Prepared Statement: Donna O'Shea, Chair of Cybersecurity, MTU, Cork

It is my pleasure to be here today to contribute to this important discussion. My name is Donna O'Shea and I hold the position Chair of Cybersecurity at Munster Technological University. My position is funded by the Higher Education Authority (HEA) Senior Academic Leadership Initiative and as part of my role I lead the HEA HCI Cyber Skills and SFI Discover Cyber Futures initiatives, sit on the board of Cyber Ireland and I have also led the design and procurements of Ireland's only cyber range infrastructure. I am here today with colleagues Dr Sean McSweeney, Head of Computer Science MTU; Dr Paul Millar Reader, School of Electronics, Electrical engineering and Computer Science and Deputy Director of the Centre for Secure Information Technologies (CSIT), QUB; Prof Tom Acton, Personal Professor in NUIG; and Dr Brian Lee, Director Software Research Institute, Technological University of the Shannon.

Cybersecurity has been growing in importance over the past decade as the rate, frequency, scale, and sophistication of cyber-attacks has increased. This importance is reflected in the growing number of EU policies and directives i.e. NIS 2, DORA, CER [i] and national policies i.e. Irelands Smart Specialisation Strategy and Harnessing Digital, The Digital Ireland Framework [ii]. These policies correctly detail the risk associated with digitalisation, which is the more we "digitalise", the greater the risk of cybercrime and the need to take cybersecurity precautions to prevent the financial loss, business disruption and potential mission/life threats of a successful cyberattack. As the rate of Ireland's digitalisation continues to increase, so too do the risks with the World Economic Forum defining cybersecurity as one of its "highest likelihood risks over the next ten years" along with climate action failure, digital power concentration and digital inequality. Cybersecurity is now considered the linchpin in building the digital resilience necessary to future-proof our businesses, society, and economies. This resilience, according to the World Economic Forum, will become the "defining mandate of our time" and will mean the difference in being able to detect, respond and recover from future digital shocks in the form of inevitable cyber-attacks of increasing frequency, scale, and sophistication.

However, the reality is that, to date, Ireland has lagged in prioritising cybersecurity and there is now a gap between our digital development and our cybersecurity readiness [3]. Over the past few years, we have witnessed first-hand the impact of this gap, with the cost of cyber-crime for Irish businesses going from €3.5bn in 2019 [iii] to €10bn [iv] in 2022. While most fraud incidents in Ireland cost less than €80K [27], the cost can be much higher. For example, the clean-up from the HSE attack to date has cost the Irish taxpayer €80m, with the cost of the remediation programme likely to be approx. €300m over the next 2-5 years [v]. Benchmarking Ireland to other countries, Irish companies are falling victim to cyber-attacks at a rate double the reported global levels, with the cost and clean-up of a cyber-incident also costing Irish businesses more. While the current cost of a cyber-crime incident can be significant, the societal impact can be much greater, with impact on critical services and loss of personal data, e.g., in the HSE cyber-attack 113,000 individual medical records were illegally accessed and copied.

Research & Development

The challenge and opportunity for the future is to ensure that Ireland has the capacity and capability to respond to the risk associated with digitalisation and bridge the gap between our digital development and our cyber readiness. One way to achieve this is by ensuring advances in cybersecurity research can be applied to improve the resilience and security of Ireland's critical infrastructure, public sector and digital economy. However in Ireland this is providing ineffective, as the landscape in cybersecurity research is highly fragmented which has led to a slow and limited impact response that follows from individual academic institutions and SFI research centres trying to address national scale urgent research challenges in cybersecurity with disconnected and small-scale responses. This fragmented and incoherent approach needs to be resolved if we wish to develop cybersecurity research solutions in sectoral applications where Ireland is leader with the aim of increasing its market position.

R1 An SFI Centre in Cybersecurity bringing together HEIs with industry, business, public sector and security forces partners.
R2 A fixed % of all national funding for Digitalisation to be specifically ringfenced for cybersecurity.
R3 Track research spend on cybersecurity by developing standard classification system for public expenditure for research in Ireland.
R4 Invest in a national cybersecurity infrastructure to support collaborative R&D and skills/training.

Innovation & North South Partnership

Ireland also lacks a mechanism to engage its highly skilled workforce to participate in the innovation economy, ensuring that as a country we can develop cyber capabilities within our own borders, enabling the rapid and agile development of indigenous innovation solutions to cybersecurity and digitalisation challenges. This is important as research has proven that even though talent can often be evenly distributed across the world, the opportunity for engaging talent in the innovation economy is not equal, and innovation driven entrepreneurship clusters develop at high concentrations in certain places around the world. In the cybersecurity sector, this clustering is particularly evident, with cybersecurity innovation highly localised to specific regions supported by government funded innovation ecosystems. Beersheva in Israel, Tallin in Estonia and Belfast in Northern Ireland are well known examples of established innovation ecosystems in cybersecurity.

Within this RD&I ecosystem, we have a lot to learn from our partners in Belfast, Northern Ireland and we have the potential in building a shared "Digital Island", which presents enormous opportunities for economic/social advancement as physical/political borders become increasingly insignificant. To realise the full potential of our Digital Island, we cannot replace those borders with a digital border where standards, policies and strategies are different: a common approach is needed.

R1 Explicitly include cybersecurity in All-Island collaborative research and innovation programme.
R2 All-Island coordination of national cyber-defences: develop cybersecurity infrastructure and cyber-defences to protect the nation as a whole: "a Firewalled Island".
R3 Invest in a specialised innovation initiative for cybersecurity to develop Ireland's innovation ecosystem.

Education & Skills

And our success in building a strong RD&I, is dependent on a highly skilled talent pool and workforce. Last year, for the first time, the International Information System Security Certification Consortium (ISC)2, reported that Ireland closed its cybersecurity skills gap to 19.5%, while the global gap grew by 26.2%. This success can be in part attributed to the investments made by the government in specialised initiatives such as the HEA HCI P3 Cyber Skills, growth in apprenticeship offerings, Springboard and HCI P1 funding. However, many challenges remain if Ireland wants to achieve its ambition of growing its cybersecurity workforce from 7,300 today to 20,000 by 2030. We need to deliver highly skilled graduates to the sector at a faster rate by investing in cybersecurity education and training at all NFQ levels. We need to achieve this goal in a way that does not compromise on the quality of education.

R1 Establish a baseline in cybersecurity education and agree key knowledge/skills/abilities that courses should teach. These baseline standards already exist NIST NICE and UK NCSC baseline standard.

R2 ENISA recommends that 50% of cybersecurity courses should be dedicated to practical activities. This should be enforced through the established baseline standard in cybersecurity education.

R3 Fund initiatives/academic programmes that focus on collaboration in the HEI sector. This is required as cybersecurity as a discipline is constantly evolving and training/education needs to adapt at a faster rate. As a result curricula is struggling to keep up, mainly because HEI providers work in silos and lack mechanisms to quickly incorporate material on emerging threats or new skills.

To summarise, the challenge and opportunity for the future is to ensure that Ireland has the capacity and capability to develop research, development & innovation solutions that deal with the increasingly complex and expanding threat landscape that is a consequence of digitalisation. To realise this opportunity, greater investment is required to ensure that we develop a more cohesive and responsive RD&I ecosystem supported by a highly skilled workforce of professionals. If we achieve this, then in the future we will ensure that Ireland can meet the demands of industry for cybersecurity products/services/solutions and talent, which will maximise our retention of existing industries and will also ensure that Ireland becomes a nexus for the growth of industries where cybersecurity is an absolute necessity.

[i] European Commission, “New Stronger Rules start to apply for the cyber and physical resilience of critical entities and networks”, Press Release, 16 Jan 2023

[ii] Department of Ireland, Harnessing Digital, The Digital Ireland Framework, 2022

[iii] Begleg, I., “Fraud and Cybersecurity cost Irish Businesses and State €3.5bn each year”, online: https://www.independent.ie/business/irish/fraud-and-cybercrime-cost-irish-businesses-and-state-35bn-every-year-expert-38120765.html

[iv] Grant Thornton, “The Cost of Cybercrime 2022 – Irish Cybercrime expected to exceed 10bn in 2022”, article, accessed Jan 2023

[v] Independent Post Incident Review, “Conti cyber-attack on the HSE”, Dec 2021, https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf