# Cyber Security Summit 2023

# Resilience and vigilance the key for the future of global cybersecurity

Summit hears how firms need to equip themselves with the right tools to fight off the emerging threats to their cybersecurity


Front row (L-R): Jenni Parry, Associate Director, Cyber Risk, Aon; Puneet Kukreja, EY UK & Ireland Cyber Leader; Eilish O' Connor, Chief Technology Officer Viatel Technology Group; Paul C Dwyer, Chief Executive Officer, Cyber Risk International
Back row (L-R): Carol Murphy, Partner and Head of Technology Risk, EY Ireland; Shay Cloherty iQuest; Richard Bainbridge, Senior Manager, Cyber Security, BT; Virginia Lee, Strategic Head, BFSI Cyber Security, Ireland Operations (Global), Catherine Williams, Threat Intelligence Specialist, BT

QUINTON O'REILLY

The latest Cyber Security Summit in Croke Park on Thursday, October 19, was set for its busiest one yet. A packed audience, numerous vendors, and the late morning having three separate streams showed just how essential this event is.

The welcomes began with summit chair Jess Kelly, technology correspondent at Newstalk and *Connected* magazine columinist, noting the stellar lineup that awaited them before being followed by Shay Cloherty, managing director of iQuest & *Business Post* LIVE, who highlighted the summit's importance.

"No organisation is completely secure, and it's a matter of when, not if, for most of us," said Cloherty. "Equipping yourself and your business with the correct cybersecurity knowledge and tools has never been more important."

Ossian Smyth TD, Minister of State, Department of Environment, Climate and Communications, gave his government address on Ireland's cyber security status to kick the summit off.

Beginning by mentioning how Ireland is a highly connected country and how the national cybersecurity centre has doubled its staff to more than 50, successful protection means everyone knows their role.

"In the same way that the fire brigade isn't going to prevent your house from catching fire, it is everyone's responsibility in businesses and as individuals to protect ourselves," he said. "The cybersecurity centre is there to provide the information, education and awareness in how to protect yourself and in an attack, will be the people who come out to help and assist you."

Following was the first international keynote address delivered by Allison Miller, CISO and senior vice president for Optum USA. In a passionate and honest address, Miller highlighted how meaningful connections and supporting people are as cybersecurity skills are learnt.

"None of us are born with cybersecurity knowledge, but we know the technology changes faster than when we can get the grass cut," she said. "If you have someone who has fire in their belly, are willing to learn, and there are people behind them, even if they know they're not going to hit the ground running, they're going to be successful."

Up next was the first panel discussion of the day on strengthening EU-wide resilience featuring Richard Browne, director of the National Cyber Security Centre (NCSC), Jacky Fox, security European lead for Accenture and board member of Cyber Ireland, and Colonel Mark Staunton, director of communications, information services & cyber defence for the Defence Forces.

When asked whether companies invest in the right areas, Browne mentioned that organisations often spend on cybersecurity in an uncoordinated and unstructured way. Instead, they need to take a step back and assess where their spending is going.

"It's not just about money, it's about structure and organisation," he said.

Before the morning sessions were done, there were three significant presentations. The first was on the importance of OT security to modern businesses, delivered by Richard Bainbridge, senior manager of cyber security at BT.

Mentioning connection as one of the keywords, he said the importance of protecting your supply chain, such as narrowing down the crucial elements of it to ensure continuity.

Next was Paul C Dwyer, chief executive of Cyber Risk International, who gave the keynote presentation on cyber risk and the upcoming Digital Operations Resilience Act (DORA). He brought up a keyword that would echo throughout the summit: resilience.

"Cyber resilience is a team sport, and while defence is good, resilience is better," he said. "Mistakes will happen, attackers will be successful at times, but will you be resilient, be able to deal with that and respond and continue business as that's the essence and spirit of DORA."

Puneet Kukreja, EY UK & Ireland Cyber Leader, wrapped up the morning sessions by discussing AI-driven cyber security. While a double-edged sword, Kukreja recommended starting with basic use cases first if you want to implement AI into security and go from there.

Once the morning coffee break and exhibition viewing were done and dusted, the summit split up into three different streams. The first concerned IT security and strengthening your systems, chaired by Kelly.

It began with an international keynote on the number one priority for strengthening systems, which was delivered by Monika Kutějová, a cyber security specialist in Czechia.


Allison Miller, Chief Information Security Officer and Senior Vice President, Optum USA


Michael Dowling, Professor of Finance, DCU Business School; Elaine Hanley, Partner, Cybersecurity Services, IBM Consulting


Oluchi Anyabuike, Postgraduate Student, UCD, Senior Software Engineer, Fidelity Investments; Donna O'Shea, Chair of Cyber Security, Munster Technological University (MTU) and Gabriel Conway, Enterprise ICT Assurance Manager, Data Protection Commission (DPC) Pictures: Leon Farrell


Donna Creavan, Director ICT, Governance & Corporate Services, Irish Prison Service; Dr Anila Mjeda, Lecturer in Cybersecurity, Munster Technological University (MTU); Carol Murphy, Partner and Head of Technology Risk, EY Ireland; Eilish O' Connor, Chief Technology Officer Viatel Technology Group; Jenni Parry, Associate Director, Cyber Risk, Aon

## Splitting up the streams

Following this was a panel discussion on emerging technologies featuring Donna O'Shea, chair of cyber security at Munster Technological University (MTU), Oluchi Anyabuike, postgraduate student UCD, senior software engineer at Fidelity Investments, and Gabriel Conway, enterprise ICT assurance manager for the Data Protection Commission (DPC) before it ended with a spotlight on Ireland blockchain opportunity delivered by Alejandro Gutierrez, chief executive of Defactor Labs.

The second stream was on cybersecurity in practice, chaired by Dr Andrea C Johnson, CIO of Pipedrive and president of Women in Technology and Science (WITS). This stream began with a keynote address from James Caffrey, head of capacity building for the National Cyber Security Centre (NCSC), who spoke about cybersecurity as an enabler for economic growth,

It concluded with a panel discussion on building cyber resilience against chronic threats, which Dr Johnson noted how it was an all-female panel. The panel included Donna Creavan, director ICT, governance & corporate services at the Irish Prison Service; Eilish O' Connor CTO for Viatel Technology Group; Dr Anila Mjeda, lecturer in cybersecurity for Munster Technological University (MTU); Jenni Parry, associate director of cyber risk at Aon, and Carol Murphy, partner and head of technology risk at EY Ireland.

The third stream was on cybersecurity policy and regulation and was chaired by Jennifer Cox, director for Ireland at Women in Cyber Security (WiCyS) UK & Ireland. This stream began with a panel discussion on implementing DORA featuring Dwyer again, joined by Gina Dollard, head of cyber resilience and strategic regulatory relations at AIB, and Ashling Cunningham, CIO of Irish Life.

Following that was another panel looking at how to prepare for compliance for the new Network and Information Security Directive Revision 2 (NIS2), which included Jane Corr, former CISO for Canada Life Group Services, Ita O'Farrell, head of compliance for the National Cyber Security Centre (NCSC), Department of the Environment, Climate and Communications (DECC), and Jan Carroll, founder of Fortify Institute.

> **It's awfully sad if we've something that has huge potential and throw it out because of the risks**

## Investing in protection

Once the afternoon arrived, the attendees reunited for the final batch of talks and panel discussions.

It started on strong with a presentation from Catherine Williams, threat intelligence specialist at BT, who covered using cyber threat intel to protect a global network.

Mentioning how security is just as much a cultural mindset, she stressed the importance of being prepared.

"If you can be proactive and prioritise what you monitor, you can be prepared for the next cybersecurity incident," she explained. "What should you prioritise? Some threats will affect you more than others, so prioritise the threats that would be most detrimental to your business."

The following presentation was from Steve Brown, VP of cybersecurity and resilience at Mastercard Europe, who looked at proactively managing systemic risk in your supply chain.

Referencing DORA as a friend to cybersecurity, he mentioned how it can be the encouragement boards need to invest more in protection and an opportunity to work with your supply chain to assess and identify vulnerabilities.

"Its not to use it as a stick to beat someone with but use it as a method of collaboration," he said. "Work with that supplier and allow them to see an actionable mitigation plan you're building with them."

The penultimate panel discussion of the day looked at the potential Ireland has for leading the charge in ethical AI, featuring Elaine Hanley, partner of Cybersecurity Services at IBM Consulting, and Michael Dowling, professor of finance at DCU Business School.

In an insightful discussion, the panel weighed up the risks and benefits of AI and gave counterpoints to the knee-jerk reactions of positivity and negativity surrounding the subject.

"It's awfully sad if we've something that has huge potential and throw it out because of the risks," said Hanley. "If you look at the internet, we can't live without it now, but when that started, there were inherent risks that made people afraid. What we need to do is to recognise those risks and have a plan on how to deal with those risks."

The final panel discussion was on creating a cyber workforce fit for the future. Cox and Dr Johnson joined by Virginia Lee, strategic head of BFSI Cyber Security, Ireland Operations (Global), Tata Consultancy Services, and Sarah Drew, director of security engineering at Salesforce.

When asked how important it is to have different types of personalities and people in cybersecurity, Lee said it was critical. As mentioned in previous talks, many people enter the industry via other careers, which helps benefit cybersecurity.

"Some of my best security engineers came in because of their language skills," she said. "We bit the bullet and brought linguists into the team, and they flew. Any job spec you see in cyber, they wouldn't have got in the door."

"They have a different way of thinking and looking at problems and became huge assets to the team."

With another cyber security summit finished, the shifting landscape requires new and original approaches to cybersecurity.

While AI gains much of the headlines, the day showed that resilience will require unlocking the creativity of its people to stay one step ahead.