FStech

CyberSecurity Live 2025

6 November 2025
Hilton London Tower Bridge

CONFERENCE OVERVIEW

Sponsored by:

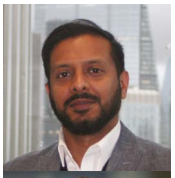
Kocho
BECOME GREATER

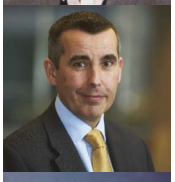
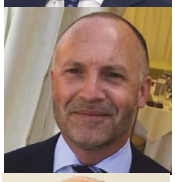
rubrik

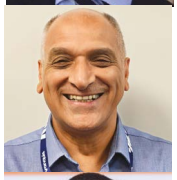
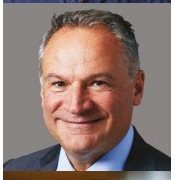
www.fstech.co.uk/cybersecuritylive
Follow the event on X: @FStechnology #CyberSecLive

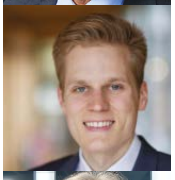
FStech

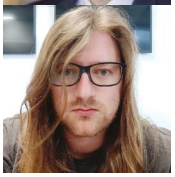
CONTENTS








CyberSecurity Live 2025

INTRODUCTION

I'm delighted to share this overview of FStech's CyberSecurity Live 2025 – a day that brought together some of the sharpest minds in financial services security to tackle the challenges reshaping our industry.

The threats we discussed bear little resemblance to those we faced even two years ago. Ransomware has industrialised. AI has moved from theoretical concern, to operational reality, both as weapon and shield. Nation-state actors and criminal enterprises increasingly collaborate. And regulatory frameworks are struggling to keep pace with technical innovation and geopolitical upheaval.

Yet what gave me confidence throughout the day was the calibre of expertise in the room. We heard from practitioners who've led their organisations through actual cyberattacks, researchers who've studied CEO decision-making under fire, and technical leaders building the defences that will protect our financial infrastructure tomorrow.

From resilience exercises that address true polycrisis situations, through the compliance maze of DORA and emerging AI regulations, to the hard questions about ransomware, zero-trust, and AI-driven threats, the conference covered significant ground – much of which is covered within this overview.

Particular thanks go to our sponsors, Kocho and Rubrik, whose support made this event possible and whose expertise enriched the conference sessions.

One theme emerged clearly: cybersecurity isn't a problem any organisation can solve alone. It requires collaboration, and that's precisely what CyberSecurity Live delivered.

Jonathan Easton,
Editor, FStech

FStech

AGENDA

08.30 - 09.15: Registration and refreshments

09.15 - 09.20: Chair's welcome
Jonathan Easton, Editor, FStech

09.20 - 09.50: Keynote speaker: From tabletop exercises to polycrisis: Evolving resilience exercises in the financial sector
Fox Ahmed, Global Head of Cybersecurity and Technology and Data Protection Regulatory Risk, BNP Paribas

09.50 - 10.20: What 40 CEOs told us about building cyber resilience
Manuel Hepfer, Research Affiliate, Oxford University's Saïd Business School

10.20 - 11.00: Panel: Navigating evolving UK and global cyber regulations: Compliance, risk, and operational strategies
Panellists:
Lorenzo Grillo, Managing Director – Europe & Middle East Cyber Risk Services Leader, Alvarez & Marsal
Peter Nota, Group Chief Information Security Officer, Vanquis Banking Group

11.30 - 12.00: AI in cybersecurity: The double-edged sword
Anna Webb, Head of Global Security Operations, Kocho

12.00 - 12.40: Panel: Ransomware reloaded: Defending financial services from modern extortion, sponsored by Rubrik
Panellists:
Eddie Lamb, Global Head of Cyber, Hiscox
Paul Mallon, Solutions Engineering Manager Major Accounts, Rubrik
Will Richmond-Coggan, Partner & Head of Data and Cyber Disputes, Freeths

12.40 - 13.10: Ransomware Inc.: The business, players, and power structures of digital extortion
Dr Jason R.C. Nurse, Reader in Cyber Security, University of Kent

14.10 - 14.50: Panel: AI versus zero-trust: Reinventing financial cyber defences
Panellists:
Temi Afeye, Senior AI Scientist, Lloyds Banking Group
Thomas Knowles, Head of Security Operations, ClearBank

14.50 - 15.20: Keynote: Intelligence in Action: A deep dive into Operation Stargrew
Craig Rice, Chief Executive Officer, Cyber Defence Alliance (CDA)

15.20 – 15.30: Chairman's closing remarks, quiz and end of conference

CyberSecurity Live 2025

BNP Paribas

Keynote – From tabletop exercises to polycrisis: Evolving resilience rxercises in the financial sector

In this keynote session, Fox Ahmed, global head of cybersecurity and technology and data protection regulatory risk at BNP Paribas, examined how financial institutions must evolve their incident response exercises to reflect a world where crises rarely occur in isolation.

Ahmed began by noting that for years, crisis simulations in financial services have been too controlled and predictable.

"For years, our crisis simulations were neat and tidy, with one system outage, one team, and one clean ending," he said. "But that's not how crises work in reality."

He explained that today's environment is far more complex, marked by sharper regulatory expectations, deeper third-party dependencies, and geopolitical shocks that can rapidly ripple through technology and operations.

"We are seeing cyber incidents colliding with vendor outages and geopolitical disruptions that test every layer of our resilience," Ahmed said.

According to Ahmed, traditional tabletop exercises are no longer enough.

"We need to move beyond paper-based scenarios to simulations that are messy, multi-layered, and test how organisations perform under compounded stress," he explained.

He described these modern challenges as "polycrises", where multiple, overlapping shocks interact and amplify one another.

He illustrated his point with a scenario involving a cyberattack on a payments processor coinciding with a cloud outage and the introduction of new sanctions overnight.

"You might face a vendor breach, a reputational issue, and regulatory pressure all at once," he said. "That's what we need to rehearse for, because when it's real, it's too late to learn."

Ahmed emphasised that effective testing should measure decision-making under uncertainty, cross-functional coordination and communication under pressure.

"Do your teams make the right calls with incomplete data? Can IT, HR, and business functions synchronise quickly when every minute counts?" he asked.

Ahmed emphasised the importance of communication with regulators as well as customers and pointed out the increasing regulatory focus on resilience through frameworks such as DORA.

"In a crisis, regulators will ask how many customers are

impacted, what your recovery plan is, and what the systemic effect could be," he said. "Regulators are no longer asking for plans on paper, they are demanding proof that you have tested your ability to recover," he explained.

However, he cautioned that resilience "is not just a compliance exercise", urging firms to see it as a strategic priority rather than a regulatory box-ticking task.

The session also explored the importance of involving third parties in resilience exercises.

"Your business is only as resilient as your partners," Ahmed said. "Leading firms are now running joint simulations with vendors and even competitors, because disruption does not respect organisational boundaries."

He concluded by advising firms to map their dependencies, bring vendors into the room, and carry out at least one qualifying test each year, with a review of lessons learned within 72 hours.

"Resilience should be a strategic conversation," Ahmed said. "It is not built in a crisis, but through rehearsal.

"We need to move beyond saying 'this is fine' and actually prove that it works in practice."

Oxford University's Saïd Business School

What 40 CEOs told us about building cyber resilience

Manuel Hepfer, research affiliate at Oxford University's Saïd Business School, presented research from the university on the role of chief executives in managing cybersecurity risks. The report was based on interviews with 37 chief executives at companies with an average turnover of $12 billion and around 8,000 employees who had experienced cyberattacks.

"The main finding of the research is that executives not only want stronger cybersecurity defences but also want to build an organisation that is resilient enough to withstand cyber-attacks and adapt to them," he told delegates. "To get there, chief executives need to change both the way they think about cyber risk and the way they behave as leaders."

Hepfer noted that there is a significant difference in how chief executives perceive the concepts of cybersecurity and cyber resilience.

"Cybersecurity, in the minds of many chief executives, is seen as a task for a specialised department, something that is managed by technical experts and is not a matter that concerns the entire organisation," he said. "On the contrary, cyber resilience is understood as a broader project, involving the entire organisation and consisting of being prepared to deal with potential problems, adapting during crises, managing risks and ensuring that the company can continue to operate even if something goes wrong."

According to Hepfer, this perspective emphasises the need for collective responsibility and constant continuity, rather than simply protecting the company individually.

The professor added that the research also revealed that, although all chief executives feel responsible for cybersecurity, those who have suffered an attack have realised that responsibility alone is not enough and that they need to be actively involved alongside their teams, sharing responsibilities rather than simply reacting when something goes wrong.

"This change from being simply accountable to being co-responsible is a core mindset shift," he explained.

Another change concerns the 'preparedness paradox' where chief executives may feel very prepared to deal with a cyberattack based on drills and plans.

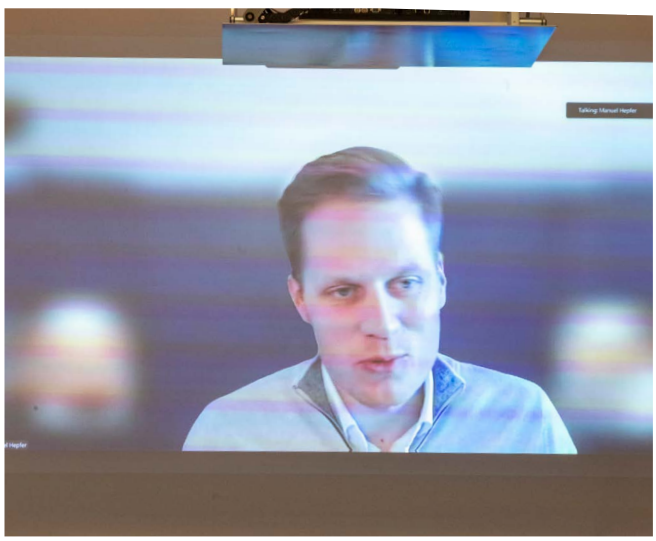
"However, those who have actually faced such situations have found that their sense of preparedness was often misleading and that true resilience requires constant challenges and active engagement," explained Hepfer.

Although chief executives typically view trust in their teams as part of their leadership role, many who have experienced a cyberattack have realised that blindly trusting their IT and cybersecurity teams was a mistake.

"These chief executives admitted that just because nothing had gone wrong before, they assumed everything was safe, but after experiencing a real attack, they learned it's important to remain engaged, ask informed questions, and work alongside their teams to improve resilience, rather than just rely on reports or the absence of problems," he said.

Another important consideration he described is the immense pressure chief executives face during a major cyber incident, with regulators, boards, customers and partners all demanding answers. Some chief executives have made the mistake of transferring this pressure onto their teams, which can be demoralising or counterproductive.

"The most constructive leaders, on the other hand, publicly support their cybersecurity teams and recognise them as the ones who help the company recover," he said.



Panel

Navigating evolving UK and global cyber regulations: Compliance, risk, and operational strategies

Financial institutions face a complex and ever-changing regulatory environment, with new frameworks and updates across the UK and globally. In this panel session, industry experts explored how firms are responding to recent developments, from DORA in Europe to updated SEC requirements and emerging AI-related policies.

Lorenzo Grillo, managing director – Europe & Middle East cyber risk services leader at Alvarez & Marsal said that new regulation, such as the NIST Cybersecurity Framework, has been launched because regulators have found that there are still important weaknesses in banks, as well as to address an evolving threat landscape, including technology advancement.

When asked what the biggest operational challenges posed by new regulatory frameworks in the UK and abroad are, he said: "It's not a question of what the challenges are – the overarching challenge is strictly the ability for a company to evolve cyber maturity and risk management."

If a firm understands that it has to evolve its strategy, then meeting NIS2 standards; preparing for third-party risk and new technology; supporting incident resilience and not just incident response; and involving the board and chief executive should already be happening.

"Are these new regulations challenging something? Yes, if they haven't already started that journey," he explained.

Peter Nota, group chief information security officer (CISO) at Vanquis Banking Group said that in the 30 years he has been working in the industry, the attitude towards cyber has shifted significantly.

"CEOs are far more aware," he told the audience, explaining that he has a monthly meeting with the chief executive.

Nota also revealed that the firm had a complicated structure around four years ago when he started at the company.

"There were four distinct divisions, and each product line had its own security team, it was messy," explained the group CISO.

When Nota joined, the structure was simplified and generic controls were made more granular. He added that the team decided to focus on the EU's NIS2 Directive because this gave the business clearer targets to hit.

"We shut down unused toys and lights, and on top of all of this tied it all back to the relevant standards," he continued.

Grillo highlighted the importance of "proper governance" of cyber risk and compliance.

"Sometimes various responsibilities across the organisation are not centralised or properly managed," he warned, stressing that firms need to understand that a cyber risk framework should be different to a cyber maturity framework.

Nota added that once a firm has partnered with their core technology vendors, they need to identify how they will apply regulatory frameworks. This involves finding what the new controls and gaps are.

"We assess technology early, and if we don't need it, we don't use it," he explained. "We could have 60 vendor calls a week saying they have the silver-bullet for cyber, but it never is. You've got to be critical in how you decide what you want to do."

Grillo said a starting point is designing a proper cyber risk operating model that includes compliance, adding that in his view the owner of cyber compliance is the CISO.

"It's important to have top level management involved – they don't have to speak about technical considerations but they do have to understand the level of risk," he added.

Kocho

AI in cybersecurity: The double-edged sword

In this session Anna Webb, head of global security operations at Kocho, explored how artificial intelligence has become both an opportunity and a threat for cybersecurity teams. She examined how threat actors are weaponising AI and how defenders must adapt with equal speed and intelligence.

Webb began by reminding delegates that the business risk landscape has shifted dramatically in recent years and noted that major retailers and financial institutions have suffered extended downtime as a result of increasingly sophisticated attacks.

"Cyber threats are no longer just an IT headache, they are now a business continuity risk," she said.

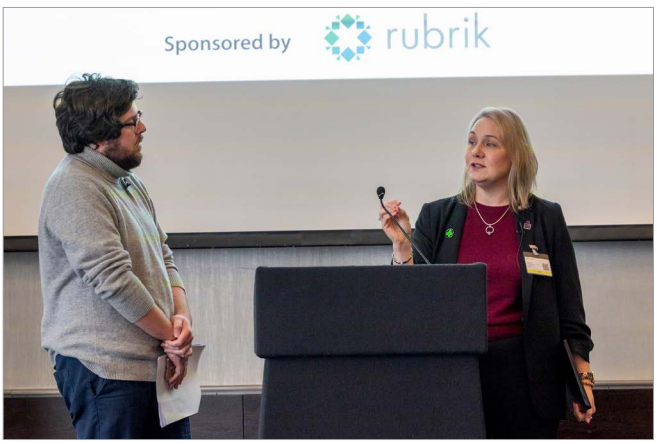
Webb revealed that 60 per cent of breaches now involve AI-enabled phishing, while identity is a factor in 99 per cent of cyberattacks.

"Attackers know that identity is the new perimeter," Webb explained. "It's often the first step in gaining access, and once they have that, they can do so much more."

Outlining the main AI threat trends, Webb said that phishing remains the dominant method of attack, with incidents rising by 77 per cent in 2025.

The rise in deepfake fraud and synthetic identity creation is also fuelling new forms of deception.

"Phishing emails look more genuine than ever, often coming from third parties you would expect to hear from," she said.



"Synthetic identity fraud is up by 700 per cent, and it is getting worse."

Webb cited cases where AI-generated voices and faces have been used to impersonate executives and authorise payments, adding that biometric verification is no longer foolproof.

"My 11-year-old daughter can unlock my phone using mobile face verification," she said. "That shows how easily biometrics can be deceived."

Webb also discussed the operational challenges facing Security Operations Centres (SOCs) and the growing issue of "alert fatigue."

"Some SOCs get more than a thousand attacks per day," she said. "Analysts can easily become overwhelmed."

Around 43 per cent of analysts' time is spent dealing with low-priority incidents, with Webb saying that AI could play a positive role in triaging alerts, improving prioritisation, and allowing teams to focus on real threats.

Despite the rise in AI-powered attacks, Webb said it is "amazing how many organisations still don't use multi-factor authentication (MFA) for all staff." She called MFA "one of the simplest and most effective controls" that too many firms continue to overlook.

Closing her session, Webb urged firms to adopt a 'zero-trust' mindset and to keep humans firmly in the loop.

"AI can help us fight back, but it is still the human element that makes the real difference," she said.

Panel

Ransomware reloaded: Defending financial services from modern extortion

During this panel, speakers discussed the evolution of ransomware tactics as technology advances.

Eddie Lamb, global head of cyber security at Hiscox, opened the session by talking about some of the most common ransomware and extortion tactics currently targeting financial institutions.

"Instead of simply encrypting company data and demanding a ransom for decryption, as in classic ransomware, attackers now primarily steal or exfiltrate sensitive data and threaten to make it public if the ransom is not paid in a practice of extortion," he said.

"Groups such as Klopp, for example, now focus on data theft rather than encryption. They target more emotionally or reputationally sensitive information, such as contracts or accounting data, rather than just customers' personal data, in order to put pressure on company executives to pay up."

He also noted that there is a discrepancy between cyber-attacks in the northern hemisphere and those in the Southern Hemisphere.

"In the northern hemisphere, companies are better prepared, so criminals are moving on to data theft for extortion purposes," he explained. "In contrast, there are still more cases of encryption-based ransomware in the southern hemisphere, probably because those areas have not adapted as quickly."

Paul Mallon, head of solutions engineering for large customers at Rubrik, pointed out that although attackers' technology and objectives have changed over time, the actual methods of attack are often still very traditional.

"The most common way attackers gain entry is by using stolen login credentials or tricking people with phishing methods; these are tried and tested techniques," he said.

He added that in the past, people used someone else's identity card to enter a building, whereas now they use digital credentials to achieve the same result.

"Furthermore, while everyone is focused on modern, sophisticated threats such as deepfakes, attackers sometimes achieve their goals using older, lesser-known tricks that people forget to defend themselves against," he said.

Will Richmond-Coggan, partner and head of data and cyber security litigation at Freeths, explained that today's cyber-attacks, particularly ransomware and extortion, are becoming increasingly sophisticated. He added that they are not limited to demands for money in exchange for the return of stolen data, instead attackers are using multi-layered threats.

"For example, if a company, especially in the financial sector, does not cooperate, attackers threaten to report the company's security flaws or data breaches to government regulators, such as the FCA, PRC or ICO," he explained. "This adds further pressure, as regulatory involvement can lead to investigations, fines and serious reputational damage.

"In short, criminals are now using the fear of legal and regulatory issues as an additional weapon to force victims to pay or comply," he continued.

Richmond-Coggan also pointed out that, with the improvement of technologies capable of detecting intruders attempting to breach systems, companies are also facing an old risk: people within their own organisation.

"Sometimes someone who already has access, such as a disgruntled or dissatisfied employee, may use their knowledge or access to harm the company or seek revenge, either acting alone or collaborating with someone outside the company," he explained.

He noted that some of the biggest data breaches or legal battles in recent times have occurred because of this type of insider threat.

University of Kent

Ransomware Inc.: The business, players, and power structures of digital extortion

Ransomware is no longer the domain of lone hackers, it's a sophisticated, profit-driven ecosystem fuelled by organised groups operating like modern enterprises. In this talk, Dr Jason R.C. Nurse, associate professor in cybersecurity, University of Kent, examined the key players behind today's most impactful ransomware campaigns, uncovering the structure, tactics, and motivations of threat actors ranging from ransomware-as-a-service (RaaS) operators to affiliates and brokers. He explored how these groups collaborate, evade law enforcement, and evolve in response to defensive measures.

Nurse said that what keeps him up at night is understanding who is behind ransomware attacks; how these groups grow, function, and conduct attacks; how they are successful, profitable businesses; and whether there is a chance of stopping them.

The associate professor spoke about some research he did in which his team gathered as much information as possible on ransomware groups, analysing over 500 documents as part of the study.

With the help of a leak of chat logs at ransomware group Conti, his research team were able to gain a sneak peek into who these people are and how they function.

"I was blown away to understand and reflect upon how these groups grow their businesses," he said.

The research found that these groups often target new recruits from previous criminal backgrounds through both underground forums and legitimate job recruitment websites.

He explained that these new recruits are vetted via interviews, deposits, proof of prior cyber work, recommendations, and evidence they have hacked before, as well as through refer-a-friend bonuses.

"They are copying how recruitment works in legitimate businesses," continued Nurse.

He shared how payments across three of the top ransomware groups work.

He revealed that at Blackcat, affiliates are paid up to 90 per cent commission, while Lockbit cyber hackers receive ransoms and pay the main group 20 per cent commission. Conti affiliates get paid a set wage.

"Blackcat would award plus status to affiliates with $1.5 million income, which gave access to DDoS services, allowing them to

be more effective," Nurse told delegates.

He said that for some groups, they even have an option to call for legal assistance on standby. This service can inform criminals of what things they can do to push the victim's buttons to make them worry about regulation, he said.

Nurse also explained that many ransomware groups are not pitching themselves as criminals, instead they call their groups facilitators of "post payment penetration testing". In other words, they are saying they are there to help highlight vulnerabilities, and that the ransomware is a request for payment for their services.

He explained that brand perception and recognition is also important for ransomware groups, with Lockbit for example paying people £1,000 to get a tattoo with the group's branding.

Panel

AI versus zero-trust: Reinventing financial cyber defences

In this session, speakers examined how artificial intelligence is reshaping attack methods and how zero-trust can offer financial institutions a more resilient defensive posture. The discussion looked at technical advances, human vulnerabilities and the organisational realities of implementing modern security models.

Temi Afeye, senior AI scientist at Lloyds Banking Group, described the dual nature of AI as a challenge. He said the sector now faces both technical and human centred threats driven by rapid advances in synthetic media and model capability.

"If you wanted to write a phishing email in the past, people had different levels of skills," he said. "Now you can deploy an algorithm that can understand what people would be susceptible to and then focus at scale."

He added that deepfake audio and video, automated reconnaissance, and model poisoning are now all part of an expanding threat spectrum.

Afeye illustrated the sophistication of hyper-personalised attacks with his own experience.

"I see phishing emails all the time, but this one was very particular because of something I was looking for," he said. "My first thought was how could somebody know I had been searching for this, so I clicked on it - thankfully it was an internal security test."

He said this demonstrated how easily attackers can harvest browsing history and behavioural data to create credible traps for their victims.

Thomas Knowles, head of security operations at ClearBank, said that banks are seeing more fraudulent documentation, more synthetic identities and a rising number of attempts to use deepfake technology to infiltrate organisations.

He noted that LinkedIn data breaches and similar leaks have created long lasting material for attacks as users do not recreate their profiles and their job history does not change.

Turning to zero-trust, Knowles emphasised that the model represents a fundamental shift in how identity and access are managed.

"With zero-trust you predominantly look at an assume breach posture as pretty much any activity has to be checked," he said. "Historically, if you were on the VPN you could talk to everything and that causes issues."

Knowles described zero-trust as "putting your users on a desert island and building little bridges with guards," which ensures continuous validation of user identity.

He stressed that zero-trust is "an umbrella term using existing platforms and taking a new approach," not a standalone technology. However, legacy infrastructures often resist this model.

"Legacy systems bring challenges to implementing zero-trust," he said. "Sometimes they cannot protect against something that does not want to be protected."

Time, cost, specialist skills and organisational culture are additional barriers in setting up zero-trust measures.

Afeye explained how zero-trust can support AI safety by enforcing accountability throughout the model lifecycle as data sources, training pipelines, and deployment processes must all be scrutinised.

"My second biggest job after building a model is the risk involved," he said. "We cannot eliminate all risk, but we build a sensible level of trust."

The panel concluded that while AI is accelerating threats, zero-trust provides a viable framework for containment and financial institutions need to be able to measure it.

Knowles noted that institutions must first establish metrics such as mean time to detection and mean time to response.

If lateral movement becomes harder and detection times fall, organisations can attribute that to the controls they included and the zero-trust methodology in place, he added.

Cyber Defence Alliance

Keynote – Intelligence in action: A deep dive into Operation Stargrew

In his keynote speech, Craig Rice, chief executive of the Cyber Defence Alliance (CDA), highlighted the organisation's role in combating large-scale phishing attacks, including its involvement in Operation Stargrew.

The operation focused on dismantling the Labhost platform, responsible for stealing 480,000 credit card numbers and 64,000 PINs worldwide, with cybercriminals creating tools to enable fraudsters to deceive people using fake text messages.

"The criminals sold these phishing-as-a-service kits through the LabHost platform, enabling other scammers, even those without technical skills, to send texts that fooled people into giving up personal information," he explained.

The operation led to nearly 40 arrests across the world, with about 70,000 people in the UK identified as victims. "The takedown followed a two-year investigation led from the UK, with police raids coordinated in 17 countries. Finally, LabHost was shut down after this major police operation."

Rice emphasised how the mission showed that the approach to fighting cybercrime is changing.

"We are no longer just reacting and defending but are now able to hit back at criminals by taking offensive actions," he said.

He then outlined the different 'levels' of intelligence work.

"Level 1 consists of trend analysis, big data-based information that helps to understand general issues but is not very usable," explained Rice.

Level 2, he said, consists of security intelligence that provides practical, often immediate advice needed to prevent specific attacks.

"Level 3, called threat intelligence, provides details on how specific attackers operate, allowing organisations to adapt their defences," he added. "These three levels are common in most organisations."

Rice said that the CDA focuses on level 4 intelligence.

"This identifies exactly who the criminals are, where they live, their contact details and why they should be arrested, information that is then passed on to the police for action," he said.

He then described how the CDA and law enforcement agencies collaborated in planning the dismantling of the cybercrime network.

"Once we had gathered reliable information on specific criminals, including evidence of crimes committed against 19 CDA member banks, we met with the police to decide who to target first," he said. "During the operation, we took care not to alert the public – especially through the media – about victim support actions, to prevent criminals from copying or abusing these communication channels."

He added that although the arrests seem impressive, the true measure of success is not just the number of people captured, but how effectively they manage to destabilise the criminal network, creating mistrust among members and concern about being targeted.

"LabHost was just one of many such platforms," he told delegates. "When they shut it down, it created panic and uncertainty among the criminals."

He stated that, to amplify this effect, law enforcement used "digital psychological operations", sending each criminal a personalised message to let them know how much law enforcement knew about them.

"This tactic is intended to cause paranoia and further fragment the criminal community," Rice explained.


FStech
CyberSecurity Live 2025
www.fstech.co.uk/cybersecuritylive
Follow the event on X: @FStechnology #CyberSecLive