Cybersecurity Summit 2022 SPECIAL REPORT

From left: Colin Gaughan, data and cyber resiliency specialist, Dell Technologies; Chris Nickerson, CIO & CISO of Damovo and CEO of LARES; Puneet Kukreja, partner and head of Cyber, EY Ireland; Joshua Green, manager, Global Data Centre Operations, Cisco; Michael McNamara, senior manager, security and compliance, BT Ireland; Donna Creaven, director ICT, Governance & Corporate Services, Irish Prison Service; Rosie Coffey, head of Enterprise Applications Group, University College Cork; Paul C Dwyer, president, International Cyber Threat Task Force and Michael Kelly, head of operations, ECAS, BT Ireland

From left: Joel Aleburu, cyber security specialist; Colin Gaughan, data and cyber resiliency specialist, Dell Technologies; Jennifer Cox, head of communications, Cyber Women Ireland and Pat Ryan, detective chief superintendent, Garda National Cyber Crime Bureau

From left: Aoife Noone, chief executive, Noone Cyber Services; Rosie Coffey, head of Enterprise Applications Group, UCC; Enda McGahern, founder, Security Consultant IPS and Donna Creaven, director ICT, Governance & Corporate Services, Irish Prison Service Pictures: Maura Hickey

Boosting cyber defences against threats

Cybersecurity is a pressing issue for all organisations, yet as the threats evolve, so too do the sector's standards and understanding, writes **Quinton O'Reilly**

From left: Sarah Drew, director, security engineering, Salesforce; Fintan Swanton, senior consultant and managing director, Cygnus Consulting and chairman, Association of Data Protection Officers; Blessing Usoro, information security manager and founder, Cyber for School Girls and Niamh Vianney Muldoon, CISO, Fenergo

From left: Katie McCarthy, head of cybersecurity, Irish Water; Mary Kennedy, European cybersecurity and information services leader, Arup; Richard Browne, director, National Cyber Security Centre and Michael Kelly, head of operations, ECAS, BT Ireland

Neil O'Hare, CIO, Children's Health Ireland

Chris Nickerson, CIO & CISO of Damovo and CEO of Lares

Jess Kelly, Technology Correspondent, Newstalk and Summit Host

In her opening remarks, Jess Kelly, technology correspondent for Newstalk and chair of Cybersecurity Summit 2022, mentioned it was European cybersecurity month and how today will be an opportunity for "plenty of pearls of wisdom to take away".

The packed audience at Croke Park on Tuesday, October 18, took away much advice, knowledge and insights from the summit, where the theme was bolstering security strategies in an evolving threat landscape.

The summit started with a bang with the keynote address from Paul C Dwyer, president of the International Cyber Threat Task Force (ICTTF), which Kelly described as having the "wisdom and insight" to demystify the cybersecurity landscape.

Speaking about how the EU cyber strategy was making physical and digital entities more resilient, Dwyer described the situation as blind people looking at the same elephant; no matter where they are, the result is always an elephant. The same principle applies to cyber attacks, no matter who or what is responsible for attacks, they're the same thing.

"All roads lead to cyber threats or cyber evil and there are lots of different motivations behind cyber threat actors," he said. "Everyone in this room who works in cybersecurity is playing their part in defending against cyber evil because all of these people work together in that same ecosystem."

"You need a combination of hope and imagination and confidence. We need men and women to dream of things that never were and ask why not, as the problems of this world will not be solved by sceptics and cynics."

After it was the theme of collaboration when protecting national infrastructure. The first panel of the day focused on defending against attacks and featured Michael Kelly, head of operations and ECAS at BT Ireland, Mary Kennedy, European cybersecurity and information services leader for Arup, Katie McCarthy, head of cybersecurity at Irish Water, and Richard Browne, director of the National Cybersecurity Centre (NCSC).

Speaking about the approach organisations should have, Kennedy said that all organisations must ensure that their supply chain management is in place from the very start as every level of your service must include security protection.

When asked what organisations should start with when organising protection, Kelly said BT took a different approach.

"The first thing we decided to do was build the infrastructure fresh; let's not import anything that already exists," he said. "The easiest way to secure the infrastructure required is to build it from the ground up with security in mind."

Following it were two presentations on threats and resilience. The first was on keeping one step ahead of national threats delivered by Joe McCann, security manager for the National Transport Authority, who brought up collaboration as a critical element of this and how third and fourth parties are one of the biggest risks on the supply chain.

The second was adopting a cyber resilience approach to dealing with sophisticated threats by Puneet Kukreja, partner and head of cyber at EY Ireland.

He gave five ways to ensure this: work with an assumed breach mindset, manage critical third parties, have the ability to detect, respond, recover and communicate when an incident occurs, have a cyber response plan and know how you determine success if you tested it.

"Having a cyber response plan is no different than having a fire evacuation plan," he said. "When a cyber incident happens do you have in your organisation [equipment], when was the last time you practised it and do people know about it."

Before the break, there was one more panel discussion on leading security awareness across your organisation involving Rosie Coffey, head of enterprise applications group at UCC, Aoife Noone of Noone cyber services, Enda McGahern, security consultant for the Irish Prison Service (IPS), and Donna Creaven, director of ICT, governance & corporate services for IPS.

One common misconception is that people are the weakest link, which Coffey states is untrue. She said people are the most targeted, which means having policies, procedures and training are key for a good security culture.

Continuing the fire safety analogy, Creaven talked about how one ambition is to have a cybersecurity officer who treats said issues similar to a health and safety coordinator.

"It's important that you record the near misses, learn from that and share the information and consistent awareness," she said.

Gavin Fox, director, Martinsen Mayer

Jenni Parry, associate director of Cyber Risk at Aon

"[For quarterly reviews], it's really important to put those processes in place as it keeps it on the agenda. So having your reporting and escalation approaches is really important."

Just before the break, Joshua Green of Cisco presented his talk on implementing a zero-trust approach to support your organisation's resilience.

The good news is that problems that were deemed unsolvable years ago now have solutions, including passwordless models. It means organisations can focus on a more proactive approach.

"Start off by building solid access controls now," he said. "Certainly, if you're not doing MFA, do it. We would say consider doing it passwordlessly. Don't be concerned if you have legacy hardware in the environment, even if you have to fall back on a PIN, it's better than a password so take the plunge, it's not as bad as you think."

Crafting the right response

After the networking break, the discussion went onto response management with two high-energy, entertaining talks. The first from Chris Nickerson, CIO & CISO of Damovo and chief executive of Lares, focused on measuring and improving the effectiveness of your security programme.

Dismantling how organisations measure attacks and protection, he spoke about the difference between precision and accuracy, two concepts that sound the same but mean different things and how while protection changes, one thing remains the same.

"What most people haven't figured out is that the most standard thing in all of security is not the standards, it's how attackers attack," he said. "Attackers have to do the same stuff every time . . . that's the lowest common denominator we can defend against."

This led to Neil O'Hare, CIO for Children's Health Ireland, speaking about the HSE ransomware attack. In it, he emphasised the damage caused by it, stating many healthcare staff found the impact felt from it was greater than what covid threw at them.

This led nicely to a panel discussion on preparing for and responding to an attack. This featured Jennifer Cox, head of communications for Cyber Women Ireland, Colin Gaughan, data and cyber resiliency specialist for Dell Technologies, Pat Ryan, detective chief superintendent for the Garda National Cyber Crime Bureau and Joel Aleburu, cybersecurity specialist.

Asked about how important it is to test your cybersecurity plan, Gaughan mentioned that it can fall foul of oversimplification when there are so many layers to it.

"The biggest thing is finding out what is normal after an event which isn't talked about enough," he said. "What systems do you bring back in the first 24 hours if it's a bad attack, what systems do you bring up, and in the instant response plan, even that base target setting isn't done often enough."

The penultimate presentation was from Blessing Usoro, information security manager & founder of Cyber for School Girls, who spoke about cyber hygiene and how many companies are failing the basics.

Her presentation focused on how such measures can be easily overlooked like giving too many privileges, improper off-boarding processes for when people leave a company and policies around 2FA being some of the elements covered.

The final panel discussion before the lunch break involved fostering a pipeline of cybersecurity talent in an industry with a well-known skills shortage.

The panel featured Sarah Drew, director of security engineering for Salesforce, Fintan Swanton, senior consultant and managing director of Cygnus Consulting Ltd and chairman of the Association of Data Protection Officers, and Niamh Vianney Muldoon, CISO of Fenergo.

Vianney Muldoon spoke about collaboration and experience and giving on-the-job training and offering the academic side of things, something apprenticeship programmes provide.

"Not everyone learns through academia, there's a lot of hands-on experience and, in my experience, running instances for 22 years, it's bringing all of those mindsets together," she said. "So the technical and organisational skills that bring the desired outcomes and reduce the business impact."

After the talks, the afternoon saw four roundtable discussions happening. The first was 'Managing Cyber Risk in the Dark – An Idiot's Guide!' with Dwyer, while the second focused on 'Executing an integrated cyber approach' with Michael McNamara, senior manager of security and compliance at BT Ireland.

The third roundtable concerned 'Investing in your cybersecurity workforce', which was chaired by Jenni Parry, associate director of cyber risk at Aon, while the fourth was on 'The joys of hiring and retaining staff in cybersecurity' by Gavin Fox, director of Martinsen Mayer.

In her closing remarks, Kelly said that this isn't only an important event, but a timely one and praised those attending for their curiosity and desire to learn more.

"It's just brilliant to see some of the questions that are coming in because it shows a real appetite for knowledge and further transparency about what goes on when tackling these types of threats," she said.