Health and Social Care

Cyber Security Strategy

HSC Northern Ireland 2022-2026

Contents

Strategic Context

Introduction 3-4

Our Cyber Landscape 5

Vision 7

Our Cyber Vision

Mission & Principles 8

Supporting the Quadruple aim 9

Integrating our Strategies 10

Our Digital Alignment 11

Our Strategic Framework 13-14

How we will deliver

Cyber Security Operations Centre 15

Our Strategic Outcomes 17-21

Our Enablers 23-26

Next Steps 27

Introduction

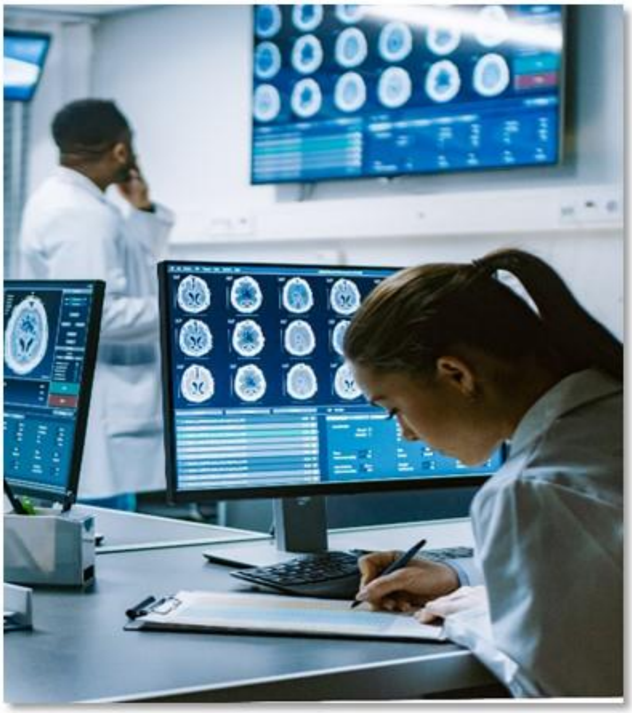
This 2022-2026 Cyber Strategy articulates the HSC plan to manage risk and maintain resilience in our digital and cyber operations in Northern Ireland.

This strategy is owned by HSC, but will require support from across the Health and Social Care ecosystem. We will assign a delivery team to ensure we meet our objectives and deliver cyber security benefits for health and social care in Northern Ireland.

Where our Cyber Security Strategy fits in

Health and Social Care Northern Ireland (HSC) is committed to fostering a stable and efficient health and care system. With cyber attacks worldwide increasing in frequency and severity, cyber security measures will be a key priority in the delivery of future services.

As part of this, our strategy will play a key role in the delivery of a safe and secure digital transformation, which was identified as one of five core enablers of *'Delivering Together'*. Our strategy must also align to the 'Quadruple aim' that was set out (*See: Supporting the Quadruple Aim)*



Our Cyber Strategy must align with wider HSC strategies (*see: Integrating Our Strategies)* to support the development and implementation of new technologies in a manner that maintains the security and integrity of our systems and data.

How we have developed this strategy

This strategy has been developed in collaboration with stakeholders from across the HSC ecosystem, as well as through engagement with our people. It is intended for all of those involved in the delivery of health and social care services.

The strategy outlines the vision, mission and objectives for cyber security across HSC and the enablers and initiatives that will enable us to deliver upon these successfully.

Introduction

Enhancing the Cyber Security Landscape in Support of Health and Social Care Transformation in Northern Ireland

As our reliance on technology grows, the continuity of our network and information systems becomes increasingly important and our systems and data become a more tempting target to cyber criminals. Responding to this threat is an essential requirement for HSC to ensure the wellbeing of our communities.

In light of this, the HSC Cyber Programme Board, representative of HSC organisations, has been working hard to secure critical network and information systems in order to keep society and essential services protected. This has included adopting innovative vendor products and introducing new security management structures to enhance our overall security position.

In an HSC organisational context we define cyber security to include

- Information;
- Applications;
- Infrastructure and
- Physical locations of our technology assets

The Cyber Assessment Framework

In response to a wider EU cyber security initiative, UK government enacted the Network and Information Systems (NIS) regulations in April 2018.

The NIS Regulations provide legal measures to boost the overall level of security for both cyber and physical resilience of network and information systems. This includes the secure provision of digital services (online marketplaces, online search engines, cloud computing) and operators of essential services (OES) including transport, energy, water, digital infrastructure services and of course – health.

Following consultation with those providers, the UK government designated all Health and Social Care Trusts in Northern Ireland (defined by Health and Social Care (Reform) Act) (Northern Ireland) 2009 as OESs. To ensure the continued application of the NIS principles following its exit from the EU, the UK National Cyber Security Centre adopted and adapted the requirements of the NIS Directive to create the UK Cyber Assessment Framework. The Cyber Assessment Framework is based on a four-objective security approach to Manage, Protect, Detect and Minimise cyber security threats. We have based our strategic outcomes on these objectives, to demonstrate compliance with the NIS Directive.

There are distinct challenges in meeting NIS objectives, but HSC organisations have already undergone an extensive review to evaluate compliance with the requirements of the framework. This strategic document is underpinned by supporting actions which comprise an actionable plan for achievement of our objectives at an HSC wide level.

Although not all HSC organisations and delivery partners are designated as OES, the objectives and principles contained in the directive provide a standard cyber security approach appropriate for all.

Our Cyber Landscape

Healthcare systems are becoming increasingly susceptible to cyber crime, as systems and data storage are progressively digitalised.

Health and Social Care Northern Ireland is committed to fostering a stable and efficient healthcare system. Given the worldwide increase in frequency and severity of cyber attacks, cyber security will be a priority for the delivery of services for many years to come.

Health & care data as a target

Healthcare systems are a known target for cyber criminals, with attackers posing a two-fold risk to safety and security.

Interference with systems has the potential to directly impact patient safety, through direct actions such as interference critical active medical devices or delay of urgent treatment,

The next most at-risk asset is a patients' health record, which includes personally identifiable information (PII) such as health care provider information, name, address, date of birth, etc. as well as protected health information (PHI) - like patient physical or mental health condition – which can all be used to steal identities or commit financial fraud. One analysis finds that a full patient record can sell for up to $1000 on the black market [REF1].

With the present move to electronic health records, these risks are amplified and must be mitigated for successful implementation.

COVID-19 Implications

Since the beginning of the Covid-19 pandemic, the World Health Organization has detected a dramatic increase in the number of cyber-attacks. The Verizon Data Breach Investigations Report for 2020 identified 521 confirmed instances of data exposure in the healthcare industry—up from 304 the previous year [REF2]. It is theorised that this has been due to a number of reasons including:

- Interest in vaccination programmes and vaccine development due to their effect on the economy, resulting in espionage aimed at stealing health data;
- Increased phishing and other cyber attacks that exploit COVID-19 as a new way to target the population;
- Increased hybrid working and staff distraction and stress leading to increased spread of data nationally and data handlers making more security mistakes;

Case Study: WannaCry Cyber Attack, 2017

The impact and severity of the 2017 WannaCry cyber attack serves to illustrate the importance of vigilance within cyber security. Hackers compromised IT across the NHSand encrypted files on infected PCs, before demanding a ransom payment in bitcoin for their retrieval. This forced clinics and hospitals across the UK to cancel or delay surgeries and X-rays and medical services were reduced following a massive outage from the attacks.

[REF1] "What Hackers Actually Do with Your Stolen Medical Records," Advisory Board, March 1, 2019.
[REF2] "2020 Data Breach Investigations Report," Verizon, April 2020

Study: 50413
Series: 603
ID: service
Date: May 31 2005
Study: 50413
Series: 603
Image: 167
leftmotorfx
TR: 0.00
TE: 0.00

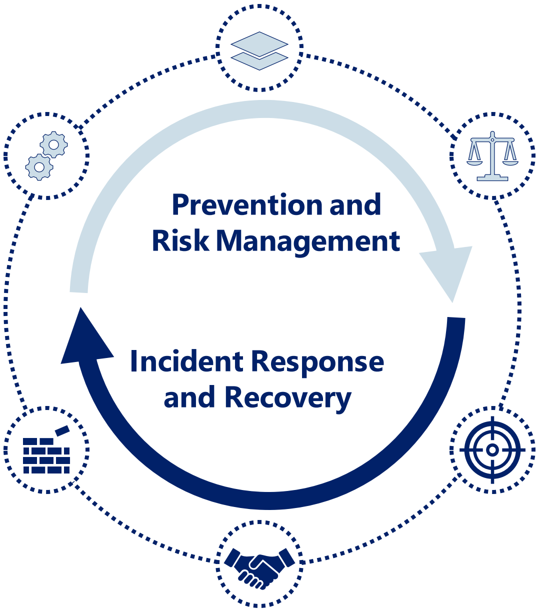
Vision

Our vision for cyber security was co-designed with stakeholders from across the health and social care ecosystem and is a core capability to the HSC Digital Strategy

To strengthen the cyber security controls and resilience of Northern Ireland Health and Social Care services against an evolving threat landscape

Our cyber vision

At the core of enabling us to deliver this vision, we are committed to valuing, developing and empowering our staff to strive for excellence and innovation whilst maintaining security, privacy, fairness and accountability in delivery and supporting services.



Our systems are protected by layered security solutions that make it harder for a cyber attack to be successful

Clinical and technology risk management is aligned and balanced across the organisation.

In the event of a breach, our systems can quickly detect and respond to halt or hinder the attack.

Strong partnerships and collaboration across HSC organisations acts to embed resilience in our systems

Our architecture and processes are designed to reduce the impact and extent of a cyber breach

Our processes and risk awareness protocol make our systems less vulnerable to attack

Prevention and Risk Management
Incident Response and Recovery

Our vision for cyber security at HSC

Mission & Principles

Whilst our vision outlines our ambition, our mission focuses on how we plan to deliver it. It communicates our direction of travel over the next 4 years and the principles that will guide us.

Our Mission

To promote the efficiency and stability of Health and Social Care Services through robust cyber security capabilities and expertise, collaboration and information sharing, with comprehensive oversight

Our Values

We value, develop and empower our staff to strive for excellence and innovation whilst maintaining security, privacy, fairness and accountability in delivering and supporting services.

The values and principles outlined in this strategy apply to any delivery partner who stores, processes, transmits or hosts our information and infrastructure. To ensure compliance, any partner organisation will be required to adopt these cyber security objectives.

Our Cyber Security Principles

We have aligned this strategy with the NCSC cyber assessment framework and identified five cyber security principles to help to anchor the Cyber Security strategy on what matters most to our patients, their carers and our clinicians, staff and partners.

Integrated

Providing a single, HSC-wide view of information assets and associated risk, including cohesive oversight and clearly defined accountabilities.

Aligned

Co-ordinating cyber activities with ongoing HSC projects and priorities and ensuring compliance with government mandated cyber standards

Effective

Embedding the necessary systems and tools that can protect our essential services from cyber attack and enable rapid response to emerging threats such that lasting impact is mitigated.

Resilient

Identification and prevention of single points of failure though implementation of layered security systems and processes that act collectively to prevent or reduce the effect of a cyber attack.

Targeted

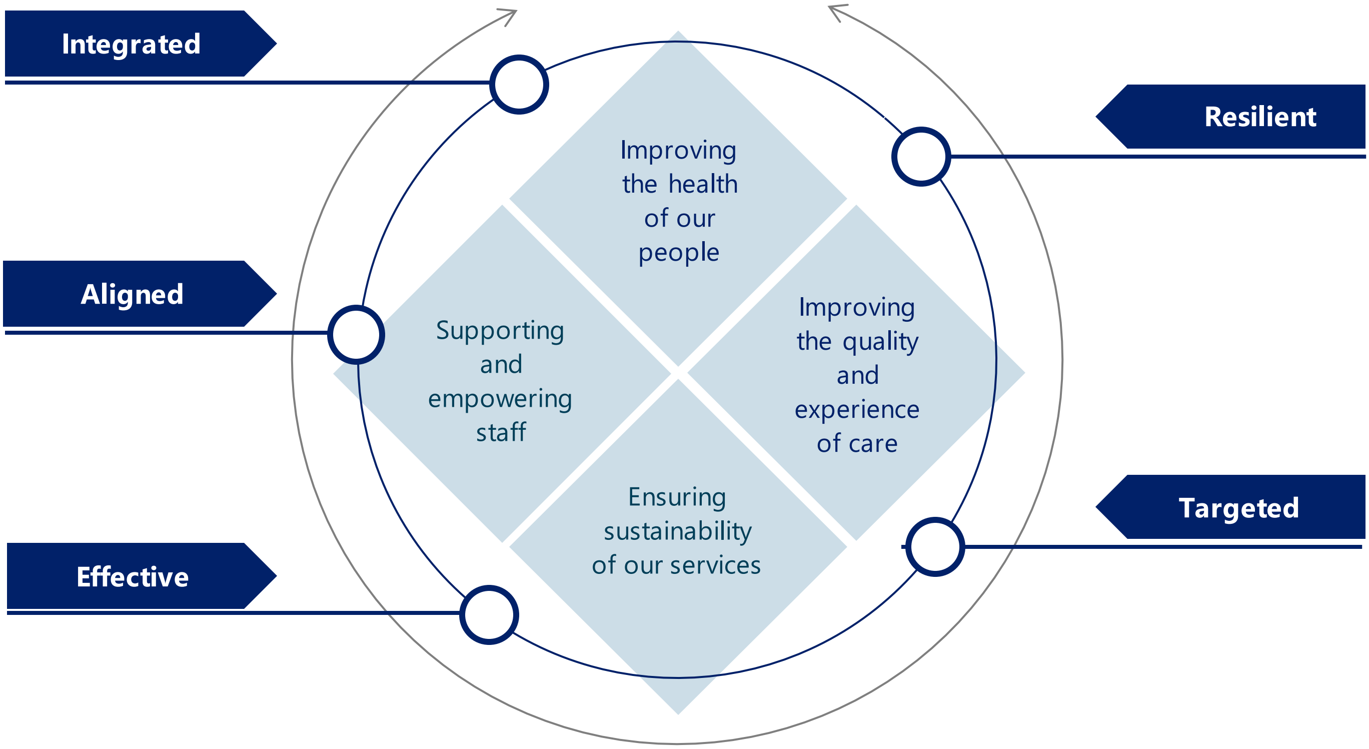
Reflecting the current and future service delivery needs and priorities for staff and patients in our cyber security considerations

Supporting the Quadruple Aim

Our five cyber principles align to and support HSC's wider Health and Wellbeing Strategy, specifically the 'Quadruple Aim' that it sets out and existing and complementary strategies.

No single team or organisation can deliver transformation in isolation, which is why alignment to wider HSC objectives and the Quadruple Aim will help us deliver on the ground. Our approach to data security will be driven from multiple sources and relies on a joint effort to develop and implement improvements.

Quadruple Aim


Integrated
Resilient
Aligned
Targeted
Effective
Improving the health of our people
Supporting and empowering staff
Improving the quality and experience of care
Ensuring sustainability of our services

> **"The realisation of [the aspirations set out in Delivering Together] must be built on the foundation of a secure IT infrastructure and support for operational management"**
>
> – Health and Wellbeing 2026: Delivering Together

Understanding and aligning the requirements of Cyber Security

This Cyber Security Strategy will form part of a suite of documents that articulates how we will protect and secure our data as part of our wider digital transformation, supporting the Department of Health's wider strategic goals (as articulated in Delivering Together). Throughout the document, we reference strategies that will be based on the mission and capabilities outlined here (*such as the HSC Data Strategy, Digital Strategy and Innovation Strategy*). At the same time, this document acknowledges the role that data security plays in supporting wider organisational strategies such as the HSC Workforce Strategy.

Integrating our Strategies

Our Cyber Strategy is just one part of a larger picture that ties together how and what we deliver for our people. Our Cyber Strategy must sit alongside – and underpin – the other documents in this suite, including digital, data and information, innovation and workforce strategies. Transformation must take place in a cohesive and comprehensive manner, with security for our systems and information embedded at every stage.

The illustration below explores the relationships between these strategies and how cyber must be aligned to support the effective delivery of their objectives and goals.

Digital Strategy

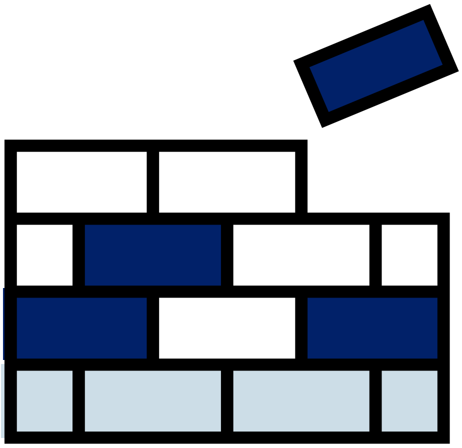
Our Digital Strategy outlines core transformational programs and initiatives that will change the way in which digital technology is used at HSC. Cyber security will form a key part of the design of new digital solutions, with security and safety fundamental to successful implementation.

Data and information

Data is the lifeblood of our health and care system and our data strategy outlines how we must expand our data usage to improve patient outcomes. In order to do this safely, we must build strong cyber security foundations to protect the sensitive data we are storing.

Innovation

As we continue to innovate and improve within our health and care ecosystem, cyber security considerations must be at the forefront. New technologies and systems are susceptible to new threats and dangers and we must therefore evolve our cyber security solutions in tandem.



Workforce

Our people are critical to delivering quality care – frequently handling sensitive health and care information. We must support our staff to build their cyber awareness and proficiency so that they understand their role in keeping data safe

A Cyber Secure Foundation

The variety of transformation programmes taking place across HSC each require built-in redundancy, crisis planning, cyber protection and risk assessment, which can only be achieved through cyber secure design principles. It is essential that cyber security is integrated into solution design from the outset so that our resulting services are resilient against attack.

Digital Alignment

Our Cyber Strategy sits alongside the wider digital transformation taking place across HSC (*See HSC Digital Strategy*). A key dependency exists between these two transformations, as our ability to deliver improved cyber capabilities is dependent on the new digital solutions that we will implement as part of this and strong cyber capabilities are key to enabling the digital transformation to take place in a secure way.

The table below describes how our cyber transformation will support the strategic outcomes of the HSC digital Strategy.

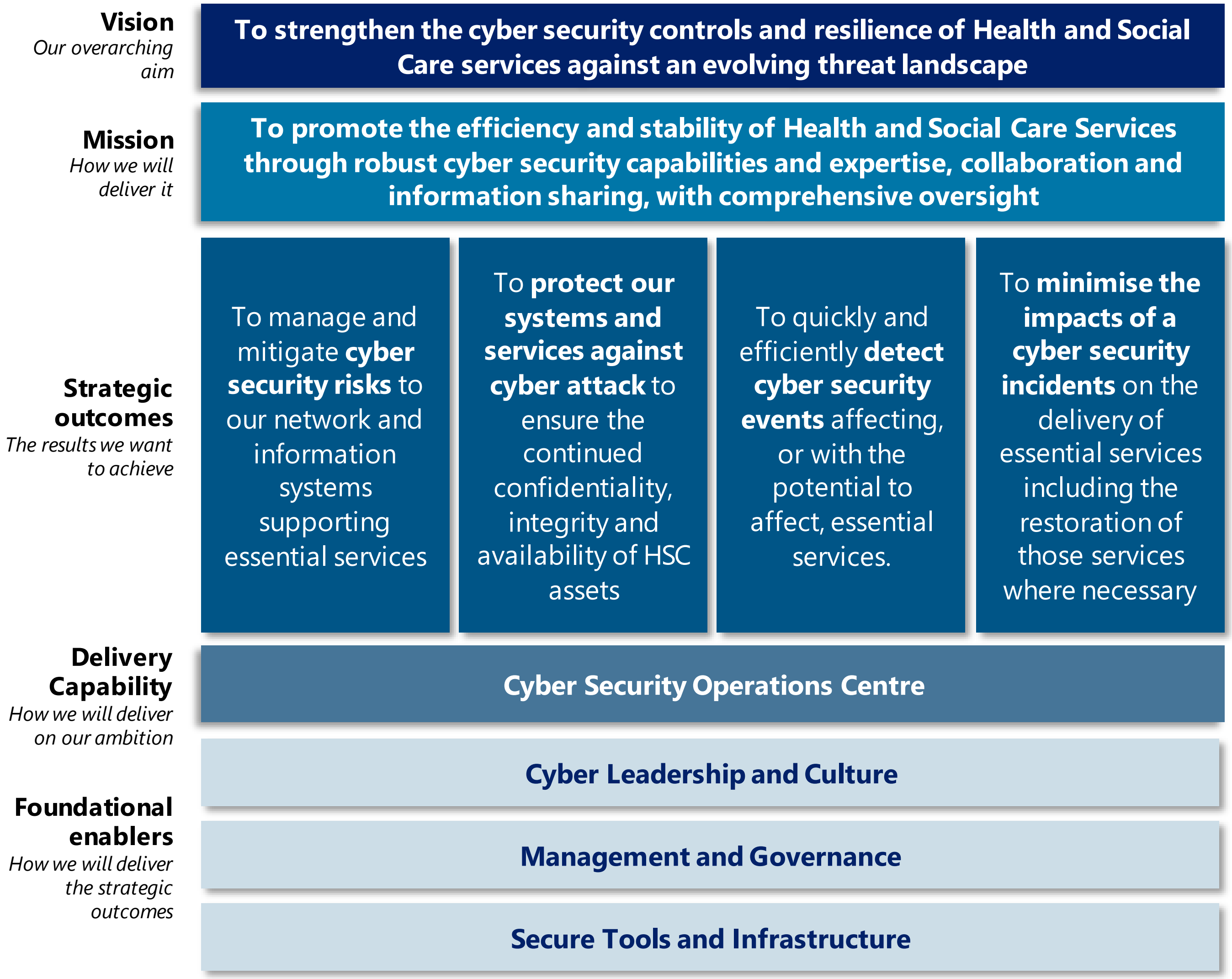
The Digital Strategic Outcomes	Cyber
Digital will provide the population of Northern Ireland greater visibility and control over treatment and care journeys	
Digital solutions will put quality and safety at the heart of all new processes, systems and ways of working across health and care pathways	✓
Effective and joined up care through systems integration and streamlined information flows	✓
Digital will enable our people to work more efficiently and collaboratively across standardised systems	
Intelligent use of data will optimise performance and harness population health insights, whilst ensuring robust data protection standards	✓
Digital will support the acceleration of research and innovation to gradually embrace system leading disruptive and cutting edge solutions	

Delivering the Cyber Security Strategy

How we plan to deliver on our ambition

Our Strategic Framework

We have established a cyber transformation journey that is underpinned by four strategic outcomes, to be delivered through supporting initiatives and relevant enablers. This strategic framework acts as a backbone to contextualise and ground the more detailed components of the cyber strategy, ensuring that our transformation is rooted at all times in our overall vision for cyber security at HSC.



Vision
Our overarching aim

To strengthen the cyber security controls and resilience of Health and Social Care services against an evolving threat landscape

Mission
How we will deliver it

To promote the efficiency and stability of Health and Social Care Services through robust cyber security capabilities and expertise, collaboration and information sharing, with comprehensive oversight

Strategic outcomes
The results we want to achieve

- To manage and mitigate **cyber security risks** to our network and information systems supporting essential services
- To **protect our systems and services against cyber attack** to ensure the continued confidentiality, integrity and availability of HSC assets
- To quickly and efficiently **detect cyber security events** affecting, or with the potential to affect, essential services.
- To **minimise the impacts of a cyber security incidents** on the delivery of essential services including the restoration of those services where necessary

Delivery Capability
How we will deliver on our ambition

Cyber Security Operations Centre

Foundational enablers
How we will deliver the strategic outcomes

Cyber Leadership and Culture

Management and Governance

Secure Tools and Infrastructure

Whilst our strategic outcomes *(page 16)* define what we will need to achieve in order to deliver on our vision and mission, our foundational enablers *(page 22)* outline how we will achieve them, through advancing the overall cyber maturity of HSC as an organisation. This will include a culture shift and strong cyber leadership in teams at all levels, alongside proper cyber governance processes and the tools, systems and infrastructure needed to secure our information and ensure continuity of services.

Our Strategic Roadmap

The strategic roadmap sets out our direction of travel and will allow us to target our effort and resources more effectively over the next ten years.

This roadmap prioritises low cost – high value efforts that will deliver cyber security improvements within the current funding landscape, enabling us to learn as we go and identify new methods and tools that enable us to get the most out of our investments. Resources will be focused on the implementation of key programmes and operations, followed by optimisation and innovation phases that will drive forward our cyber capabilities in the years to come. By developing this roadmap, we will be able to identify when new digital capabilities will be available and what we must put in place to enable the successful adoption of solutions for the people we serve.

Our Strategic Roadmap for Cyber

PHASE ONE IMPLEMENTING

We invest our time and resources in **implementing the key cyber initiatives and programmes** that will deliver security improvements to health and care services. This phase will also look to address a number of the capability and enabler requirements that will support implementation and set HSC up for the future phases.

PHASE TWO MAKING BETTER USE

We invest our time and resources in **making better use and improving** the security infrastructure, processes and systems that we have implemented. The lessons and momentum gathered during the Implementing phase is advanced and we turn our focus to developing new cyber skills and capabilities and building redundancy into our systems. Other programmes from the wider digital portfolio will have expanded the level of data and information we record onto our systems, which will require further cyber security intervention.

PHASE THREE INNOVATING

We invest our time and resources in **new and exciting technologies and initiatives** that will help us to protect our essential services from evolving cyber threats. In this phase, we have the right skills, capabilities and enablers in place to embrace new technologies and ideas, incubate them and scale across our portfolio. We will continue to implement and optimise solutions, but will rely on our history of successful cyber transformation and a strong change culture.

Box 1. Our three-phased approach to transformation
Our strategic roadmap is in line with the three-phased approach taken for our digital strategy. This is to ensure that our organisation-wide transformation efforts are co-ordinated and aligned to make efficient use of available resources and to facilitate cohesive systems and services for our H&SC staff and patients.

Cyber Security Operations Centre (SOC)

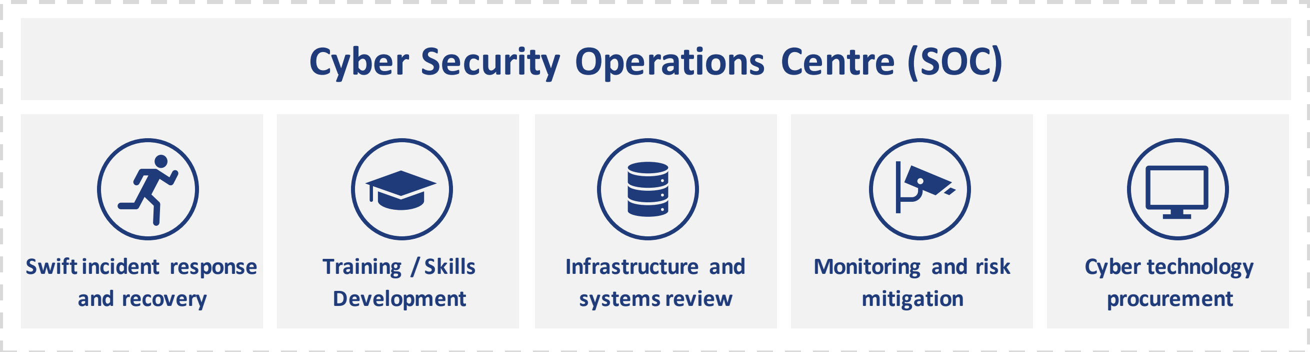
Our Cyber Strategy will be delivered in part via the development of a Cyber Security Operations Centre (SOC) to bring together the teams and tools required for effective, centralised monitoring of our cyber position at HSC

Why build the SOC?

Multiple, separate approaches to cyber security risk management have the potential to introduce gaps in our system. We must therefore continue to drive our 'Once for NI' agenda through the adoption of a single and HSC-wide view of cyber risk. We require a body that can centralise capabilities and make data driven, insight led security management decisions. The SOC will act as a hub for management and oversight of our security position, leveraging our internal cyber resources to support the optimisation of networks and information systems. As part of this, we will build collaborative cross-sectional cyber teams for skills sharing and contextualised decision making, including a built-in swift response function and clearly defined risk ownership and accountabilities. The SOC can be consulted to support other teams and organisations to strengthen their cyber protocol, through development of cyber skills and capabilities, tech and infrastructure procurement and recruitment/ hiring support.

How might this look?

The SOC will have dedicated functions in place to centralise cyber operations at HSC. One of these functions will facilitate the fast and efficient response to a suspected cyber breach, with the right skills and tools on hand to mitigate the effect of an incident. Further to this, the SOC will support education and cyber awareness in the wider HSC, with built-in cyber career pathways to upskill hub resources into the best cyber professionals. The SOC will conduct continuous review of our current and legacy systems to eliminate potential gaps and identify a potential breach as soon as possible. Finally, the SOC will support the procurement of further cyber software and support cyber secure system design for future HSC systems.



Cyber Security Operations Centre (SOC)

Swift incident response and recovery

Training / Skills Development

Infrastructure and systems review

Monitoring and risk mitigation

Cyber technology procurement

Diagram 1 – Functions of the SOC

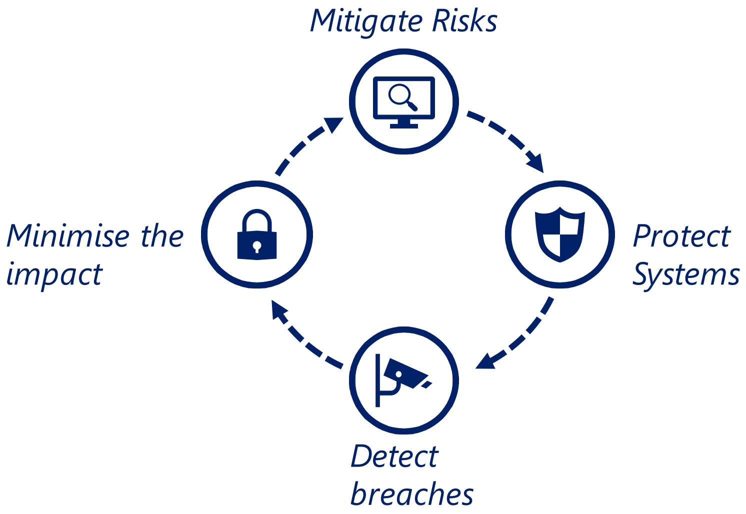
Our Strategic Outcomes

How we plan to deliver our strategy

Our Strategic Outcomes

The Cyber Assessment Framework is based on a four-objective security methodology to Manage, Protect, Detect and Minimise cyber security threats. We have based our strategic outcomes on these objectives; reflecting a 360° approach to information security and recognising the need for protection from all angles.

Our strategic outcomes will act as critical focus areas to help us build redundancy and fortify our systems to withstand the evolving cyber crime landscape. In doing so, we can maintain the trust of our population, enabling us to deliver better care for people and patients.



Our Strategic Outcomes

To manage and mitigate **cyber security risks** to our network and information systems supporting essential services

To **protect our systems and services against cyber attack** to ensure the continued confidentiality, integrity and availability of HSC assets

To quickly and efficiently **detect cyber security events** affecting, or with the potential to affect, essential services.

To **minimise the impacts of a cyber security incident** on the delivery of essential services including the restoration of those services where necessary.

The following sections will provide further clarity on each strategic outcome and describe the initiatives and relevant enablers that will help us to deliver against each outcome.

Strategic Outcome 1

To manage and mitigate cyber security risks to our network and information systems supporting essential services

In order to mitigate and reduce the risk of cyber attack to our systems and services, we must implement organisational structures, policies and processes that enable us to understand, assess and systematically manage security risks. We must develop and revise our governance and risk management framework to include to capabilities listed below.

How will we meet this objective?

Cyber Leadership and Culture

We must **revise and expand the cyber security training** that we are delivering to our leaders, so that they can drive best practice within their teams. We must train our staff at all levels to understand their **individual responsibilities** towards cyber security, including **raising awareness around potential risks** and methods of attack. On top of this, we can build **cyber accountability** through establishment of cyber specific roles and senior risk owners.

Management and Governance

Multiple, separate approaches to cyber security risk management have the potential to introduce gaps in our system. We must therefore continue to drive our **'Once for NI'** agenda through the adoption of a **single and HSC-wide view of cyber risk**. Building on this, a **cyber risk alignment exercise** must be carried out with respect to other business risks such as health and safety or financial governance, to ensure cohesion in all that we do. We will ensure proper enforcement of the ***need to know*** **and** ***need to hold*** **security principles** of sensitive user identity information.

Secure Cyber Infrastructure

We will implement tools and technologies that enable us to mitigate any potential risks to our systems. This will include **device access management and asset inventories**, user accounts and **account deactivation** and enhancement of **vulnerability management processes** across the organisation.

Strategic Outcome 2

To protect our systems and services against cyber attack to ensure the continued confidentiality, integrity and availability of HSC assets

The continued confidentiality, integrity and availability of HSC assets from cyber-attacks require us to implement proportionate security measures in the form of clearly defined systems and processes and 'best in class' protective security solutions.

How will we meet this objective?

Cyber Leadership and Culture

The proper and best practice usage of systems is key to their ability to keep data and information safe. As such we will **refine our current training programme** and ensure that actions across all network and information systems are **assigned to a responsible party**. Leveraging our skillsets to optimise networks and information systems, we will build **collaborative cross-sectional cyber teams** for skills sharing and contextualised decision-making. We will build **cyber champions** into teams at all levels to ensure system-wide cyber-aware culture.

Management and Governance

We will implement a **cyber security operations centre** to centralise monitoring and decision making, in order to ensure a unified view of organisational activities. We will conduct a **review of our system usage protocols**, including device authentication and application 'allow' policies, alongside ensuring adherence to **NCSC End User Device Security Principles**. Privileged access to systems will be consistently managed and monitored alongside the most up to date **multifactor authentication protocols** as standard across HSC.

Secure Cyber Infrastructure

We will continue to implement **network and host security measures** that provide and leverage near real-time blocking responses from the cloud - with **traffic scanning and data encryption** - and ensure advanced email and browsing protections to provide **verification** of links in emails and documents prior to granting access. We will ensure proper **backup protection** from ransomware or other forms of malicious compromise to support Mean Time To Recovery (MTTR) objective requirements.

Strategic Outcome 3

To quickly and efficiently detect cyber security events affecting, or with the potential to affect, essential services.

The time taken to respond to a cyber security breach directly affects the amount of damage that can be incurred. It is therefore essential that our detection systems are comprehensive and our security detection controls framework is well developed.

How will we meet this objective?

Cyber Leadership and Culture

We will ensure that our cyber professionals are trained in **emerging cyber threats** to enable them to more quickly identify warning signs and new types of attack. As part of this, we will ensure that all staff across the wider HSC ecosystem understand the **proper protocol for cyber attack reporting** and recognise the importance of responding immediately.

Management and Governance

We will implement a **cyber security operations centre** to ensure a holistic view of our information security systems, making it easier to **identify potential breaches** and accelerating the time taken to respond to new threats. The cyber security operations centre will house an **information security team responsible for monitoring** the organization's security posture and detecting and responding to cybersecurity incidents using a combination of **technology solutions and pre-defined processes.**

Secure Cyber Infrastructure

We will insure **alert protocols** are in place across all of our systems to **detect unusual access patterns** and other security events in order to limit unauthorised access to a user's data. The identification of users and their actions will remain **attributable to a single entity** for both accountability and traceability. The SOC will be responsible for **continued review of our systems and infrastructure** to identify and mitigate any single sources of failure.

Strategic Outcome 4

To minimise the impacts of a cyber security incidents on the delivery of essential services including the restoration of those services where necessary

Reducing the impact of a cyber security breach depends both on the speed of response and efficacy of the breach protocols that are in place to reduce the spread of a malware or its access to information. It is therefore essential that our systems are well prepared for a potential cyber attack event and service restoration can be achieved as quickly as possible.

How will we meet this objective?

Cyber Leadership and Culture

We will maintain a **dedicated on-call function** that can address and manage cyber security incidents with immediate effect, through cross organisation collaboration and response, as part of the **cyber security operations centre**. The people and personnel who form part of these teams will be properly trained in **breach protocol** that includes isolation of networks affected by the breach and efficient service restoration

Management and Governance

We will **test our emergency cyber protocols** frequently, to ensure our incident response is as seamless and efficient as possible. We will also **implement structures for the identification of necessary evidence** where required to support or refute legal action. Responsibility for minimising the effect of a cyber security incident will rest within the SOC, although an ecosystem-wide incident response is required to do this most efficiently.

Secure Cyber Infrastructure

We will act to reduce the effect of any cyber breach through **segmentation and segregation of trust networks** to include defined choke points for each entity, restricting movement of malware. We will ensure **effective sandbox protocols** are in place to provide effective defence against zero-day and known exploits

Cyber Enablers

What we need to help us deliver our digital strategy

Our Cyber Enablers

Successful cyber transformation relies on many things, from the leaders of the organisation through to the infrastructure that supports it. Establishing these foundational enablers is a critical component of the implementation process and will enable us to deliver on our stated vision and mission for cyber security at HSC.

Our three enabling categories outline the ways in which we will prepare for successful cyber transformation, addressing existing challenges and blockers to make it easier for people and systems to work effectively. For each of these categories, we have collated a set of commitments that will sit alongside our digital portfolio, supporting effective implementation.

Our Cyber Enabler Categories

Cyber Leadership and Culture

Management and Governance

Secure Tools and Infrastructure

Cyber Leadership and Culture

We will develop a culture that is fully cyber aware, from our leadership through to our front-line people. Our vision for a cyber aware culture starts with shared accountability for data security, with leaders advocating best practice and project teams integrating cyber considerations from the outset. Our people must invest time in their own cyber learning.

What does a strong Digital Culture and Leadership mean?

Leaders are ambassadors for cyber security awareness and integration

Our people invest time in understanding cyber risks and their role in data security

We feel secure in the knowledge that everyone at HSC is working together to keep systems secure

We work collaboratively to ensure that cyber security is considered from the outset of any programme implementation and built into projects by design.

Our Commitments

Targeted awareness training will be provided on key subjects based on prevalent compromise methodologies such as phishing, ransomware and social engineering

We will operate an open culture of security incident reporting, empowering our staff to understand the methodologies in place to facilitate this.

We will identify training requirements and needs relative to specific roles, reflecting a positive security culture across HSC organisations

We will foster a cyber culture that is agile and adapting to lessons learned to prevent the same issues reoccurring.

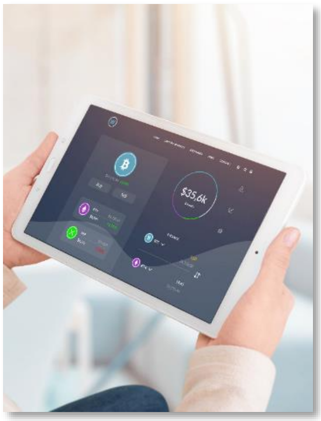
Individuals will be identified and trained to respond to an adverse incident impacting essential services

Changes to our cyber processes or operations will be effectively communicated to staff

We will attract cyber skillsets and talent through development of cyber career pathways as part of the cyber security operations centre.

Management and Governance

We will provide transparency for our people in how we manage and govern cyber security across HSC. Our vision for robust management and governance includes system redundancy, cyber security integration from the outset of all nascent programmes and an internal audit process that examines any existing risks and vulnerabilities. Importantly, our cyber security will be underpinned by well-defined pathways and processes that are standardised across HSC.



What does effective Cyber Governance mean?

Cyber is represented in all major forums and decision-making bodies across HSC

Our cyber security governance is transparent and provides assurance and clarity for how decisions on cyber investments are made

There is careful control over our portfolio and the decisions we make, with the right tools and systems to monitor performance against our objectives

Governance is open and accessible and balances the need for expediency with fair risk and control processes

Our Commitments

We will centralise responsibility and accountability for cyber security, to ensure a comprehensive 'single view' of security operations system-wide, with responsible parties empowered to make decisions regarding service protection

Risk management processes will establish a clear understanding of the threat landscape and any vulnerabilities

We will establish a dedicated business engagement process to strike a balance between clinical and cyber security risk considerations from the outset of new projects, with procurement activities in place to ensure that all risks are fully examined and mitigating controls are applied and working effectively.

We will implement clear governance structures with well-defined lines of responsibility and accountability for the security of network and information systems. We will support a more formal and structured approach to enable decision-makers at all levels to make informed cyber decisions, enhancing current practices and making cyber solutions easier to implement.

Where we rely on 3rd parties, we will ensure that all relevant security requirements are met, in adherence to the supplier framework, supporting robust information security from the outset of new supplier relationships.

We will implement effective forensic readiness planning and related response and recovery actions to ensure the relevance, sufficiency and timeliness of the information that we use to make our decisions.

Business continuity and disaster recovery plans will be tested and exercised on a regular basis, with systematic review following any incidents.

Secure Tools and Infrastructure

We must provide effective infrastructure and programmes for our people to do their jobs effectively. Our vision is that our staff can rely on the safety of stored information across our systems, accessible only to those who definitively require access. We will continue to deliver core programmes and improve data and information security for our community.

What does effective Infrastructure mean?

The hardware, software and tools we provide are fit-for-purpose and meet the needs of the users

There is confidence in the programmes and technologies we implement across our workforce

Systems are safe, robust and reliable – they are accessible at all times

Our Commitments

We will maintain a clear understanding of our service dependencies, including physical assets, software, data, essential staff and utilities. These will be clearly identified and recorded with any single points of failure or security risks mitigated.

Legacy technology will be managed to maintain clinical services, but minimising the potential impact of compromise to the wider HSC.

Our infrastructure will continue to facilitate the protection of sensitive data during transit (through network infrastructure and cryptographic means) with stringent information access control measures in place alongside regular back up data copy collection.

We will ensure stringent access authorisation and authentication processes are in place, with security protocols reflecting the proportionate risks to the service.

Our hardware will be well maintained and built to include additional contingency capabilities, with interfaces used for ICT administration subject to additional protections.

Network and information systems supporting the delivery of services will be designed with proactive security inherent within procurement and project requirements.

Next Steps: *2026 and Beyond*

The future of digitally connected health within the HSNI will give staff and the public access to approved technologies that can save lives without introducing risks to patient safety. The rapid pace of change in delivery models (including those enabled by 5G+, autonomous vehicles and drone technology and the ability to integrate robotic processed and AI into services) will present security challenges on a similar scale of change.

In securing the expanding Northern Ireland healthcare ecosystem, we will equally need to establish a singular vision and approach to both identifying and managing the inherent risks that existing and transformational technologies will present in the future.

Through the HSC Cyber Programme Board, we will continue to realise the promise of connected technologies through centralisation of monitoring and incident response functions and standardisation of security controls implementation and security risk management practices.

By developing and utilising the combined security intelligence and skills on a regional level, we will be better able to leverage digital technologies to diagnose, treat, communicate and administratively support superior patient care and outcomes, while protecting clinical systems, sensitive information and increasing our network resilience further.

HSC will continually develop an innovative cyber security strategy to address the risks faced by the public, staff and delivery partners whilst maintaining strong budgetary management through the realisation of benefits from collaborative and agile delivery methods.

> ***"The future state of cyber security risk management will thrive through combined risk visibility, skills sharing and tightly integrated collaboration across the HSC that will build on the strong security foundation of current practices and those initiatives implemented in accordance with the 2022-2026 strategy"***

We will continue to place citizens at the centre of cybersecurity through;

Seeking opportunities to deploy new technology that replaces legacy applications in order to reduce clinical and operational technology risks.

Establishing and maintaining the secure future state of the regional and cloud hosted Enterprise.

Centralisation of key security functions for coordinated regional management.

Standardisation of security products, tooling and associated processes.

Driving Enterprise Cyber Security Governance leading to the creation of a centre of excellence for information and cyber security within HSC.

Appendices

Glossary of terms

Term	Description
DHCNI	Digital Health & Care Northern Ireland
SOC	Cyber Security Operations Centre
Health Ecosystem	The entire health care system mapped out to include all the people and groups involved in delivering healthcare in Northern Ireland.
HSC	Health and Social Care
Cyber Assessment Framework	A Framework developed by the NCSC to provide a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible.
NCSC	National Cyber Security Centre
Quadruple Aim	A set of four key principles set out in 'Delivering Together' including; Supporting and empowering staff; Improving the health of our people; Improving the quality and experience of care; and Ensuring sustainability of our services
NIS	Network and Information Systems
CAF	Cyber Assessment Framework
OES	Operators of Essential Services