Cyber Security Summit SPECIAL REPORT

Adnan Ahmed, head of ICT and chief information security officer, Ornua; Justin Ralph, chief technology officer, RCSI; Jonathan Healy, broadcaster and summit host and Paul Collins, SVP, regional information security officer, Europe, Elavon Financial Services (EFS) Maura Hickey

Nicola O'Connor, chief information security and IT risk officer, AIB and Tim Hynes, chief information officer, AIB Maura Hickey

Response, awareness and resilience key weapons against cyber attacks

In a landscape where even the largest and most influential organisations are subject to attack, this year's Cyber Security Summit brought together experts to discuss strategies and offer solutions, writes **Róisín Kiberd**

Six months after the HSE fell victim to ransomware, and the morning after a historic outage of Facebook, Instagram and WhatsApp around the world, 2021's Cyber Security Summit brought together experts in the field to discuss cyber strategy, best practice and industry trends, as well as an evolving threat landscape where no organisation – local or global – is safe from attack.

Ossian Smyth, Minister of State with Special Responsibility for Public Procurement and eGovernment, delivered a ministerial address to kick off the event. "Last year, our national cybersecurity centre had over 3,000 reports for the first time, and that number is going to climb in the future," Smyth said. "Irish businesses can expect as much attention from criminal gangs as businesses in other parts of the world."

After a review of the National Cybersecurity Centre, the government has decided to recruit 20 new members of staff and to introduce further measures to strengthen the centre, including the launch of a cybersecurity graduate training programme.

The first panel of the day, on responding to attacks on national critical infrastructure, was moderated by Tim Hynes, group chief information officer at AIB. "We've all read a lot about ransomware in the media," said Ashling Cunningham, chief information officer at Ervia, "I think we need to acknowledge that this is not personal; to criminals, this is business."

Nicola O'Connor, chief information security and IT risk officer at AIB, said that boards deeply wish to understand cybersecurity, and need to be kept constantly on alert.

Fran Thompson, chief information officer at the HSE, said that the organisation's attitude to cybersecurity has dramatically shifted: "We've been through a significant, and very damaging cyber attack, and our focus has changed from being an organisation that wants to improve the functionality of what it has, to now delivering an operation that is entirely bulletproof."

Discussing prevention, Richard Price, security and compliance leader with the worldwide public sector team at AWS, said that organisations need to take stock of their culture as part of their approach to cybersecurity: "Moving to the cloud causes organisations to think differently and ask if they truly have a culture of cybersecurity. The cost is distributed throughout the business. It is truly an entire business's problem."

Eoin Carroll, principal engineer at McAfee Enterprise, and Raj Samani, chief scientist at McAfee Enterprise, took part in a fireside chat on the impact of cyberattacks. Samani said that it's important to acknowledge the consequences of attacks: "The job has become higher profile, and the adversaries are getting better."

Fran Thompson, chief information officer, Health Service Executive, presenting virtually at the Cyber Security Summit

Richard Browne, acting director, National Cyber Security Centre and Steve Benton, director protect BT, deputy chief information security officer at BT Ireland

Discussing 'risk appetite' and the inevitability of threats, Carroll said that resilience is key: "When you talk about your threat model, and who you can and cannot defend against, ask yourself how quickly can you get back to business afterwards?"

Discussing "the current state of play for security in Ireland", Richard Browne, acting director of the National Cyber Security Centre, began by commenting on Facebook's recent outage, blamed publicly on a "faulty configuration change" which shut out not only their users, but Facebook's own employees.

"It goes to show that many of the systems we use to underpin this global network were thrown together 30 or 40 years ago," Browne said, "and we're still reliant on them today." Handling around 3,000 attacks, data breaches and incidents over the last year, Browne said that the centre's three focuses – response, awareness and resilience – work together: "The information we learn from response can be fed back into situational awareness building, and that can be fed back to resilience-building too."

Tom Digan, cyber resilience director of Dell Technologies Ireland and Northern Ireland, said "it's important to understand the motivations behind cyber attacks".

"Eighty per cent of attacks are motivated by financial gain, but we're seeing other reasons too, which need to be taken into account." "Malicious insiders" at companies including Tesla are responsible for a rising number of data breaches, as are "hacktivists" using their attacks as a form of protest.

Richard Price, security and compliance leader, Worldwide Public Sector team, AWS

Raj Samani, chief scientist, McAfee Enterprise

Roland Cloutier, global chief security officer at TikTok

Jan Carroll, cyber security lecturer at UCD Professionals Academy

Ian Porteous, Check Point's regional director of security engineering, UK and Ireland, was interviewed by Hugh McGauran, country manager for Ireland at the same company, on the subject of a "prevent-first approach" to risk-reduction. "By prevention-first, we mean neutralising attacks and neutralising malware, before it can get to the payload stage," said Porteous. "If you can prevent it from executing in the first place, then all of that downstream damage is prevented."

They were followed by a panel titled 'There's no such thing as perfect protection'. Justin Ralph, chief technology officer at RCSI, said that while the threat landscape has been radically altered by the explosion of IoT and working from home, the good news is that organisations are now more aware of the risks: "The more we communicate and share knowledge between companies, the more we'll be able to bridge the gap."

Adnan Ahmed, head of ICT and CISO at Ornua, said organisations need to constantly evolve: "In most cases, even if you invest everything it won't resolve everything, and some risks will remain."

Paul Collins, SVP and regional information security officer for Europe at Elavon Financial Services, said that it's important for cybersecurity experts to keep their message simple, and to explain the reality of these threats in full: "We can put 100 per cent of our budgets into technology, but we'll still always be open to attack."

Speaking "from the front line of security", Steven Benton, director of Protect BT and deputy CISO of BT Ireland, said that the past 18 months have changed how we understand cyber risk. "Organisations have massively increased and distributed their attack surface," he said. "Traditional perimeters around corporate networks have simply ceased to be."

Richard Dunne, IT compliance officer at Technological University Dublin, presented a case study on how TU responded to an attack on their systems. Within the first 24 hours, the university reset and recreated all privileged accounts, imaged the PC showing unauthorised access and took its servers offline, carefully monitoring and recording activity on their network in case of intrusions. "Containment is hugely difficult in a hybrid environment," Dunne said. "You can't just disconnect people anymore."

Speaking on cloud security and risks to cloud, Brian Cooke, CISO at Permanent TSB, said that cloud adoption and online banking has led to a cybersecurity tipping point. "I think there's a corollary with other sectors too," Cooke said. "Vendors are leading us into the cloud, whether we like it or not."

In a panel asking "How can we strike the balance between investment in technical defence and human factors solutions?" Stuart Halford, chief information officer at Goodbody, said that engagement and education are key. "Users need to understand the 'why'," Goodbody said. "Why is this useful, and why should they care? If you secure things too much they'll become unusable, and employees will bypass those measures just to get their job done."

Jan Carroll, a lecturer at UCD Professionals Academy, said that SMEs need to move away from viewing cybersecurity as purely an IT issue: "If they concentrate on high-priority issues like phishing attacks, and take the extra time to verify emails, and regularly review passwords and use of external hard drives, these are easy wins for small SMEs."

The programme concluded with an international fireside chat with Roland Cloutier, global chief security officer at TikTok.

"The work I get to do every day protecting this company is really fulfilling," Cloutier said, listing "ATOs" (account takeovers), bots and advanced malware among the threats he's tasked with mitigating. While the rapid growth of TikTok has brought challenges, Cloutier said that scale also brings new opportunities: "It means the business can accomplish things it needs to have. Scale gives you the capacity to deliver, deep into the business."

The number of ransomware attacks taking place in Ireland has increased by 413 per cent since last June of last year, and shows no sign of slowing down. 2021's Cyber Security Summit surveyed a landscape where even the largest and most influential organisations are subject to attack, and resulting reputational damage, but where simple measures – such as education, engagement and awareness training – can make a powerful difference.

Hugh McGauran, country manager for Ireland at Check Point and (below), Ian Porteous, regional director, Security Engineering UK & Ireland

Tom Digan, cyber resilience director, Dell Technologies Ireland and Northern Ireland