FStech

CyberSecurity Live 2023

5 October 2023

Hilton London Tower Bridge

CONFERENCE OVERVIEW

Sponsored by:

Bottomline. CISCO Fortanix® Security, *wherever* your data is THREATLOCKER

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

CONTENTS

CyberSecurity Live 2023

Jonathan Easton
Editor, FStech

Welcome to the CyberSecurity Live 2023 Overview.

Within, you will find a summary of the key themes and topics that emerged throughout the conference in central London, along with a glimpse of the presentations, panel discussions and keynote speeches that took place.

Two main overarching themes dominated much of the conference and informed much of what was talked about on the day.

The first was a very timely theme and one which appears to be an inevitable part of speculating on the future in 2023: artificial intelligence.

AI is revolutionising the defence strategies of financial institutions against cybercrime, and groundbreaking applications such as anomaly detection, behaviour analysis, and predictive modelling are helping FIs to tackle the increasing sophistication of threats. However, cybercriminals are also leveraging the emerging technology, and the alarming availability of malware on the dark web is making it easier than ever for malicious actors to target the sector.

The second theme is one which has been an ever-present in the digital age: operational resilience.

The theme was addressed both from the technical side – in the adoption of Zero Trust principles to dismantle traditional security perimeters – and from a cultural perspective of ensuring that FIs are protected from insider threats and making sure that everyone inside the business is on the same page when it comes to security.

These themes were littered through the day and directly addressed through panels and keynote speeches, while also informing excellent presentations on wide-ranging topics including cyber insurance and the future of quantum computing.

We hope that you find this overview a useful source of key insights, and we look forward to welcoming you to our future conferences!

AGENDA

08.30 - 09.00: Registration and refreshments

09.00 - 09.10: Chairman's welcome

- Jonathan Easton, Editor, FStech

09.10 - 09.40: Keynote speaker - Navigating today's threats and beyond: Cyber and operational resilience

- Suman Ziaullah, Head of Technology, Resilience and Cyber, Financial Conduct Authority (FCA)

09.40 - 10.10 Expect the Unexpected: Insider Threat-as-a-Service

- Ruud Grotens, Head of Solution Consulting, Bottomline

10.10 - 10.40: Panel session: A culture of cyber resilience: Empowering FSIs to foster company-wide cybersecurity responsibility

Panellists:

- Dr Maria Bada, Lecturer in Psychology, Queen Mary University and RISCS Senior Fellow on Cybercrime
- Guillaume Ehny, CISO, Kroo Bank
- Craig Parker, Information Security Officer, Investec Specialist Bank London
- Oge Udensi, Head of Cyber GRC, Sumitomo Mitsui Financial Group (SMBC) EMEA

10.40 - 11.10: Confidential Computing in Finance: Bridging Innovation, Cyber Security and Regulation

- Rob Stubbs, Regional Sales Director – EMEA, Fortanix Inc.

11.10 - 11.40: Coffee break

11.40 - 12.10: Is cyber insurance helping to mitigate the threat of ransomware?

- Dr Jason R.C. Nurse, Reader in Cyber Security, University of Kent

12.10 - 12.40: Panel session: Navigating the Future: AI Advancements in Safeguarding Financial Services

Panellists:

- Deepak Bhandari, Information Security Manager, Oaknorth Bank
- Darren Kangurs, Head of IT, Al Rayan Bank
- Mona Schroedel, Managing Associate, Freeths

12.40 - 13.10: Embracing Zero Trust to Remain Secure

- Scott Manson, Director, UKI Cyber Security Practice, Cisco

13.10 - 14.10: Lunch break

14.10 - 14.40: Panel session: Breaking barriers: Zero Trust and Cyber resilience strategies for safeguarding financial services – *sponsored by Cisco*

Panellists:

- Lorenzo Grillo, Managing Director – Europe & Middle East Cyber Risk Services Leader, Alvarez & Marsal
- Scott Manson, Director, UKI Cyber Security Practice, Cisco
- Peter Smith, Chief Information Security Officer, Allica Bank

14.40 - 15.10: The Purpose of Endpoint Security: Stopping cyber threats or making you feel good?

- Seamus Lennon, Solutions Engineer, ThreatLocker

15.10 - 15.40: Keynote session: Cybersecurity challenges presented by advancements in quantum computing

- Adam Avards, Principal for Cyber and Third Party Risk, UK Finance

15.40 - 16.40: Chairman's closing remarks, quiz and drinks reception

The Financial Conduct Authority

Keynote – Navigating today's threats and beyond: cyber and operational resilience

Cybersecurity is a key part of a firm's operational resilience, as is dealing with cyber incidents. Over the past few years, there has been a significant increase in the number of cyber threats. It is now not enough for firms to only consider the threats they face today, they also need to protect themselves from those that are coming down the track.

In this opening keynote, Suman Ziaullah, Head of Technology, Resilience and Cyber at the Financial Conduct Authority (FCA) offered perspectives on the growing cyber challenges firms are facing today; how firms can get on track to comply with the FCA's operational resilience rules; how firms should be working to ensure supply chains are protected and what the FCA is doing on Critical Third Parties; and how seriously firms should be considering cyber insider threat.

Ziaullah began by drawing sectional comparison between the pace of change and adaptation needed in the field of medical research and cyber resilience in financial services, explaining that across both industries there is a lot at stake.

"It can feel like an arms race. On one side you have a threat that is constantly mutating and adapting, and on the other you have the experts trying to play catch up," the FCA executive told delegates.

He added that the regulator is seeing cyber challenges increase and adapt – threatening crucial infrastructure, with cyber-attacks becoming more sophisticated, including through integration of AI. As well as this, he said, there are increased digitalisation of business models, a larger attack surface with hybrid working, and more insider threat issues because of fewer cultural ties to organisations.

"The trouble with an advancing threat is that it is not just a question of whether defences can catch up, it's also about how quickly," he said. "It's not enough to just consider threats we're facing today. We need to prepare for those coming down the track too."

Talking about what firms should do to address these challenges, Ziaullah referred to the latest operational resilience rules, which state that by April 2025 firms must be able to deliver their important business services within impact tolerance within severe but plausible scenarios.

"That is less than 18 months away now, or just one budget cycle," he warned attendees, adding that the UK financial watchdog had seen some firms make positive steps while others have room for improvement.

He said that the FCA would like to see financial services providers testing for continuous or periodic assurance and to incorporate what they've learned from real life scenarios and simulations to test their ability to remain within impact tolerance. It is also key that firms include the rationale behind the type of testing conducted.

"Firms need to be open and honest with us as regulators over any concerns," he told delegates. "It's crucial you are doing the work now and don't take your foot off the pedal".

He emphasised that operational resilience pertains to the firms' supply chains and "firms remain primarily responsible, and ultimately accountable, for managing risks to their resilience arising from their third parties".

Regulators are proposing to oversee Critical Third Parties due to the systematic risks they might pose to the financial sector. Ziaullah said the ongoing work is supported by responses by firms to understand their reliance upon third parties, and is carried out in cooperation with FCA's partners. Notwithstanding this work on Critical Third Parties, the delegates heard Ziaullah emphasise that firms should be taking a proactive approach to managing their wider third party risks.

On emerging threats, Ziaullah touched on AI and Quantum. He warned that threat actors could use AI to tailor their ransomware and phishing attacks to firms. The speech concluded with Ziaullah stressing that the concept of Harvest Now-Decrypt Later attacks – stealing encrypted data for Quantum Computing to decrypt at a later point – could make Quantum a problem now, not just in the future.

Bottomline

Expect the Unexpected: Insider Threat-as-a-Service

Ruud Grotens, head of solution consulting at Bottomline opened his talk by sharing some statistics from a research report Bottomline recently undertook.

"The research found that 24 per cent of FSIs were concerned about insider fraud when it came to financial theft, while 22 per cent held concerns over insider fraud with respect to data leakage," he said.

Grotens noted the combined 46 per cent figure made insider fraud almost as worrisome to FSIs as external fraud.

Explaining further, Grotens told attendees that a major concern for FSIs was collusion between internal employees and external bad actors.

"This is what insider threat-as-a-service is all about," he said.

In the most common cases of insider fraud, Grotens explained that employees are approached through social media or other channels by external fraud rings to commit bad behaviour in return for money.

"However, it can be difficult for organisations to detect insider threat as-a-service or insider fraud in general," he said, noting there is often a lack of evidence when determining if insider fraud has occurred.

"This is the reason insider fraud is underreported, not reported at all, or incorrectly categorised as external fraud," he explained.

In taking a risk-based approach to mitigating insider fraud, Grotens suggested a "layered approach" including having strict procedures and policies in place, separation of duties, awareness training of staff, and detection monitoring to identify changes in internal behaviour such as a spike in in internal financial documents being viewed, which may not comprise an everyday part of employees' work duties.

In his conclusions around approaching insider fraud mitigation, Grotens told attendees: "There needs to be a healthy balance between trust and control."

Panel

A culture of cyber resilience: empowering FSIs to foster company-wide cybersecurity responsibility

In this session, panellists explored the pivotal role of organisational culture in fortifying cyber resilience. They delved into strategies that empower financial institutions to embed cybersecurity as an integral responsibility across all levels and departments, while real-world case studies illuminated how effective leadership, continuous education and a shared commitment can engrain a proactive cybersecurity mindset.

It also addressed challenges in shifting attitudes, the role of executive buy-in, and fostering collaboration between IT and non-technical teams.

Exploring how financial institutions foster a cultural shift that makes cybersecurity a collective responsibility across all levels of the organisation, Craig Parker, information security officer at Investec Specialist Bank London said that culture is "borne out of a company's experience over time". He added culture represents "rituals of things you do together and the behaviours when you're alone and no one is watching".

Guillaume Ehny, chief information security officer (CISO) at Kroo Bank said that the most important consideration in terms of strategy is understanding that everyone is responsible.

"It needs to be applied all the way through an organisation," he said. "Security culture is what employees do when the security team is not around."

Talking about the "human factor", Dr Maria Bada, lecturer in psychology at Queen Mary University and RISCS senior fellow on cybercrime said that companies "cannot expect employees to have more active behaviour when they don't have adequate training".

"If they don't have that understanding they can't prevent it," she said.

Oge Udensi, head of cyber GRC at Sumitomo Mitsui Financial Group (SMBC) EMEA, said that it is important firms consider the language they choose.

"Are you getting punished or being retrained?" she asked. "It's about identifying how to make language inclusive and clear, putting employees responsible for their own security."

Talking about what approaches FSIs adopt to educate and sensitise employees at every level, Ehny said that it is important to understand your audience.

"We're not talking to our engineers in the same way as marketing or board level," he told delegates. " It's important to use the right language and tools to foster that message."

Parker said that while it can be useful to use frameworks that are well established you "need to be a bit more innovative" because there's "not a one-size-fits-all approach".

Udensi said that the CISO should be part of the board and c-suite as they have the most responsibility on security.

"If they're not at that level, then you're not doing it right," she said.

Dr Bada agreed by saying that leadership and top management should be playing a key role.

"Top management must have clear communication and always follow best practice themselves," she explained.

Fortanix

Confidential Computing in Finance: Bridging Innovation, Cyber Security and Regulation

Rob Stubbs, regional sales director – EMEA at Fortanix began his presentation by highlighting the key challenges for FSIs around cybersecurity and compliance.

"Banks and FSIs are targeted by organised crime, and you need to have the best cyber protection available," he said. "Similarly, compliance is ever more important."

Stubbs then began explaining what confidential computing was and how it could help in these areas.

"Confidential computing is a means of protecting data in-use by performing computation in a hardware-based, attested, trusted execution environment," he explained. "It provides the ability to encrypt data or code while it is in use – something which was not previously possible."

Explaining its use cases, he said: "It's ideal for data protection applications including cloud security, and for AI and machine learning applications such as credit decisions, financial risk and fraud detection."

Stubbs went on to share that Fortanix products are built on a systems tool kit (STK) which is also open source for developers.

"Our enclave platform underpins all our products; data security manager is our unified data security platform and is used by over 150 enterprises worldwide; and our enterprise computing manager enables the deployment of new and existing within the confidential computing environment," he said.

Stubbs then shared how a large investment bank had benefitted from its service provision when it wanted to modernise its on premises data backup environment by migrating it to AWS.

Stubbs said the bank chose Fortanix because its encryption capabilities were "easily integrated into their data backup workflows," and noted that this client always has full control of their encryption keys and therefore the data.

In summary, Stubbs said: "Fortanix solutions are built on confidential computing technology that can enable you to improve the security and compliance of your existing systems."

University of Kent

Is cyber insurance helping to mitigate the threat of ransomware?

In this session Jason R.C. Nurse, associate professor in cybersecurity, University of Kent, looked at whether having insurance has increased the risk of cyber attacks and whether it is something financial services institutions should put on their shopping list.

He said that two of the main reasons that businesses buy cyber insurance are the legal support they are offered following a breach and insurance against loss of earnings.

"Insurers can be really good at helping organisations assess where they are with their security practices and they can offer an objective perspective on what you are doing," Nurse said. "They can come in and say 'I will underwrite your policy, but you have to implement this standard. If you have this framework, I'll give you a discount on your premium'."

However, Nurse warned that not all insurers have adequate knowledge of the cyber industry and are often unaware of what good cybersecurity practices are.

He said that different insurers evaluate and review risk differently from each other and this could lead to varying levels in coverage.

Next, Nurse explored the accusation that insurers are funding organised crime by paying ransomware claims.

He said that cyber criminals are targeting organisations that have cyber insurance.

The associate professor pointed to a case where a cyber criminal had hacked their way into the system, worked their way through the company's list of clients, and then targeted the insurer.

"There are a lot of people saying that the insurance industry is the problem because people are getting hacked, people are getting breached," said Nurse. "The people then go to their insurer and tell them they have been breached. But the question for me is, is this happening enough to be systemic?"

He said that his research had shown that cyber insurance was good at providing access to a support system after a breach. Companies have access to lawyers, PR specialists as well as financial support to get their systems running again. However, Nurse said, insurance has no influence on whether a payment was made during a cyberattack.

"Often insurers are not clear that the ransomware payment is the option of last resort," Nurse told delegates. "Insurers say 'there are your options', they provide access to liquidity for payments."

Insurers, Nurse said, are now doing everything to make sure that payment is the last possible thing to happen.

Nurse quoted a subject from his research, who said that no one wants to go on record stating that insurance has amplified ransomware attacks but was grateful for the support it could provide.

"The net effect of cyber insurance is ambiguous," Nurse said. "But it is still not adopted by organisations that could use it."

Nurse finished off the session by warning that cyber insurance could lull people into a false sense of security and offer help when needed, but the threat of reputational risk remains.

Navigating the Future: AI Advancements in Safeguarding Financial Services

The panellists began the discussion by sharing how their organisations were currently using AI.

Deepak Bhandari, information security manager at Oaknorth Bank said it was using AI in areas including transaction monitoring and around actions users make.

"This can tell us whether the traffic from a customer perspective is expected or anomalous," he said.

Darren Kangurs, head of IT at Al Rayan Bank said that AI is helping the organisation identify anomalies.

"In order for that to be effective, you need reliable, high-quality data and the AI needs to have the right data to perform functions like anomaly detection effectively," continued Kangurs.

He also pointed to the importance of maintaining a continuous update of the models used for AI since the threat landscape develops rapidly.

"If you don't stay updated, then you're very quickly going to be out of kilter with the threats that are coming through," he said.

Deepak Bhandari pointed out that as collaboration in cyber risk between FSIs rises and sensitive information is being shared, the right access controls must be in place and general data protection regulations (GDPR) should be adhered to.

Next, Mona Schroedel, managing associate at Freeths reflected on the implications of FSIs adopting biometric authentication.

"This data is more than someone's address because once it's gone, you can't change it," she said. "This why it is extremely important that this data is forever protected."

Deepak Bhandari noted that with rising AI sophistication, it has become easier for bad actors to use biometrics such as a person's voice to circumvent these security parameters.

"Biometrics was originally better at fraud prevention, but AI has unfortunately problematised this," he said.

Mona Schroedel shared that she was advising a client on a tool which sifts out spoof calls for the elderly, analyses the way a conversation develops, and raises an alarm when it deviates from the anticipated progression.

She closed out her thinking by suggesting a higher degree of training will be needed moving forward to make organisations appreciate just how important the data of individuals is, and therefore how important it is to handle and secure it effectively.

On the evolution of human expertise alongside AI, Schroedel added her feeling there was a conceptual problem that AI is the answer for everything and humans can rest easy.

"I think this view is wrong," she said. "AI should be viewed as a supportive tool."

Darren Kangurs was in agreement that human-AI interaction is more of a partnership.

"AI provides the data so that humans can make decisions on the basis of that data," he said.

Cisco

Embracing Zero Trust to Remain Secure

While the flexibility of hybrid working has empowered employees in the financial sector with greater control over their schedules, leading to improved focus and better work performance, many CISOs now find themselves dealing with the challenge of securing network access across multiple locations.

In this session, Scott Manson, director of the UKI cyber security practice at Cisco, discussed the benefits of Zero Trust Networks as a solution to address these security challenges. He explored how investments in this area could support financial institutions in their journey towards implementing a complete Secure Access Service Edge (SASE) framework.

Manson started by asking how companies could ensure that all their systems work together.

"How do we avoid creating chaos for our customers by bringing more things into the mix," said Manson. "Our approach is platform play. "

He continued: "You need to have a platform that can counter the noise, understand, report and is a joy to be around."

He said that Zero Trust benefits are aligned to users, IT, and developers. He added that it is essential to develop these for everyone.

"It's all about trying to put together the use case of the problem you are trying to fix," he added. "It's all about simplification.

"Customers have complicated ways of accessing applications. Different users have different access needs. Everyone wants to access all the applications, but they don't often play perfectly together."

He explained that platforms need to deliver the right applications at the right time. Additionally, Manson said, platforms need to connect users to apps in a way that is secure.

Manson concluded the session by recommending that firms test themselves against the cyber readiness index and urged attendees to keep their systems simple.

"Less is more," he told delegates. "You need integrated systems rather than the best ones.

"Research shows that the average customer only uses about 30 per cent of a programme. Amazingly few features are switched on."

Panel

Breaking barriers: Zero Trust and Cyber resilience strategies for safeguarding financial services – sponsored by Cisco

In this session, a panel of experts discussed the essential factors that underpin a resilient cyber landscape. They looked at the intricacies of Zero Trust adoption and how it is enabling the proactive mitigation of threats in interconnected digital systems.

Peter Smith, chief information security officer at Allica Bank, started off the session by saying that financial institutions needed to strike a balance. They need to keep on top of cybersecurity threats, but not annoy their customers by limiting their ability to make payments, he explained.

Lorenzo Grillo, managing director – Europe & Middle East cyber risk services leader at Alvarez & Marsal said that it is important for financial institutions to remain adaptable.

"Being 100 per cent compliant with regulations does not mean that you are resilient," he said. "It is not enough, if it were, business would be booming.

"It is more important to focus on the impact they have."

Grillo added that he was uncomfortable with fully trusting anything that claimed to be fully secure. "The Zero Trust model is a good idea, but you have to focus on the constant monitoring of your systems, your devices, your users" he said.

Scott Manson, director, UKI cyber security practice at Cisco said that firms need to decide what their priorities are when it comes to security. Firms should not "just throw technology at it," but look at where they currently are on their journey and what they need to do to get where they want to be.

"Financial services is an industry which is more mature than others," Manson said. "When you reach maturity, how can you get incremental gains? You need to use frameworks to assess where you are and find the industry mean."

Smith said that the Zero Trust models can take many forms, adding that it is important to connect different users to different models to make it work properly.

"With the Zero Trust model we need to have a way of connecting you to all these different systems with different methods," explained Smith. "Customers shouldn't have to worry about switching between VPNs to access what they need.

"Additionally, we have to hold a lot of data on people and keep it confidential. We have to make sure that people can't accidentally download it."

Manson said that that while cloud applications have benefitted the financial services industry by providing agility and cost savings, they have created other problems.

"We are still catching up to a scenario that involves opening your laptop and connecting to the application you require without it being onerous," he told delegates. "VPNs, proxy, multifactor authentication – it's a disaster to be honest. It's very hard for people who are just trying to use an application. We are moving towards systems that can do that."

Manson concluded the session by saying that that financial services firms need to cut out the noise and look at real solutions.

"To get the most out of the product, you need to make sense of the data," he said. "You need to set a minimum threshold and build on top of the bassline you set."

Lorenzo Grillo, Managing Director – Europe & Middle East Cyber Risk Services Leader, Alvarez & Marsal
Scott Manson, Director, UKI Cyber Security Practice, Cisco
Peter Smith, Chief Information Security Officer, Allica Bank

Lorenzo Grillo, Managing Director – Europe & Middle East Cyber Risk Services Leader, Alvarez & Marsal
Scott Manson, Director, UKI Cyber Security Practice, Cisco

Threatlocker

The Purpose of Endpoint Security: Stopping cyber threats or making you feel good?

The plethora of security vendors operating in today's marketplace can be overwhelming. With so many options, it's easy to be distracted with the latest, greatest, shiny tool. In this session, Eoin McGrath, solutions engineer at Threatlocker took a deep dive into the purpose of cybersecurity and how firms can use that to their operational advantage today.

McGrath explained that it's very important when thinking about Zero Trust to acknowledge that the breach is going to happen before it happens.

"We want to limit the lateral movement, the possibility to stop what the bad people can do," he told delegates, talking through some of the biggest cyber threats and remedies.

He talked about how everyone in IT has an IP scanner and that if they observe a recent breach on a system, this is one of the first pieces of software they'll find.

"They can use it to discover lots of things – printers, laptops, desktops – from that they can infer a lot from your system," explained McGrath. "A legitimate piece of software can give a threat actor quite a bit of intelligence."

McGrath explained how Threatlocker's technology allows through what is needed and blocks out everything else.

"Blocking everything sounds drastic, but we have a learning part where we can identify legitimate systems," he explained. "We all want to think our environment is as secure as we could possibly make it, for example when we have a burglar alarm, it makes us feel safe."

He continued: "It's exactly the same with security posture environments – people will say, we have all of these tools and we're protected against viruses, but are you protected against insider threats? Probably not."

He explained that the majority of ransomware attacks take place outside of business hours.

"No matter how many protections are in place, there is always risk and you need to mitigate against that risk," he said.

UK Finance

Keynote – Cybersecurity challenges presented by advancements in quantum computing

Adam Avards, principal for cyber and third-party risk at UK Finance, began his presentation by referencing mathematician Peter Shaw.

He shared that in 1994, Shaw determined that if applied in a certain way, it was possible for a quantum computer above a certain power to crack RSA encryption (a public key cryptosystem) and a Diffie–Hellman elliptic curve, which is a mathematical method of securely exchanging cryptographic keys over a public channel.

Avards said that these encryption methodologies underpin many of the encryption algorithms still used today to secure data in sectors including finance.

"Quantum computing is not just a faster method of classical computing, this is technology which ultimately operates in a completely different way," he explained. "In doing so, it manages tasks that are built to be intractable tasks, such as those that underlie our security and use of public key encryption."

Avards went on to explain that quantum computers run on Qubits, which can be either '01' or anywhere in between with an infinite number of possibilities between the two – "and that is the core of what makes it different."

He said that the ability of quantum relates to information security, but the likes of password length and strength will "go out the window" once there is a cryptographically relevant quantum computer. That's because, he continued, "what's underlying the security of much of this is the encryption algorithms", which would no longer be viable with the advent of quantum computing.

He went on to tell attendees that when engineering catches up with the theory to achieve a cryptographically relevant quantum computer, "we can term this as 'Q Day' – it will happen, and it will change the world."

"One thing UK Finance has been looking at is how those in the financial sector can upskill themselves to be able to leverage this technology in an advantageous yet protective and informed manner," he told delegates.

On when we can expect quantum computing to begin affecting the world, Avards told attendees that while the rate of technological advance is unsure, there's "probably a one per cent chance of Q-day happening within the next year" but around an "80 per cent chance of it happening within the next 10 years."

On the advent of quantum, Avards also pointed out that "without proper preparation, this change to the world could be more negative than positive", with regard to hostile states who could make malicious use of the technology.

In closing, Avards told attendees: "Today, as representatives within your respect fields, I hope you came away knowing quantum computing is no longer the grounds of science fiction – it is going to happen and awareness needs to increase among not only the technology and cybersecurity staff in your respective organisations, but amongst the business leadership."

FStech

CyberSecurity Live 2023

www.fstech.co.uk/cybersecuritylive

Follow the event on twitter: @FStechnology #CyberSecLive