QUEEN'S UNIVERSITY BELFAST | CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Perspective Economics

NORTHERN IRELAND CYBER SECURITY SNAPSHOT

CENTRE FOR SECURE INFORMATION TECHNOLOGIES (CSIT)

AUGUST 2023

Sam Donaldson & Conor Tinnelly (Perspective Economics)
David Crozier (CSIT)

CONTENTS

Executive Summary

The Centre of Secure Information Technologies (CSIT) is the UK's Innovation and Knowledge Centre (IKC) for cyber security, delivered in collaboration with Innovate UK, the Engineering and Physical Sciences Research Council (EPSRC) and Invest Northern Ireland. CSIT is committed to world class research in and accelerating translation activity for economic impact. The centre also works collaboratively with the National Cyber Security Centre (NCSC), ensuring that the UK is the safest place to live and work online.

In February 2023, CSIT secured an £18.9m investment in the region's cyber security ecosystem, including £11 million UK Government funding through the New Deal for Northern Ireland, to help develop a pipeline of cyber security professionals in NI and provide collaborative research and development opportunities with industry through the creation of a Cyber-AI Hub. This is also supported by £3.3m of funding from the EPSRC, to deliver the third phase of CSIT's IKC programme, focused on "Securing Complex Systems" cementing its position as a world-leading centre for research and innovation until 2027.

Perspective Economics were commissioned by CSIT to undertake this overview of the Northern Ireland cyber security ecosystem. It finds that we are an international hotspot for cyber security activity, and our firms deliver products, solutions and services to a broad range of markets including national security, government, health, automotive, critical infrastructure, financial services, legal, e-commerce, e-learning and more.

Cyber security is a success story for this region with over 2,700 related roles generating over £230m direct GVA to the economy. There are big ambitions for growing the sector to 5,000 cyber security professionals by 2030.

OVERALL THIS REPORT FINDS:

Number of Companies:

- There are 124 companies with commercial or R&D-driven cyber security teams in Northern Ireland.
- We estimate that 46 of these are 'dedicated 'or 'pure-play, where all of the firm's activity is cyber security related. 78 of these are 'diversified', where we have identified a cyber security team undertaking commercial or R&D activity, but the wider business may offer broader services such as professional services, aerospace and defence, or finance.
- This research highlights particular strengths in Northern Ireland in risk, compliance and fraud, identification, authentication and access control, and OT security.
- Belfast is one of the world's most concentrated cyber security clusters, with more than 100 cyber security businesses and teams.
- Northern Ireland is an attractive location for both inward investors, and indigenous start-ups, spin-outs and scale-ups. 66% of firms are headquartered overseas.
- Northern Ireland is not only the number one global destination for US FDI, but over 1,700 cyber security jobs in NI are backed by US FDI. NI also attracts inward investment from Canada, Europe, Japan, Israel, and the wider UK and Ireland.
- Northern Ireland has secured 26% of UK inward investment projects in cyber security from the United States since 2016, Further, these projects have supported (or are expected to support) over 1,750 roles in Northern Ireland. This is the highest in the UK, reflecting 45% of new roles created in cyber security in the UK by US FDI.

Economic Contribution:

- These firms employ an estimated 2,750 FTEs in cyber security (in 2023).
- The average cyber security salary advertised in NI in 2022 was £53,800[1].
- We estimate direct Gross Value Added (GVA) generated by the NI cyber security sector is approximately £236m. This is a 47% increase in GVA since the 2021 baseline study (£161m).
- The sector has a target employment figure of 5,000 jobs by 2030, which we view is on track. We estimate that if the cyber sector achieves the targeted number of employees, the sector will have an estimated GVA of £505m per annum by 2030.
- Over the decade (2021-2030), we expect that the Northern Ireland cyber security sector could contribute up to £3.2bn in cumulative GVA.

Skills:

- Overall, we estimate that there are **approximately 300 new entrants** into the cyber security sector each year (200 through HE and 100 through retraining, apprenticeships and conversion initiatives). The current higher education system, and use of retraining and reskilling initiatives broadly meets the needs of industry; however, as the sector grows and as more people retire or exit the workforce, there is a need for sustainable supply.
- Northern Ireland has increased its skills supply in cyber security significantly over the last two years (since the 2021 baseline report). It should continue these efforts to help meet the 5,000 jobs target by 2030. There is absorptive capacity and demand to **train an additional 100 – 150 people per annum** to support industry demand.
- Demand for cyber security professionals has more than doubled in Northern Ireland within the last three years. In 2022, there were almost 1,100 unique job postings (Lightcast, 2023) in demand for cyber security professionals.

[1] DSIT (2023) UK Skills in the Labour Market.

01 Introduction

1.1. BACKGROUND AND CONTEXT

The Centre of Secure Information Technologies (CSIT) is the UK's Innovation and Knowledge Centre (IKC) for cyber security. It is delivered in collaboration with Innovate UK, the Engineering and Physical Sciences Research Council (EPSRC) and Invest Northern Ireland.

In February 2023, CSIT secured £18.9m investment in the region's cyber security ecosystem. This included £11 million UK Government funding through the New Deal for Northern Ireland, which is being used by CSIT to further develop the pipeline of talent within the region and to provide collaborative research and development opportunities with industry through the creation of a Cyber-AI Hub. Further support to CSIT has been provided through the EPSRC, which includes £3.3m of funding which will be used to deliver the third phase of CSIT's IKC programme. This work is focused on 'Securing Complex Systems' and will support CSIT until 2027.

Perspective Economics have been commissioned by CSIT to undertake an annual Cyber Security Sector Snapshot (2023 – 2025), with additional market intelligence support to enable further strategic and monitoring and evaluation activities.

This provides an update to the Centre for Secure Information Technologies (CSIT) Northern Ireland Cyber Security Snapshot 2021 and includes an overview of the cyber security market in Northern Ireland up to Q2 2023 across key themes such as key products and services, financial performance, investment, research and innovation, and labour market activity.

It will support CSIT in tracking growth within the cyber security sector in Northern Ireland, and will also inform the process and impact evaluation activity for this investment in CSIT, drawing on novel and agreed Key Performance Indicators (KPIs) for the Cyber-AI Hub project.

1.2. RESEARCH SCOPE AND DEFINITION

The cyber security sector does not have a formal Standard Industry Classification (SIC) code. The research team have therefore worked closely with CSIT to develop a sector definition and taxonomy that reflects the unique cyber security offering within Northern Ireland, but is also closely aligned to national strategy, and previous research conducted on behalf of the Department for Science, Innovation and Technology (DSIT).

Cyber Security is defined in the context of this study as:

"The protection of internet connected systems (to include hardware, software, and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm, or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so."

UK National Cyber Security Strategy 2022

Table 1.1 provides an overview of the taxonomy adopted by the research team to identify cyber security businesses in Northern Ireland. These classifications have been developed to reflect the specialisms offered by firms operating in the sector specific to Northern Ireland, acknowledging the region's particular strength in securing inward investment, and the establishment of high-value Research and Development (R&D) offices and Security Operation Centres (SOCs).

TABLE 1:1 SECTOR TAXONOMY CLASSIFICATION

Sector Specialism	Definitions
Identification, Authentication and Access Control	Systems designed to support the verification of users accessing systems.
Risk, Compliance and Fraud	Solutions to identifying risk (such as harmful actors or anomalies), ensuring compliance with cyber security standards.
Securing Applications, Networks & Cloud	Customisable solutions for identifying and patching potential software or network exploits or applying secure parameters to network or cloud environments.
Threat Intelligence, Monitoring, Detection and Analysis	Information security professional services focusing on network administration or network engineering, that helps counter the activities of cyber criminals such as hackers and developers of malicious software.
Operational Technology (OT) Security & Connected	Manufacture and distribution of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment).
Managed Security Service Provision (MSSPs) & Advisory	Outsourced cyber security solutions focused on monitoring, network security, patching and remote device management, penetration testing, and wider security and IT advice.

Source: Perspective Economics, CSIT

02

The Cyber Security Sector in Northern Ireland

2.1. INTRODUCTION

Northern Ireland has a globally recognised cyber security ecosystem, which is gaining increasing attention from companies, investors, academia, and governments. In April 2023, Belfast hosted the National Cyber Security Centre's flagship event – CyberUK 2023, bringing over 2,000 global cyber security leaders to the region.

The growth of Northern Ireland's cyber security sector is not a sudden phenomenon, nor overnight success. It is, rather, the result of consistent effort and sustained investment, arguably over the last twenty-five years.

FIGURE 2:1 NORTHERN IRELAND CYBER SECURITY TIMELINE – KEY DATES

PRE-2000

1998
Belfast (Good Friday) Agreement

1999
Northern Ireland Science Park (now Catalyst) set-up in Titanic Quarter Allstate Northern Ireland founded.

2000-2010

2003
MetaCompliance (previously Baronscourt Technology) founded.

2004
Mail Distiller founded (email security) The Institute of Electronics, Communications and Information Technology (ECIT) founded.

2006
Verticle Structure, LoughTec founded.

2007
Skurio, ANSEC IA founded.

2008
ECIT at Queens University Belfast chosen to host an Innovation and Knowledge Centre (IKC), the Centre for Secure Information Technologies (CSIT), which opens it's doors in 2009. IBM (Security) sets up presence at Titanic Quarter.

2010 - 2015

2011
CSIT one of the first six Academic Centres of the Excellence in Cyber Security Research recognised by GCHQ. CSIT hosts 1st Annual World Cyber Security Summit.

2012
Salt DNA founded.

2013
Mail Distiller acquired by Proofpoint. Belfast secures an IBM Smarter Cities Challenge Grant.

2014
Emergence of NI's domestic cyber security sector: Ampliphae. B-Secur founded, Cyphra (now Cybit), AuditComply founded.

CSIT sets up one of the first MSc in Applied Cyber Security - which has enrolled almost two hundred students since starting.

Rapid7 establishes offices in NI.

2015
Liopa founded (commercialism over 15 years of research at QUB in the field of speech and image processing).

CSIT Awarded The Queen's Anniversary Prize for it's work in strengthening global cyber security and protecting billions of internet users around the world and for its economic impact.

2016 - 2020

2016
Inward Investment: Oosto (formerly AnyVision), Black Duck by Synopsys.

2017
CSIT co-founds Global EPIC., Belfast hosts OWASP Appsec Europe 2017 conference. Anomali creates 120 jobs.

2018
CSIT partners with a new cyber innovation centre, LORCA. Signifyd, Imperva, NI Cyber (cluster) set up.

Northern Ireland confirmed as the Number 1 international investment destination for US sourced FDI projects in cyber security.

2019
Contrast Security announces 120 jobs. Aflac announces 150 jobs (1/4 cyber), Angoka founded.

2020
Microsoft opens an 85 person cyber security centre

Cygilant establishes a global SOC in Belfast (65 jobs)

Titan IC acquired by Mellanox, then Nvidia (now based in NI).

2020+

2021
Rapid7 opens a new office in central Belfast with room for 400 employees, and is Rapid7's largest engineering hub globally.

KPMG runs Cyber Security Assured Skills Academy with DFE.

Telefonica Tech expands its Belfast SOC.

Agio, Nihon Cyber and Nisos announce NI offices.

CSIT partners with the Royal Air Force on pioneering innovation node for Northern Ireland to develop the cyber related defence supply chain in the region.

2022
BT opens state-of-the-art Security Operations Centre in Belfast, following £6.3m DoF SIEM and SOC managed services award.

Outsource Group and Ansec IA merge to create and NI security 'powerhouse'.

CSIT awarded £3.3m by EPSRC for delivering the next phase of the IKC.

CSIT becomes only the third research Centre to join the Rolls-Royce Global Cyber Technology Research Network.

2023
UK Government announces £18.9m investment in CSIT's Cyber-AI Hub

Belfast hosts CyberUK

CSIT joins the International Cyber Security Center of Excellence (INCS-CoE).

2026
Global Innovation Institute (58m) set to open.

This chapter sets out the evidence base underpinning Northern Ireland's strength and opportunity within its cyber security industry. It explores the number of cyber security businesses in Northern Ireland, including what they offer, their location, and classification by size, type, and industry focus.

2.2. NUMBER OF CYBER SECURITY FIRMS

The research team has identified **124 companies** in Northern Ireland that **either provide a cyber security product or service to market, or are actively employing a cyber security team** in Northern Ireland that contributes to a commercial outcome (e.g. an insurance firm with a dedicated cyber security operation in Northern Ireland).

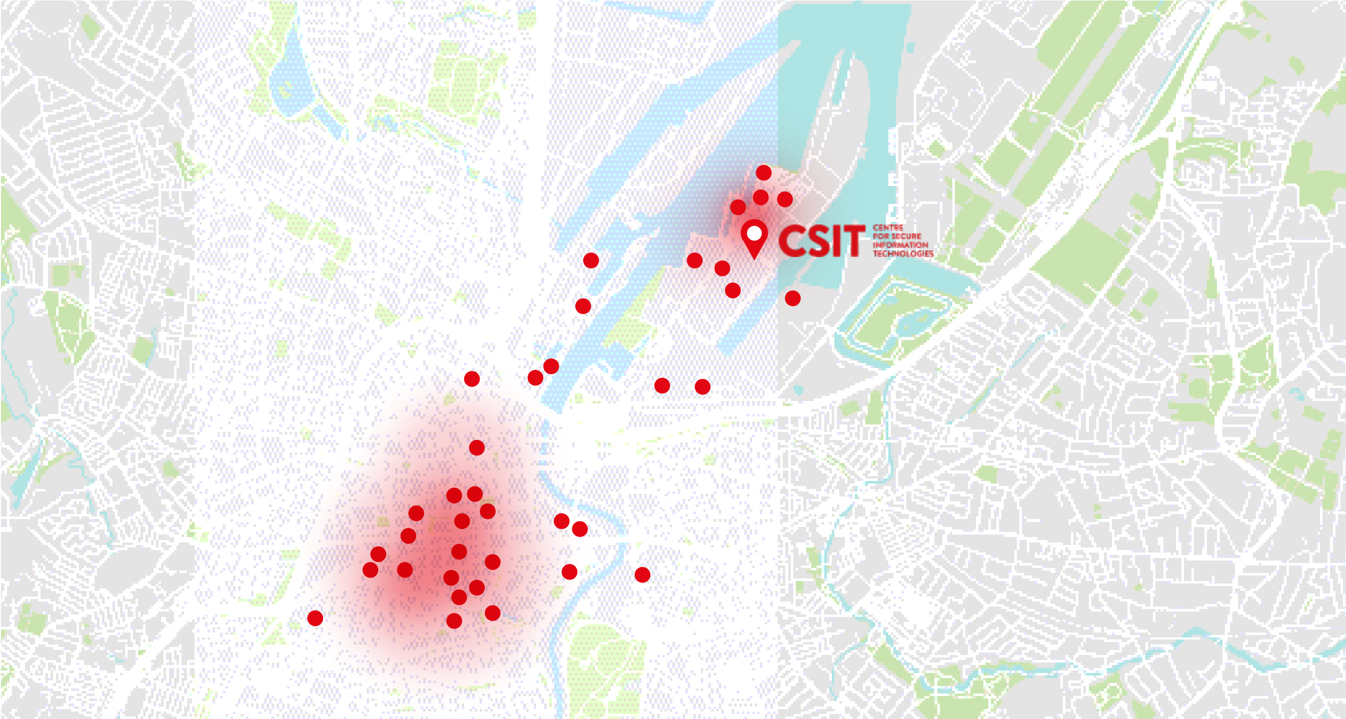
This is an increase of 20 firms since the Northern Ireland Cyber Security Sector Snapshot 2021, an increase of 19% in two years, reflective of the inward investment and growth in the local industry, with new entrants including firms such as Nisos, Wolfspeed, Smarttech247, Agio, Pytilia, and Riskonnect as well as firms setting up cyber security teams such as ASOS.

The methodology used to identify cyber security businesses and employees operating within Northern Ireland is consistent with the UK Cyber Security Sectoral Analysis 2023 research undertaken for DSIT.

2.3. LOCATION

The research team also conducted analysis into the location of cyber security firms in Northern Ireland. A map of NI office locations is provided below, highlighting the strong presence of cyber security firms in Belfast, which is home to 85% of Northern Ireland cyber security firms. However, there are also opportunities to build and scale teams within the North-West region.

FIGURE 2:2 NORTHERN IRELAND (AND BELFAST) CYBER SECURITY OFFICE LOCATIONS



● Cyber security businesses and teams

Source: Perspective Economics, CSIT

NORTHERN IRELAND CYBER SECURITY OFFICE LOCATIONS

Londonderry/
Derry
Belfast
Lisburn
Armagh
Newry
apbox © OpenStreetMap

2.4. CYBER SECURITY CAPABILITIES

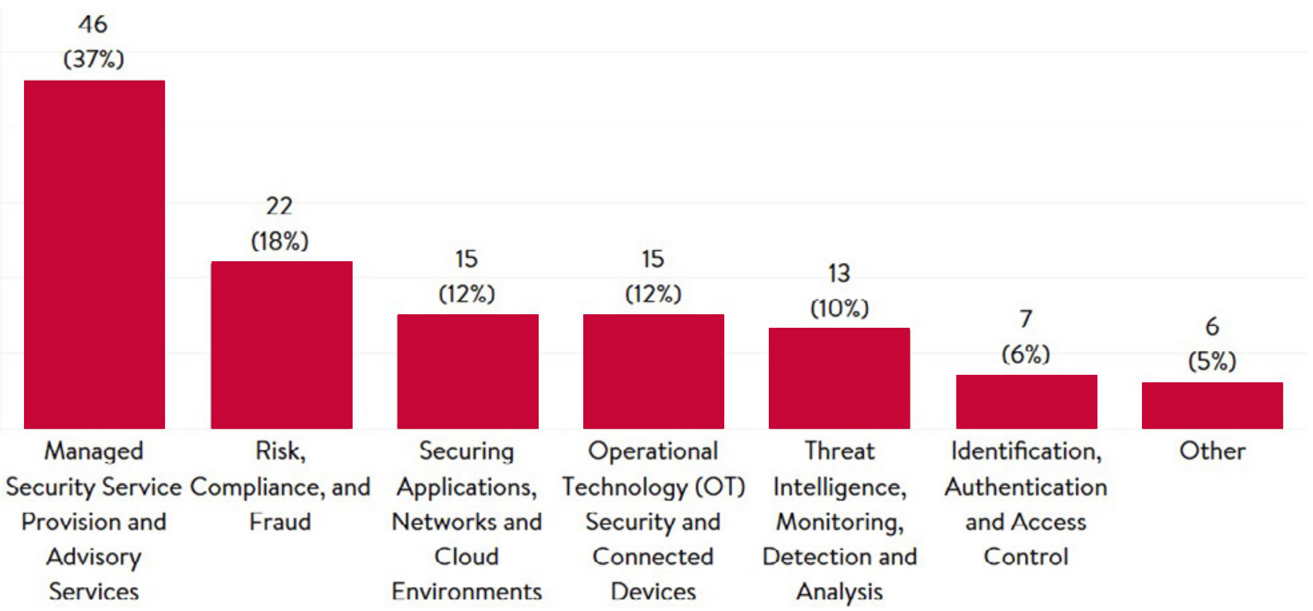
We classify the cyber security products and services offered by firms operating in Northern Ireland into seven distinct areas, as the research team has identified relative strengths in the following areas:

- Managed Security Service Provision and Advisory Services
- Risk, Compliance and Fraud
- Securing Applications, Networks and Cloud Environments
- Operational Technology (OT) Security and Connected Devices
- Threat Intelligence, Monitoring, Detection and Analysis
- Identification, Authentication and Access Control
- Other

BEST FIT CLASSIFICATION

We use a 'best-fit' for each company initially, followed by a wider capability classification (covering multiple areas).

FIGURE 2.3 BEST-FIT TAXONOMY CLASSIFICATION



Please note that the classification above is based on the basis of "best-fit" service offering. On the basis of this categorisation the above figure suggests that:

- 46 firms offer managed security service provision and advisory services, including employers such as: PwC, Kainos, Fujitsu, and Capita
- 22 firms provide risk, compliance, and fraud services, including employers such as: Allstate, Metacompliance, Signifyd, and Cybersource.
- 15 firms secure applications, networks, and cloud environments, including employers such as: Rapid7, Synopsys, IBM, and BT.
- 15 firms provide services-related to operational technology, security, and connected devices, including employers such as: Kigen, Johnson Controls, Nvidia, and Sensata.
- 13 firms provide threat intelligence monitoring, detection and analysis, including employers such as: Proofpoint, Imperva, iManage, and Anomali.
- 7 firms provide services relating to identification, authentication, and access control, including employers such as: Core Systems, Oosto, Salt Communications, and Liopa.
- 6 firms provide other diversified services, or have hired cyber security staff to support internal activity, e.g., ESO Solutions, Bank of London, and ASOS.

Identification, Authentication and Access Control

Salt Secure Communications liopa B-SECUR core

Risk, Compliance and Fraud

Signifyd MetaCompliance AuditComply AMPLIPHAE

Securing Applications, Networks & Cloud

RAPID7 cloudsmith IBM Security SYNOPSYS

Threat Intelligence, Monitoring, Detection and Analysis

imperva ANOMALI SKURIO SilverSky proofpoint.

Operational Technology (OT) Security & Connected Devices

ANGOKA NVIDIA. Cynalytica Kigen

Managed Security Service Provision (MSSPs) & Advisory

kainos VerticalStructure Cybit OUTSOURCE GROUP

Table 2.1 below offers insight into how the sector composition has changed since baseline analysis in 2021.

TABLE 2.1 NUMBER OF FIRMS BY TAXONOMY CATEGORY, BASELINE AND UPDATE

Sector Specialism	2021 (baseline)	2023 (current)
Managed Security Service Provision (MSSPs) and Advisory	39	46
Risk, Compliance and Fraud	19	22
Securing Applications, Networks & Cloud	18	15
Operating Technology (OT), Security, and Connected Devices	14	15
Threat Intelligence, Monitoring, Detection and Analysis	8	13
Identification, Authentication, and Access Control	8	7
Other	-	6
Total	104	124

Source: Perspective Economics, CSIT

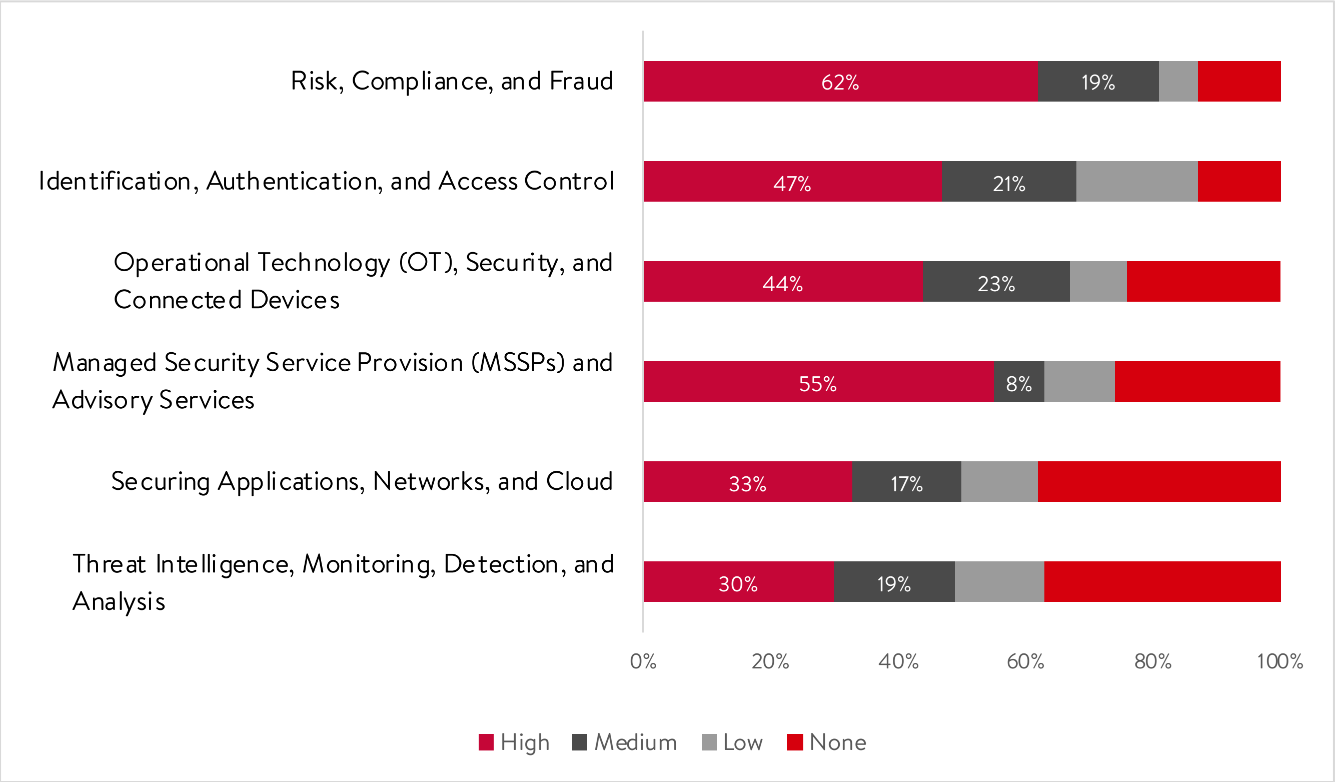
WIDER CAPABILITY CLASSIFICATION

We have also applied a marker for each taxonomy grouping based on firm descriptions (in their own words) to identify if each firm is likely to provide some form of cyber security capability against the taxonomy.

This highlights particular strengths in Northern Ireland in risk, compliance and fraud, identification, authentication and access control, and OT security.

Where the company's web description is closely aligned with the taxonomy category definition, we mark this as 'high', followed by 'medium', 'low' or 'none'.

FIGURE 2.4 WIDER TAXONOMY CLASSIFICATION



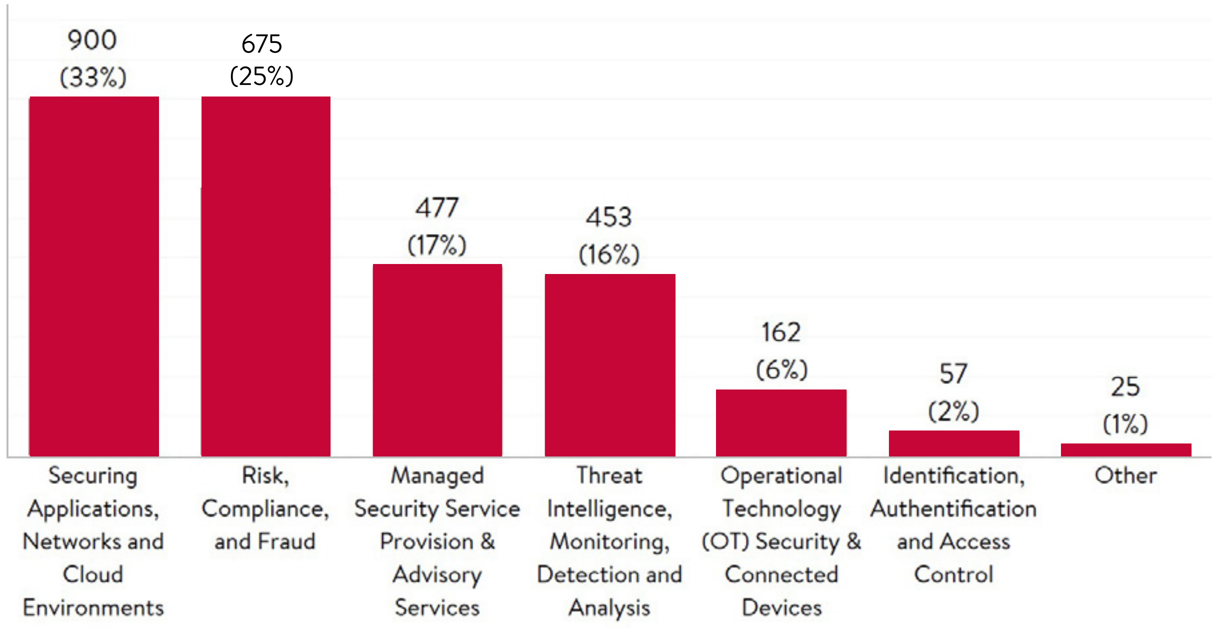
2.5 EMPLOYMENT

2.5.1. NUMBER OF CYBER SECURITY EMPLOYEES

There are an estimated 2,749 employees working within Northern Ireland's cyber security sector, which suggests a 20% increase in sector employment since baseline or 450 new entrants to the sector between 2021 and 2023.

Figure 2.4 provides an indicative overview of where employment sits across the best fit taxonomy categories outlined above.

FIGURE 2.5 EMPLOYMENT BY BEST FIT TAXONOMY CATEGORY



Source: Perspective Economics, CSIT

Figure 2.4 suggests that a third of Northern Ireland cyber security professionals are employed by firms that focus on securing applications, networks, and cloud environments. A further 25% are employed in firms that focus on risk, compliance and fraud, and despite making up close to 40% of all firms, managed security service provision and advisory services make up just 17% of total employment. Key employers across each taxonomy category include:

- Securing applications, networks and cloud environments: Rapid7, Synopsys, IBM, and BT;
- Risk, compliance, and fraud: Allstate, Metacompliance, Signifyd, and Cybersource;
- Managed security service provision and advisory services: PWC, Kainos, Fujitsu, and Capita;
- Threat intelligence, monitoring, detection and analysis: Proofpoint, Imperva, iManage, and Anomali;
- Operational technology (OT) security and connected devices: Kigen, Johnson Controls, Nvidia, and Sensata;
- Identification, authentication, and access control: Core Systems, Oosto, Salt Communications, and Liopa;
- Other providers: ESO Solutions, Bank of London, HP, ASOS.

2.5.2. THE ROLE OF INWARD INVESTMENT IN THE NI CYBER SECURITY SECTOR

Northern Ireland is the leading location for US FDI in cyber security projects (FT, 2021). This is reflected significantly when exploring employment figures by country of origin.

The table below highlights that almost two-thirds of roles in the NI cyber security sector are backed by US FDI (64%) driven by firms such as Rapid7, Proofpoint, Imperva, and Synopsys.

TABLE 2.3 NUMBER OF FIRMS AND EMPLOYEES BY COUNTRY OF ORIGIN

Country of Origin	Number of Companies	Estimated Cyber Security Related Employment
United States	43	1,771
Rest of UK	26	460
Northern Ireland	41	372
Japan	2	53
Republic of Ireland	5	41
France	3	20
Germany	2	16
Israel	1	14
Canada	1	2
Grand Total	**124**	**2,749**

Source: Perspective Economics, CSIT

We cover this in further detail in Section 5.1.

2.6. ECONOMIC CONTRIBUTION (GVA)

We estimate that Gross Value Added (GVA) per employee within the Northern Ireland cyber security sector has increased from £70,000 in the 2021 study to £85,920 in 2023. This takes the average cyber security salary advertised in NI (£53,800)[2], and the estimated profit per employee (uplifted from the UK cyber security sectoral analysis project).

Based upon the current workforce size of 2,749 employees, this suggests the Gross Value Added (GVA) of the NI cyber security sector is approximately £236m. This is a 47% increase in GVA since the 2021 baseline study (£161m), suggesting that the increased level of employment, salaries and profitability are all leading to increased economic impact for Northern Ireland.

[2] DSIT (2023) UK Skills in the Labour Market.

03

Policy, Regulation, & Threat Landscape

3.1. INTRODUCTION

This section of the report provides a brief overview of the cyber security threat landscape. It subsequently outlines current strategy towards countering cyber security threats in the UK, Northern Ireland and globally.

3.2. CYBER SECURITY THREAT LANDSCAPE

The ENISA Threat Landscape provides a European level assessment of some of the prime threats, major trends, threat actors, and mitigations against cyber risk. In 2022, it identified eight top threats to western societies. These include:

- Ransomware:
- Malware
- Social Engineering, including phishing, whaling, smishing and vishing
- Threats against data
- Threats against service availability (DDoS)
- Threats against internet infrastructure
- Disinformation and misinformation
- Supply chain targeting

In tandem, zero-day exploitation, increasing hacktivism, DDoS attacks against mobile networks and critical national infrastructure, and AI-enabled disinformation and deep-fakes are all major increasing trends faced by governments and industry. Threat actors include state-sponsored actors, cybercrime actors, hackers-for-hire actors, and hacktivists.

The UK Cyber Breaches Survey (2023)[3] highlights some significant findings regarding cyber resilience among the UK's industry and public sector organisations, including those based in Northern Ireland.

It highlights that larger businesses and organisations are more likely to recall breaches or attacks on their organisation within the past twelve months (69% of large businesses) than smaller businesses (32%). Further, the proportion of micro businesses saying cyber security is a high priority has decreased from 80% in 2022 to 68% in 2023, suggesting that the UK's smallest businesses are finding it challenging to balance the need for investment in cyber security with other commercial challenges on a day-to-day basis.

Further, whilst larger firms are generally more able to invest in cyber security, either internally or through outsourced providers - they are increasingly exposed to threats such as ransomware, data leakage, service disruption or third party attacks.
There is a challenge therefore, that larger organisations are increasingly targeted at scale, whilst smaller organisations are limited in resources to identify, mitigate and respond to incidents. This challenge is particular pronounced within Northern Ireland's economy:

- **Among large businesses:** Northern Ireland has one of the smallest proportion of large (250+ employees) businesses of any region in the UK. These businesses are also highly concentrated into sectors such as retail, manufacturing, construction, and agriculture. The UK Cyber Breaches Survey (2023) reports that these sectors are typically less likely to have formal controls or high prioritisation for cyber security compared to sectors such as finance, professional services and healthcare.

- **Among small and medium businesses:** Small (10-49 employees) and Medium (50-249 employees) businesses are often in a challenging position with respect to cyber security requirements. On one hand, they need to ensure they have secure IT systems that are scalable across the organisation, which means that outsourcing is most common among medium (50%) and small (58%) businesses, compared to 36% of businesses overall (larger firms are more likely to have in-house teams, and micro firms with limited coverage). However, this can also create challenges in that, many firms may use Managed Service Providers (MSPs) rather than Managed Security Service Providers (MSSPs) – in the view that their security is taken care of through third-party coverage, when this may not be fully covered (e.g. limited backups, incident response coverage etc). Further, these businesses may also face cost pressures at a board or management level, and security spending may be relatively low per employee.

[3] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

- **Among micro businesses:** Only 32% of micro businesses in the UK have an external cyber security provider, and less than one in four (24%) have a formal policy covering cyber security risks. This can attributed to many reasons, including perceived cost, awareness, and time among leadership teams. In Northern Ireland, 89% of businesses are micro, and only 2% have more than 50 employees – reflecting the challenge in embedding cyber security standards across the economy.

- **Among charities:** There are over 6,000 voluntary sector organisations in Northern Ireland[4]– of which a third report an income of less than £10,000. These organisations often work with vulnerable groups, and can hold particularly sensitive data. However, due to financial constraints, they often have legacy IT systems or limited security practices, and can be exposed to risks such as data leaks and ransomware. The National Cyber Security Centre and IASME have recently funded an initiative to help VCSEs achieve Cyber Essentials Plus certification, delivered by Vertical Structure in Northern Ireland.

- **Among public sector organisations:** Northern Ireland has a significant public sector consisting of devolved and local tiers of government, as well as public bodies in the domains of health, education, utilities, and wider regulation. Whilst public budgets are challenging in the current fiscal year, there are unique challenges for the NI public sector, particularly with respect to NIS regulations (ensuring that essential services are aligned to high cyber security standards), and securing Critical National Infrastructure. This requires significant resourcing, but also creates opportunities for the cyber security sector through contracting and procurement. The public sector also has a role to play in setting cyber security standards through regulatory and procurement channels e.g. Cyber Essentials as a minimum.

3.3. NATIONAL AND SUPRANATIONAL POLICY

It is important to acknowledge the connected nature of the threats that the cyber security sector seeks to address. With this in mind, we have also included a brief overview of recent national and supranational strategy relevant to the cyber security sector.

The most recent EU Cybersecurity Strategy (2020) reflects the threats that have emerged in an increasingly interconnected world, outlining the important of cyber security in essential services such as hospitals, energy grids and railways, alongside the importance of connected objects in homes, offices, and factories.

To address these threats the European Commission has set up a revised Directive on Security of Network and Information Security (NIS 2 Directive), which aims to improve cybersecurity risk management and introduce reporting obligations across sectors such as energy, transport, health and digital infrastructure. All non-EU entities engaging with the region must designate an EU representative as a result of this directive.

Further proposed EU acts[5] strengthening regional cyber security include the Cyber Resilience Act, which will help secure hardware and software products; the Cybersecurity Act, which will strengthen the role of the European Union Agency for Cybersecurity (ENISA); and the Cyber Solidarity Act which was proposed in April 2023 and aims to improve the response to cyber security threats in the EU.

The EU is also working on an EU-wide certification framework, has included additional cyber security investment in its coronavirus Recovery Plan for Europe, and has committed to supporting research and innovation through Horizon Europe's Civil Security for Society cluster.

The UK's Government Cyber Security Strategy (2022 – 2030) provides insight into the UK ambitions to significantly harden the Government's critical functions by 2025, while increasing resilience across the whole public sector by 2030.

The UK's National Cyber Strategy (2022) is aligned to EU policy, also highlighting the increased interconnectedness of society, and how this increases the risk of cyber security breaches. In line with EU strategy, the National Cyber Strategy highlights the importance of international collaboration in addressing cyber security threats, while also setting out five pillars to be used to guide the UK Government's approach. These pillars focus on: i) an increased investment in people and skills, and partnership working, ii) increasing resilience by reducing cyber risks so businesses can maximise the economic benefits of digital technology, iii) building industry capability and developing frameworks to secure future technologies, iv) advancing UK global leadership and influence in the area of cyber security, and v) detecting, disrupting and deterring cyber crime while enhancing UK security in and through cyberspace.

3.4. NORTHERN IRELAND

Northern Ireland is recognised as a global cyber security hub for several reasons. Whilst it has over 120 businesses within its cyber security sector, it is also considered attractive for a talented labour market (with Queen's University, Ulster University, The Open University, and Belfast Metropolitan College offering degree pathways in computer science and cyber security), its low operating cost base (with lower office costs than other regions of the UK), tax relief for R&D and support and grants for inward investment, and competitive salary costs.

Much of this is supported by policy and strategy initiatives at the regional level. There are three core themes set out within the Northern Ireland Cyber Security Strategic Framework for Action (2017-21), and supported by the NI Cyber Leadership Board. These include the need to

- **Defend** through investment in network and application resilience, and provide awareness, training and support to public, private and third sectors.

- **Deter** cyber-crime and bad actors through crime prevention and prosecution, and through cyber threat intelligence and incident response.

- **Develop** the cyber security ecosystem (in its ambition to reach 5,000 jobs by 2030) through talent and skills development, and supporting the activities of the region's cluster.

Cyber security reaches across a number of policy domains, and as such, there is a role for several public bodies in embedding cyber security at all levels. We set out some key organisations and policy leads below:

- **Department of Finance** is the lead for the 'Defend' strand of the Strategic Framework. It is the core sponsor for the **NI Cyber Security Centre** (supported by the National Cyber Security Centre), and is designated as the Network and Information Systems (NIS) competent authority for operators of essential services. The Department also leads on the role of cyber security and pathways within the public sector, and procurement of external cyber security solutions for public bodies.

- **Department of Justice** has oversight for the 'Deter' strand, with support from the **Police Service of Northern Ireland.** This includes the work of the PSNI Cyber Crime Centre, as well as Cyber Prevent and Cyber Choices schemes.

- **Department for the Economy** is the lead for the 'Develop' strand, where Northern Ireland can have a skilled workforce, is internationally competitive in cyber security R&D, and where the growth of the cyber sector facilitates economic growth. This also includes the work of Invest NI in promoting the region and supporting inward investment. Cyber security is recognised as a priority cluster for growth within the DfE 10x Economic Strategy.

- **Local Government** also has a role to play in supporting cyber security at all levels. For example, the Belfast Region City Deal includes £58m for the Global Innovation Institute, an expansion of the Institute of Electronics, Communications and Information Technology (ECIT) which will be completed by 2026.

[4] https://www.nicva.org/article/comparing-vcse-sectors-of-ni-england-wales-scotland-ireland

[5] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

3.5. KEY FINDINGS & POLICY HORIZON

Northern Ireland has recognised its emergent strengths and opportunities in cyber security as part of its regional economy. The NI Strategic Framework establishes a core ambition of reaching 5,000 cyber security jobs by 2030.

However, whilst the policy landscape provides a number of welcome initiatives to support cyber security at a regional level, this is a fast-moving domain, and requires sustained and ongoing support to maximise the opportunities for Northern Ireland.

Firstly, there is a need for further strategic direction at a local level. At a national level, the UK Government has published the National Cyber Strategy (2022), which sets out a vision to strengthen the UK's ecosystem, build resilience, lead technologically, advance global influence, and detect and disrupt adversaries to 2030. In addition, the UK Government also published the Government Cyber Security Strategy (2022-30) which covers the role of the public sector in detecting and managing risk, protecting against attacks, and developing talent.

Comparatively, the NI Strategic Framework for Action covered the 2017-2021 period, and despite a review document being published in early 2022, no strategic update has been published by the relevant departments. The Framework Review also provides a high-level overview of the activities that have been undertaken since 2017; however, outcomes, impacts and next steps are more limited within this review.

As such, we consider that Northern Ireland's cyber security ecosystem would benefit significantly from enhanced strategic and policy direction in the immediate future. Much has changed since the 2017 framework with respect to cyber security risks and threats, technology, regulation, and skills and resource allocation. The development of an updated regional strategy that further develops the Deter, Defend and Develop strands would be a welcome step to support the cyber security ecosystem.

Further, this could and should be aligned to a 'moonshot' strategy to 2030 and beyond. Potential moonshot ambitions could include reaching world-leading levels of cyber security literacy (embedded secure digitalisation across the economy), or ensuring that the Cyber-AI Hub and GII investments cement Northern Ireland's place as a global hub for cyber security research and commercialisation.

Policy support for cyber security in Northern Ireland has rightly focused on attracting inward investment, using a skilled workforce and financial incentives as key draws. However, to build a sustainable ecosystem, a renewed emphasis on workforce development is needed. This should include funding for courses and research to address the skills gap, as well as measures to attract and retain high-quality talent within academia and R&D. Additionally, support for indigenous growth should be increased, by promoting entrepreneurship and innovation through accelerators and startup grants, funding new infrastructures, and facilitating access to venture capital for external investment. The subsequent chapters within this research set out a baseline regarding each of these measures – however, policymakers must recognise the dual opportunity of supporting the cyber security ecosystem, as well as the high social and economic costs in failing to meet the potential of a secure and prosperous Northern Ireland.

04

Building the Skills Pipeline: Demand and Supply

4.1. INTRODUCTION

Northern Ireland's cyber security sector currently employs an estimated 2,700 people, with ambition to grow to 5,000 people by 2030. In addition, other employers such as those in the public sector, academia, and wider sectors also require talent with cyber security skills to help secure their organisations.

There are many opportunities and challenges associated with increasing the level of cyber security talent within Northern Ireland's economy, including:

- Significant demand for cyber security talent:
- An increasing need for cyber security awareness at all levels:
- A tight labour market, where demand for cyber security talent exceeds supply:
- A need to train and attract talent to live and work in Northern Ireland

This chapter explores the:

- Current state of the labour market in the cyber security sector in Northern Ireland.
- The provision of skills, education and training, including the role of educational institutions and training programs in preparing individuals for careers in cyber security.
- Discussion of any skills gaps and potential measures to address them.
- Growth scenarios for cyber employment in the region to 2030.

4.2. CURRENT CYBER SECURITY WORKFORCE IN NORTHERN IRELAND

4.2.1. WORKFORCE SIZE

Growing the cyber security workforce in Northern Ireland is a key priority for both economic growth and ensuring access to talent among employers across the private and public sectors.

There are two key considerations:

- How can we define the cyber security workforce – recognising the breadth of capabilities and skills required?
- How can we measure the size of the workforce, acknowledging limitations in official statistics?

Defining and Measuring the Cyber Security Workforce

The cyber security workforce is broad in definition, and can include those with technical and non-technical skills, as well as spanning a range of technologies and industrial domains. As such, the UK Cyber Security Council has developed a Cyber Career Framework. This sets out sixteen common specialisms requested by cyber security roles. These include:

- Cryptography and Communication Security
- Cyber Security Audit and Assurance
- Cyber Security Generalist
- Cyber Security Governance and Risk Management
- Cyber Security Management
- Cyber Threat Intelligence
- Data Protection and Privacy
- Digital Forensics
- Identity and Access Management
- Incident Response
- Network Monitoring and Intrusion Detection
- Secure Operations
- Secure System Architecture and Design
- Secure System Development
- Security Testing
- Vulnerability Management

The DSIT Cyber Skills in the UK Labour Market (2022) research also identifies how the cyber security workforce can contain both 'core' or 'technical'[6] roles as well as cyber 'enabled' roles (e.g. broader roles that are not typically considered purely cyber security focused, but may have aligned skills such as project management, risk assessment, network engineering, system administration, and technical support.). This study also estimates that the UK's cyber security workforce consists of c. 131,000 individuals across the entire economy. Of these:

- an estimated 58,000 work within the UK's cyber security sector (c. 2,000 businesses typically focused on cyber security provision)
- an estimated 12% (16,000) work in cyber security roles in the public sector
- The remaining 57,000 work in other sectors in cyber security related roles (e.g. finance, insurance, manufacturing, professional services etc).

These are estimates based upon the data available; however, this highlights the size, scale and breadth of skills within the UK's cyber security workforce. This study also estimates that up to 3-4% of the UK's cyber security workforce could be located in Northern Ireland across all sectors. **In other words, there could be approximately 4-5,000 people working in cyber security related roles in the region.** Looking at the broader cyber security workforce in Northern Ireland, we find evidence of cyber security professionals working in employers such as the NI Civil Service, Allen & Overy, NI Water, Almac, Ulster Bank (NatWest), Randox, Queen's University, and Lloyds Banking Group.

However, we focus on the 2,750 employees that we have identified within the 124 cyber security businesses in Northern Ireland, due to data availability. We recognise this figure will be higher across the entire economy, and utilise other datasets to highlight some key measures and statistics for the local ecosystem.

> We estimate there are an estimated 2,750 employees working within Northern Ireland's cyber security sector, which suggests a 20% increase in sector employment since baseline or 450 new entrants to the sector between 2021 and 2023.

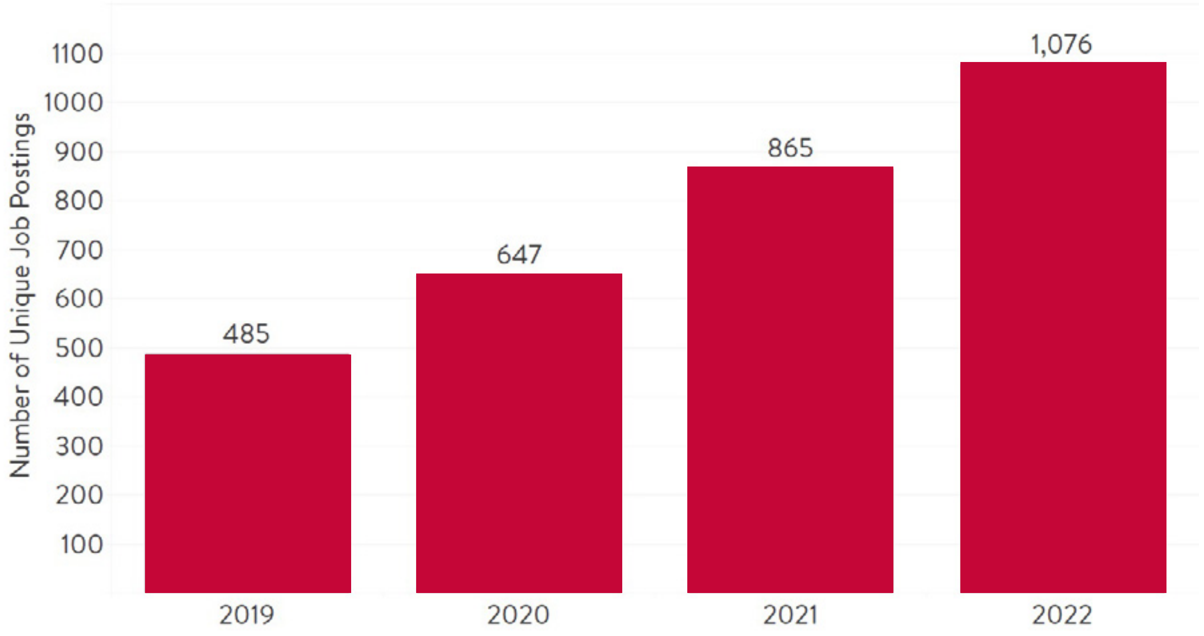
4.3. DEMAND FOR CYBER SECURITY TALENT

Demand for cyber security professionals has more than doubled in Northern Ireland within the last three years. In 2022, there were 1,076 unique job postings (Lightcast, 2023) in demand for cyber security professionals, from over 200 different employers and recruitment agencies.

[6] Commonly recognised as cyber security jobs. They have a greater demand for skillsets and tools directly related to cyber security, such as information systems, cryptography, information assurance, network scanners, and security operations. In other words, these are job roles where some aspect of cyber security is the main job function. This would typically include job titles such as Cyber Security Architect, Cyber Security Engineer, Cyber Security Consultant, Security Operations Centre (SOC) Analyst and Penetration Tester

4.3.1. NUMBER OF CYBER SECURITY JOB VACANCIES

FIGURE 4:1 NUMBER OF CYBER SECURITY VACANCIES POSTED IN NORTHERN IRELAND



Source: Lightcast

The review of vacancies posted in 2022 suggests highest demand among employers for:

- Cyber Security Analysts
- Cyber Security Engineers
- Cyber Security Managers
- Penetration Testers
- Cloud Security Consultants
- Technology Risk Analysts

Within Northern Ireland, the Lightcast data suggests that almost 200 different employers competed for cyber security talent across all sectors in Northern Ireland, with roles advertised online by firms such as Allstate, PA, Deloitte, Synopsys and SilverSky. Further review also indicates that recruitment agencies such as VANRATH, MCS, and Hayward Hawk were also highly active in 2022 in seeking cyber security talent for local businesses and inward investment projects.

4.3.2. LOCATION

As expected based on employer location, almost 95% of roles are posted within the Greater Belfast area, with c. 2% of roles in Derry/Londonderry and <1% in areas such as Newry, Mourne and Down, and wider Antrim.

However, of the 1,076 roles posted in 2022 in Northern Ireland, 221 (21%) stated that remote working could be undertaken for the role, with a further 105 (10%) mentioning hybrid working.

Further, the review of cyber security employment data within Northern Ireland does suggest that there is a small but growing proportion of the workforce that are employed by firms that do not necessarily have a presence or office in Northern Ireland, but permit remote working – for example, people living in Northern Ireland working remotely for large tech firms such as Meta.

4.3.3. SALARY AND REMUNERATION

For the cyber security roles advertised in 2022 in Northern Ireland, only 35% of these provided an indicative salary range. This means that almost two-thirds of roles either advertise as 'competitive' or will vary the salary based on candidate experience and skills depending on availability of talent.

However, for the third of roles that do provide salary data, in 2022, Lightcast suggests that the mean advertised salary was £53,800 (and median salary £44,900). Preliminary data for early 2023 also suggests that the median advertised salary for cyber security professionals has also increased to £48,500 to May 2023 – suggesting a c. 12% increase over the last year – reflecting wider inflationary pressures.

For the 377 roles with salary data, the following salary distribution is noted:

- 12% of roles are advertised between £20k to £30k per annum
- 19% of roles are advertised between £30k to £40k per annum
- 21% (median) of roles are advertised between £40k - £50k per annum
- 17% of roles are advertised between £50k - £60k per annum
- 17% of roles are advertised between £60k - £70k per annum
- 12% of roles are advertised at more than £70k per annum.

This highlights how salaries for cyber security roles can increase significantly with experience over the medium to long-term, particularly after four years+ of experience. One of Northern Ireland's largest recruitment firms, VANRATH, also conduct an annual salary survey which sets out indicative salaries for newly placed candidates.

TABLE 4.1 ESTIMATED SALARY BANDS FOR CYBER SECURITY CANDIDATES IN NORTHERN IRELAND

Role	Junior (1-3 years experience)	Intermediate (4-9 years experience)	Senior (10+ years)
Security Consultant / Auditor / GRC Specialist	£40k - £60k	£60k - £85k	£85k - £110k+
Information Security Specialist	£35k - £65k	£65k - £90k	£90k - £120k
Security Engineer / Engineering Manager	£40k - £70k	£70k - £100k	£100k - £140k+
Security Operations (SOC) Analyst	£40k - £50k	£55k - £65k	£70k - £100k+
Security and Compliance Analyst	£35k - £45k	£50k - £65k	£70k - £100k+
Security Specialist	£45k - £60k	£65k - £80k	£85k - £120k+

Source: VANRATH Salary Survey 2023

This highlights the significance of the cyber security sector in generating high-value, high-productivity roles within the Northern Ireland economy; whilst also maintaining international competitiveness compared to other Western regions.

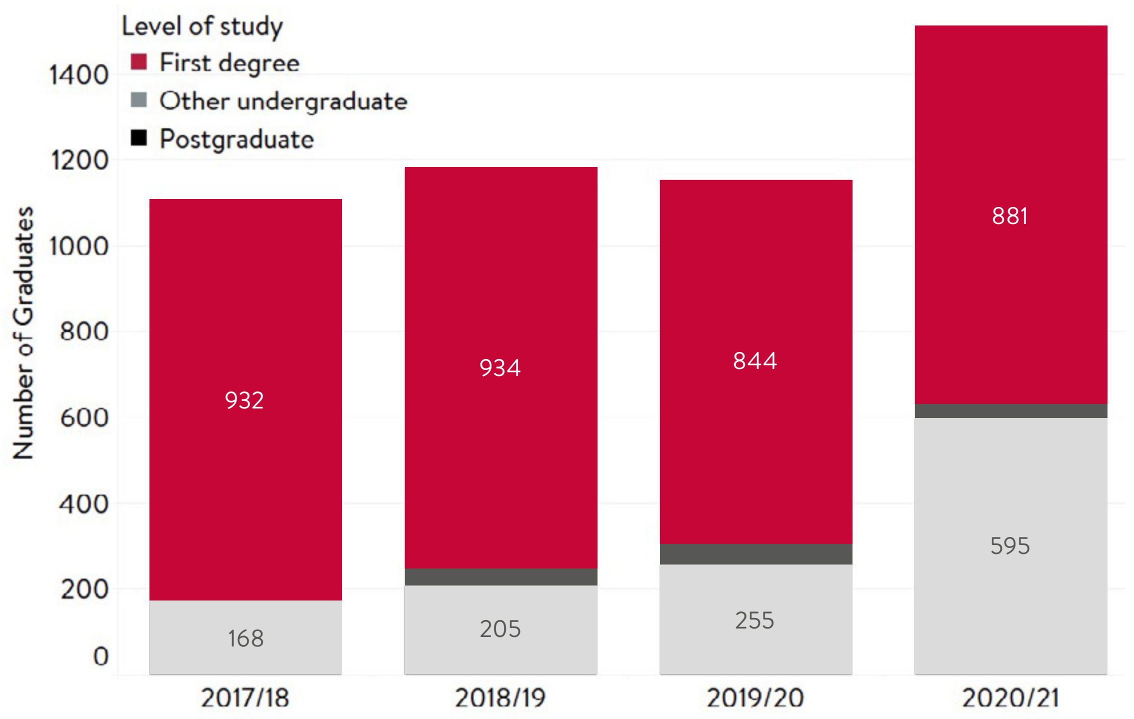
4.4. SUPPLY OF CYBER SECURITY TALENT

In order to meet the demand among cyber security employers, and grow the workforce, there is a need for a sustained focus on the supply of new talent coming through the education system and retraining initiatives. There are several routes into cyber security training and ultimately, a career in cyber security. This can include studying a relevant course at higher education level (e.g. a degree in cyber security or Computer Science) or further education level. It can also include individuals undertaking retraining and reskilling through Assured Skills Academies, bootcamps, or online learning initiatives. Further, many employers will also fund training initiatives to help get individuals into a cyber security role. Within job vacancies, employers most commonly request that candidates have degree level education within a relevant pathway, either at undergraduate or postgraduate level. As such, this is often one of the major routes for supply of new talent into the cyber security industry.

Higher Education:

Queen's University Belfast offers an MSc in Applied Cyber Security, alongside several opportunities for post-graduate training and post-doctoral training within CSIT. It, alongside Ulster University, and The Open University also provide a range of computing and computer science related courses, often which will contain modules in cyber security, and be in high demand among employers building teams locally. In 2020/21, there were over 1,500 graduates from Queen's University and Ulster University across all disciplines (relatively split across the two, with Queen's having a slightly higher proportion of postgraduates). This was an increase of 31% from the previous year – driven by both universities offering funded conversion places (PgCert) in software development and data science due to COVID-19, with funding provided by the Department for the Economy.

FIGURE 4:2 NUMBER OF GRADUATES IN COMPUTING COURSES IN NORTHERN IRELAND



Source: HESA, Cyber Skills in the UK Labour Market (2022)

Prior to this, the number of graduates in computing related courses in Northern Ireland has remained relatively static (c. 1,100 per annum), constrained by capacity and the 'student cap' on places within the region.

Review of Graduate Outcomes Survey data (2019/20, most recent) for students graduating in computing courses in Northern Ireland suggests that 78% of graduates enter full time employment within nine months of graduating, and a further 6% combine employment and further study. This is considerably higher than the wider UK estimate for students graduating from computing courses – at 63%. This suggests that Northern Ireland has a relatively strong pipeline (in volume) between students graduating in computing courses, and finding full time employment relatively quickly – potentially furthered by QUB and UU initiatives for one-year placements and graduate events with employers. Queen's also has the lowest percentage of graduates within the Russell Group who are unemployed (2.6%), similar to Ulster University (2.8%).

The DSIT Cyber Skills in the UK Labour Market (2022) research estimated that approximately 85% of those students that graduate in a computing related course and enter full time employment will enter an IT related role.

The data regarding cyber security professionals is more limited; however, this study estimates that across the UK:

"up to 4,000 graduates are likely to enter the broader cyber security labour market each year. This is because the SOC 2135 code is likely to significantly underestimate the volume of cyber security professionals (e.g. individuals working in cyber security related roles in programming, networks, consultancy etc)."

Exploring the Graduate Outcomes Survey data, we estimate that 4.6%[7] of these roles (rounded to 5%) at a UK level are likely to be in Northern Ireland.

This suggests that in Northern Ireland, up to 200 graduates enter the cyber security workforce each year. However, a much wider number (up to 1,000) will also enter the broader IT sector each year.

Further, this data also suggests that approximately 3% of graduates will move into full-time postgraduate or PhD level training. It is also crucial to build a sustainable pipeline of talent within academia, with the ability to work alongside industry and develop cutting-edge research.

Retraining and Reskilling:

Northern Ireland's Department for the Economy (DfE) has highlighted cyber security as a priority area for growing the region's economy in its 10x Strategy. It supports Assured Skills Academies (demand-led, pre-employment training programmes) in cyber security alongside employers such as KPMG, Deloitte, and Microsoft - with Belfast Met providing training through a bespoke cyber academy. These are intended to provide c. 12 weeks of training to help graduates from alternative disciplines enter the cyber security sector. DfE, with funding from Northern Ireland Office and the Department of Finance has also offered 7,000 free further education and training opportunities through its Skill Up Initiative. This has included hundreds of students that have taken part in PGCert (and potentially continued to MSc level) training in software, data, and cyber security modules.

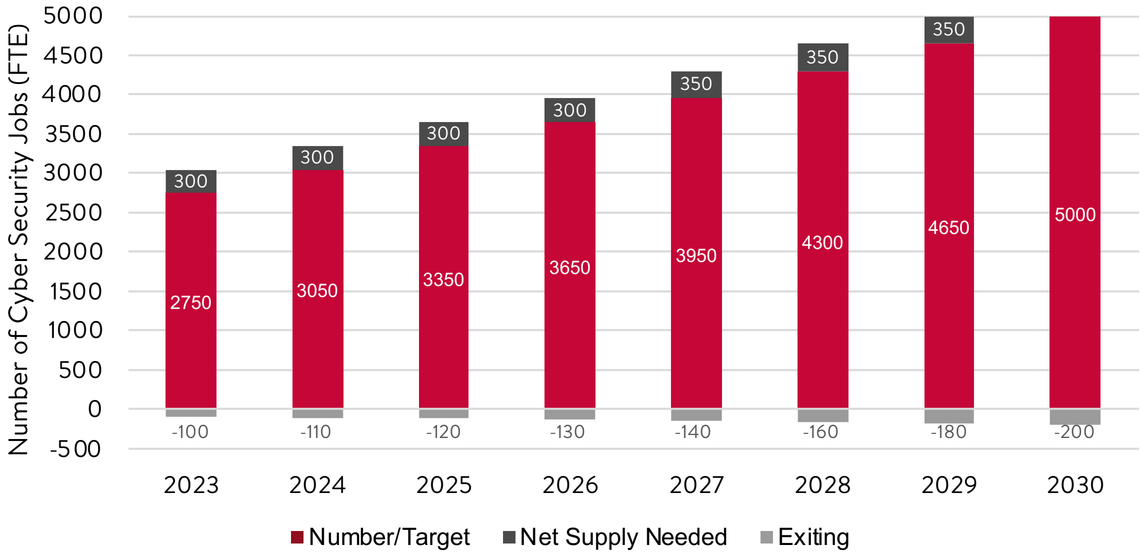
Further, there are also other routes available to support people get into the cyber security sector. This can include self-training (through online certification and training providers such as CompTIA, Hack the Box, Immersive Labs etc as well as cloud provider security certifications), retraining with an existing employer (where the employer can train and convert someone from a similar role in IT or risk into cyber security alongside training providers), publicly funded schemes such as DSIT's Upskill in Cyber programme or retraining for ex-armed forces. Apprenticeships also play a core role in supporting new talent into cyber security and broader IT roles.

[7] Based on 530 students reporting FT employment from an NI institution compared to 11,630 at a UK level = 4.6%.

We estimate, based on consultations with regional skills leads, that **approximately 100 people enter the cyber security sector each year through these routes.** However, further research should be undertaken to explore this in greater detail.

However, this relates to the gross supply of talent coming into industry. It does not account for individuals leaving roles, retiring, or exiting the workforce. The DSIT Cyber Skills in the UK Labour Market (2022) research estimates that 9% of individuals will leave their role in a given year, and that c. 4% of staff will leave the workforce entirely. This means that between 100 – 150 individuals are typically likely to leave the cyber security workforce each year in Northern Ireland, and should also be factored into workforce planning considerations.

FIGURE 4:3 NEW ENTRANTS, EXITS, AND OVERALL SUPPLY - WORKFORCE TO 2030



Overall, we estimate that there are approximately 300 new entrants into the cyber security sector each year. The current higher education system, and use of retraining and reskilling initiatives broadly meets the needs of industry; however, as the sector grows and as more people retire or exit the workforce, there is a need for sustainable supply.

Initiatives such as Assured Skills Academies and support for postgraduate study have helped meet much industry demand to date e.g. the Microsoft Cloud Academy, and KPMG Cyber Security Academy. However, we recommend that Northern Ireland should explore how to train additional talent in cyber security – potentially through additional support for HE to create further places (particularly at postgraduate level), sustained support for Assured Skills Academies and apprenticeship models, and continued liaison with leads in NCSC and DSIT on cyber skills policy.

Northern Ireland has increased its skills supply in cyber security significantly over the last two years (since the 2021 baseline report). It should continue these efforts to help meet the 5,000 jobs target by 2030. There is absorptive capacity and demand to **train an additional 100 – 150 people per annum to support industry demand.**

05

Driving Innovation & Growth

5.1. INWARD INVESTMENT INTO NORTHERN IRELAND

Northern Ireland is frequently cited as a leading location for inward investment whereby leading cyber security companies establish operational and R&D offices. Northern Ireland is the leading international investment location for US cyber security firms, and firms Proofpoint, IBM Security, Rapid7, Imperva, Anomali, Contrast Security and SilverSky all have operations in the region. It is also home to a number of international financial services companies such as Allstate, Aflac and CME, that have located their Cyber Security Operation Centres in Belfast (Invest NI).

Northern Ireland is frequently cited as a leading location for inward investment whereby leading cyber security companies establish operational and R&D offices. Northern Ireland is the leading international investment location for US cyber security firms, and firms Proofpoint, IBM Security, Rapid7, Imperva, Anomali, Contrast Security and SilverSky all have operations in the region. It is also home to a number of international financial services companies such as Allstate, Aflac and CME, that have located their Cyber Security Operation Centres in Belfast (Invest NI).

Using the FDI Markets / FT Intelligence platform, we explore this data further below. We find that inward investment has been a catalyst in shaping Northern Ireland's cyber security sector, driving significant employment growth particularly over the last five years.

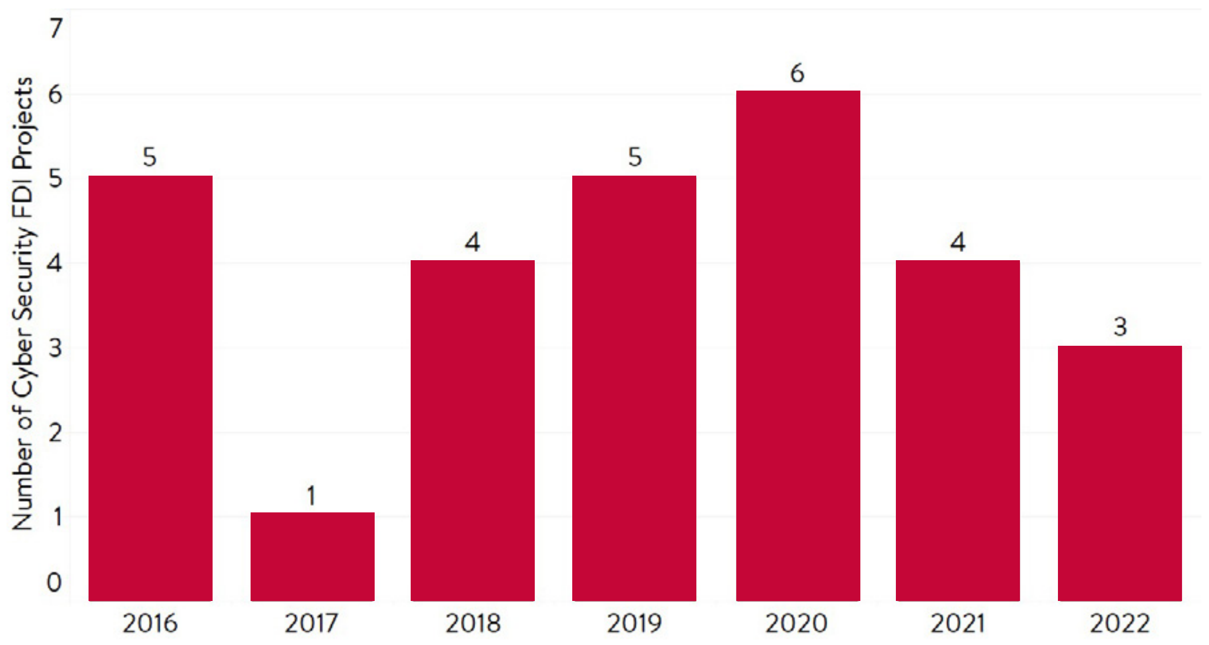
Northern Ireland remains an attractive location for inward investment, and this will be reflected in the upcoming Northern Ireland Investment Summit announced by the UK Government following US President Biden's visit to Belfast in which the role of US FDI in tech and cyber security was mentioned as transformational for the region's economy.

However, sustaining inward investment requires several factors to maintain competitiveness -including access to affordable and high-quality talent, availability of office space and facilities, and attractive fiscal and commercial benefits from undertaking the investment. Further, inward investment can support growth within the wider ecosystem, but it is crucial to ensure that there is sufficient current and upcoming talent supply to meet these investments, whilst also building a pipeline of local and indigenous start-ups and scale-ups.

5.1.1. NUMBER OF INWARD INVESTMENT PROJECTS

Using the FDI Markets platform, there have been 28 inward investment projects (from 23 unique companies) into Northern Ireland that have included a cyber security focus since 2016.

FIGURE 5.1 NUMBER OF INWARD INVESTMENT PROJECTS INTO NI IN CYBER SECURITY SINCE 2016



Source: FDI Markets

These projects have also collectively announced over 1,800 new cyber security (and wider digital) jobs in Northern Ireland since 2016 – an average of 250 new jobs each year.

Some of the major recent investments have included pure-play cyber security companies such as Rapid7 (2016), Anomali (2017), Imperva (2018), Nihon Cyber Defence (2018), Contrast Security (2019), Proofpoint (2019), Cygilant (2020), large IT firms such as Microsoft (2020), consultancies, and financial services firms such as Aflac.

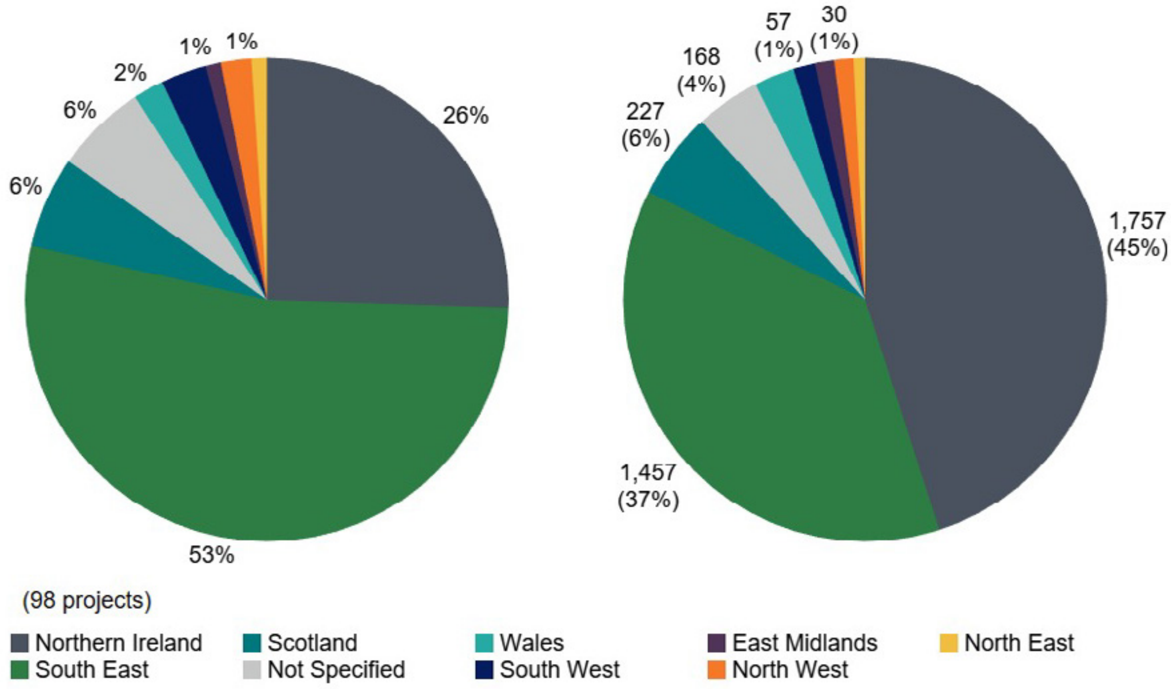
The data also highlights how Northern Ireland has placed a strong emphasis on securing US based FDI. Of the 28 inward investment projects, 25 are from US based companies.

Indeed, as the figure below demonstrates, Northern Ireland has secured 26% of UK inward investment projects in cyber security from the United States.

Whilst the majority have located in London and the South East (53%) –we note that Northern Ireland has secured 26% of projects despite being home to c. 3% of the UK's population reflecting the significance of investment activity. Since 2016, there have been more cyber security FDI projects in Northern Ireland than the combined volume of all other UK regions outside of London and the South East.

Further, the FDI Markets data suggests that these US FDI projects have supported (or are expected to support) over 1,750 roles in Northern Ireland. This is the highest in the UK, reflecting 45% of new roles created in cyber security in the UK by US FDI among announced greenfield investments.

FIGURE 5.2 PROPORTION OF INVESTMENT AND JOB CREATION (ANNOUNCED) IN EACH UK REGION



5.1.2. KEY CONSIDERATIONS ON INWARD INVESTMENT

Northern Ireland has performed strongly, particularly since 2016, in attracting inward cyber security investment. It is a leading region in Western Europe for securing new projects. However, since 2021, the volume of projects has softened slightly – and wider macroeconomic conditions may impact this in future, particularly as larger tech platforms cut workforce sizes and seek operational efficiencies. Further, Northern Ireland policymakers should consider the potential impact of increasing public investment in technology being made by countries such as Ireland (e.g. the recent AMD investment in Cork backed by IDA Ireland), Germany (with its High Tech Strategy 2025 seeking to invest 3.5% of GDP in R&D, and providing support for digitalised chip plans, and quantum computing), and in the United States itself (with the Department of Commerce announcing a Regional Technology and Innovation Hubs (Tech Hubs) programme for creating tech jobs across the country.

As such, there is an increasing need for strategic planning and investment in cyber security in Northern Ireland to maintain competitiveness – and this must cover strands such as capital investment, access to talent and equipment, and the wider health of the NI ecosystem, including access to wider funding and support for innovation.

However, Northern Ireland is and remains an attractive destination for inward investment. This is reflected by Belfast hosting CyberUK in April 2023, which could help to encourage further investment. Additionally, it is reflected in the investment motives cited across several jobs announcements in Northern Ireland – e.g.:

"The financial support from Invest Northern Ireland, high quality of talent, infrastructure and academic expertise, and the positive experiences of other companies convinced us this was the right location for a strategic investment,"

David Costar, SVP, Wolfspeed

"We are confident that a Northern Ireland base will continue to add excellent talent to our service organisation. Invest NI has been extremely helpful and has given us key insights to the ICT sector, provided introductions to key stakeholders and information on the skills on offer. By tapping into this talent, we will add to our world-class technology team. The Northern Ireland team is central to our growth plans and will enable us to deliver 24/7 'Follow the Sun' support to our global customer base. It will also support the development of our products and services for our planned European expansion,"

Garvin McKee, Chief Revenue Officer, Agio.

"When we decided to expand into the European market, we quickly realised there was no better place than Belfast. The city is full of great people who have an unbelievable work ethic truly matching and embodying the customer service first culture we have here at Cygilant. Belfast is also the sister city to Boston and is easily accessible within EMEA and from our home in Boston...The city is also quickly becoming an innovation hub for technology companies including a growing cyber-security sector, so all the pieces just fit nicely together."

Rob Scott, CEO, Cygilant

"One of the things we've said before that we love about Belfast is that it's resilient, reinventive and adaptable, and we're proving that right now by doing things the way we are."

Keith Farley, Aflac

5.2. VENTURE CAPITAL AND ANGEL INVESTMENT

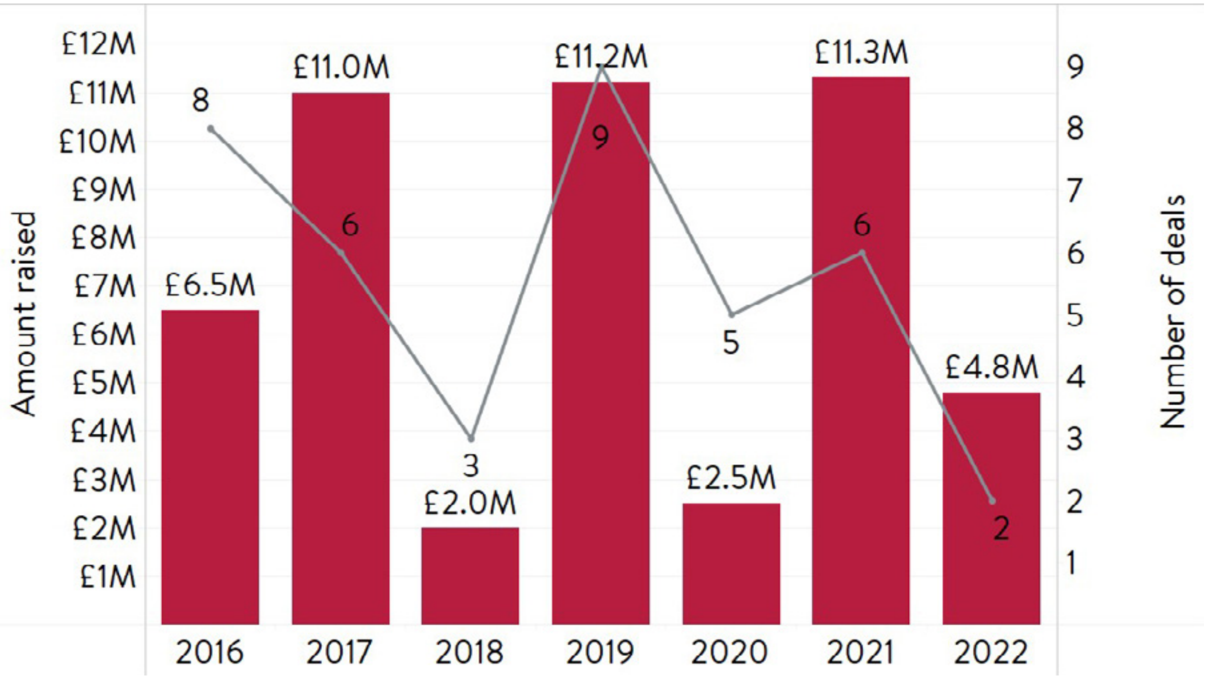
This section explores investment secured by cyber security companies (based in Northern Ireland) through venture capital and angel investment. This can provide useful insight into the local sector for several reasons, including reviewing the extent of investment within the ecosystem, investor interest and capital, and the propensity for firms to use external investment as a route to grow and scale their business.

The UK Cyber Security Sectoral Analysis sets out that £302 million was raised across 76 deals within dedicated cyber security firms in 2022. This is significantly lower than levels in 2020 and 2021, and securing investment can be challenging for early-stage firms. In this study, it is estimated that approximately 1 in every 5 cyber security firms has received some form of external investment or fundraising at some point in its operation. Using the full list of cyber security firms in Northern Ireland, we re-run this analysis for the region since 2016.

5.2.1. INVESTMENT RAISED

We find that 11 NI domiciled cyber security businesses have raised investment since 2016. Collectively, we identify approximately £49m in investment raised, and since 2016, key firms have included B-Secur (£19m raised), Skurio (c. £9m), AuditComply (>£5m), Titan IC (£4m prior to sale to Mellanox then Nvidia) and Angoka (over £3m raised). However, the value of VC investment in cyber security is typically 1-2% of that raised across the UK each year, highlighting regional imbalance in investment raising.

FIGURE 5.3 VC INVESTMENT RAISED



Source: Beauhurst

5.2.2. FUNDING LANDSCAPE

Review of investment data highlights that top funders in Northern Ireland by number of fundraisings include Co-Fund NI (managed by Clarendon Fund Managers), Accelerated Digital Ventures, Kernel Capital, Qubis (Queen's University), Techstart Ventures and YFM Equity Partners. With regard to volume of funding, a similar breakdown is noted.

However, this highlights a potential lack of investment in Northern Ireland by some of the UK (or global) funds – likely driven by the size and scale of firms moving from seed to venture stage. Further, many of the investments typically contain multiple partners – suggesting more limited capital to invest among NI funds compared to other regions.

Sustained engagement with centralised funds such as those provided by the British Business Bank, as well as the use of schemes such as Co-Fund, and initiatives to connect NI firms to the rest of the UK or Ireland (e.g. Cyber Runway) may help to unlock further private investment.

5.3. PARTNERSHIPS AND COLLABORATION

The Centre for Secure Information Technologies (CSIT) at Queen's University Belfast is a global research and innovation hub for cyber security, and the UK's Innovation and Knowledge Centre (IKC) for cyber security research. As such, it places a strong emphasis on industry and global academic engagement to build partnerships, and develop new technologies that are embedded in everyday products and solutions. In CSIT Phase 3 (until 2027), CSIT will build hubs of impact with industry partners, modelled on the 'Cyber-AI Technologies Hub' in which CSIT will partner with eight cyber security technology companies to collaborate on the development of new solutions to shared challenges.

There are three strong mechanisms for partnership and collaboration in the Northern Ireland cyber security ecosystem, that we explore below.

5.3.1. THE ROLE OF CSIT

CSIT plays a key role in industry, academic and government engagement for the NI cyber security ecosystem. This includes:

- **Direct industrial collaboration through research and engineering support:** CSIT has provided high quality engineering support to a range of local and multinational companies to test new products, grow and scale. The engineering team has worked with firms such as Liopa and Titan IC, helping create successful academic start-ups. It has also worked with established firms such as Direct Line and Citi. The upcoming Cyber-AI Hub project will also work with leading industry partners (who will provide £4.6m in private funding) for novel AI cyber security solutions to be embedded within their firms.

- **Engagement with NI, UK, and global policy-makers:** CSIT also engages very closely with policy-makers at all levels. Locally, it supports the Department for the Economy and Invest NI in shaping the cyber security proposition, and led on the NI Strategic Framework for Action in Cyber Security, and the NI Cyber Leadership Board. At the UK level, it has a strong relationship with UK departments, working closely with the Department for Science, Innovation and Technology on a range of cyber security research projects and policy design.

- **Building collaboration at a global level:** Globally, CSIT is a founding member of the Global EPIC (Global Ecosystems Partnership in Innovation and Cybersecurity) network, which brings together over 30 cyber security hubs. Further, CSIT has a strong relationship with industry and academia across the United States (e.g. Boston College, UC Berkeley), Germany, Ireland, Israel, and South Korea. Recently, CSIT has been involved in a US-NI-Ireland alliance[8] of cyber security research.

[8] https://www.rit.edu/news/rit-researcher-brings-together-cybersecurity-experts-us-ireland-and-northern-ireland

- **Developing the infrastructure to support R&D:** The growth of CSIT has also ensured that the wider industry can have access to the physical and technical infrastructure that is beneficial to growth. In addition to providing physical space for teams, CSIT has a state of the art Cyber Range to support Red Team and Blue Team activity, as well as ECIT's wider Edge Computing Hub and anechoic chambers.

- **Developing the skills pipeline:** CSIT plays a key role in skills supply, as set out in the previous chapter.

- **Supporting the acceleration of cyber start-ups and spin-outs:** CSIT is also a key partner to Cyber Runway, the UK's largest cyber security accelerator scheme which will support the growth of 160 entrepreneurs, start-ups and SMEs. CSIT provides technical and commercial advice to newly established firms, and has also supported NI start-ups benefit from the support available from DSIT and Plexal.

- **Unlocking wider funding opportunities for cyber security firms:** CSIT has also built several routes for enabling local firms to take part in international or wider research funding initiatives, including Horizon2020 and PEACE PLUS. It will also play a substantive role in the Belfast Region City Deal with £58m allocated by the UK Government towards the creation of a Global Innovation Institute at ECIT by 2026.

5.3.2. THE ROLE OF NI CYBER

The Northern Ireland Cyber Security Cluster (NI Cyber) consists of several leading companies in the region that are developing cyber security solutions. Its role is to act as a leader and facilitator for the sector, to allow companies to collaborate and compete globally. It is recognised as an established cluster by the UK Cyber Cluster Collaboration (UKC3) body.

As the region's cyber security cluster, NI Cyber promotes collaboration for business, innovation, skills development and peer-to-peer learning at every level, and represents the sector regionally, nationally and internationally. Members represent the diversity of the sector including innovative start-ups, SMEs and multinational corporations delivering products and services globally, academic research, education and skills partners; and government.

5.3.3. INDUSTRY COLLABORATION

The NI cyber security sector also undertakes significant collaboration and outreach activity as part of its ambition to give back and sustainably grow the pipeline. This includes active collaborations with the DfE Assured Skills Academies and Belfast Met - (demand-led, pre-employment training programmes) in cyber security alongside employers such as KPMG, Deloitte, and Microsoft - with Belfast Met providing training through a bespoke cyber academy. It also includes active engagement with schemes such as the NCSC CyberFirst Schools and Colleges Programme which inspires and encourages young people to develop their skills and explore opportunities in cyber. This initiative is frequently supported by companies such as Allstate, Cybit, and Vertical Structure.

06

Growth Ambitions

6.1. INTRODUCTION

As set out throughout this report, Northern Ireland has become a global cyber security hub, with academic expertise alongside high levels of inward investment and a burgeoning cluster of cyber start-ups. Despite wider macroeconomic conditions, demand for cyber security products and solutions is expected to grow between 8 – 12% per annum until 2030, and wider cyber security workforce gaps remain persistent globally. Northern Ireland is therefore in an opportune position to continue to attract inward investment, grow and scale its start-ups, and build research and academic teams central to cyber security and AI research.

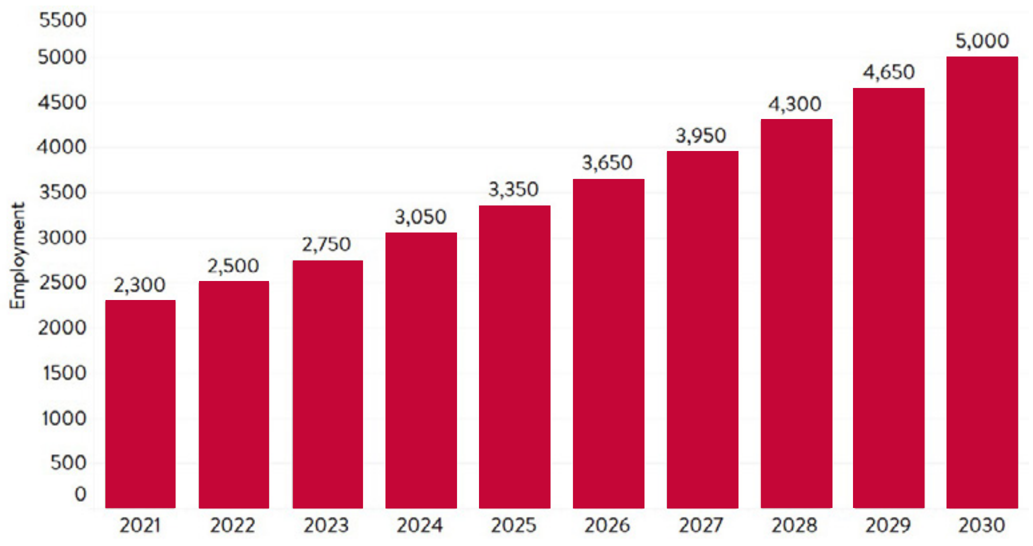
The legacy of CyberUK being held in Belfast in 2023 will enable Northern Ireland to secure further investment, and deepen existing partnerships across public and private sectors. Further, the recent UK Government investment in the Cyber-AI Hub project at CSIT will enable the region to recognise the value of AI in responding to cyber threats, and building novel and powerful solutions to mitigate against harm.

We set out growth ambitions to 2030 for Northern Ireland (based upon reaching the 5,000 jobs figure). We also set out the potential economic contribution of the sector to the Northern Ireland economy over this period.

6.2. TARGETS TO 2030

There is considerable opportunity in growing Northern Ireland's cyber security sector. The New Decade, New Approach agreement backed by the UK Government formalised the ambition to grow the sector to 5,000 FTE jobs by 2030. This means creating an additional 300 – 350 jobs each year within the sector to 2030.

FIGURE 6.1 CYBER SECURITY EMPLOYMENT TARGET – SCENARIO TO 2030



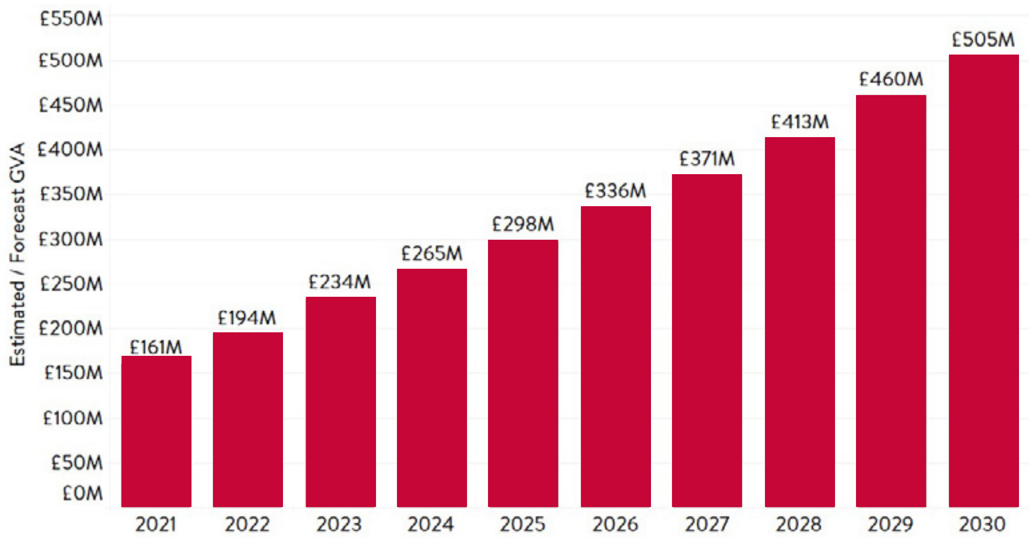
Source: Perspective Economics estimates

Where these targets can be achieved, we anticipate the following direct GVA to be generated within the local economy. This assumes that GVA per employee is currently c. £85,000 per annum, and is assumed to grow at c. 2.5% per annum to 2030 (reaching £101,000 per employee per annum by 2030).

Over the decade (2021-2030), we expect that the Northern Ireland cyber security sector could contribute up to £3.2bn in cumulative GVA.

As set out in the baseline report, this illustrates both the need to promote entry into cyber security roles and ensure sustainable employment growth to meet the targets, and the direct value in supporting the growth of the sector through co-investment and partnership.

FIGURE 6.2 CYBER SECURITY GVA TARGET – SCENARIO TO 2030



Source: Perspective Economics estimates

07

Findings and Recommendations

7.1. KEY FINDINGS

Number of Companies:

- There are 124 companies with commercial or R&D-driven cyber security teams in Northern Ireland.
- We estimate that 46 of these are 'dedicated 'or 'pure-play, where all of the firm's activity is cyber security related. 78 of these are 'diversified', where we have identified a cyber security team undertaking commercial or R&D activity, but the wider business may offer broader services such as professional services, aerospace and defence, or finance.
- This research highlights particular strengths in Northern Ireland in risk, compliance and fraud, identification, authentication and access control, and OT security.
- Belfast is one of the world's most concentrated cyber security clusters, with more than 100 cyber security businesses and teams.
- Northern Ireland is an attractive location for both inward investors, and indigenous start-ups, spin-outs and scale-ups. 66% of firms are headquartered overseas.
- Northern Ireland is not only the number one global destination for US FDI, but over 1,700 cyber security jobs in NI are backed by US FDI. NI also attracts inward investment from Canada, Europe, Japan, Israel, and the wider UK and Ireland.
- Northern Ireland has secured 26% of UK inward investment projects in cyber security from the United States since 2016, Further, these projects have supported (or are expected to support) over 1,750 roles in Northern Ireland. This is the highest in the UK, reflecting 45% of new roles created in cyber security in the UK by US FDI.

Economic Contribution:

- These firms employ an estimated 2,750 FTEs in cyber security (in 2023).
- The average cyber security salary advertised in NI in 2022 was £53,800.
- We estimate direct Gross Value Added (GVA) generated by the NI cyber security sector is approximately £236m. This is a 47% increase in GVA since the 2021 baseline study (£161m).
- The sector has a target employment figure of 5,000 jobs by 2030, which we view is on track. We estimate that if the cyber sector achieves the targeted number of employees, the sector will have an estimated GVA of £505m per annum by 2030.
- Over the decade (2021-2030), we expect that the Northern Ireland cyber security sector could contribute up to £3.2bn in cumulative GVA.

Skills:

- Overall, we estimate that there are approximately 300 new entrants into the cyber security sector each year (200 through HE and 100 through retraining, apprenticeships and conversion initiatives). The current higher education system, and use of retraining and reskilling initiatives broadly meets the needs of industry; however, as the sector grows and as more people retire or exit the workforce, there is a need for sustainable supply.
- Northern Ireland has increased its skills supply in cyber security significantly over the last two years (since the 2021 baseline report). It should continue these efforts to help meet the 5,000 jobs target by 2030. There is absorptive capacity and demand to train an additional 100 – 150 people per annum to support industry demand.
- Demand for cyber security professionals has more than doubled in Northern Ireland within the last three years. In 2022, there were almost 1,100 unique job postings (Lightcast, 2023) in demand for cyber security professionals, from over 200 different employers and recruitment agencies.

7.2. RECOMMENDATIONS AND SUGGESTED ACTIONS

Within the 2021 baseline report, there were six core actions suggested to support the growth of the sector. We review the progress of each of these below.

Baseline Recommendation	Score	Positives	Considerations
Support the development of a sustainable pipeline of talent, including the education and entry of talented high value cyber security professionals, as well as opportunities for career retraining and apprenticeships for those employed in sectors with similar skill sets.	4/5	Northern Ireland has increased its skills supply in cyber security significantly over the last two years. It has made progress with respect to: • Rollout of industry approved Assured Skills Academies through the Department for the Economy, working with regional cyber security employers to retrain people into early-stage cyber security careers. • Increased provision and investment in postgraduate courses e.g. hundreds of funded places for people seeking to retrain or learn new skills in software development, data analytics, and cyber security. This has significantly increased supply of PgCert provision across the NI workforce. • Queen's University Belfast (CSIT) now holds Academic Centre of Excellence in Cyber Security Education (ACE-CSE) through the NCSC. This means that cyber security as a discipline is taught and embedded across non-computer science pathways, opening up the potential of cyber security as a career pathway.	Whilst significant improvements in the skills landscape are noted, Northern Ireland policy should consider: • The need to track career pathways and longer-term outcomes. Initiatives such as Assured Skills academies are welcome; however, whilst they track the number of interviews and placed candidates, they should also consider tracking pre-placement data (e.g. previous status, salary), salaries over time, and progression from entry to mid-level roles to help understand the longer-term return on investment. • The higher education system is effectively capped by the Maximum Aggregate Student Number (MASN) formula. This means that, without reform, the volume of students graduating in computer science, and or entering cyber security roles is likely to 'bottleneck' at c. 200 places per annum. The demand for PgCert places through Skill Up etc highlights that reform should be considered urgently to enable Northern Ireland to undertake workforce planning beyond the 2030s. • Northern Ireland should also consider its offer with respect to attracting and retaining talent in the region.
Increase the strength of relationship between academia and private sector, e.g., support the development of joint research projects, research projects with a commercial application, as well as supporting the development of academic spinouts.	4/5	There have been several announcements and initiatives intended to boost collaboration between academic and the private sector in cyber security over the last two years. This includes: • The £18.9m announcement for the Cyber-AI Hub includes eight collaboration R&D projects with industry with private match-funding. • CSIT is part of a shared US-NI-Ireland research network in cyber security. • CSIT hosted the UK Research Institute in Secure Hardware and Embedded Systems (RISE) in 2022, with speakers from Intel, NVIDIA, Arm, and Angoka. • CSIT provides lead engineering and business growth support to the DSIT funded 'Cyber Runway' cyber security accelerator programme. • There has also been ongoing activity with respect to acquisitions, mergers, and growth among several of QUB's academic spin-outs e.g. Titan IC acquired by Mellanox, later NVIDIA.	There are opportunities to embed commercialisation through other mechanisms than academic spin-outs. This might include: • Sustained investment or support for collaborative events and activities between academia and private sector. • Opportunities for short / part-time secondments and visiting lecturer roles. • Increasing start-up activity across the NI cyber security ecosystem, through early entrepreneur events, network building etc.
Promote knowledge sharing in Northern Ireland's cyber security ecosystem, embedding academic staff in industry, and creating channels to allow industry to inform the curriculum of local institutes to meet industry needs.	3/5	Knowledge sharing is key to the growth of the regional ecosystem. There are already several examples of good practice: • The NI Cyber cluster has grown in recent years. It has sustained engagement with local stakeholders, as well as NCSC, CyberFirst, DSIT and UKC3. This has meant that NI Cyber has been well placed to deliver events alongside CyberUK etc. • The Cyber-AI Hub will include the opportunity for industry to sit / embed within the Hub, enabling collaboration between academia and industry on projects. • The position of CSIT means that is already has effective co-location with cyber security businesses within the Titanic Quarter.	Areas for further consideration include: • A need to balance skills requirements across private and public sectors, and academia (e.g. ensuring attractiveness at all levels to prevent skills mis-match). A commonly cited challenge is that high quality staff or researchers can be offered roles by other parts of the ecosystem, which can impact on R&D and projects. • Skills initiatives should be tailored to current industry needs; however, there is a need for forecasting and future planning to ensure that 'bleeding-edge' skills are always in development to inform the next wave of commercial products.

Baseline Recommendation	Score	Positives	Considerations
Support the development and fostering of partnerships with sister cities, that is, relationship building between NI cities and other global cyber hotspots. An example of this includes the growing connection between Belfast and Boston as a result of Rapid7's presence in Northern Ireland.	4/5	Northern Ireland's cyber security ecosystem has come to global attention throughout 2023. This includes: • Belfast hosted NCSC's CyberUK conference in 2023, bringing over 1,000 global delegates to Belfast. • Strengthened relationship with the United States, with US President Biden supporting increased investment to the region (cyber security) and the appointment of US Special Envoy to Northern Ireland for Economic Affairs promoting tech investment. • UK Government backed Northern Ireland Investment Summit to be held in Autumn 2023, with potential cyber security and technology investors. CSIT are leading engagement with departments such as the Department for Business and Trade (DBT) and Department for the Economy (DfE)	This is an area that Northern Ireland performs well in. However, there may be both potential to widen investment outreach beyond United States – e.g. with Israel, Canada, and Middle East, as well as undertake further engagement with Northern Irish diaspora working in tech firms globally.
Foster AI and ML-related training and technology, supporting the diversification and future-proofing of skillsets in the sector, in turn increasing the resilience of the sector in the region which supports firms in meeting future cyber security needs.	4/5	CSIT has placed a focus on AI and ML in cyber security through: • The UK Government announced £18.9m investment in CSIT's Cyber-AI Hub, to provide 15 PhD places, and 40 MSc bursaries in cyber security, AI and data analytics. • NI has benefitted from inward investment and acquisition activity from AI leaders such as Nvidia, Microsoft, and Oosto– positioning Northern Ireland as a cyber-AI leader.	There is further potential to embed AI and ML across the wider cyber security ecosystem, and wider economy. Further, the recent push for AI related growth among the wider tech ecosystem highlights a sustained need for co-investment in new sites, equipment, and projects to ensure global competitiveness.
Promote NI as the location for commercial R&D in cyber security. NI is home to a strong R&D-focused ecosystem, offering fewer advisory services than the rest of the UK, and more product development services. CSIT should engage partners in the UK, publicising existing R&D activity in NI, and promoting engagement in the region for development needs	3/5	As set out, there are eight businesses that will undertake commercial R&D projects with CSIT through Cyber-AI Hub project. This places Northern Ireland in a good position for being the location for commercial R&D.	Globally, there is a more challenging environment for firms (and governments) seeking to increase R&D expenditure given wider macroeconomic pressures and interest rates. This also may have a negative impact on embedding secure digitalisation in other sectors such as manufacturing and finance. It may be worth Northern Ireland exploring how it can track and establish regional targets for business expenditure on R&D (within cyber security) in any upcoming strategy,

Further Recommendations:

In addition to the recommendations set out within the 2021 baseline, we provide further recommendations for consideration by policy-makers.

- **Update the NI Strategic Framework for Action in Cyber Security to 2030:** There is a need to update this strategy to ensure policy direction and co-investment with industry, academic and the public sector.

  This should include:

  - **Workforce and Skills Planning:** a clear route towards funding, tracking, and supporting skills supply to 2030.
  - **Public Sector Cyber Security Strategy (NI):** the development of a public-sector cyber security strategy as a standalone resource, similar to the Government Cyber Security Strategy by UK Government. This would provide clear direction for securing public infrastructure, as well as alignment to support for industry and wider society.
  - **Technology Foresight exercise:** Northern Ireland should consider the current strengths of the ecosystem, and consider how technology future scenarios might apply or impact the sector.
  - **Adjacency to 10x Strategy and Programme for Government:** Any strategy should be aligned with wider government policies to maximise resources available.
  - **Widening 'cyber' to all citizens:** a strategy should also account for cyber security at all levels of society, including support for vulnerable individuals, SMEs, voluntary sector organisation, and the wider role of NI Cyber Security Centre.

- **Reconvene the NI Cyber Leadership Board, including industry and civic engagement.** This should include an updated Terms of Reference with a whole of society focus on cyber security, R&D, innovation and impact.
- **Create a NI cyber security envoy role, similar to Fintech.** This should enable national and international engagement with industry and investors. This role should be backed by UK Government.
- **Explore and research the long-term ambitions of cyber security businesses to enable strategic planning for investment** in office accommodation, R&D projects, skills initiatives, and cyber security infrastructure. This should also review the funding available (private and public) and how further investment could be secured. This should also consider where stakeholders may have initiatives that could be supported to boost skills or infrastructure.
- **Increase outreach and engagement to sustain interest in the NI cyber security ecosystem.** This should include funded support for trade missions, international visits, attendances at trade events, events for VCs and inward investors.
- **Sustained investment in skills provision**, including funding for one-year conversion courses, Assured Skills Academies (including multi-party SME programmes where there is demand), and apprenticeships to maintain supply. There should be an increased focus on tracking outcomes over time (how candidates perform over several years) to understand impact.

.

QUEEN'S UNIVERSITY BELFAST
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES
Perspective Economics

SECURING COMPLEX SYSTEMS

Centre for Secure Information Technologies (CSIT)
ECIT Institute
Belfast
BT3 9DT
Telephone: 028 9097 1700
Website: http://go.qub.ac.uk/csit
Twitter: @CSIT_QUB