COLLABORATORY

CYBER SECURITY HUB AT TU DUBLIN

Cyber Security Training Needs & Skills Gap Analysis in the Fingal Region

Report 2021-22

Dr Ayuna Murphy

TU DUBLIN
ENTERPRISE IRELAND
where innovation means business

COLLABORATORY

CYBER SECURITY HUB AT TU DUBLIN

Collaboratory is the newest innovation, technology and industry solutions hub from Technological University Dublin, in partnership with Enterprise Ireland, and will specialise in Cyber Security, Internet of Things and Artificial Intelligence.

It is accepted that the development of skills and capacities in AI and IoT technologies will be a key driver of competitiveness and innovation in the SME sector. As technology advancements result in new ways of doing business, emerging job roles will require new and different skillsets, particularly in AI and IoT. Concomitant with progress in these two areas will be the absolute necessity to provide wraparound expertise in Cyber Security.

Focusing primarily on Cyber Security, Collaboratory will partner with industry to address emerging threats, including those that arise when AI and IoT advancements are vulnerable to or threatened by cybercrime.

Collaboratory will develop structured and accredited industry training programmes across Cyber Security, IoT and AI to feed skills development and ensure a pipeline of future talent for SMEs & MNCs in Ireland.

Collaboratory will provide industry partners with research and development capacity; skills development assistance; access to technical development, prototyping and live testing facilities; and access to market development support in the areas of Cyber Security, IoT and AI, to increase innovation, productivity and competitiveness.

Collaboratory is co-funded through the European Regional Development Fund and is located at the Learning & Innovation Centre (LINC) at the TU Dublin Blanchardstown Campus.

www.collaboratory.ie

TU DUBLIN TECHNOLOGICAL UNIVERSITY DUBLIN

ENTERPRISE IRELAND where innovation means business

Published February 2022

Contents

Executive Summary

Report Overview

The purpose of this research is to develop knowledge of the current and emerging skills needs, gaps, and training programme requirements within industry in the Fingal region, with a particular focus on small and medium enterprises (SMEs). The research seeks to help Collaboratory establish areas of potential offerings for cyber security training programmes that are relevant to organisations' needs to upskill and reskill their current employees and to help them to build cyber resilience and become cyber secure.

The report provides a review and analysis of current cyber security training provisions in the Republic of Ireland, including the private and public sectors. This analysis allows Collaboratory to strategically position its training offerings in the Irish market.

Key Findings

The desk research indicates that companies are experiencing cyber security skills gaps, and our survey supports this finding.

Cyber security is developing and evolving in Ireland and enterprises require better knowledge and understanding of cyber risks and the importance of cyber security for business continuity.

Cyber security training needs have increased in the last year with an emphasis on cyber awareness. However, it has been found that leaders, management, and boards of directors have insufficient knowledge of cyber security. As a result, cyber professionals face challenges in communicating its significance and securing investment for it.

All roles and industries increasingly require some level of cyber security knowledge and awareness. This trend generates a need for specific training programmes targeting professionals outside the IT sector.

Trends such as remote work and the increasing adoption of Internet of Things (IoT)-enabled devices are creating new vulnerabilities for the industry. IoT and cloud security educational programmes are expected to be in high demand.

There is a low level of investment in cyber skills training and development in organisations. Limited expertise in cyber security among management and business owners, together with difficulties in communication due to excessive use of technical jargon, creates obstacles in justifying return on investment (ROI) in cyber security measures.

The educational sector in Ireland offers over 150 cyber security-related training programmes. Most of these courses focus on technical aspects of cyber security and there is a lack of training provision targeting SMEs' cyber needs, as well as a lack of suitable guidelines.

The most in-demand training areas identified are: data protection; network security; baseline cyber security; intrusion detection; incident handling and response; application security; cloud computing; and risk and compliance auditing.

Organisations indicated a preference for short-term training programmes of one-to-two days in duration and which include an element of practical application. Flexible learning options (online with a facilitator, blended approaches) were also seen as an advantage.

Companies see certification as important. They are more likely to take up a training programme if a recognised qualification is awarded on completing the course.

Key Recommendations

Based on the research findings, the following are recommendations on potential training programmes and courses that could be offered by Collaboratory:

1. Cyber security training for executive teams
2. Plain speaking and cyber jargon-busting short courses
3. Offer open learning access to cyber security modules
4. Regulatory compliance short courses for Chief Information Security Officers (CISOs) and senior IT managers
5. Industry-specific workshops
6. Training programmes in line with NIST NICE1[1] or Mitre Att&ck[2] frameworks
7. Soft skills for cyber security
8. Cyber supply chain risk management
9. Penetration testing simulation training
10. Cyber security courses targeting females to improve gender diversity
11. Cloud security training due to adoption of remote working
12. Bespoke training to organisations based on their industry or work functions
13. Free of charge one-hour workshops

For more information contact:

Dr. Ayuna Murphy, Training, Education and Communications Manager, Collaboratory

Email: ayuna.murphy@tudublin.ie

[1] NIST NICE framework categorises and describes the tasks, knowledge, and skills that are needed to perform cyber security work performed by individuals and teams. https://www.nist.gov/nice

[2] Mitre Att&ck stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge (Att&ck). Mitre Att&ck framework is a comprehensive matrix of adversary tactics and techniques based on real world observations. https://attack.mitre.org/

The survey was voluntary and anonymous and was open to respondents over a five-week period from June 24th to July 28th 2021

Research Methodology

The research methodology implemented the following elements:

1. Desk research was conducted to establish what information was available on the current state of the cyber security sector globally and in Ireland, emerging trends and challenges, and current national initiatives that strive to address the needs of the evolving cyber security ecosystem. Observations made through participation in webinars and industry events that took place in June and July 2021 also fed into this research.
2. An online survey was the dominant research instrument and feedback from phone conversations was encapsulated in this report. The survey comprised four sections, with 31 questions in total. Section One aimed to identify a company's profile and consisted of three questions. Section Two sought to understand current cyber security training practices and had 11 questions. Section Three focused on the current state of organisations' cyber security and upcoming training needs and comprised seven questions. Section Four concentrated on identifying requirements for future training programmes. This section consisted of nine questions. The last question gave respondents an opportunity to share any comments and additional information they felt useful for the purpose of this research. The survey consisted of closed questions, Likert type scale questions, open questions and multiple choice questions, where participants were asked to choose one or more responses to a question from a list of pre-determined options. All questions were mandatory to complete except open-ended questions and questions regarding companies' projected training budgets for 2022. The survey was voluntary and anonymous and was open to respondents over a five-week period from June 24th to July 28th 2021.
3. Review and analysis of current cyber security training provision offered by Irish higher education institutes and commercial providers that were open for enrolment from June 2021.

Desk research

Today, in the era of the digital economy, every organisation goes through digital transformation in some form. As companies' reliance on technology increases, so too does their vulnerability to cyber threats and attacks, which makes them prone to cyber crime and data breaches if they do not implement adequate controls. The more organisations become digital, the more attention they should pay to their cyber security – but many European businesses do not do so. Only 12% of businesses strongly agree that increasing use of technology leads to higher risks of cyber-attacks, and 21% of European businesses have invested in digital technologies but did not implement a cyber security strategy[3]. Thus, one in five European businesses are ill prepared to tackle cybercrime.

Cyber crime incidents in Ireland are increasing, with 61% of Irish organisations reported to have suffered incidents such as online fraud in the 2017-2018 period, with an estimated loss on average of €3.1m[4]. Organisations need to rethink their business approach with cyber security in mind and integrate it not only into the business decision-making processes but make it part of the overall organisational culture.

Another critical challenge organisations encounter is cyber security gaps and skills shortages. It is estimated that industry currently needs 3.1m cyber security professionals globally, and 64% of cyber security professionals report that they are affected by this cyber security skills shortage[5]. Cyber Ireland issued a Cyber Security Skills Report in 2021, which identified that 41% of Irish-based organisations had understaffed cyber security teams and a further 5% were significantly understaffed. Some 43% of companies have open or unfilled cyber security roles, taking roughly six months or more to fill these roles[6] . It is evident that organisations in Ireland require a greater supply of skilled cyber security professionals, and education providers are tasked with designing and developing solutions to meet this growing demand.

[3] Catch-22 Digital transformation and its impact on cybersecurity
[4] National Cyber Security Strategy 2019-2024
[5] (ISC)2 Cybersecurity workforce study, 2020
[6] Cyber Ireland Cyber security skills report 2021

Cyber Security Challenges

A review of publicly available reports identified that the industrial and education sectors globally are experiencing the following cyber security challenges:

- Novelty and low maturity of cyber security as a profession
- Poor awareness of cyber security as a career option
- Despite existing cyber security frameworks and standards such as NIST NICE, ISO[7] standards, Mitre Att&ck, CVE[8], CVSS[9] scoring etc., there is an absence globally of an accepted cyber security risk management framework that identifies and aligns threats, vulnerabilities, risks, remediation, actions, all identified with relevant metrics, including the requirements and procedures for cyber security and business continuity
- Lack of an auditable, referenced security governance framework
- Perception and belief that cyber security is a highly technical IT area
- Gender diversity issues (cyber security is typically male dominated, as the IT sector in general tends to be).

Challenges higher education institutes face in developing cyber security training programmes to fulfil growing demand include:

- Insufficient number of qualified cyber security educators
- Relatively low numbers of students specialising in cyber security compared to the number of the jobs available in the labour market
- Shortage of cyber security academic programmes that meet industry requirements
- Difficulties in sourcing staff capable of delivering hands-on experience and certifications required by industry
- Students lack hands-on experience, resulting in skills shortages
- Interdisciplinary nature of cyber security poses challenges for curriculum designers
- Complex accreditation processes result in relatively low responsiveness of curricula to the rapidly evolving cyber security landscape.

[7] ISO 27001 is the international standard that sets out the specification for an information security management system.ISO 27032 is the definitive standard providing guidance on cyber security management. ISO 22301 provides a best-practice framework for establishing, implementing, maintaining, and improving a business continuity management system. https://www.iso.org/

[8] Common Vulnerabilities and Exposures (CVE) score is used to prioritise the security of vulnerabilities.

[9] Common Vulnerability Scoring System (CVSS) evaluates the threat level of a vulnerability.

Companies face the following challenges in developing their cyber security strategy and building resilience in the constantly evolving cyber security threat landscape:

- Low investment in cyber security human capital leads to a deficit of sufficient and suitable training provided to employees
- High expectations from companies regarding the skill level of candidates currently in the labour market or those about to enter the market following graduation results in unrealistic entry requirements for many cyber security professionals
- HR departments and learning and development teams have insufficient knowledge of the specific requirements of cyber security, leading to a disconnect between training plans and delivery
- Lack of understanding of cyber security risks and seriousness of the consequences of potential cyber-attacks creates difficulty in justifying a return on investment (ROI) on cyber security spending
- Inadequate understanding of cyber security's role as a business enabler and its importance for business continuity
- Low level of knowledge of cyber security technical language by business leaders, executives, C-suites and boards, which makes it problematic to communicate cyber security within businesses.

Cyber Security Trends

The cyber security landscape is constantly evolving as cyber criminals develop new threats and types of attacks, with new and greater degrees of sophistication. Organisations need to keep up with these changes to ensure they are equipped to manage these risks effectively. They must continuously review and update their cyber security policies, processes and procedures, hardware and software, develop new business approaches, educate their staff, and put necessary measures in place to strengthen their cyber security positions. Some of the emerging trends are listed below:

- Security automation and use of artificial intelligence to recognise vulnerabilities
- Security validation
- Ransomware
- Cloud security
- Supply chain attacks
- Increased remote work exposes businesses to new vulnerabilities.

Current National Initiatives

The cyber security sector is still a developing industry with a relatively low level of maturity. The Irish Government has taken proactive action to address cyber security skills gaps and shortages outlined in the National Cyber Security Strategy 2019-2024. At present, there are several initiatives that support cyber skills development in the country:

- Technology Skills 2022: Ireland's Third ICT Skills Action Plan was created to support the development of the ICT sector in Ireland and outlines measures to increase the number of ICT graduates. This plan includes the expansion of ICT-focused provision in higher education and Skillnet Ireland programmes, developing new reskilling and upskilling pathways, growing the number of ICT apprenticeships, and attracting more females to take ICT careers. This Action Plan is funded through the National Training Fund and the Human Capital Initiative (from 2020).
- Cyber Ireland is a national cluster organisation representing the needs of the cyber security ecosystem in Ireland. Its goal is to ensure innovative growth and development of the organisations within the cluster and strengthen their competitiveness in the Irish and international markets.
- Cyber Skills is an initiative funded under the Human Capital Initiative Pillar 3 scheme that aims to address cyber security skills gaps and shortages nationally and improve Ireland's competitiveness in supplying highly qualified cyber security professionals. It collaborates closely with industry, academic, and government bodies to ensure the delivery of relevant cyber security programmes to bridge the gap between industry requirements and current training provision. Cyber Skills has developed three pathways in line with the NIST NICE framework: secure network operation, secure software development, and secure systems architecture. These programmes are part-time and online, where students can enrol in the whole programme as well as individual modules.
- ICT Skillnet is a portfolio of unique industry-led ICT training programmes. ICT Skillnet offers subsidised technology training courses for jobseekers, upskilling opportunities for technical and engineering staff, and online Bachelor's and Master's degree programmes for employees of companies that are members of the network.
- Skillnet Ireland is a business support agency that helps businesses to address their current and future skills needs. Skillnet Ireland has a nationwide business network where businesses in various sectors collaborate and support each other in identifying training needs specific to each sector and designing bespoke solutions to meet these needs to ensure businesses within the network stay competitive.
- itag (Innovation Technology AtlanTec Gateway) is a non-profit association that aims to lead and support innovation in Ireland's technology community. Companies in the network actively collaborate to share challenges and trends in the technology sector and share best practice through industry events and workshops, as well as responding to members' technical and non-technical skills needs.
- Cyber Women Ireland aims to tackle gender diversity issues in the cyber security sector in Ireland. CWI builds a network of women who are passionate about a career in cyber security and fosters their visibility, brings awareness of the challenges women face in the sector, and provides mentorship opportunities aimed at attracting females to careers in cyber security.

- Cyber security apprenticeship programmes offered by Fast Track to IT (FIT). FIT is a non-profit organisation dedicated to helping unemployed people gain technical skills to start their careers in the IT sector. FIT developed a two-year cyber security apprenticeship programme in 2019.
- Higher education in Ireland offers 19 Bachelor's and 22 Master's degree programmes starting in September 2021, five of which are funded by Springboard.
- There are over 130 cyber security courses with online and classroom options available that offer a recognised certificate or diploma.

Survey Findings

The survey consisted of 31 questions and was designed to be relevant and understandable to a broad range of organisations: those with an in-depth understanding of cyber security and those with limited knowledge about it. We were also mindful of the length of the survey to avoid respondents' fatigue.

The survey was conducted over a five-week period starting from June 24th, 2021. A total of 378 companies in the Fingal region were contacted via email or phone. Of that number, 281 were reached directly by phone, targeting small and medium enterprises, and 57 were not interested in taking part in the survey. In addition, information about the training needs analysis was shared by Fingal Chamber and Regional Skills in their newsletters and social media. We distributed our survey to 321 organisations, with a response rate of 8% which is in the range of average external response rates of between 5%-30%, according to smartsurvey.co.uk. It is important to note that this response rate is skewed, as we cannot define if companies we couldn't reach by phone had opened and read our emails. This is understandable, considering the international news coverage regarding the recent cyber-attack on the HSE and companies being mindful and vigilant when receiving emails from unknown senders. We believe the number of responses and the response rate is sufficient for this to be a valid survey focusing on SMEs in the Fingal region. We have come to this conclusion from comparisons with similar surveys conducted nationally[10].

Below are observations gathered during phone conversations with company representatives. It is possible that these representatives may have also completed the survey thus replicating their phone feedback, but due to the anonymous nature of the survey there is no way of confirming whether or not this is the case.

- Over 30 companies confirmed that they outsource their IT function and/or do not have a person with IT or cyber security skills in house
- One organisation confirmed that it had been breached
- Many organisations confuse cyber security with other IT roles and skills
- Companies perceive that once they outsource cyber security, it is no longer their concern, and their provider takes full responsibility for all their cyber security needs and risks
- Businesses don't always understand the level of cyber security risk, and the value of protecting against this risk.

[10] Cork "Cyber security National development strategy published in May 2021"
Cyber Ireland "Cyber security skills report 2021"

Profile of Respondents

Survey participants represent a diverse range of sectors with slight predominance of technology, construction, financial and public sectors. Most respondents operating in the Fingal region are primarily small and medium in size. It is common for companies of these sizes to outsource their cyber and IT functions.

- 16% of organisations are from the technology sector, 16% from construction, 12% from finance and 12% from the public sector with the remaining 44% of respondents coming from a diverse range of other sectors (Figure 1)
- 48% of the respondents are micro-organisations of 1-10 people, followed by 32% small (10-50 people). Only 8% are large organisations (over 250 people) (Figure 2)
- 44% of companies outsource their cyber security function, 32% don't have dedicated cyber security staff and 24% of respondents have a cyber security professional in house. (Figure 3)

Figure 1. Industry Sector

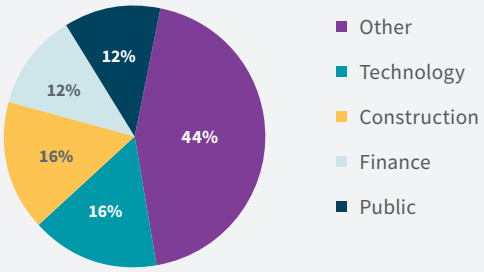


Figure 2. Organisation Size

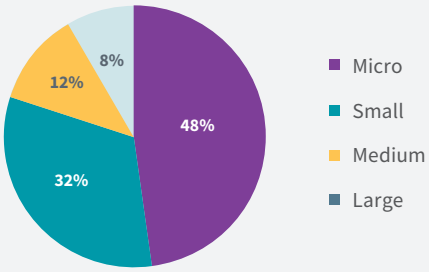
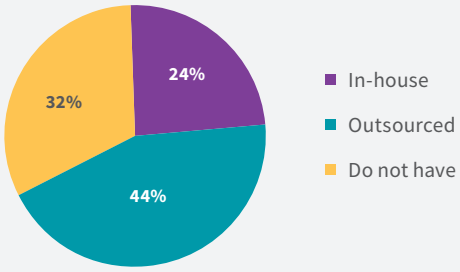


Figure 3. Cyber Security Staff

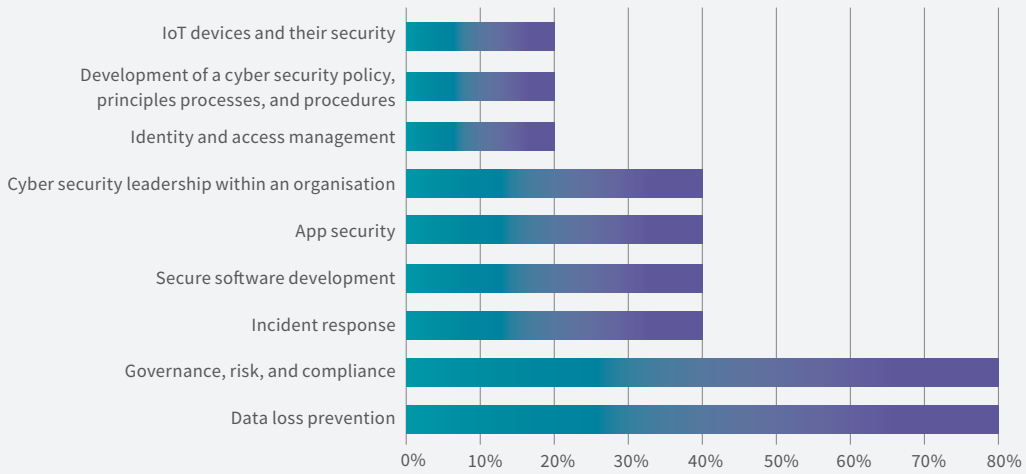


Current Cyber Security Training Practices

- 72% of the companies did not conduct a cyber security training needs analysis in the past 12 months
- 60% of respondents experience cyber security skills gaps
- Most of the organisations (80%) did not provide any cyber security training to their employees
- 20% of the respondents that did provide cyber security training covered the following areas; Data loss prevention, Governance, Risk and Compliance (GRC), Incident response, Secure software development, App security, Cyber security leadership within an organisation, Identity and access management, Development of cyber security policy, principles, processes and procedures, IoT devices and their security (Figure 4).
- Below is a breakdown of results collected from the companies that provided cyber security training in the last 12 months:
  - 60% of organisations trained 1-10 people. None of the respondents upskilled more than 50 people. This is consistent with the companies' size, as 80% of respondents are small and medium companies
  - 100% of organisations that delivered cyber security awareness training did so for all employees
  - 17% of respondents provided advanced cyber security training for IT/cyber teams
  - 60% of the companies used an external training provider.

Cyber security is not top of respondents' training agendas, despite organisations agreeing that they experience cyber security skills gaps. A positive finding is that cyber security awareness training was provided to all employees in organisations that provided cyber security training in the last 12 months, with the majority outsourcing the delivery of these training courses. That means companies focus on cyber security awareness. However, there is a lack of focus on training for cyber leaders and management teams that would improve overall cyber security culture and resilience in organisations.

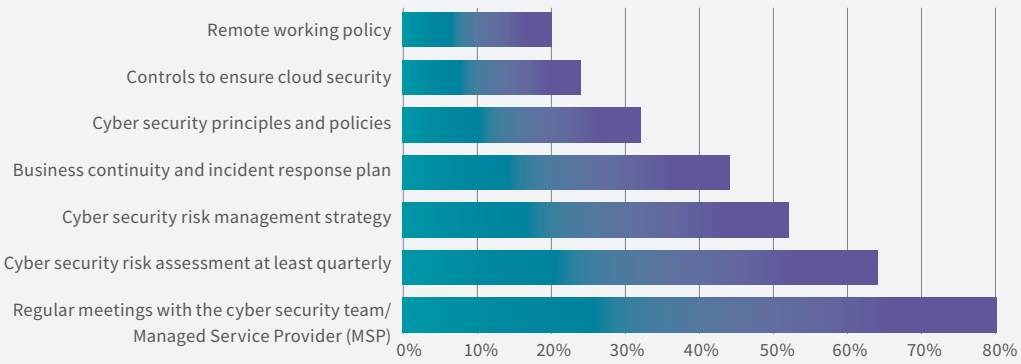
Figure 4. Cyber Security Training Topics Delivered



Current State of Organisations' Cyber Security Training Provision and Upcoming Training Needs

- 64% of organisations do not have a dedicated training function or training manager. This is an expected result as the majority of respondents are micro and small companies with fewer than 50 employees
- 56% of respondents state that the current training provision within their companies meets their needs. The remaining 44% identified the training needs that are not met: cyber security risk assessment and strategies; understanding of cyber threats and potential attacks; and overall comprehensive cyber security training programmes
- Figure 5 presents the top seven cyber security measures implemented by the respondents
- Companies are most concerned about the following cyber threats: ransomware; phishing; data breaches; third-party (vendors, partners, contractors) vulnerabilities; and cloud-based threats. The lowest rated concerns are: patch management; crypto jacking; and IoT attacks
- 52% of organisations plan to upskill all employees in cyber security in the next 12 months. The number of people to be upskilled per organisation does not exceed 30 for most respondents
- Organisations identified the most in-demand skills as data protection and network security, requiring both basic and advanced training. There is high demand for basic training in baseline cyber security training and intrusion detection skills
- Incident handling and response, application security, cloud computing, and risk and compliance auditing are in medium demand and companies are seeking basic training for all these skills
- The lowest demand amongst the respondents is for: forensic analysis; AI automation; DevSecOps; threat intelligence; IoT security; cyber security leadership; and security architecture. Respondents said these skills were not relevant to their company's activity.

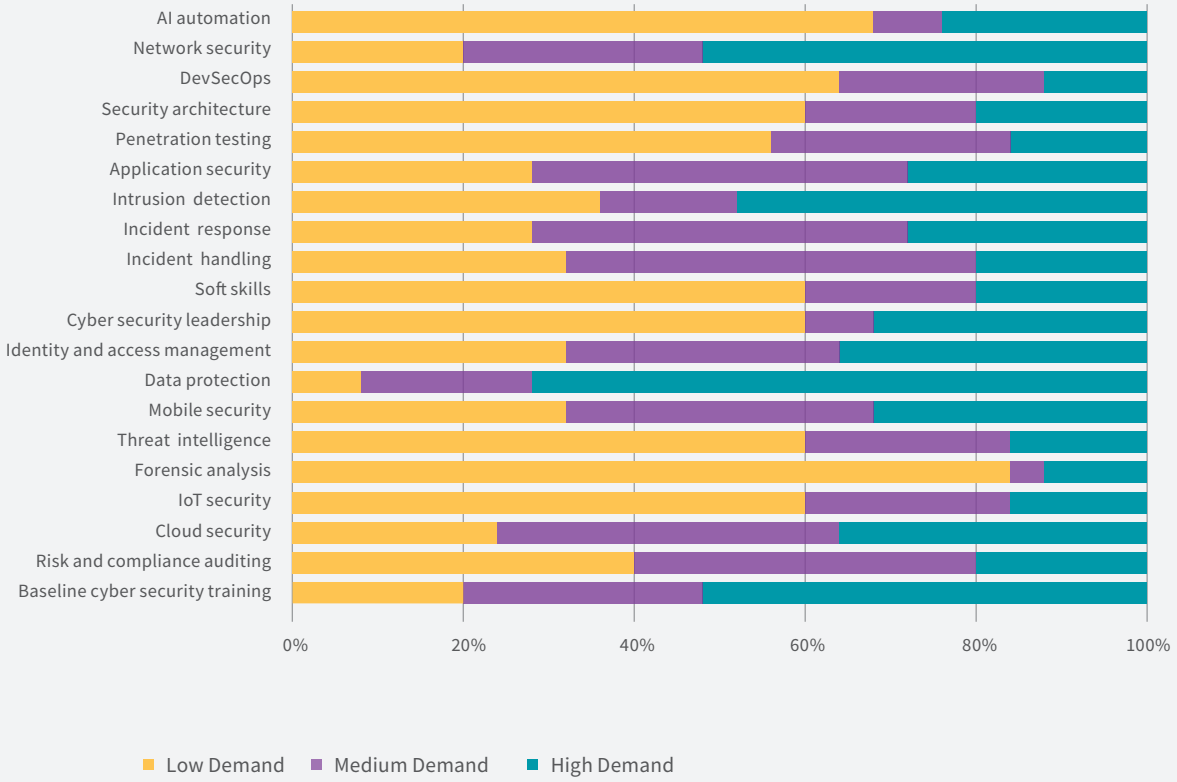
Figure 5. Implemented Cyber Security Measures



- Figure 6 shows the level of demand for cyber security skills amongst the respondents. Figure 7 presents the level of training for cyber security skills required by the organisations.
- It is interesting to note that demand for soft skills is indicated to be low. This result is slightly at odds with findings of similar reports conducted by IT@Cork Skillnet[11] and Cyber Ireland[12] , FIT[13] and government reports[14] that found soft (transversal) skills are increasingly important for enterprises as well as enabling people to get and maintain employment. It is possible that soft skills are more important for medium and large companies than for micro and small enterprises represented by the respondents. However, the top six soft skills that companies identified which could contribute to their success in becoming and remaining cyber secure are:

1. Communication
2. Plain speaking and jargon busting
3. Critical thinking
4. Problem solving
5. Teamwork
6. Leadership

Figure 6. Demand for Cyber Security Skills



[11] Cyber Security Skills Development Strategy, May 2021
[12] Cyber Ireland Cyber security skills report 2021
[13] FIT ICT Skills Audit 2018
[14] National Cyber Security Strategy 2019-2024, Ireland's National Skills Strategy 2025, Future Jobs Ireland 2019

The top five training topics identified as essential are:

1. Data protection regulations and established security related to the business activity
2. Cyber risks and threats specific to the business, sector, or industry
3. How to perform cyber security risk management
4. How to protect against cyber-attacks due to remote working
5. Compliance obligations around cyber security that apply to the organisation

Over half of the respondents show the growing need for cyber training. There is demand for all areas of cyber security to a certain extent, with the highest demand being for data protection and network security at advanced and basic training levels. The respondents also indicate a high demand for foundation training in incident handling and response, application security, cloud computing, and risk and compliance auditing skills. These results reflect the findings of cyber security skills reports conducted by IT@Cork Skillnet[15] and Cyber Ireland[16] . Despite low demand indicated by the respondents, communication, plain speaking and jargon busting, critical thinking, problem solving, teamwork, and leadership were judged to be important. Training provision needs to keep pace with the demand for the areas identified. Industry must be able to access up-to-date education and training programmes relevant to the specific needs of its sectors.

Figure 7a. Level of Training for Cyber Security Skills Required

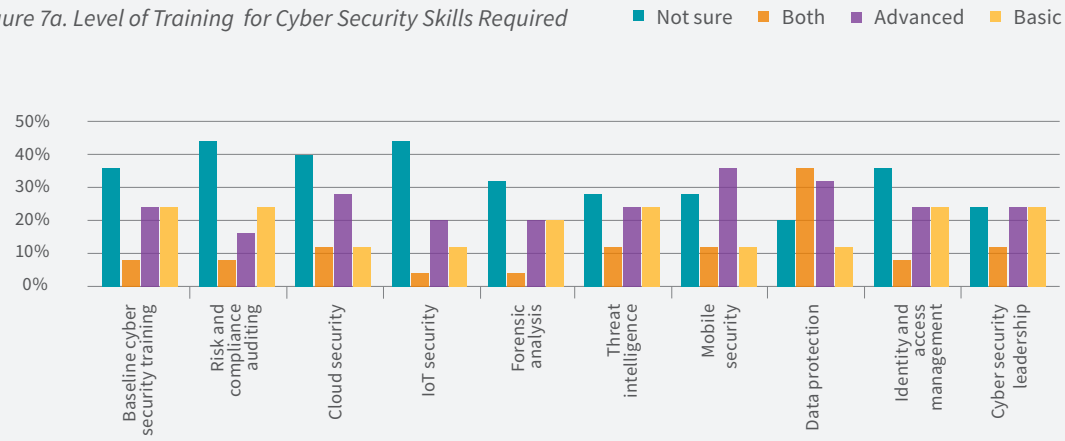
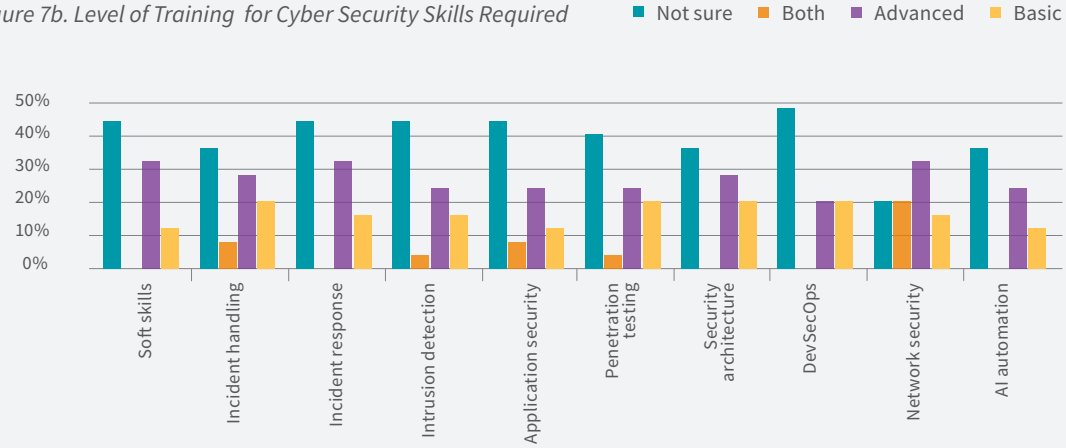


Figure 7b. Level of Training for Cyber Security Skills Required



[15] Cyber Security Skills Development Strategy, May 2021 [16] Cyber Ireland Cyber security skills report 2021

Future Training Requirements

- 44% of respondents reported that bespoke training was not an option for them. Opinions divided equally between those who are certainly and possibly interested in bespoke training
- On-the-job and hands-on training were identified as the most effective training methods, followed by online training with facilitator support, classroom, and blended training. Webinars and workshops were also selected as useful training methods
- Nearly all organisations prefer one- or two-day training programmes, or programmes that would take one or two hours and not longer than five hours per week
- A large majority of respondents (76%) see certification as important
- A recognised qualification would increase a training programme's value and make it more attractive for both companies (64%) and their employees (68%)
- More than half of respondents identified the most important outcomes of training programmes as: general improvement of cyber security awareness (68%) and ability to ensure regulatory compliance (60%)
- Estimated cyber security training budgets for 86% of organisations is up to €5,000 and not exceeding €10,000
- Time and budget constraints are major factors that could affect training programmes.

Short-term training programmes are viewed as more attractive compared to mid- and long-term options. Programmes that include a practical application are preferred, with both classroom and online options welcomed. The presence of an instructor who could guide and clarify a material is considered necessary for the programme's successful delivery. Findings indicate that certification is important for companies. There is evidence of low levels of investment in cyber security training that results in slow implementation of cyber security best practice and insufficient cyber skills development within organisations.

Cyber Security Training Provision

The research identified training providers located in Ireland only. We did not review online training providers based outside the country.

The research discovered a vast number of university programmes offered by higher education institutes across Ireland. We identified 19 Bachelor's and 22 Master's degree programmes that are currently open for applications and start in September 2021. Most of the programmes offer full-time and part-time programmes which make them accessible not only for recent school graduates but also for people in full employment. Some universities offer online and blended learning options, giving students an opportunity to study from the comfort of their own homes and save time on commuting.

New approaches to learning offered by universities increase the programmes' attractiveness and enable more people to enrol. Three Bachelor's and two Master's programmes are offered through Springboard, giving an opportunity to unemployed people to upskill or reskill and enter the labour market, while also providing subsidised higher education to employed individuals who are interested in switching their careers to cyber security or gaining new knowledge in this area and learning new skills.

There are over 130 cyber security programmes, including Cisco courses, offered by the universities in addition to their BSc and MSc programmes, and by further education and commercial training providers. Classroom learning remains as a traditional type of programme delivery. However, there is an increased number of online and blended courses due to COVID-19. Using digital technologies to facilitate effective delivery of such programmes is rising. Graduates of these programmes receive a recognised certificate or diploma. The cost and duration of these offerings vary depending on the course.

Most of the training programmes on offer focus on the technical side of cyber security. We observed a lack of offerings targeting the development of cyber security leaders, managers, and senior executives.

Currently there is only one cyber security apprenticeship programme, offered by FIT. It is a full-time two-year programme, and graduates will be awarded a QQI Level 6 qualification on completion. More apprenticeship programmes need to be developed in the country as they have been proven to be a critical success factor in skills development.

A full list of training programmes is provided in Appendix 1.

Recommendations

The research identified that the majority of SMEs in the Fingal region outsource their cyber security functions and do not have a comprehensive understanding of cyber security, its risks, and the role it plays in their business continuity.

The existence of cyber security skills gaps in companies was found to be a challenge that industry is attempting to address by increasing staff training. Only 20% of companies surveyed provided cyber security training, but more than half of companies plan to offer cyber security training in the next 12 months. There is clearly an increased demand for relevant and up-to-date training in cyber security.

Although there is a vast number of training programmes available in the Irish market, the majority focus on technical skills and there is a lack of training courses available to meet business requirements. The survey results indicate a need for short-term (one-to-two days) training programmes that offer hands-on experience and flexible learning options (online with a facilitator, or blended approaches). Organisations still rely on certifications and recognised qualifications, which are important for both companies and their employees. The most in-demand training areas are: data protection; network security; baseline cyber security; intrusion detection; incident handling and response; application security; cloud computing; and risk and compliance auditing.

Collaboratory is in a unique position to meet the demand for cyber security training by designing accelerated training programmes focused on specific skills. Based on the desk survey findings and research results, there are several short-term training options Collaboratory could offer to the industry. These training programmes should preferably have a TU Dublin micro credential or certification attached.

Recommendations

Recommendation 1

▶ Cyber Security Training for Executive Teams

Executive Cyber Workshops targeting the development of cyber leaders, high level managers, and the C-suite. The course could include topics such as foundation of cyber security, regulatory compliance, financial risk assessment of cyber risks, and cyber leadership skills. It should run for a maximum of two days and be delivered by an instructor online or be classroom based (subject to COVID-19 restrictions and guidelines).

Recommendation 2

▶ Plain Speaking and Cyber Jargon-Busting Short Courses

The survey results and desk research findings indicate that boards of directors, executive teams and management teams need to understand cyber security better, which requires knowledge of its terminology. A short course demystifying cyber security could improve awareness of the subject, and of the importance of investing in it for business growth and continuity.

Recommendation 3

▶ Offer Open Learning Access to Cyber Security Modules

Collaboratory and TU Dublin could adopt an 'open learning' approach to offer standalone access to specific cyber security modules. Credits earned by taking the modules could contribute to an undergraduate degree. For example, an individual can take a module 'Business Continuity Management and Cloud Security' and earn credits without being a full-time degree student.

Recommendation 4

▶ Regulatory Compliance Short Course for CISOs and Senior IT Managers

There are various industry-specific cyber security regulations and standards. For example, the healthcare industry needs to meet Health Insurance Portability and Accountability Act (HIPAA) compliance requirements, whereas businesses that accept payments through a point-of-service (POS) device need to meet Payment Card Industry Data Security Standard (PCI DSS) requirements. Companies that serve customers or do business with individuals in the European Union must comply with the EU General Data Protection Regulation (GDPR). The Irish Government published The Public Sector Cyber Security Baseline Standards in November 2021. The Baseline Standards provide a framework for necessary measures and control that all Public Service Bodies are required to implement in order to improve cyber security and the cyber resilience of public sector ICT systems. This course could help organisations to put robust compliance measures in place.

Recommendation 5

▶ Industry-Specific Workshops

Provide a series of workshops for industry focusing on: understanding cyber risks and threats specific to business activities; cyber security risk management; cyber hygiene; cyber awareness; cyber security in remote working, and data protection and compliance obligations specific to each sector. Each topic could be offered to organisations individually or in a package that covers multiple topics.

Recommendation 6

▶ Map Training Programmes to Established Standards and Frameworks

There is a lack of established standards and frameworks in cyber security careers, resulting in a mismatch of skills requirements and salaries offered by organisations. Collaboratory could design its training programmes around NICE NIST or Mitre Att&ck cyber frameworks. This would help companies to standardise and better understand their cyber security skills requirements when recruiting.

Recommendation 7

Soft Skills Training Programmes

Despite the survey results not identifying soft skills to be in high demand, other reports indicate the increasing importance of transversal skills. Collaboratory could provide training courses on soft skills, focusing on applying them in real-life situations. For example, Collaboratory could contract consultants who bring an experimental and practical value to the theory around soft skills through role playing various experiential situations, allowing participants to apply new techniques and approaches in a safe and constructive environment. Soft skills modules could be a part of any training programme delivered by Collaboratory or could be delivered as a separate course, 'Soft Skills for Cyber Security'.

Recommendation 8

Supply Chain Security Training

Supply chain attacks are one of the emerging trends in cyber security. Desk research and survey findings confirmed that organisations are concerned about vulnerabilities with their third party suppliers (e.g. vendors, contractors, partners). It is evident that more training is required around this topic. Collaboratory could design a short course aiming to help organisations to understand the importance of supply chain security, how to identify and manage cyber-attacks in supply chains, and apply best practices in cyber supply chain risk management.

Recommendation 9

Intrusion Detection Training

Intrusion detection is identified as one of the most in-demand skills. Collaboratory could run penetration testing training programmes when its facilities are in place. Students can practice their intrusion detection skills and find system vulnerabilities in a simulated safe environment.

Recommendation 10

Gender Diversity in Cyber Security

Gender diversity is a proven challenge in the cyber security industry, and Collaboratory could take part in addressing the gender diversity issue by attracting females to cyber security careers through specifically designed and marketed cyber training programmes for females.

Recommendation 11

Cloud Security Training

Remote work brought cyber security to a different level. Many companies had to move their data to the cloud to enable employees to access it while working from home. Cloud security is one of the main concerns in cyber security. Training is required around cloud security for SMEs, and it should be one of Collaboratory's offerings.

Recommendation 12

Bespoke Training Provision

Collaboratory could offer bespoke training programmes to organisations based on their sector (for example, critical infrastructure, financial services, healthcare etc.) or work functions (human resources, finance, procurement operations, etc).

Recommendation 13

Free of Charge Workshops

Collaboratory could run monthly free short sessions for companies in the region on various topics. These workshops will help build a community of practice and support for companies in the region.

Appendix 1

All information presented in this report was accurate at the time when the research was carried out between June-July 2021. Please contact the training providers for the current cyber security training provisions.

Training Provider	Course Name
Technological University of the Shannon	Software Design with Cybersecurity
Munster Technological University	Bachelor of Business (Honours) in Information Systems
Munster Technological University	IT Management (BSc Honours)
Munster Technological University	Information Technology (BSc)
Munster Technological University	Cybersecurity (MSc)
Munster Technological University	Cybersecurity Management (MSc)
Dublin Business School	MSc in in Cybersecurity
Dublin City University	International Master in Security, Intelligence and Strategic Studies
Dublin City University	MSc in Computing (with Major Options)
Galway-Mayo Institute of Technology [17]	BSc in Network Cybersecurity
Griffith College Dublin	MSc in Network and Information Security
Griffith College Limerick	MSc in Network and Information Security
Institute of Technology Carlow [18]	Bachelor of Science (Honours) in Cybercrime and IT Security
Institute of Technology Carlow	Bachelor of Science in Cybercrime and IT Security
Institute of Technology Carlow	Master of Science in Cybersecurity, Privacy and Trust
Institute of Technology Carlow	Master of Science in Industrial Networks and Cybersecurity
Institute of Technology Sligo [19]	Bachelor of Engineering (Honours) in Electronics and Self Driving Technologies
Institute of Technology Sligo	Bachelor of Science in Computer Networks and Cloud Infrastructure
Institute of Technology Sligo	Bachelor of Science in Computer Networks and Cyber Security
Letterkenny Institute of Technology [20]	BSc in Computer Security & Digital Forensics
Letterkenny Institute of Technology	BSc Hons Computer Security & Digital Forensics
Letterkenny Institute of Technology	BSc Hons in Computing in Cybersecurity
Letterkenny Institute of Technology	MSc in Cybersecurity
Letterkenny Institute of Technology	MSc in Cybersecurity Research

Training Provider	Course Name
National College of Ireland	Master of Science in Cyber Security Starts January 2022 (Funded by Skillnet Ireland)
National College of Ireland	MSc in Cybersecurity
Technological University Dublin	MSc in Applied Cyber Security
Technological University Dublin	BSc in Computing - Digital Forensics and Cyber Security
Technological University Dublin	BSc in Computing - Digital Forensics and Cyber Security
Technological University Dublin	BSc (Honours) in Computing - Digital Forensics and Cyber Security
Technological University Dublin	MSc in Applied Cyber Security
Technological University Dublin	BSc in Computing in Digital Forensics and Cyber Security
Technological University Dublin	BSc Hons in Digital Forensics & Cyber Security
Munster Technological University	Cyber Risk for Business MSc - provides students with a portfolio of business and project management skills, as well as enhancing knowledge of IS concepts and core technical skills.
University College Dublin	MSc Forensic Computing and Cybercrime Investigation
University College Dublin	MSc Digital Policy
University of Limerick	Master Of Engineering In Information And Network Security
University of Limerick	Information and Network Security
Waterford Institute of Technology [21]	Bachelor of Science Software Systems Development
Waterford Institute of Technology	Bachelor of Science (Honours) Applied Computing (Computer Forensics & Security)
Athlone Institute of Technology	Certificate in Operational Security and Crime Risk Management
Blackrock Further Education Institute	Computer Networks and Cyber security
CCT College Dublin	Diploma In Cyber Security Fundamentals Course
CCT College Dublin	Diploma in Networking Technology And Security Course
CCT College Dublin	Diploma in Cybersecurity Essentials
CCT College Dublin	Diploma in Networking and Systems Security
City Colleges, Dublin	Introduction to Cybersecurity – CompTIA's Security+ (Certificate Exam Preparation)

[17] Due to became Atlantic Technological University in April 2022.
[18] [21] Due to become Technological University of South-East Ireland in May 2022.
[19] Due to become Atlantic Technological University in April 2022.
[20] Due to become Atlantic Technological University in April 2022.

Training Provider	Course Name
City Colleges, Dublin	Diploma in Cybersecurity - Advanced
CMIT College of Management and IT	IT Cyber Security Certification eLearning Bundle (CISA, CISSP, CISM)
CMIT College of Management and IT	CompTIA Security+
CMIT College of Management and IT	Certified Information Security Manager (CISM)
CMIT College of Management and IT	IT Security Master Certification Bundle
CMIT College of Management and IT	CompTIA CySA+ (Cybersecurity Analyst)
CMIT College of Management and IT	CISA – Certified Information Security Auditor
CMIT College of Management and IT	Certified Information Systems Security Professional (CISSP)
Munster Technological University	Cybersecurity Management (PGDip)
Dublin Business School	Diploma in Cybersecurity
Dublin Business School	Diploma in Ethical Hacking
Dublin Business School	Cybersecurity for Business
Dundrum College of Further Education	Network Professional/Cyber Security
Dundrum College of Further Education	Software, Coding and Cybersecurity)
Firebrand	EC-Council - Chief Information Security Officer Training | EC-Council CCISO
Firebrand	(ISC)2
Firebrand	Amazon Web Services (AWS) - Certified Security - Specialty
Firebrand	Amazon Web Services (AWS) - Security Engineering on AWS
Firebrand	Amazon Web Services (AWS) - Security Essentials
Firebrand	AXELOS - Cyber Resilience: Foundation & Practitioner (RESILIA®)
Firebrand	BCS - CISMP Course
Firebrand	CertNexus - Cyber Secure Coder (CSC)
Firebrand	CertNexus - CyberSec First Responder (CFR)
Firebrand	CompTIA - Network Security Professional (CNSP)
Firebrand	CompTIA - Network Vulnerability Assessment Professional (Security+/ PenTest+)
Firebrand	Cyber Crime - Management
Firebrand	CompTIA - Cybersecurity Analyst (CySA+)

Training Provider	Course Name
FIT	FIT Cybersecurity Apprenticeship
FIT (Colaiste Ide, Cardiffsbridge Road, Finglas West, Dublin 13)	Computer Systems & Networks with Cyber Security
FIT (Drogheda Institute of Further Education & Blackrock Further Education Institute)	Computer Networks & Cyber Security
FIT (Greenhills Community College, Dublin)	Comptia Cyber security Analyst (CySA+)
FIT (Killester College Dublin)	Computer Network Technician & Cybersecurity
FIT (Killester College of Further Education, Dublin)	Computer, Network Technician & Cybersecurity internship program
FIT (St John's College, Cork)	Networks and Cyber Security
Galway-Mayo Institute of Technology	Certificate in Network Cybersecurity
Galway-Mayo Institute of Technology	Higher Diploma in Cybersecurity Risk & Compliance
Galway-Mayo Institute of Technology	Certificate in Data Cybersecurity
Galway-Mayo Institute of Technology	Certificate in Cybersecurity Operations
Griffith College Limerick	Postgraduate Diploma in Network and Information Security
IBAT College, Dublin	Diploma Cyber And Digital Security
IBAT College, Dublin	Diploma in CompTIA Security+
IBAT College, Dublin	Diploma in Introduction to Computer Hacking
IBAT College, Dublin	Springboard+ Certificate in Cyber-Security for Managers
IBAT College, Dublin	Cyber Professional
IBAT College, Dublin	Diploma in Cloud Computing Essentials For Business
ICT Skillnet	Certified Cyber Risk Specialist course (CCRS)
ICT Skillnet	Certificate In Emerging Digital Technologies
ICT Skillnet	Certified Cyber Risk Officer Course (CCRO)
Institute of Technology Carlow	Certificate in Data Protection
Institute of Technology Sligo	Certificate in Computer Networks and Cloud Infrastructure
Institute of Technology Sligo	Certificate in Secure IT and Deep/Machine Learning
Institute of Technology Sligo	Higher Diploma in Science in Computing
International Cyber Threat Task Force, Dublin	Certified Cyber Risk Officer

Training Provider	Course Name
International Cyber Threat Task Force, Dublin	Certified Cyber Risk Specialist
International Cyber Threat Task Force, Dublin	NIST Cyber Seurity Expert
International Cyber Threat Task Force, Dublin	Cyber Security Bootcamp for Women (CSBW)
International Cyber Threat Task Force, Dublin	Ransomware Uncovered Specialist Certificate
National College of Ireland	Higher Diploma in Science in Computing (CyberSecurity)
National College of Ireland	Postgraduate Diploma in Science in Cybersecurity
New Horizons	EC-Council Certified Ethical Hacker (CEH)
New Horizons	EC-Council Computer Hacking Forensics Investigator (CHFI)
New Horizons	EC-Council Certified Network Defender (C|ND)
New Horizons	EC-Council Certified Chief Information Security Officer (C|CISO)
New Horizons	EC-Council Certified Security Analyst (ECSA) v10.0
New Horizons	EC-Council Disaster Recovery Professional (EDRP)
New Horizons	Certified Information Security Manager® (CISM)
Rathmines College of Further Education, Dublin	Cyber Security with Software Development
Technological University Dublin	Certificate in Cyber Security & Agile Programme Management (Minor Award)
Technological University Dublin	Certificate in Networking Scripting & Security (Minor Award)
Technological University Dublin	Certificate in Networking, Security & Scripting
Technological University Dublin	Cloud, Provisioning, Management & Security with AWS Cert.
University College Dublin	GradCert Forensic Computing & Cybercrime Investigation
University College Dublin	GradDip Forensic Computing and Cyber Crime Investigation
University College Dublin	ProfCert Digital Policy
University College Dublin	Forensic Computing & Cybercrime Investigation
UCD Professional Academy	Professional Diploma in Ethical Hacking
UCD Professional Academy	Professional Diploma in Cybersecurity
UCD Professional Academy	COMPTIA A+ (Core Series) Certification
UCD Professional Academy	Professional Diploma in AWS (Solutions Architect SAA-C02)

Training Provider	Course Name
University of Limerick	Information and Network Security
Letterkenny Institute of Technology	Postgraduate Diploma in Computing in Cybersecurity
National University of Ireland, Galway	Postgraduate Certificate in Cybersecurity for Business
Bray Inst of Further Education, Wicklow	Computer Networks & Cyber Security
Munster Technological University (CyberSkills)	Certificate in Secure Network Operations
Munster Technological University (CyberSkills)	Certificate in Secure Software Development
Munster Technological University (CyberSkills)	Certificate in Secure Systems Architecture
Munster Technological University (CyberSkills)	Module CYBR8001 - Cybersecurity Standards & Risk
Munster Technological University (CyberSkills)	Module CYBR9001 - Secure Software Development
Munster Technological University (CyberSkills)	Module CYBR9004 - Cryptography and Protocols
Munster Technological University (CyberSkills)	Module CYBR9005 - Information Security Architect
Munster Technological University (CyberSkills)	Module CYBR8003 - Secure Network Systems
The Knowledge Academy	RESILIA® Foundation Training
The Knowledge Academy	RESILIA® Practitioner Training
IT @Cork Skillnet	Cyber Quest
itag Skillnet	Cyber Security Online Programme
itag Skillnet	Cyber Security Analyst Bootcamp
SANS Institute	Blue Team Operations
SANS Institute	Cloud Security
SANS Institute	Cyber Defense Essentials
SANS Institute	Digital Forensics and Incident Response
SANS Institute	Industrial Control Systems Security
SANS Institute	Penetration Testing and Ethical Hacking
SANS Institute	Purple Team
SANS Institute	Security Management, Legal, and Audit
Dublin Coding School	Cyber Security Fundamentals

Bibliography

1. ECS European Cyber Security Organisation survey analysis report, “Chief Information Security Officers’ (CISO) Challenges and Priorities”, April 2021
2. Cyber Ireland, “Cyber Security Skills Report 2021. National survey”
3. ESET, “Cyber Security Trends 2021: Staying secure in uncertain times”
4. FireEye/Mandiant, “A Global Reset: Cyber Security Predictions 2021”
5. Integrity360, “Guide to 2021: What’s Next in Cyber Security”
6. ENISA, “Cyber Security Skills Development in the EU”, December 2019
7. Government of Ireland, “National Cyber Security Strategy 2019-2024”
8. Government of Ireland, Department of Education and Skills “Technology Skills 2022. Ireland’s Third ICT Skills Action Plan”
9. (ISC)2, “Cyber Security Professionals Stand Up to a Pandemic. (ISC)2 Cyber Security Workforce Study, 2020”
10. RSM, “Catch-22: Digital Transformation and its Impact on Cyber Security”
11. Allen Parish, John Impagliazzo, Rajendra K. Raj, Henrique Santos, Muhammad Rizwan Asghar, Audun Josang, Teresa Pereira, Eliana Stavrou, “Global perspectives on cyber security education for 2030: a case for a meta-discipline”
12. ECESM Tempus, “Report on EU practice on cyber security education”
13. Hays, “Cyber Security Talent Report: Addressing the Skills Gap”
14. WIN Workforce Intelligence Network, “Cyber Security Emerging Technologies Skills Gap Analysis” Spring 2020
15. IBM Report, “It’s not where you start – it’s how you finish. Addressing cyber security skills gap with a new-collar approach”
16. ENISA, “Cyber security for SMEs Challenges and recommendations", June 2021
17. Keeper Security, “2021 UK Cyber Security Census Report”
18. Queen’s University Belfast / CSIT Centre for Secure Information Technologies “Northern Ireland cyber security snapshot 2021”
19. IT@Cork Skillnet, “Cyber security skills development strategy", May 2021
20. McKinsey & Company, “Perspectives on transforming cyber security", March 2019
21. NIST Special publication 800-12 Revision 1 “An introduction to information security”
22. Ponemon Institute “Cyber security in the remote work era: a global risk report. October 2020”
23. Kaspersky, “The Cyber Security Skills Gap: A Ticking Time Bomb”
24. Ireland’s National Skills Strategy 2025
25. Debate Security research report, “Cyber Security Technology Efficacy: Is cyber security the new ‘market for lemons’?”
26. Capgemini Research Institute, “Reinventing Cyber Security with Artificial Intelligence: A new frontier in digital security”
27. Government of Ireland report, “Future Jobs Ireland 2019. Preparing Now for Tomorrow’s Economy”
28. Bruce Schneier, “The Coming AI Hackers”
29. FIT “ICT Skills Audit 2018”
30. World Economic Forum “The Global Risks Report 2021. 16th edition”
31. CISA “Cyber security career path and progression. February", 2019

COLLABORATORY

Collaboratory, LINC, TU Dublin Blanchardstown Campus,
Blanchardstown Road North, Blanchardstown, Dublin, D15 VPT3

Tel: 01 2208130
Email: collaboratory@tudublin.ie
www.collaboratory.ie

@CollaboratoryIE
www.linkedin.com/company/collaboratoryattudublin