

# CYBER SECURITY

A Strategic Framework  
for Action **2017-2021**



**Northern Ireland will be one of the world's leading cyber economies, delivering a thriving knowledge economy, due to exemplary talent; pioneering research and innovation; and the secure and resilient infrastructures needed to support businesses and safeguard the public.**

# CYBER SECURITY

A Strategic Framework for Action 2017-2021



## CONTENTS

Foreword	2
Executive Summary	4
Introduction	6
Strategic Context	8
Approach	12
Theme 1 – Defend	20
Theme 2 – Deter	26
Theme 3 – Develop	30
Conclusions	34
Summary of Outcomes/Indicators/Activities	36



# FOREWORD

The world is connected in a way never before imaginable.

There are more mobile devices in use across the globe than there are people. The media estimate the world is now home to more than 7.5 billion gadgets. They are multiplying five times faster than we are. Many businesses are entirely dependent upon the digital economy for survival: indeed, locally the Northern Ireland Executive drives a Digital First agenda. Such is the dependence and reliance upon ICT that we need to aggressively safeguard its operation and integrity.

For all organisations, data is a key asset. This Framework aims to support the protection of those assets through the development of new digital solutions which have security in-built as part of their DNA. Developing a culture of ongoing training, awareness and being alert to potential threats are all vital aspects to maintaining resilience, particularly as cyber threats escalate and are becoming even more complex.

The Framework aims to create more opportunities to develop cyber talent within the public and private sectors. The digital environment has made cyber and ICT careers more accessible: the Framework will focus efforts in ensuring the education pipeline is well aware of the needs of business and the opportunities which digital skills have to offer in relation to employment.

The Framework will guide the exploitation of new technologies and data communications whilst ensuring that responsible levels of security and good governance are enabled. A Cyber Leadership Board will have strategic oversight over cyber planning and skills development in a coordinated way.

Enabling an international cyber centre of excellence is a very ambitious aim – but one that can be achieved through collaborative working across public and private sectors and liaising closely with academia.

# CYBER SECURITY

A Strategic Framework for Action 2017-2021



I am very pleased to present this Framework for Action and look forward to seeing a local evolution into a world-wide centre of cyber excellence.

**HUGH WIDDIS**  
**Permanent Secretary**  
**Department of Finance**

**October 2017**



# EXECUTIVE SUMMARY

Being connected is now becoming the ‘norm’ in society, creating new opportunities for innovation and growth for all. To be competitive, businesses need to be online, but this also brings risks. To access public services the public are encouraged to go online. To minimise the impact of attacks a robust law enforcement regime is needed, to deter criminality.

Cyber attacks are increasingly being reported in the media. Large scale attacks which disrupt services, other attacks which impact directly on a business or organisation are now seen regularly. The sad truth is however, that these are only the tip of the iceberg and many attacks are going unreported. This demonstrates the potential scale of the threat we all have to address. All of us—governments, businesses and individuals—need to work together to build resilience to cyber security threats and to make the most of opportunities online.

To grow, Northern Ireland needs to innovate and further diversify its economy—to access new markets and new forms of wealth creation. We must embrace disruptive technologies; those that have the potential to fundamentally change traditional business

models and the way people live and work. They will open up new possibilities for agile businesses in ways as yet unimagined.

The potential of digital technologies depends on the extent to which we can trust the Internet and cyberspace. Getting cyber security right will mean we capture more of the opportunities the connected world offers. It will also make Northern Ireland a preferred place to do business. This in turn will boost our prosperity. We can also expand our cyber security businesses and export capability.

If an organisation is connected to the Internet, it is vulnerable to compromise. As people and systems become ever more interconnected, the quantity and value of information held online has increased. Equally efforts to steal and exploit that

# CYBER SECURITY

A Strategic Framework for Action 2017-2021



information, harming our economy, privacy and safety. Cyberspace, and the dynamic opportunities it offers, is under persistent threat.

Malicious cyber activity is a security challenge for everyone. Organisations across the public and private sectors have been compromised by state-sponsored or non state actors. Overseas, large multinational companies and government organisations have been targeted, losing substantial amounts of sensitive commercial and personal information or incurring major damage to their business and reputation.

To grow our cyber security capabilities to anticipate and respond to cyber threats, we must address our shortage of cyber security professionals. It is critical that we build our stock of cyber security skills, which are becoming increasingly essential for life and work in our connected world.

This Strategic Framework for Action aligns to the UK National Cyber Security Strategy and adopted the key themes of **Leadership, Defend, Deter** and **Develop**.

Ultimately, to deal with all these challenges we must elevate cyber security as an issue of significant importance. Leadership will be critical to achieving this goal.

The Northern Ireland Executive will take a lead role and in partnership with others, promote action to protect our online security.

Much of our digital infrastructure is delivered by the private sector, so securing our cyberspace must also be a shared responsibility. It will be important that businesses and the research community work with governments and other stakeholders to improve our cyber defences and create solutions to shared problems.

Under the themes of Defend, Deter and Develop lies a comprehensive body of work and actions for public, private and academia to engage on and this work will develop through implementation of this Strategic Framework for Action.

Our skills and talent need to be enhanced; we want to capitalise on opportunities to secure investment and growth in our cyber sector and research; more effective law enforcement is needed to deter future threats and criminal activity; and we must build trust in public services. This Strategic Framework for Action sets the blueprint for building on what has been achieved to date.

The timing of threats doesn't wait, criminal activity doesn't wait for a convenient time – we therefore cannot wait to protect our public, businesses and services.



# INTRODUCTION

Northern Ireland will be one of the world's leading cyber economies, delivering a thriving knowledge economy, due to exemplary talent; pioneering research and innovation; and the secure and resilient infrastructures needed to support businesses and safeguard the public.

The purpose of this Strategic Framework for Action is to set out the key areas of ambition to ensure that Northern Ireland (NI) is best placed to tackle head on the demands and needs of cyber security for the public, businesses and public services.

**We have a real opportunity to cement NI's position globally as a leading cyber region, with the potential of creating upwards of 5000 high value knowledge jobs by 2026 and creating a safe and secure environment for all.**

This Strategic Framework for Action puts forward a leadership approach to ensure we are equipped to deter potential attacks both for individuals and all organisations; build trust in the safety and online integrity of public services and invest in the development of the NI cyber security industry to support growth and competitive advantage for the local economy.

With the move to 'mainstream' online services, processes and activities into the life of business and society, there is the increased risk of criminal activity to exploit the public and all organisations, whether private or public sector. The threats can come from internationally organised criminal organisations, opportunistic individuals, with various motivations, including political, financial and specific activist issues, and are well documented and reported. Recent years have seen an exponential growth in cyber crime and cyber attacks against individuals, businesses and UK interests.

Citizens, businesses and government all have responsibilities to protect their online activities, services, systems, data and networks from criminal attack. Furthermore, the Executive has a commitment to deliver trusted and secure public services – whether this is



# CYBER SECURITY

A Strategic Framework for Action 2017-2021



managing patient records in the health service, through to providing online services such as Access NI Enhanced Check.

By 2020, businesses will spend £83 billion on cyber security<sup>1</sup>, which equates to a 38% increase from the £60 billion in 2016, which is a compound annual growth rate of 8.3% (more than twice the rate of spending in IT overall). Global cyber security unemployment rate is at zero and there are currently 1 million unfilled cyber security jobs. This figure is predicted to rise to 1.5 million by 2019<sup>2</sup>.

Northern Ireland has a growing reputation as a region of expertise and knowledge in cyber security – not only within the UK, but internationally. It is a business sector which is expected to grow exponentially and with the right physical and digital infrastructures in place, world class research and the right talent pool available, we can capitalise on international opportunities to create a world class cyber security eco-system. The Centre for Secure Information Technologies (CSIT) is the UK's National Innovation and Knowledge Centre (IKC) for cyber security, based at Queen's

University Belfast. CSIT was established in 2009 and was awarded a Queen's Anniversary Prize for Higher and Further Education in 2015, it has recently been re-accredited by the National Cyber Security Centre as a UK Academic Centre of Excellence in Cyber Security Research.

The growing cyber business sector here covers a wide range of products and services – from Data Security, Device Security and Network Security, through to Web Application Security, Compliance, and Real-time Security Intelligence, in addition to Biometrics for Secure Payments, Fraud Detection and Secure Internet of Things.

This Strategic Framework for Action is purposefully brief to focus on key outcomes and activities which can be progressed in NI. It is closely aligned to the UK National Cyber Security Strategy 2016-2020<sup>3</sup> which further details types of threats, criminal activity and broader global context.

For the purposes of this document any reference to business or wider business community includes all organisations whether private sector, voluntary and community and charitable sectors, social economy sector and public sector organisations.

**More crime is committed online than offline and the cost of cyber crime to the economy is substantial**

1 International Data Corporation, Oct 2016. <http://www.idc.com/getdoc.jsp?containerId=prUS41851116>  
2 <http://www.scmagazineuk.com/cybersecurity-unemployment-rate-at-zero/article/523643>  
3 <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>

# STRATEGIC CONTEXT

Northern Ireland is increasingly being regarded as a leading European player in the specialist area of cyber security and has the potential to become a world class innovator in this field. We must build on this and work more closely with the implementation of the UK National Cyber Security Strategy.

## UK Strategy

The UK National Cyber Security Strategy 2016-2021 has adopted a three pronged approach – **Defend, Deter** and **Develop** with a significant focus on national security and protecting critical infrastructures and organisations. The Strategy aims to work to ensure the UK is secure and resilient to cyber threats, and prosperous and confident in the digital world. The UK Government has committed £1.9 billion to the implementation of the strategy over the 5 year period, it will create two new cyber innovation centres to drive the development of cutting-edge cyber products and dynamic new cyber security companies, in addition to helping deliver programmes to address the skills shortage needed to stay ahead.

The UK Government recognises it's responsibility internationally to influence legitimate actions to address criminal activity – whether to protect national security, develop leading skills and push cyber security standards. This is reflected in the UK adoption of the EU Directive on security of network and information systems (NIS Directive). The NIS Directive is the first piece of EU-wide legislation on cyber security. The aim is to bring cyber security capabilities to the same level of development in all the EU Member States and ensure that exchanges of information and cooperation are efficient, including at cross-border level.

# CYBER SECURITY

A Strategic Framework for Action 2017-2021



The UK Government published 'A Digital Strategy for a Digital Economy' in March 2017, stating that "Belfast is a leader in Cyber Security"

## Northern Ireland Alignment


This NI Strategic Framework for Action fully aligns with the UK National Strategy, and it is important that we contribute to and are supported by the national agenda. It addresses issues of particular need for NI within the devolved settlement and will ensure those identified needs, which are reserved or excepted to the UK Government, are appropriately addressed. The outcomes/activities will correlate to those in the UK National Strategy where there is potential synergy and we will look

for opportunities to capitalise on initiatives and connections with national organisations and other nations in the UK.

Cyber Security can only be effective when it is wholly embedded in the culture and psyche of all our citizens and all our businesses. Each of us is vulnerable from attack – whether this is through personal e-mail fraud, online banking and e-commerce or indeed through attack on the custodians of our digitised personal information, be that businesses or public service agencies.

In November 2016 Camelot reported that it believed around 26,500 player accounts for the national lottery were accessed in a fraudulent cyber attack. Internet banking fraud rose by 64% to £133.5m in 2015 with a growing trend to target business and high-net-worth customers<sup>4</sup>. It is therefore clearly evident from the number of high profile hacks of businesses, including digital businesses, that we must place a high emphasis on cyber security right across society to ensure we are as well protected as we can be.

4 <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>



Cyber crime is a growth area. It is an activity which offers anonymity and allows criminals to operate outside the law enforcement jurisdiction.

The NI Executive recognises the excellent work which is already happening to protect the public and business, and indeed the leading cyber innovations taking place in NI. However we also recognise the potential for significant growth in cyber security for the local economy, coupled with the vital need to protect the public and local businesses and prosecute those who undertake criminal activity against us. There will be an increasing demand for cyber risk analysis and assessment from many organisations and business, increased priority attached to network and data integrity from all businesses, along with investment, external sales and export growth from the growing cyber sector in Northern Ireland.

### **Programme for Government and Industrial Strategy Alignment**



The draft **Programme for Government** rightly places a focus on progressing a strong competitive economy, which has innovation and creativity embedded so that people can fulfil their potential. Equally there is a need to have safe communities where we have respect for the law and each other, and can deliver safe and effective public services. It is also important that our citizens have access to online services through high quality infrastructures which are safe and trusted. This Strategic Framework for Action will be an important delivery mechanism of the Programme for Government (PfG) and is closely aligned to key Outcomes and Indicators of the PfG.



# CYBER SECURITY

A Strategic Framework for Action 2017-2021



49% of private and public sector businesses at a Belfast seminar do not have a properly tested cyber security response plan

The draft Department for the Economy (DfE) **Industrial Strategy** has identified Cyber Security as one of four related digital sectors where NI has real potential for growth and being positioned as world class in terms of research and innovation; our ambition therefore is to make Northern Ireland a global innovation hub for cyber security supporting over 5,000 jobs by 2026 in this highly specialised area. Similarly Belfast has an ambition to become a 'Smart City' and while this will afford the city many fantastic opportunities it will also bring greater risks from the cyber-criminal world. The city is well placed to capitalise on the opportunities and manage potential risks by focusing attention on the contribution that cyber security can play – through growth of the cyber security sector and supporting ecosystem to well

informed city citizens and trusted online services. This Strategic Framework for Action is also aligned to the work which is being championed by Belfast City Council in driving the 'Smart City' initiative in the growing area of cyber security.

Through good coordination and collaboration with other stakeholders all Councils have a major role to play locally in progressing the Vision.



# APPROACH

We will scale up our ambition to drive competitive advantage in the field of cyber security and ensure our citizens, businesses and public services have access to the latest cyber innovation, which is interoperable, trustworthy and respects fundamental rights to privacy. This will be done in line with the UK National Cyber Security Strategy, identifying where we can contribute and benefit from the national programme.

Cyber security needs to be a strategic priority in Northern Ireland, as in other UK jurisdictions and internationally. In assessing the needs and opportunities for NI we have engaged with the other UK jurisdictions and further afield, to learn from their experiences and help shape the approach put forward in this document. This will help deliver on our aspirations for a safe, yet pioneering society in cyber security.

Taking into account key areas of resilience, critical infrastructures, digitally aware businesses and citizens; along with strong crime prevention and prosecution; and the development of a world class cyber cluster, it is considered that strategic activities can be progressed in line with the key

themes of the UK National Strategy, within which Outcomes and related Activities have been devised. There is clearly synergy across these and taken as a collective, with strong leadership, will make a marked contribution to supporting economic growth, social cohesion and protection.

# CYBER SECURITY

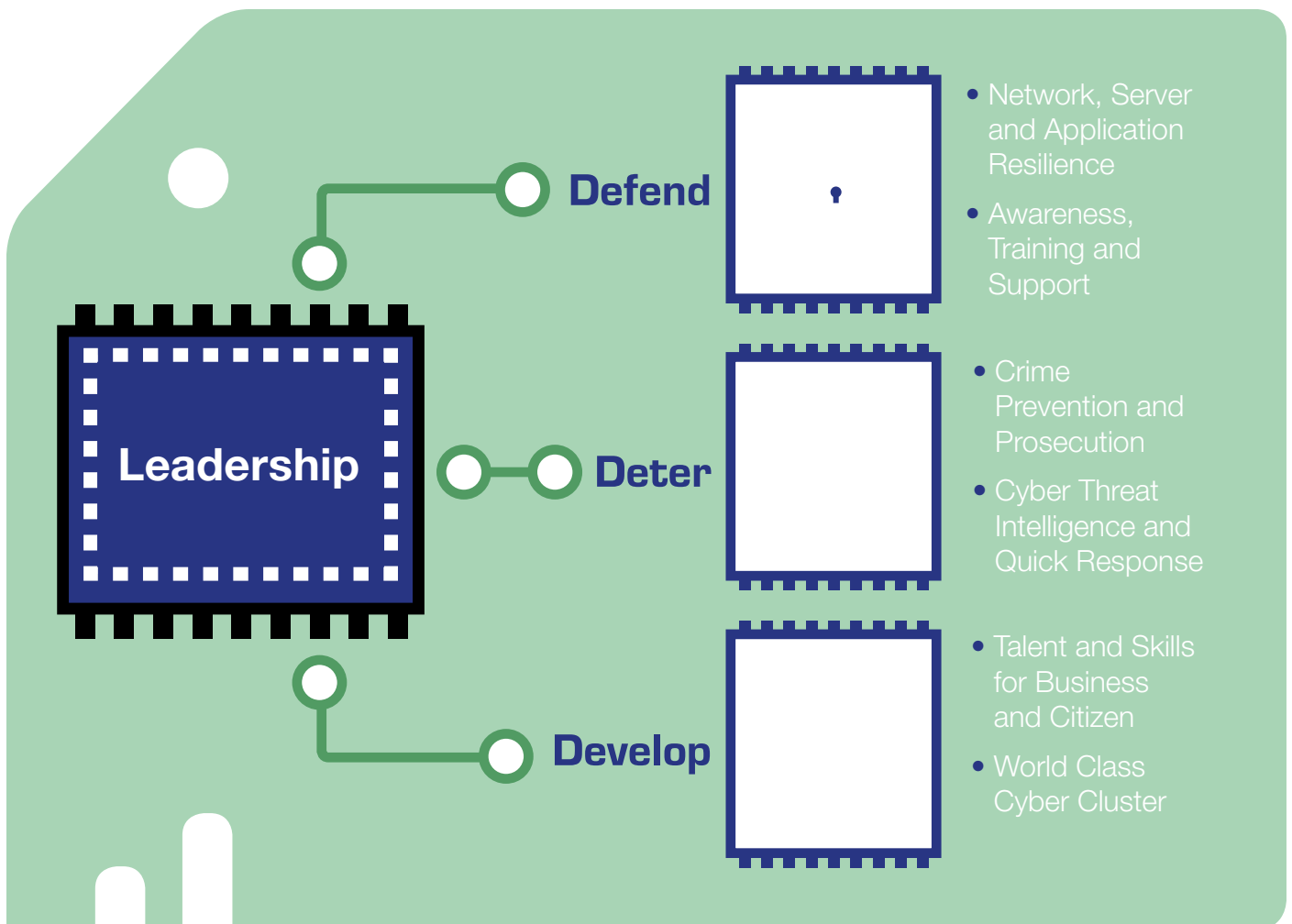
A Strategic Framework for Action 2017-2021



**THEME 1: DEFEND**

**THEME 2: DETER**

**THEME 3: DEVELOP**





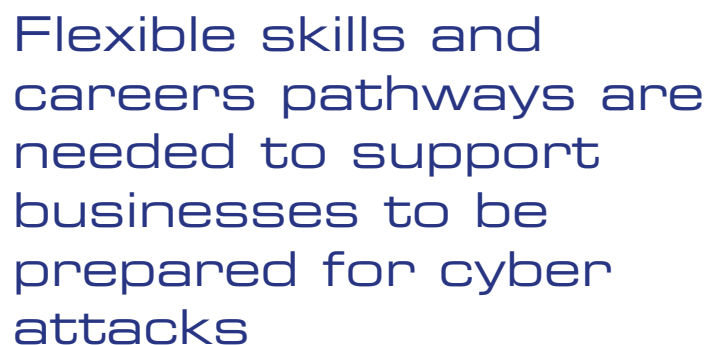
## The Vision

**Northern Ireland will be one of the world's leading cyber economies, delivering a thriving knowledge economy, due to exemplary talent; pioneering research and innovation; and the secure and resilient infrastructures needed to support businesses and safeguard the public.**

While this is a bold vision, it is justifiably so, since much of the initial infrastructure, organisations and initiatives are in place, underpinned by an appetite and enthusiasm to build on opportunities across the sector and more widely to support Northern Ireland society.

The image opposite is a thematic representation of the cyber security eco-system capturing current activity, opportunities for growth and where action is directly needed. In addition to showing key infrastructure requirements to ensure growth takes place, we can effectively achieve a cyber economy in NI which has embedded the fundamentals of protection across all aspects of society.

**Flexible skills and careers pathways are needed to support businesses to be prepared for cyber attacks**





# CYBER SECURITY

A Strategic Framework for Action 2017-2021



## CYBER ECO-SYSTEM

### CYBER CENTRE

Skills and Talent

Future Trends

Safe and Protected Society

All Business  
Citizens  
Critical Infrastructures

Cyber Security Sector

Product  
Development  
Services

Leading Edge Research

Innovation  
Pure Research  
Commercialisation

Support

Resilience Incident Response  
Engagement  
Awareness and Promotion  
Digital Infrastructure  
Access to Information and Support



There is a responsibility for all in society to actively engage in cyber security and this approach aims to ensure that the public, businesses, government and the cyber security sector all take their responsibilities seriously to help protect Northern Ireland and demonstrate this is one of the most cyber secure region with a closed door to cyber crime.

We can scale up our ambitions in a number of key areas to build one of the world's most secure societies in which to live and work:

- (a) network resilience – across all services, organisations and companies in NI
- (b) critical infrastructures on which society and life in NI is dependent
- (c) awareness & training for the public and business
- (d) intelligence and quick response to prevent attacks or reduce impacts
- (e) cyber crime prevention, protection, investigation and prosecution
- (f) world class cyber cluster underpinned by market focused cutting edge research; models of innovation and collaboration; and a demand led flow of talented people with transferable skills

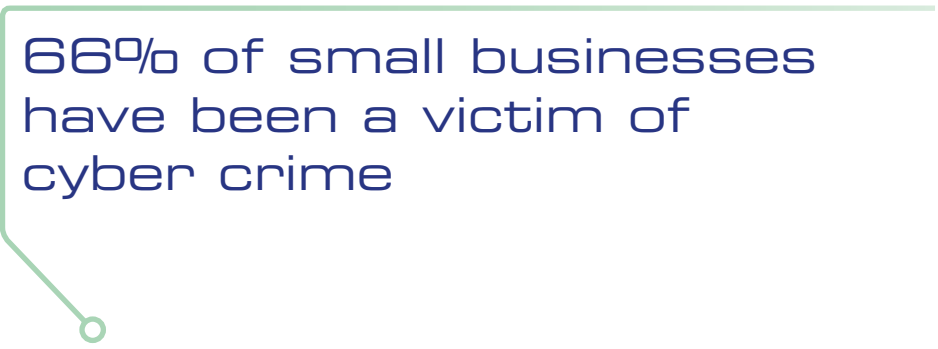
## Leadership

---

The NI Executive recognises the importance of having strong leadership in this area to ensure we are doing all things necessary to grow and protect our economy, our businesses, our citizens and our society at large. Effective leadership and coordination will also contribute to supporting activities across all parts of the public sector, including the Belfast 'Smart City' initiative; and will ensure that greater synergy can be achieved from the investments in skills, infrastructures, research, innovation, and public awareness leading to a more secure, trustworthy and resilient environment for people to live and work.

Integral to this approach will be the establishment of an appropriate governance and leadership structure which will ensure good coordination across all activities; provide consistent representation for Northern Ireland on the international stage; and be in a position to advise on future activities whether for government, citizens or businesses.

The UK Government has committed to investing heavily in a national cyber security programme until 2021 and it gives recognition to the excellent reputation of Belfast as a leading cyber security city in UK terms. While NI will secure some direct funding from the UK Government to help in progressing the cyber agenda locally, it is vital, through



**66% of small businesses have been a victim of cyber crime**



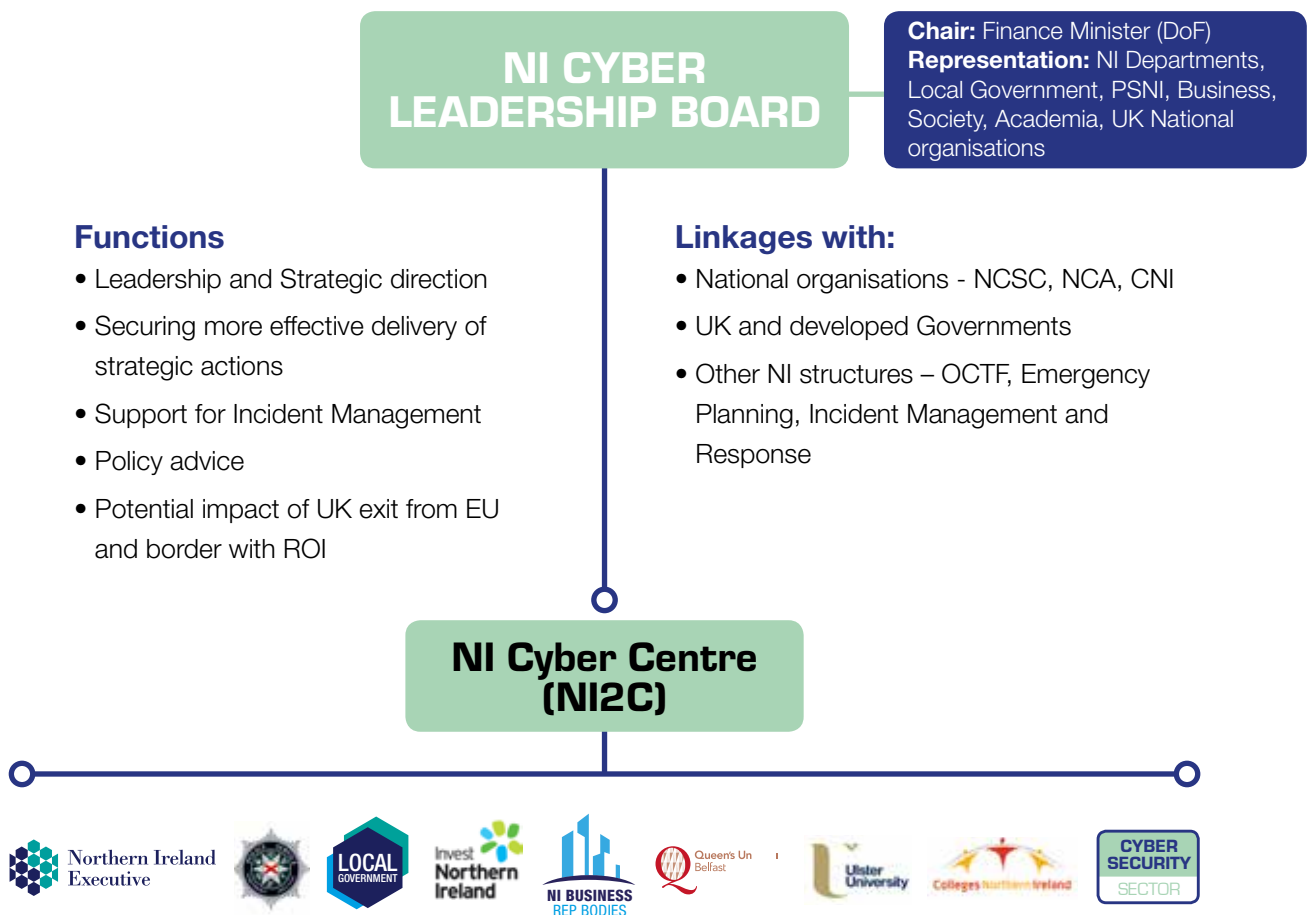
# CYBER SECURITY

A Strategic Framework for Action 2017-2021

strong and effective leadership, that we can maximise on the impact in NI of the wide range of UK Government initiatives relating to cyber. Whether this is through skills programmes, schools initiatives, research agendas, exports schemes or awareness raising initiatives we can effectively secure a more significant investment for Northern Ireland.

The Police Service of Northern Ireland is a leading regional police service in e-crime and has strong and effective relations with the National Cyber Security Centre (NCSC) and the National Crime Agency (NCA). We need to capitalise on the skills base locally and utilise both the NCSC and NCA to further strengthen the capabilities and skills in NI to enhance our role to protect the public.

The following schematic gives a potential representation of a leadership and governance structure which will clearly require further consideration to ensure it is right for Northern Ireland.



\* not exhaustive list of partners

The Northern Ireland Cyber Leadership Board can set the agenda and strategic direction as the threats, skills and technologies evolve. It is critical that this Board can command the confidence of Ministers, the public and the wider business community as a Team which will build the right relationships and establish contacts nationally and internationally to help ensure Northern Ireland stays safe online.

The creation of a cyber centre as proposed is a new initiative and of itself will present a number of challenges, however it has the real potential to effectively bring together a strong team to secure a more effective response to the growing threats of cyber. It must be recognised that many excellent initiatives are underway in NI, some of which are not securing the right profile or having the intended impact.

Northern Ireland Cyber Centre (NI2C) will play a vital role in being the custodian of knowledge on all activities underway, look to support delivery partners in profiling and linking to relevant communities and sectors and identify gaps in what is available or planned and look to how these can be addressed.

## NI CYBER CENTRE (NI2C)

### Functions

- Profile, Outreach, Voice for media
- Single point of contact for signposting
- Reporting on implementation of Strategic Framework, performance, future issues etc
- Maximising impact of initiatives
- Link to national priorities – e.g. critical infrastructures
- Coordination across all delivery channels
- Influencing development of relevant and needed services
- Links/engagement with stakeholders
- Internationalisation

### Resources

(team of between 5-8. Mix of short/long term contracts/secondments from stakeholder organisations)

### Director & Staff to undertake

- Project Management
- Marketing/Communications
- Engagement/signposting
- Business Development
- Incident Management

### FUNDING

- Contribution from UK Government until 2021
- Co Funding from NI Executive/Departments



\* not exhaustive list of partners

# CYBER SECURITY

A Strategic Framework for Action 2017-2021



Northern Ireland cannot go on this journey in isolation and it is therefore important that we have the most effective relations with national institutions, including the National Cyber Security Centre, National Crime Agency, the other devolved administrations in the UK and Innovate UK among others.

It is proposed that in the first 3 years NI2C will aim to have a staffing level of 6-8 people. It will be a shop front for all cyber related activities and will bring together expertise from different parts of the public sector, business and academia. Co-funding available from the UK Government and the NI Executive could be utilised for this.

Further work will be required however to assess the longer-term status and role of NI2C. It is widely recognised that cyber security is a necessity and will evolve and grow in importance for many years to come. NI cannot afford to simply invest up front for a number of years and say 'job done'. We need to recognise that this will be a longer commitment and as such must prepare for that.

In the medium to longer term NI2C can be located in Queen's University's Centre for Secure Information Technology (CSIT), in the heart of the growing cyber hub in the harbour area.

## Outcome:

Effective leadership and governance

## Key Activities:

- 1 Implementation of the proposed structures outlined above, supported with appropriate Terms of Reference accountability and funding support
- 2 Assess longer term implications for establishing NI2C on a stronger footing, including funding and resourcing options.

To seize the benefits of technological change, economies need ICT specialists, including cyber security

# THEME 1:

# DEFEND

**In recent years, the world has seen a massive leap in the number of people who offer their skills and knowledge for sale on the global marketplace irrespective of location and national borders. This is a key driver of the single European market for goods and services. Businessweek estimates this number will reach 100 million in the U.S. alone by 2020.**

**The United Kingdom is bullish about the potential of the contribution of the digital market, and we need to ensure we embed effective resilience into networks and infrastructures to protect against criminal activity but equally to have a secure and trusted platform on which the digital market relies. The European Union is placing significant emphasis on the Digital Single Market and regards the successful completion of this as boosting GDP some €500bn per year.**

Recent national malware incidents have demonstrated that the impact of widespread cyber crime on Critical National Infrastructure, Government and industry alike cannot be underestimated. Northern Ireland has not been immune from these attacks and the risk posed by such criminality continues to increase. The Police Service of Northern Ireland (PSNI) currently deals with more than 300 requests a month relating to cyber incidents and PSNI has estimated that one in ten people will be victims of a cyber-crime and that nine out of ten large organisations have reported suffering a cyber breach in Northern Ireland (NI).<sup>5</sup>

In October 2016 the BBC reported that £13m was stolen from people in Northern Ireland through different forms of electronic deception and theft over the previous year, however the true amount is assessed to be far in excess of this and there is a recognised and identified under-reporting of cyber crimes both nationally and locally.

It is a fundamental of any business operating online that it needs to demonstrate to its customers – current and potential – its resilience and integrity in protecting customer data and information. This responsibility is equally true of Government in the provision of public services.

In the digital age many new opportunities exist but also new risks. The Internet of Things (IoT) brings a host of potentially useful applications and new data services but also new threats to our digital environment.

There are a number of areas where we will take action to enhance both the **reactive operational response to cyber crime** and the **proactive steps** we can take to **mitigate against risk of attack**.



<sup>5</sup> <http://www.bbc.co.uk/news/uk-northern-ireland-37683642>

# CYBER SECURITY

A Strategic Framework for Action 2017-2021



## Proactive protection against cyber crime

The changing landscape of cyber crime and the evolving and developing cyber crime tactics and attack vectors means we have to build a protective and evolving environment for the individual in the community, for Government and for industry alike. This is being developed through a number of initiatives:

- Cyber Security Information Sharing Partnership (CiSP) – a joint government and industry platform to exchange cyber threat information in real time in a secure, confidential and dynamic environment;
- Cyber Essentials – a Government-backed cyber security certification scheme that sets out a good baseline for cyber security, suitable for all organisations in all sectors;
- Cyber Aware – an online Government initiative that encourages consumers and small businesses to adopt good online habits and which will protect their devices and information from the majority of online threats; and

- Get Safe Online – a public/private partnership, supported by the NI Executive and leading industry partners, and the leading source of easy to understand accurate information on online safety to the public.

These initiatives are currently delivered and supported by the Department of Justice and the PSNI but we need to expand the ownership. Working in partnership

with statutory agencies, business, industry and academia, will be a key driver in developing cyber security protection in future years. This resilience capacity will continue to develop as we work in collaboration with partners.

There is a need to foster greater vigilance across public and private sector organisations and improve the way we report, coordinate and share cyber issues.

### Outcome:

Northern Ireland society and business community informed about the threat from cyber crime and what steps they can take to protect themselves from it. Better intelligence and incident reporting will help to inform an effective response.

### Activities to contribute to Outcome:

- 1 Enhance and promote reporting mechanisms in order to encourage reporting of incidences of cyber crime.
- 2 Ongoing promotion and delivery of key support resources to see a marked increase in awareness of and engagement with these tools (including CiSP, Cyber Essentials, Cyber Aware and Get Safe Online).
- 3 Establishment of dedicated PROTECT role within PSNI.
- 4 Fully utilise existing resources, including NIDirect, Go On NI and NIBusinessInfo and other communications activities to promote safe cyber activity
- 5 Establish lowest cyber security standards to be included in all public sector procurement contracts.





## Public Services

One of the most important foundational components of a functioning digital society is a secure digital identity. When government services are provided over the internet, the government needs to build trust with the public to ensure that any services accessed or data provided are secure and protected.

NIDirect is the NI's Public Sector portal aimed at providing the public with a single point of access to public services and relevant information. It facilitates better communication and transaction between the public (including businesses) and government. It is vital to ensure and protect the trust through easily accessible and more efficient services.

Significant progress has been made on the digital transformation agenda across the public services in Northern Ireland and many online services are fully embedded and operating effectively, giving the public and businesses choices in how and when they engage

with government. It is however necessary to build on this and through focusing on cyber security and digital by design, citizens will think digital first when engaging with any public service in NI.

The information held by the public sector must be protected robustly. The threat of data exposure is faced across both the public and private sectors, but also individually by people who have a digital presence, whether through e-mail, social media or transacting with businesses and organisations online.

Department of Finance's Digital Shared Services manage much of the digital infrastructure and host a wide range of digital services, and will take a lead role in the context of this Strategic Framework for Action to strengthen and enhance protection of the digital network and manage the digital environment. It will continue to invest in firewalls, security software, virus scanning and development capability.

Criminal activity can exploit the most vulnerable groups in society, as well as business and public services. It is therefore imperative that all parts of society feel they can trust organisations they interact with and that they can also build their knowledge and skills to protect themselves in their day to day lives.

There is a need for greater vigilance and an onus on central and local government to ensure all organisations which deliver public services on their behalf (e.g. through the voluntary, community and charitable sectors) are diligent in providing resilient trusted services and can clearly demonstrate their commitment to deterring cyber attacks.



# CYBER SECURITY

A Strategic Framework for Action 2017-2021



## Outcome:

The public and businesses trust, and want to use public digital services, which have appropriate measures for protection in place.

## Activities to contribute to Outcome:

- 1 Introduction of an effective identity assurance scheme for the public.
- 2 Embed a culture of 'security by design' within the design of online public services.
- 3 Collaborate with private sector, public organisations and other public sector realms to advance protections to public services with latest technologies.
- 4 Development of a secure platform for government services to engage with the public, affording citizens control over the information they chose to share with government services.
- 5 Continue high levels of vigilance on existing and legacy systems, ensuring an aggressive approach to upgrade and patching to ensure compliance.
- 6 Ensure government contracts contain appropriate clauses for cyber essentials, GDPR and data protection.
- 7 Collaborate with the Health and Social Care Trust NI and other public sector organisations to assess any key cyber security issues.
- 8 Mitigate against vulnerability through a strategic awareness and education programme.

NI is the international location of choice for the leading cyber security firms



## Access to Information and Support for Business

Businesses, organisations and individuals must take responsibility for the protection and integrity of their respective online services and presences, and the data and information entrusted to them. Equally there is an onus on government and others to ensure that information and support is accessible to help them better understand the risks and to prepare for, and respond to, potential cyber attacks.

Where there is demand for information, signposting, guidance or support to assess potential cyber risks in business systems and processes through to where to access re-skilling or up-skilling staff we must deliver a coordinated service to meet the increasing appetite for information and support. A coordinated trusted service which is respected and has effective links to all aspects of the cyber eco-system, will help support the progress of Northern Ireland being a safe place to work, live and do business.

The Council for Curriculum Examination and Assessment recognises the need to provide a digital skills pathway for all learners, working in partnership with government, employers, schools and the wider community.

Equally in a broader sense in preparing young people for life, cyber security will become a main stay as the 'Internet of Things' and 'Industrial Internet of Things' increase to support our lives.

### Outcome:

An informed and supported business community in Northern Ireland which has fully embedded cyber security into their respective business processes and product/service developments.

### Activities to contribute to Outcome:

- 1 DOJ and OCTF communications to educate and raise awareness of cyber crime, through support and promotion of CiSP, Get Safe Online, Cyber Essentials and Cyber Essentials Plus campaigns.
- 2 Map existing information sources, identify gaps and provide an effective signposting service for businesses and the public in NI.
- 3 Assess what support mechanisms can be utilised by businesses to assess their cyber security risks and devise a tiered service solution based on risk and impact to local economy.
- 4 Utilising its interaction with the public, the public sector will help to improve the digital knowledge and skills of all citizens.

# CYBER SECURITY

A Strategic Framework for Action 2017-2021



## Critical Infrastructures

The Centre for Protection of National Infrastructures (CPNI) is the government authority for protective security advice to the UK national infrastructure. Its role is to protect national security by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats.

There are also other nationally important assets or events, including high-profile iconic targets, where impact of damage

would be equally serious even though these do not deliver an essential service. CPNI advice delivery extends to help the protection of such assets and events.

The work of CPNI also covers those critical infrastructures in Northern Ireland. We will however look to foster stronger links and understanding of the work of CPNI in the context of cyber security to ensure all relevant organisations are effectively linked up.

PSNI is investing in new mobile laboratories to support front line policing investigating cyber crimes in NI



## THEME 2:

## DETER

**Law enforcement is becoming increasingly aware and equipped to deal with the threats associated with cyber crime, with multi-agency forums established at national level to tackle these threats. Within Northern Ireland the Department of Justice and PSNI have key roles in ensuring that the justice system is equipped to deal with cyber criminals and in providing the operational response to cyber crime. However across all sectors of society – whether public sector, business, civil society or individuals, we must all accept responsibility for taking fundamental practical steps to protect ourselves against cyber attack through good cyber hygiene.**

Cyber crime consists of two main interrelated forms of criminal activity:

- **cyber-dependent crimes** – crimes committed through the use of Information and Communications Technology (ICT) devices. This includes the cyber attacks incorporating widespread malware deployments and the denial of service or unauthorised intrusion; and

- **cyber-enabled crimes** – traditional crimes which can be increased in scale by the use of ICT. This includes traditional crimes now committed at scale using the cyber environment, such as Fraud, Extortion, criminal commodity supply such as drugs or firearms, prostitution, human trafficking and Child Sexual Exploitation.

In addition 'Internet Facilitated Crime' such as the use of social media to commit treat, grooming, stalking or harassment and the disposal of criminal property on online auction sites continues to challenge policing and increases the digitisation of crime.

The UK National Cyber Security Strategy 2016-21<sup>6</sup> states that much of the most serious cyber-crime – mainly fraud, theft and extortion – against the UK continues to be perpetrated from Organised Crime Groups, primarily in eastern Europe with emerging threats from south Asia and west Africa, of increasing concern. The UK strategy provides more detail on the type of criminal threats which are posed and of direct concern to the UK and indeed NI governments.

The PSNI is represented at the highest level in UK law enforcement capability including with NCA National Cyber Crime Unit (NCCU) as well as its strategic groups. PSNI also continues to develop strong linkages to the UK National Cyber Security Centre (NCSC) and operates within a national network of Regional Cyber Crime Units supporting the National Cyber Crime Unit.

It has also developed enhanced capability through collaboration with international partners such as Europol, Interpol and academic centres of excellence and is leading innovative and investigative opportunities in several areas.

The PSNI's existing Cyber Crime Centre has successfully investigated high level of cyber criminality and attacks across Europe. The Centre is highly regarded nationally and internationally, leading Joint Investigation Teams through Europol and Eurojust, identifying, arresting and disrupting suspects and criminal groups targeting Northern Ireland business and industry. The PSNI's cyber capability has recently been enhanced with the design and launch of innovate mobile

<sup>6</sup> <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>

# CYBER SECURITY

A Strategic Framework for Action 2017-2021



laboratories – which can attend victim crime scene or suspect environments to recover the necessary and relevant evidence of cyber crime activity. This has enabled a high level of expert crime scene analysis, assisting in effective gathering evidence at scenes.

Businesses and organisations need to fully recognise their responsibilities in deterring potential cyber crime and attacks, and basically demonstrate that we are a protected society which deters cyber criminal activity and therefore not a target on the radar of organised crime or opportunistic attacks.

## Effective law enforcement

The PSNI Cyber Crime Centre has been significantly enhanced over the last number of years and the three main Departments: Forensic, Technical and Investigations will be housed within a new Cyber Crime Centre with a high level of interoperability with national and international law enforcement partners. The Cyber Crime Centre continues to develop and this will continue.

### Outcome:

Outcome: Enhanced PSNI investigations and operational response to cyber crime.

### Activities to contribute to Outcome:

- 1 PSNI will undertake a comprehensive strategic analysis of cyber crime as it affects Northern Ireland.
- 2 Develop and expand the PSNI Cyber Crime Centre, through:
  - a. Technical: develop the ability to protect against cyber attacks through enhanced technical improvements to support law enforcement;
  - b. Forensic: enhance and improve forensic examination and analysis techniques and solutions to improve the evidence recovery and presentation;
  - c. Investigation: expand the investigation capacity and expertise in cyber crime activities in order to enhance law enforcement ability to detect those involved in cyber crime;
  - d. Protect: increase the interaction with Northern Ireland business and industry, developing the protection initiatives and assist in making Northern Ireland the most secure place to live and be online;
  - e. Collaboration: the PSNI will continue to develop and enhance its relationships and partnerships with national law enforcement agencies such as NCCU, NCSC, Government Departments, as well as international law enforcement partners to increase NI's law enforcement capability and capacity;
  - f. Innovation: continued investment in research, partnering with academia and industry for innovative solutions and capabilities to enhance cyber security and law enforcement;
  - g. Creation of new state of the art facility for Northern Ireland; and
  - h. Skills: develop and expand skills capacity resulting from training needs analysis for cyber crime.
- 3 Develop and expand frontline policing's capacity within Districts and Areas to respond to cyber crime, through the development and enhancement of Cyber Support Units.
- 4 Joint partnership work between law enforcement agencies in relation to tackling cyber crime.
- 5 Assess how better to use academic research to help combat cyber dependent/enabled crime.



## Diversion from cyber crime

Recent events have highlighted the increasing extent to which young people are becoming involved in cyber crime, and the ease with which young people can access the criminal environments on the internet is an increasing challenge for society. There is an onus on society and Government to clearly show those who may be considering criminal activity both the consequences of such criminal activity and that there are alternatives through which a more productive and inclusive contribution to society can be made.

The Careers Service is available to all to learn about career opportunities and is one means through which we will promote the growing cyber security sector as a route for those with the right skills and aptitude to make a positive contribution to the local economy and society.

There is also a need to develop methods of identifying and responding to young people who may be at risk of becoming involved in criminal online activity in order to divert them away from such activity, through contacting,

developing and supporting families, carers and/or guardians/ teachers and through offering positive alternatives. PSNI is seeking to address this through its Prevention Strategy, in partnership with the Department of Justice, academia, Government stakeholders and industry partners.

This strategy delivers a three phased approach:

1. A **baseline education campaign** for young people and parents / guardians highlighting the risks of becoming involved in online criminality. This social media based campaign delivers regular interactions to discourage and report criminality (CyberChoices);
2. A **challenge programme** which seeks to identify talented and developing young people. This strand uses the Cyber Centurion Programme which challenges teams of young people in a competitive Cyber Security Challenge Program to educate and enhance their skills in defending networks and systems from attacks whilst being mentored by industry partners. This challenge programme, underpinned by

The National Cyber Security challenge, seeks to deter young people for becoming involved in cyber crime whilst developing skills for further education and employment (Cyber Centurion);

3. A **workshop development programme** with law enforcement, academia and industry partners focussed on those young people on the cusp of criminality or involved in cyber crime. The programme educates young people on when and how offences and crimes have taken place and uses cyber security industry collaboration to demonstrate where employment opportunities may be and how these can be disrupted with criminal activity.

The Strategy further aligns the work in Northern Ireland to existing national projects to understand why young people might be drawn into criminal activity and how to stop young people using their skills for criminal purposes.

# CYBER SECURITY

A Strategic Framework for Action 2017-2021



## Outcome:

Individuals in Northern Ireland choose not to engage in cyber crime and therefore reduce the risk to the public and economy.

## Activities to contribute to Outcome:

- 1 Assess what opportunities exist through the Careers Strategy.
- 2 Promotion of the 'Cyber Choices' campaign.
- 3 Engage in initiatives offered by NCSC such as 'Cyber Centurions' school / college educations programme and 'Cyber First' and look to expand take up in NI.
- 4 Formalise and continue to engage in the TEACH (Teaching Ethical Alternatives to Child Hackers) programme with QUB's Centre for Secure Information Technologies (CSIT).

Advanced niche skills support is needed to grow the NI cyber security sector





## THEME 3:

## DEVELOP

**Cyber security and resilience was the 2016 super trend, and it continues to grow in importance as more organisations experience losses in value and reputation that result from security gaps in their organisations, which have been exploited by those wishing harm through theft and sabotage. This area of great concern will grow as more reliance is placed on the internet and all things cyber. The 'Internet of Things' and the 'Industrial Internet of Things' represent everyday objects with internet connectivity and with this comes greater risk. Cyber criminals are becoming more skilled in infiltrating technology architectures and systems that were not designed from the ground up through a security lens.**

Key areas of concern over the coming years include increased attacks on the mobile market; increased attention given to supply chains' data security; resilience and recovery will become commercial differentiators; and the impact of new regulatory regimes to afford greater safeguards to data.

Northern Ireland has long held a reputation for its educational standards and preparing skilled and talented people for rewarding careers. In addition we are developing a strong international reputation for academic and industry funded innovative research. Furthermore with a growing private sector base, as a region we need to ensure that cyber security is a 'board room' priority for all businesses, including the third sector and public sector. We need to ensure our underlying digital infrastructures are future proofed and are designed to support growth and demand for increased activity across all of society.

With a growing cyber community, high quality staff, increasing focus on cyber exports and enviable reputation for foreign investment in cyber, there is a real potential for us to develop a world class cyber cluster.

From education through to sector growth and resilient businesses, and by staying ahead of the game we can develop a protected society where criminal activity is discouraged.

We need to take action in a number of key strategic areas to ensure we can deliver this ambition and cement NI as a leading region in new sectors where we have real potential to succeed.



# CYBER SECURITY

A Strategic Framework for Action 2017-2021



## Skilled and Talented People

A strong start has been made in designing a skills development programme with various pathways to educational success for our people, and current and future employees - from highest level PhD and MSc courses in Cyber Security, through to Degree course modules, apprenticeships (including higher level) and cyber security academies for re-skilling unemployed and under employed. A Digital Skills Roadmap is in place to support young people, which is aligned to a Digital Foundations Programme to support those delivering digital skills in the classroom. Industry needs are demanding and to ensure we can stay ahead of the game we must deliver a pipeline of talented people to meet these demands. Further work is therefore needed to identify the core skills and competencies to put in place a comprehensive range of skilling and up-skilling solutions which are validated and accredited to world class standards.

### Outcome:

A knowledgeable and skilled workforce and society which can take responsibility for online security and contribute to Northern Ireland being one of the safest places to live and work

### Activities to contribute to Outcome:

- 1 Assess current and future skills needs of NI businesses and organisations to support growth in cyber security profession and the sector.
- 2 Consider continuous professional development to help future proof the skills base.
- 3 Support up-skilling of the teaching profession to deliver valid and accredited courses, building on current emerging collaborative arrangements within the further education sector.
- 4 Map existing skills delivery tools and identify gaps.
- 5 Deploy all skills channels available to suit the differing needs of business, public and employee.
- 6 Raise awareness of the opportunities for successful careers in cyber security and resilience.
- 7 Assess the potential for introducing cyber security and resilience into education at post primary level (including within the existing curriculum).
- 8 Public sector to assess current and future skills needs and drive the skills demands for cyber security.
- 9 Retention of home grown talent in Northern Ireland.



## World Leading Research Agenda

The approach to research is changing and a greater recognition is given to the input and impact of industry in helping to shape research agendas, achieve greater commercialisation of academic research and to further enhance the skills of those involved in specialist areas such as cyber security. Whether 'cloud' or wifi security, network or data security, Northern Ireland's two universities are increasingly being recognised internationally as key 'go to' institutions for leading research. They both have developed strategic partnerships and collaborative agreements with many organisations from government to international and local industry businesses.

The Centre for Secure Information Technologies (CSIT) is increasingly looking to the commercialisation opportunities of its research programme and actively engaging with local and international industry on research initiatives. Ulster University is also focusing on niche areas of cyber security research with blue chip industries.

With such a reputation created it is vital that in the area of cyber security the research programmes progressed in Northern Ireland add value to the NI cyber cluster, support growth of the local economy and contribute to a recognised skills supply of talented and creative people for careers in the digital knowledge workplace.

### Outcome:

Northern Ireland recognised as one of the leading regions/nations in the world on the competitive index for cutting edge primary and industry supported research on cyber security.

### Activities to contribute to Outcome:

- 1 Review and assess the numbers of PhDs and Masters available in Cyber Security and related disciplines.
- 2 Secure an increase of 30% in industry sponsored cyber security research.
- 3 Increased support for R&D by cyber security companies through InvestNI.
- 4 Determine the world ranking of NI's cyber security research to support its growing reputation.
- 5 Scaling up of the provision of our two Universities, including the more effective networking and linkages with related disciplines, and areas of expertise.

# CYBER SECURITY

A Strategic Framework for Action 2017-2021



## Growing a Dynamic Cyber Security Sector

**We have the potential to create upwards of 5000 new high value knowledge jobs in cyber security by 2026. Challenging as this may seem, the cyber security sector in Northern Ireland, with some 30+ companies already involved (employing some 1200 people), is one which is attracting significant international interest and there is real potential for not only growth of existing companies and new start ups but overseas investment too. A ready supply of talented and skilled people; leading edge research both academic and commercially funded; supply of appropriate high spec accommodation provision and a growing effective cluster are all needed to help attract further investment in the cyber sector.**

We have the capacity and capability to capitalise on the global growth of cyber security and Northern Ireland can be positioned as a leading region and recognised as such on the world stage. InvestNI is well positioned to deliver a strong and compelling message to potential investors - from the skills and supporting research agendas, through to appropriate office accommodation solutions and supporting infrastructures. A growing cluster naturally attracts greater attention and to have a comprehensive eco-system will further enhance our position as a global cyber region.

The development of technologies will be necessary to grow the sector, enhance the products and services available and rely on leading edge research. We will continue to use existing networks and structures to support companies in this sector, for example through Digital Catapult NI and Invest NI to facilitate strategic matches for business growth and to access new markets.

### Outcome:

World class cyber security sector in NI, making a greater contribution to GDP and output, with increased above average wage costs.

### Activities to contribute to Outcome:

1. Increased opportunities for existing cyber security companies to showcase their products and services both locally, nationally and internationally.
2. Increased Foreign Direct Investment (FDI) secured for NI - attracted by the skills and wider cyber security eco-system.
3. Increased opportunity to nurture entrepreneurs and innovators taking their ideas and research to commercialisation.
4. Supply of appropriate grade accommodation for investors.

# CONCLUSIONS

Good work is progressing across many parts of society in relation to cyber security – protecting our communities and individuals, taking robust action against cyber criminals, raising the profile of cyber security as an exciting and rewarding career, supporting research and growth of niche solutions to address security issues and build by design resilient public services.

Cyber security is a growth industry, fuelled in part by the criminal activity – opportunistic and organised – already causing havoc and distress. Northern Ireland, and in particular Belfast, has a growing reputation as a leading cyber region and we must build on that and demonstrate NI as the go to place for cyber solutions.

We have an effective policing infrastructure in place to tackle cyber crime whether at home, nationally or internationally, and the PSNI is widely regarded as a leading regional policy force with integrity in responding to cyber crime. Our public services are increasingly relying on online technologies to deliver more effectively for the taxpayer, however with this comes new challenges on security.

The work undertaken across government, business and academia to develop this Strategic Framework for Action clearly demonstrates the need to focus more heavily on the growing threats and opportunities presented by cyber and to work towards a safer community in which to work and live. The key message however is that we can be significantly more effective through a strong leadership structure with better collaboration across all stakeholders and delivery partners. Each part of society must take their respective responsibilities, and government will ensure it plays its part in protecting public services, supporting growth of the cyber sector and signposting to services, information and initiatives in helping to deliver on the Vision:





**Cyber crime is a growth area. It is an activity which offers anonymity and allows criminals to operate outside the law enforcement jurisdiction.**



# SUMMARY OF OUTCOMES/ ACTIVITIES

## LEADERSHIP

**Outcome:** Effective leadership and governance

**Key Activities:**

1. Implementation of the proposed structures outlined above, supported with appropriate Terms of Reference accountability and funding support
  2. Assess longer term implications for establishing NI2C on a stronger footing, including funding and resourcing options.
- 

## DEFEND

### Proactive protection against cyber crime

**Outcome:** Northern Ireland society and business community informed about the threat from cyber crime and what steps they can take to protect themselves from it. Better intelligence and incident reporting will help to inform an effective response.

**Activities to contribute to Outcome:**

1. Enhance and promote reporting mechanisms in order to encourage reporting of incidences of cyber crime.
2. Ongoing promotion and delivery of key support resources to see a marked increase in awareness of, and engagement with, these tools (including CiSP, Cyber Essentials, Cyber Aware and Get Safe Online).
3. Establishment of dedicated PROTECT role within PSNI
4. Fully utilise existing resources, including NIDirect, Go On NI and NIBusinessInfo and other communications activities to promote safe cyber activity.
5. Establish lowest cyber security standards to be included in all public sector procurement contracts.

### Public Services

**Outcome:** The public and businesses trust, and want to use public digital services, which have appropriate measures for protection in place.

**Activities to contribute to Outcome:**

1. Introduction of an effective identity assurance scheme for the public.
2. Embed a culture of 'security by design' within the design of online public services.
3. Collaborate with private sector, public organisations and other public sector realms to advance protections to public services with latest technologies.

# CYBER SECURITY

A Strategic Framework for Action 2017-2021



4. Development of a secure platform for government services to engage with the public, affording citizens control over the information they chose to share with government services.
5. Continue high levels of vigilance on existing and legacy systems, ensuring an aggressive approach to upgrade and patching to ensure compliance.
6. Ensure government contracts contain appropriate clauses for cyber essentials; GDPR and data protection.
7. Collaborate with the Health and Social Care NI and other public sector organisations to assess any key cyber security issues.
8. Mitigate against vulnerability through a strategic awareness and education programme.

## Access to Information and Support for Business

**Outcome:** An informed and supported business community in Northern Ireland which has fully embedded cyber security into their respective business processes and product/service developments.

### Activities to contribute to Outcome:

1. DOJ and OCTF communications to educate and raise awareness of cyber crime, through support and promotion of CiSP, Get Safe Online, Cyber Essentials and Cyber Essentials Plus campaigns.
2. Map existing information sources, identify gaps and provide an effective signposting service for businesses and the public in NI.
3. Assess what support mechanisms can be utilised by businesses to assess their cyber security risks and devise a tiered service solution based on risk and impact to local economy.
4. Utilising its interaction with the public, the public sector will help to improve the digital knowledge and skills of all citizens.

---

## DETER

### — Effective law enforcement

**Outcome:** Enhanced PSNI investigations and operational response to cyber crime.

### Activities to contribute to Outcome:

1. PSNI will undertake a comprehensive strategic analysis of cyber crime as it affects Northern Ireland.
2. Develop and expand the PSNI Cyber Crime Centre, through:
  - a. Technical: develop the ability to protect against cyber attacks through enhanced technical improvements to support law enforcement;
  - b. Forensic: enhance and improve forensic examination and analysis techniques and solutions to improve the evidence recovery and presentation;



- c. Investigation: expand the investigation capacity and expertise in cyber crime activities in order to enhance law enforcement ability to detect those involved in cyber crime;
  - d. Protect: increase the interaction with Northern Ireland business and industry, developing the protection initiatives and assist in making Northern Ireland the most secure place to live and be online;
  - e. Collaboration: the PSNI will continue to develop and enhance its relationships and partnerships with national law enforcement agencies such as NCCU, NCSC, Government Departments, as well as international law enforcement partners to increase NI's law enforcement capability and capacity;
  - f. Innovation: continued investment in research, partnering with academia and industry for innovative solutions and capabilities to enhance cyber security and law enforcement;
  - g. Creation of new state of the art facility for Northern Ireland; and
  - h. Skills: develop and expand skills capacity resulting from training needs analysis for cyber crime.
3. Develop and expand frontline policing's capacity within Districts and Areas to respond to cyber crime, through the development and enhancement of Cyber Support Units.
  4. Joint partnership work between law enforcement agencies in relation to tackling cyber crime.
  5. Assess how better to academic research to help combat cyber dependent/enabled crime.

## — Diversion from cyber crime

**Outcome:** Individuals in Northern Ireland choose not to engage in cyber crime and therefore reduce the risk to the public and economy.

### **Activities to contribute to Outcome:**

1. Assess what opportunities exist through the Careers Strategy.
2. Promotion of the 'Cyber Choices' campaign.
3. Engage in initiatives offered by NCSC such as 'Cyber Centurions' school / college educations programme and 'Cyber First' and look to expand take up in NI.
4. Formalise and continue to engage in the TEACH (Teaching Ethical Alternatives to Child Hackers) programme with QUB's Centre for Secure Information Technologies (CSIT).

---

## DEVELOP

### Skilled and Talented People

**Outcome:** A knowledgeable and skilled workforce and society which can take responsibility for online security and contribute to Northern Ireland being one of the safest places to live and work.

### **Activities to contribute to Outcome:**

1. Assess current and future skills needs of NI businesses and organisations to support growth in cyber security profession and the sector.



# CYBER SECURITY

A Strategic Framework for Action 2017-2021



2. Consider continuous professional development to help future proof the skills base.
3. Support up-skilling of teaching profession to deliver valid and accredited courses, building on current emerging collaborative arrangements within the further education sector.
4. Map existing skills delivery tools and identify gaps.
5. Deploy all skills channels available to suit the differing needs of business, public and employee.
6. Raise awareness of the opportunities for successful careers in cyber security and resilience.
7. Assess the potential for introducing cyber security and resilience into education at post primary level (including within the existing curriculum).
8. Public sector to assess current and future skills needs and drive the skills demands for cyber security.
9. Retention of home grown talent in Northern Ireland.

---

## World Leading Research Agenda

**Outcome:** Northern Ireland recognised as one of the leading regions/nations in the world on the competitive index for cutting edge primary and industry supported research on cyber security

### Activities to contribute to Outcome:

1. Review and assess the numbers of PhDs and Masters available in Cyber Security and related disciplines.
2. Secure an increase of 30% in industry sponsored cyber security research.
3. Increased support for R&D by cyber security companies through InvestNI.
4. Determine the world ranking of NI's cyber security research to support its growing reputation.
5. Scaling up of the provision of our two Universities, including the more effective networking and linkages with related disciplines, and areas of expertise.

## — Growing a Dynamic Cyber Security Sector

**Outcome:** World class cyber security sector in NI, making a greater contribution to GDP and output, with increased above average wage costs.

### Activities to contribute to Outcome:

1. Increased opportunities for existing cyber security companies to showcase their products and services both locally, nationally and internationally.
2. Increased Foreign Direct Investment (FDI) secured for NI - attracted by the skills and wider cyber security eco-system.
3. Increased opportunity to nurture entrepreneurs and innovators take their ideas and research to commercialisation.
4. Supply of appropriate grade accommodation for investors.

Back page details to come