Cyber Security Vision for Ireland.

People & Skills.

Skills Shortage and Skills Gaps - Context.

Cyber security skills shortages and skills gaps are the number one challenge facing the cyber security sector in Ireland. These gaps have a knock-on effect on all aspects of the economy. All sectors have digitalisation plans, including the public sector.

These are all at risk.

Therefore, all Citizens have a need for cyber security knowledge and skills.

Ireland's cyber security sector and employment is growing rapidly, reflecting global growth in the cyber security market. Various reports have identified almost 7,500 professionals working in the cyber security sector with the potential for 17,000 jobs by 2030.

Additionally, there is a requirement for cyber security skills across all sectors of the economy.

There are a range of training and education programmes in cyber security for cyber security professionals and skills. Cyber Ireland has mapped over 70 accredited courses.

This does not meet the demand, courses are too long and become outdated quickly.

The Cyber Security Sector Report found that over 60% of firms surveyed have staff-related issues, including lack of suitable candidates, skill-level and unaffordable salaries. The Report identified significant skills shortages for the sector; 46% of security teams were understaffed, 48% of firms had open or unfilled, security roles and almost 20% of roles took six months or longer to fill.

In many cases, the organisation does not know that it has a Skills Gap**.** Cyber is not discussed by managers and is often left to the IT People, who are often ill-equipped to determine needs and pray their firewalls are secure.

This is particularly pertinent to SMEs and Manufacturing companies who also experience addidtional threats due to their Operational Technology (OT) that runs lines, controls stock and manages supply chains

Legislative requirements for Cyber Vision.

There are both EU and Irish regulations that try to protect us from cyber threats. The list is lengthening and trying to ensure compliance, as a minimum standard.

> **GDPR (General Data Protection Regulation)** is the best-known legislation designed to protect personal data. Cyber awareness is critical for GDPR.
>
> **DORA (Digital Operational Resilience Act**), it is designed to prevent and mitigate against cyber threats for financial entities, in particular.
> DORA requires organisations to train their employees on cyber resilience and it also requires suppliers to organisations to have the same level of understanding. Hence the training requirement is pushed out to suppliers. Boards and senior management should specifically be trained on incident response.
>
> **The Network and Information Security (NIS2) Directive** is proposal strengthen the security requirements, address the security of supply chains, streamline reporting

obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU.

EU is upgrading the current rules governing digital services by introducing the **Digital Markets Act (DMA)** and the **Digital Services Act (DSA),** which will create a single set of rules applicable across the EU to address the power of large digital platforms.

The EU is trying to strengthen capabilities for effective operational cooperation, solidarity and resilience through amendments to the **Cyber Security Act.**
This will enable the future adoption of European certification schemes for 'managed security services'.
It is also calling for pledges to close the cyber skills gap in Europe by building Cyber Security Skills Academies and creating cyber reserves.

Skills Definitions.

Good work has been done by NICE/NIST and ENISA to define Cyber Competencies. There are now 52 Cyber IT and 9 OT roles.
Some Leadership Competencies are included but they lack Transversal Skills that reflect Emotional Intelligence and Team work. These are essential in promoting Cyber Awareness and influencing Senior Managers.

Some good work has been progressed across the country but it is not coordinated, intensive or impactful as it should be.

Schools.

Cyber Ireland has taken several initiatives with regard to schools. They have taken this from a careers perspective in promoting cyber security as a career for all and providing education relevant to a career in cyber target at Secondary Schools, mainly 15-18 years.

There's a Working Group under the NCSC with UCD that has developed a Cybersecurity Course for Transition Year Students.

Cyber Awareness training and education is handled by Cyber Safe Ireland and WebWise.

How to identify and move the Youth into Cyber careers earlier?

Zero Days CTF (Capture-the-Flag) is a gamified cybersecurity challenge which has been running annually since 2015.
Initially, aimed at attracting third-level students to pursue careers in cybersecurity, the event has grown year-on-year and now has three sections aimed at Colleges, Schools and an Open Section for industry professionals and graduates.

The success of the event has seen record interest in cybersecurity courses and degrees offered by TU Dublin, with a record number of students joining the first year in September 2022, including a growing percentage of females.

There are potential synergies with organisations and programmes run by the Advanced Manufacturing Centre and UCD's Cyberwise programme.

Apprentices.

Ireland's first Cybersecurity Apprenticeship was launched in 2019 by FIT (Fast Track Into Information Technology) in collaboration with the National Apprenticeship Alliance.

The uptake of the Cybersecurity Apprenticeship by the sector has been extensive with over 60 global and indigenous employers across Ireland employing Cybersecurity Apprentices, now numbering 100 in total.

The Cybersecurity Apprenticeship is a complementary addition to the talent pipeline for cybersecurity professionals in Ireland and it is planned to expand the provision of this career pathway to an annual intake of 150 Cybersecurity Apprentices by 2025.

FIT is the Coordinating Provider of the Cybersecurity Apprenticeship which is delivered nationally in collaboration with the Education and Training Boards (ETBs) enabling greater access, inclusion and career opportunities for learners throughout Ireland.

Demonstration and Development of Cyber Skills.

The Advanced Manufacturing and Training Centre of Excellence (AMTCE) is about to launch its own Cyber Programme to support Industry 4.0. This programme has built upon the various expereinces shown above at home and abroad. It's purpose is to reduce the skills shortage and address the skills gaps, primarily in Manufacturing and SMEs.

The programmes are accelerated learning with current content and skills based from Awareness to Advanced Cyber Skills designed for the cyber roles defined in NIST 2 primarily.They including additional digital skills that cyber practitioners need in mnore advanced roles. The emphasis is on skills development and application. Plans are in play to build a Training SOC Trainees to Cyber ranges, Operational Technology simulations and how indigenous software can be deployed to prevent, defend and react to attacks.

AMTCE is part of LMETB and is supported by Solas and Enterprise Ireland, the Cyber Skills model in development can be applied in all of the ETBs.

Attracting younger people into cyber work is now critical.

Both the FIT Apprenticeships and the AMTCE Skills provide learning pathways for Trainees who would consider third and fourth level qualifications.

Conclusions.

There is a lot of activity in the Skills area in Ireland but it is not coordinated nor strategic.

EU regulations are clearly indicating the need for compliance, change and improvement. Engagement with ETBs and teachers in particular, is vitally important.

This needs to be managed without losing any of the commitment shown by various organisations and to reset the cyber skills agenda for all citizens and organisations, not just cyber companies.