesses secure their sensitive data and stay compliant with industry regulations. He highlighted practical strategies for preventing data breaches and improving operational efficiency in the financial services sector.

Van Enckevort began by pointing out that data used to live "in the backroom" but as Saas sits outside of the network, a lot of which is invisible, security is harder to manage.

This is particularly important as a lot of security access is based on who needs to access something, he said. But often, van Enckevort continued, there are no measures in place to control how this access is used or what employees can do with data and information when they access it.

"FSIs can have many security layers, DLP is another layer to keep information confidential," he explained. "All your information can be used by an enemy to get further information.

"While DLP should not be the first layer of defence, it can help to reduce the vulnerable surface area."

Van Enckevort said that some companies are inputting data into systems that span years and that they need to put in controls around this data. Automation is necessary, van Enckvort said, as there is so much data to protect and process.

In order to implement DLP properly, van Enckevort said that

FSIs needed to have the right strategy in place.

"Figure out what is important to every single department," van Enckevort advised. "Not many people are aware of DPL programmes and many people hate it because it means that they are unable to do business.

"This is one of the biggest pushbacks and you can't go in with a big blunt hammer, it's not realistic."

Van Enckevort advised implementing a system that could respond instantly and recommended putting a response in place that can go out with automatic remediation which would invite the individual involved to take a specific action.

"No-one buys a DLP solution to increase efficiency, but if you don't have one in place you risk the system going down and your business going even slower," he told delegates.

University of Kent

Ransomware Harms and the Victim Experience

Speaking at this year's CyberSecurity Conference, reader in cybersecurity at the University of Kent Dr Jason R.C. Nurse examined the profound impacts of ransomware attacks beyond financial losses.

Nurse kicked off the session by highlighting a major ransomware incident where a third-party supplier for London hospitals was targeted, with the attack leading to severe operational disruptions including blood shortages and stolen test data.

"Speaking to various professionals, including security experts, organisations, law enforcement, and others, we noticed a strong focus on the financial costs and losses from ransomware attacks," Nurse said. "However, ransomware can cause significant damage that extends well beyond the monetary costs."

He talked about his research, based on insights from 100 security professionals, which analysed ransomware's disruptive potential, showing how businesses are often unable to operate overnight, access file systems, pay employees, and conduct business and trade.

"Ransomware can lead to staff burnout, loss of client trust and reputational harm," Nurse said. "Criminals behind ransomware attacks have become more sophisticated. They often spend months infiltrating the organisation and encrypting not just the primary systems, but also the backups.

"Consequently, when organisations try to recover from backups, the attackers can simply re-encrypt those backups, making the recovery process futile."

The research also examined how ransomware can cause dramatic and significant impacts throughout the supply chain by spreading through supply chain connections and causing harm not just to the initial target, but also to other organisations that are linked to it.

Nurse warned of how the normalisation of ransomware is becoming a growing trend among institutions.

"When people hear about yet another ransomware attack, their reaction is often to say, "not ransomware again", indicating a sense of resignation and acceptance that these incidents are becoming commonplace," the cybersecurity expert explained.

Nurse added that ransomware can also have a significant impact on the mental and physical well-being of the staff dealing with the incident, which is often overlooked by companies.

"A security professional who was dealing with a ransomware incident said he forgot to eat and drink properly, he was drinking excessive coffee and not enough water, as he was just trying to stay awake and deal with the situation, and a member of his team was hospitalised for a few days due to not caring for themselves," explained Nurse.

"What we see in a lot of security professionals is that they feel that the incident is their fault."

According to Nurse, factors aggravating harm caused by ransomware attacks include poor communication, insufficient management support, and treating ransomware as an IT issue rather than an operational problem.

"Instead, a robust security culture and overall company culture helps organisations respond more effectively," he said. "Organisations with cyber insurance were also able to quickly access a suite of support services."

Nurse concluded by providing key statistics from the large-scale study he conducted as part of his ransomware research.

"Over the past five years, the researchers have identified around 120 different ransomware groups that have emerged, and almost 1,000 different streams or variants of ransomware," he said, emphasising that the proliferation of ransomware threats is significant.

Panel

Operational resilience under DORA and beyond: Strategic approaches to implementation

Ahead of the introduction of the European Union's Digital Operational Resilience Act (DORA), operational resilience has become a critical focus for financial institutions as they navigate an increasingly complex risk landscape.

In this session, expert speakers explored strategies for building robust operational resilience frameworks to ensure continuity of critical business services and meet key regulatory requirements. Speakers discussed the key components of operational resilience, including business impact analysis, mapping of important business services, and setting impact tolerances.

The session examined regulatory expectations, such as those set by the UK's PRA and FCA, and offered guidance on compliance. Attendees learned about integrating operational resilience with existing risk management practices, conducting effective scenario testing, and leveraging technology to enhance resilience capabilities.

"It's not just a question of compliance," said Lorenzo Grillo, managing director – Europe and Middle East cyber risk services leader, Alvarez & Marsal, when talking about how a large number of financial institutions admit they will miss the DORA deadline. " It's more important to be resilient and not have a crisis than not being compliant – DORA or not, you have to be ready for important crises. It shouldn't be a tick box exercise."

Richard Breavington, partner and head of cyber & tech insurance at RPC said that there is limited risk to the "wait and see approach".

"The main risks are regulatory, although firms are statistically unlikely to get a fine, the problem is if there is a real impact from non-compliance," he explained. "For example DORA is newsworthy, so firms may find they are in the cross hairs."

Daniela Waugh, IT security manager at insurance business Markerstudy said that even if it's unlikely, there is still the risk of a licence being revoked.

"I think that this is really worth considering before you 'wait and see'", she told delegates.

Adam Avards, principal for cyber and third-party risk at UK Finance, said that even though not all firms are in scope, DORA will likely act in a similar way to GDPR globally.

"There is not just acceptance amongst firms that they probably won't be ready in time for DORA, but somewhat unusually

the regulators too," continued Avards. "They want to see that roadmap and journey towards compliance rather than ticking boxes."

Sarah Pearce, partner at Hunton Andrews Kurth (UK) LLP said that firms need to navigate areas where there is murky water whilst still building compliance.

She explained that one of the key elements of DORA is reporting timelines for incidents.

"That's one of the pieces that's quite critical to how you're going to build your incident response," continued Pearce. "The regulators want to see some degree of compliance but they appreciate that some areas will not be fully defined within an organisation."

Waugh said that the regulation could be more detailed as it isn't clear on with who or where firms should be sharing intelligence.

But Avards pointed out that granularity when it comes to the regulators can be a "double-edged sword".

"It tells you what to do but takes away your freedom on those principles," he continued.

Cisco

Zero Trust Security: Reinventing Financial Services in a Digital-First Era

As financial institutions lead digital innovation, they face increasing cyber threats that traditional security models can no longer manage.

In this session, Cisco's solutions engineer leader Mustafa Mustafa explored how the financial sector can use Zero Trust as a key strategy to fight these risks by shifting from perimeter-based defences to a "never trust, always verify" approach.

He highlighted why Zero Trust is essential for protecting critical assets like customer data and financial transactions and explained how it can enable FSIs to meet compliance regulations and build trust amongst their customers.

"AI is being pushed into the fabric of everything that we do today and criminals are using it to their advantage to conduct cyber-attacks," Mustafa said. "You need to know how many people are connecting with your service and if it's fully secure."

Mustafa added that while it is important to verify the user, organisations need to verify the network they are connecting from. He pointed out to the audience that they had probably accessed the internet through at least three different IP addresses, adding that their remote workers might be dialling in from potentially risky locations such as public coffee shops.

"Zero Trust is a journey, there are lots of different building blocks," he said. "You should never assume trust on a device until it has been verified."

Mustafa added that there are certain factors which contribute to the successful implementation of a Zero Trust policy, such as adjusting the policy to the level of risk and ensuring a level of consistency across different environments.

He ended the session by highlighting the cost benefits of a Zero Trust strategy. Since the implementation, Cisco estimates that it has saved around $3.4 million from a productivity perspective and 86,000 potential compromises every per month.

The Payment Systems Regulator (PSR)

Leading the charge on APP fraud

Ben Woodside, APP policy manager at the Payment Systems Regulator (PSR) spoke about the decisions, considerations and future evolution of the PSR's authorised push payment (APP) reimbursement scheme.

Woodside kicked off the session by explaining that Faster Payments was not originally designed with adequate fraud prevention measures, which has led to the rise of APP scams that are now causing significant financial losses and impacting victims in the UK.

"When the Faster Payments system was launched in 2008, it was the first instant payment system of its kind in the world," he said. "However, it was not designed with fraud prevention in mind."

Woodside highlighted how the system initially lacked basic measures to protect people from fraud. "Some steps have been taken to build in protections, but they have not proven to be enough, and APP scams have become one of the most common types of fraud globally," he noted.

He added that authorised fraud tends to have a higher emotional and psychological impact because of the role that victims play in authorising the payments.

"In the UK, almost half a billion pounds a year is lost due to these APP frauds, impacting around 200,000 victims," he explained. "These include homebuyers losing deposits and pensioners losing life savings."

Because of these scams, over a third of people who are victims of those frauds are less confident making a payment using a new payment method, with APP fraud also impacting the payments industry, society and the economy at large, Woodside added.

To prevent this, Woodside said that the PSR introduced new reimbursement requirements, effective on 7 October, mandating payment service providers to reimburse most APP fraud victims.

"This means that individuals, smaller charities, and micro businesses can now expect their payment service provider to reimburse them for losses incurred through APP fraud, in most circumstances," he said.

The new reimbursement requirement for payment firms replaces the previous voluntary industry code, aiming to provide a more consistent and comprehensive level of protection for victims of APP fraud.

"According to research, the negative feelings experienced by victims of APP fraud, such as anxiety, loss of trust, and lack of confidence, were reduced among those clients who had been reimbursed," he said.

Woodside also recognised consumers must also play their part and act carefully when making payments, as firms are not required to reimburse if the consumer has acted with gross negligence.

"We recognise consumers must also play their part, said Woodside. "They still need to act carefully when making payments, because if a firm can demonstrate that someone has acted with gross negligence, then there's no requirement for reimbursement."

He added that the new reimbursement requirements do not cover international payments, only payments made across the Faster Payments or Clearing House Automated Payment System (CHAPS) systems between two relevant UK accounts.

Woodside concluded by saying that the PSR will review the effectiveness of the policy in 12 months and will continue to work on data transparency and industry collaboration to improve fraud detection and prevention.

Fireside chat – sponsored by Trustmarque

Revolutionising financial security: Driving innovation and resilience with Zero Trust

As financial services embrace digital transformation, traditional security models are struggling to keep pace with the growing sophistication of cyber threats. In this fireside chat, Elliott Morgan, solution sales specialist (cybersecurity) at Trustmarque explored how Zero Trust security is reshaping the financial sector's approach to safeguarding critical assets such as customer data and financial transactions.

Zero Trust adopts a "never trust, always verify" mindset, offering a more robust framework to protect against internal and external threats. This discussion delved into the practicalities of implementing Zero Trust architecture, from integrating a unified security platform to simplifying threat detection, enhancing data privacy, and ensuring compliance with evolving regulations.

Talking about perimeter-based defences, Morgan said that VPNs are still a massive part of this type of security.

"We absolutely need to move away from that," he said, emphasising that there are many threats on the horizon.

When asked about whether the approach following covid has changed, he said that working from home has driven the adoption of security services to secure users wherever they are.

He talked about how the CrowdStrike-Microsoft 365 outage brought a lot of challenges, adding that "we're still catching up from a security perspective."

Morgan said that the number one criteria for whether Zero Trust will be successful is stakeholder engagement.

"Needs to be from the executives to the lowest level user, otherwise it's not going to work," he continued.

Having your house in order and user profiling is a massive thing that's overlooked, explained Morgan.

"If you're blocking access on something you need, you'll get massive disruption," he added. "Most banks are in a hybrid model – multi cloud and those apps on legacy infrastructure are really hard to migrate – they are hugely costly and disruptive to move them.

"From a compliance perspective there are multi elements. One of those key parts is the monitoring aspects, I think this is where Zero Trust-enabled tech is really important."

Morgan went on to say that he doesn't think perimeter security has much of a future.

"It might not be a case of fully Zero Trust," he explained. "But I can't see a situation where Zero Trust isn't the main way."

Keynote - Collaborative cybersecurity: Leveraging intelligence sharing in financial services

The final presentation of the day was by Theresa Walsh, chief intelligence officer and managing director EMEA of the Financial Service Information Sharing and Analysis Centre (FS-ISAC), who outlined how financial firms can leverage intelligence and knowledge sharing in trusted communities to advance their cybersecurity programmes, build resilience and comply with new regulations.

Walsh explained that she runs the intelligence team at FS-ISAC, which receives threat information from the organisation's over 5,000 members across 70 different countries, including banks, insurance companies, holding companies, and stock exchanges, as well as companies with financial services components such as oil and gas companies and car manufacturers.

Walsh emphasised that protecting the financial sector currently requires more collaboration than in the past. "In a constantly evolving threat landscape, cyber risks have evolved to address a wide range of threats that impact the financial services sector, not just traditional banks and financial institutions," she said.

To prevent cyber breaches, she noted how the ecosystem requires a collaborative, intelligence-driven, risk-focused approach.

"Response to these threats should not be about competition between institutions, but rather about collaborating to improve the security and resilience of the entire financial services sector," Walsh said, emphasising that collaboration is now "a matter of national and economic security."

Walsh added there is currently a lot of "hype" and "propaganda" around emerging AI threats, but stated that when analysing cyber threats, organisations should try to take a risk-based approach rather than a technology-focused approach. "The bad actors are still primarily trying to steal data, secrets, and money - the same core objectives they have had for a long time. The methods may evolve, but the underlying motivations remain," she said.

She went on to explain that the cyber threats organisations face, while technologically sophisticated, ultimately stem from deliberate human actions and social engineering tactics.

"The primary method these attackers use to deliver malware is through social engineering - trying to trick people into clicking on links or downloading files, such as through phishing emails

or SMS messages posing as legitimate entities like banks," she added. "The focus should be on understanding and mitigating these human-driven threats, rather than just the technical aspects of the malware itself."

She then highlighted how geopolitical events like Russia's invasion of Ukraine have disrupted the previously well-organised cyber-crime ecosystem, leading to leaks, and a breakdown in relationships.

"Because of that, intelligence is crucial to help organisations understand what they should be looking for in terms of cyber threats and fraud," explained Walsh. "To effectively address threats that originate outside an organisation's perimeter, collaboration and open conversations are necessary."

Walsh highlighted that cyber threats and fraud are no longer just about data loss or financial loss: they also cause a significant reputational risk.

"It is not about playing the "blame game" between different entities like banks, social media companies," she concluded. "Instead, the focus should be on understanding how to collectively improve and fight the fraudsters impacting everyone."

FStech

CyberSecurity Live 2025

SAVE THE DATE

6 November 2025
Hilton London Tower Bridge

www.fstech.co.uk/cybersecuritylive
Follow the event on X: @FStechnology #CyberSecLive


FStech
CyberSecurity Live 2024
www.fstech.co.uk/cybersecuritylive
Follow the event on X: @FStechnology #CyberSecLive