NATIONAL CYBER-SECURITY STRATEGY

2022 - 2027

Contents

Ministerial Foreword

The rapid increase in digital technology and services continues to transform the way in which we live our lives. Digital services and technologies connect us more easily to the rest of the world, but also connect the rest of the world to us. This presents both challenges and opportunities for the Island.

In this changing world we can no longer rely on some of the traditional protection provided from being an Island surrounded by the Irish Sea.

Central to the Government's Island Plan is the desire to build a secure, vibrant and sustainable future for our Island. The latest version of the National Cyber Security Strategy is aligned with this goal and has as its vision that the Isle of Man is considered a safe, secure and resilient place in the digital world.

This strategy sets out five priority areas to improve Cyber Security and builds on the previous strategy published in 2018. Whilst much has changed in the World since 2018 the key challenges of thriving and remaining safe in a digital world are still largely the same.

In publishing this strategy we recognise that the Government cannot improve Cyber Security in isolation and that partnership working with businesses and community groups will continue to be required if we are to achieve success. Raising awareness, improving resilience, fighting cyber-crime and playing our part in the wider global response is something we can all contribute to.

I hope that I will see you at a future CyberIsle Conference, to both update you on our progress and to hear experts educate us on how to keep safe in a digital world.

Hon. Jane Poole-Wilson MHK
Minister for Justice and Home Affairs

Executive Summary

Vision

The Isle of Man is considered a safe, secure and resilient place in the digital world.

Guiding Principles

This strategy establishes five pillars of action to deliver the vision. To do this will require a collaborative approach with all stakeholders, both inside government and across the private sector, working collectively in an approach that:

- Is open and accountable.
- Builds and maintains trust.
- Is people-centric, respectful and inclusive.
- Uses our collective strengths to deliver better results and outcomes.
- Balances risk to be safe whilst also being agile and adaptive.

Five Priority Areas

There are five priority areas of this strategy, each of which attracts its own actions and areas of activity. These will serve to improve the cyber-security posture of the Island and in turn allow the Isle of Man to operate in a safer and more secure manner in the digital environment.

- Safer and secure citizens in cyber space.
- Resilient and responsive digital Island.
- Education and skills for a safe, secure and resilient digital economy.
- Deter, detect, disrupt and respond to cyber-crime.
- Internationally responsible.

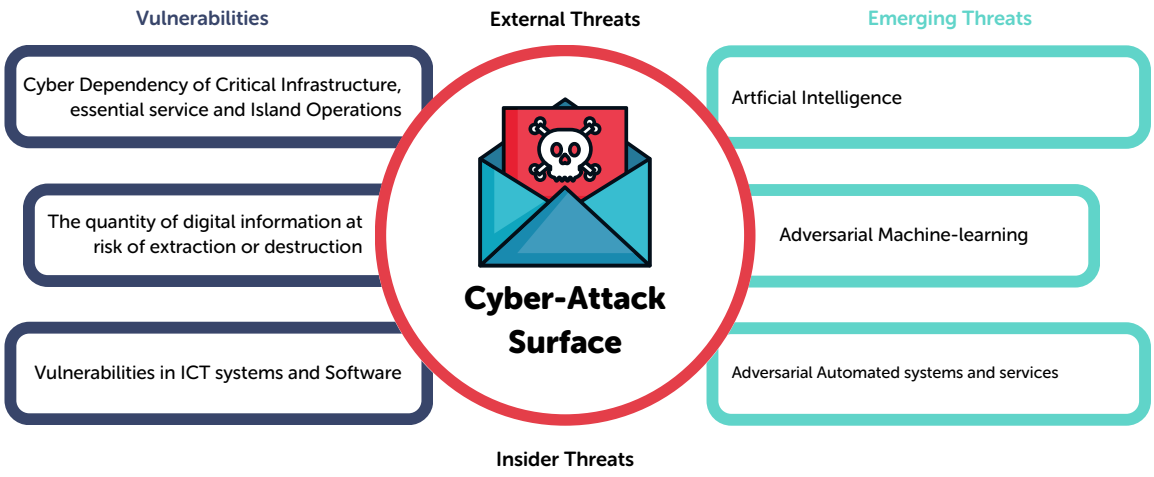
The Challenge Ahead

Cyber-enabled threats to our security continue to grow in number, scope and scale. Cyber-criminals, some of whom may be backed by hostile states, are now targeting the Isle of Man. Previously we have seen cyber-attacks indirectly impacting the Island but more recently we have seen them actively target Island companies and residents.

Regularly, we all see attempts to gain access to our personal information, bank accounts, intellectual-property and nationally important data or services. These attempts, some of which are successful, are not time-specific and can occur anytime; day or night. They often occur when we are least expecting them or even at times when the workload may be higher than normal, and time is critical. These are times when our guard may be down, or we cannot afford the time to check as thoroughly as normal.

From home-users to businesses, to government and critical national infrastructure everyone using the internet faces a constant and ever-evolving threat. The recent pandemic (COVID) has changed the way some of us work, with working from home (WfH) becoming a normal practice in some businesses. As a result, we saw the cyber-criminals evolve their attack techniques with phishing and spamming picking up themes like 'COVID' and 'Vaccination', as well as attacks being focused on WfH employees such as emails purporting to contain the Remote Working Policy or help desk support attempting to obtain information from the unsuspecting individual.

Constant vigilance and active protection of our sensitive data and systems is no longer an option. We need to all be AWARE, SECURE and RESILIENT to enable us to detect, respond and recover from any cyber related incidents or intrusions.



The rapid pace of technological change...

Cyber-incidents can vary greatly depending on the victim, the attacker's motive, the nature of the incident, the preparedness of the target and the subsequent response. In short, if you have undertaken some preparatory work, established a plan, keep the systems as up to date as possible and are able to identify / respond quickly the impact of any cyber-incident will be less.

Technologies are continually developing and evolving. As vulnerabilities are identified, fixes or patches are released and should be reviewed and installed as soon as practically possible. If for some reason a serious business risk prevents this course of action then measures should be considered to minimise any impact of that vulnerability being exploited.

This rapid pace of change serves to highlight the ever-growing need for us to be able to adapt and respond quickly.

The huge growth of Internet-enabled technologies collectively called the Internet of Things (IoT), which includes devices such as -

- Home Broadband Router
- Smart TV's
- Digital Assistant's (Google, Alexa, etc...)
- Refrigerators, Washing Machines, Dishwashers,
- Mobile Phones and Tablets,
- Doorbells,
- in fact anything that can connect to the internet,

can be at risk if they are not regularly maintained with security patches, fixes or even something as basic as having the correct security configuration.

As people become more informed about the risks posed to their computers and other digital devices, cyber-criminals will seek out new attack vectors and new ways to trick victims.

A real life example was in October 2016, when millions of IoT devices were taken over to form the Mirai botnet, which was used to launch a massive denial of service attack that disrupted the internet for almost the entire eastern United States.

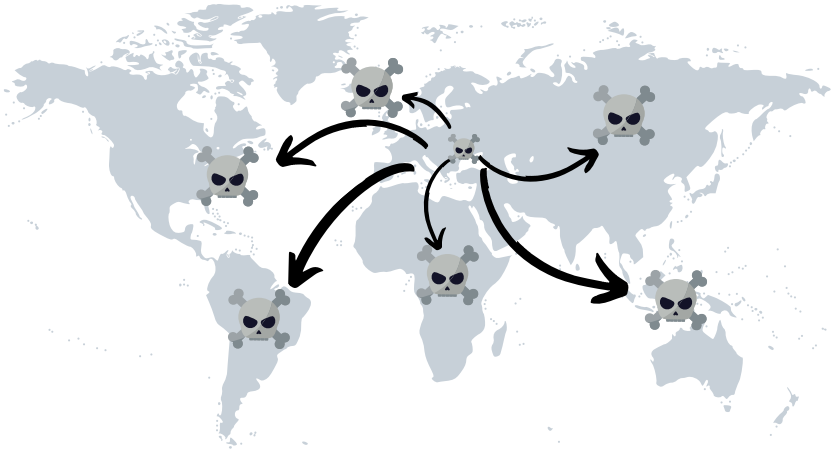
As can be seen, maintaining cyber-security is a complex problem. Previously, businesses and technology teams have considered cyber-security to be a technology problem and they embed those responsible within the technology teams and deploy technical solutions to remediate any identified risks. BUT it's not that simple - Cyber-Security is about people, policies, technology and trust.

An effective cyber-security regime will involve -

- Defining and implementing effective policies suitable for the business.
- Establishing a regular staff awareness regime and keeping it relevant to the business and threats posed.
- Deploying technologies commensurate with the business model and perceived threats.
- Ensuring systems and processes are regularly tested and updated as appropriate.
- Developing a culture of reporting suspicious activity.

It is not easy to keep pace with the change or even predict the pace of change. The emergence of Artificial Intelligence (AI) and Machine Learning (ML) are examples of a technological shift where the impact for cyber-security is largely unknown. The shift in mobile communications and the adoption of 5G may, in itself, bring with it potential issues or national security risks.

AND.... Not to be forgotten, cyber-attacks can also have unintended consequences: the 'Not Petya' malware initially only targeted Ukrainian entities but it ended up spreading globally to cause damage and disruption worldwide.



...the increase in threats and their sophistication.....

Cyber-crime is, unfortunately, a business and it evolves to serve its customers and identify new ways to make profits. The more sophisticated threat actors (cyber-criminals) will utilise their products to gain as much benefit from them as possible and then make them available for less sophisticated persons to purchase either the service or the product to use themselves.

As a result, the number of malicious actors seeking to do harm on the internet also continues to rise. Threat actors of all kinds are increasingly bold, brazen and disruptive. Locating themselves in jurisdictions where the legislation, government or enforcement capabilities are less effective or possibly even favourable to their activities.

As our economies evolve, becoming ever more digitised so more and more people use and do business on the internet, the payoffs from cyber and cyber-enabled crimes will also increase, attracting greater numbers of cyber-criminals.

Almost every cyber-attack is a criminal act, regardless of who is behind it or where they are situated.

Case Study 1: WannaCry

The WannaCry ransomware spread across the globe in May 2017 in one of the most disruptive cyber-attacks seen to date.

WannaCry affected over 200,000 computers in at least 100 countries. The United Kingdom's National Health Service was particularly badly affected, with systems down in hospitals across the United Kingdom, forcing the cancellation of nearly 20,000 hospital appointments. The attack also affected major companies, including French car manufacturer Renault and international shipping company FedEx.

In December 2017, the United Kingdom, USA and other countries publicly attributed the WannaCry attack on the DPRK (Democratic People's Republic of Korea aka North Korea).

… So, we must be ready and equipped to deter and respond accordingly.

The Isle of Man is a Crown Dependency by definition and whilst it is independent in regard to domestic legislation and activities, the Island is reliant upon the United Kingdom for its defence and national security. In this regard it needs to be responsible for its behaviour in cyberspace, an advocate for international oversight to ensure a stable and peaceful online environment, and leverage relevant support and assistance from the United Kingdom as required.

The Isle of Man must be ready to deter and respond to cyber-threats when they arise. As, globally, nations improve their cyber-security so the threat actors will seek out new vulnerabilities and opportunities. The Isle of Man must stay at the forefront of these changes if we are to maintain our status on the world stage and a place to do business.

The ability, afforded by the internet, of being able to commit crimes from the other side of the world, with the belief that there is an element of anonymity is a major factor in the rapid growth of cyber-crime. As a result the Island has no choice but to act and attempt to erect barriers against these threat actors, whoever they are.

The challenges with cyber-security are multi-faceted and diverse. The challenges for a home user compared to that of varied and different sized businesses are not the same, although some very simple actions might form a common approach. What is clear is the need for the population of the Isle of Man, individuals, government and businesses to have trust and confidence in the internet and our digital infrastructure. This is vital for the Isle of Man to continue to flourish by evolving our economy and attracting new business.

What Have We Done So Far?

The Isle of Man issued its first National Cyber-Security Strategy in 2018, shortly after the Council of Minister's directive had established the Office of Cyber-Security & Information Assurance (OCSIA).

OCSIA was charged with delivery of the strategy and in order to do this the strategy was distilled into its core objectives and deliverables. These core objectives and deliverables were then used to develop a mission statement.

Since 2018 the office has undertaken annual cyber-security surveys attempting to benchmark awareness across the Island. The first such survey identified a lack of understanding in how to report suspicious cyber activity such as spam emails, phishing attacks and social media account takeovers.

Cyber Concerns Reporting Service

OCSIA had already started to develop a reporting portal and the issue identified in the survey informed the creation of a public reporting point for cyber issues or concerns with the option to make a report to the Police at the same time. This portal has seen steady growth in reports which has resulted in the prevention of funds being lost by partnership working across OCSIA, the Police and the banking industry.

The reports received into the portal are reviewed regularly and where there appears to be a campaign targeting the Island or something of particular concern is seen, warnings and advisory notices are produced for dissemination through mailing lists, social media accounts and the OCSIA website. Equally, when particular security patches or fixes are released, a communication will be sent out.

Case study 2: UK Scammers arrested after targeting Island Pensioner

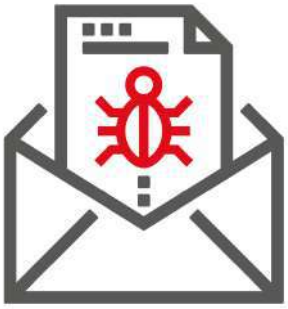
A recent example saw a local resident narrowly avoid losing £6,000 to scammers in the UK. The 76-year-old woman was duped into sending cash to Northampton after engaging in a phone call with the criminals who managed to convince the victim her bank account was compromised. The criminals encouraged the victim to take out £6000 cash from the bank and send it via post to an english address, whilst at the same time destroying tracking information.

Thankfully the victim kept her tracking details and as her suspicions grew she contacted the Office of Cyber-Security and Information Assurance (OCSIA) with her concerns. As a department we fast tracked an investigation liaising with our colleagues in the Isle of Man Constabulary who then linked up with officers in the UK to conduct an interception of the funds. Undercover officers were able to arrest four people in Northampton before funds reached the criminals and the cash was returned to the victim in full.

Suspicious Email Reporting Service (SERS)

Another OCSIA delivery during this period has been the development of the Suspicious Email Reporting Service (SERS). More information about SERS can be found on our website. WWW.OCSIA.IM.

The SERS service allows for SPAM emails and phishing emails, which have not resulted in the recipient becoming a victim, to be sent to a specific mailbox - sers@ocsia.im - from where they are examined, and any intelligence contained within them stripped out and used to disrupt the criminal ventures behind them. The systems behind his service provide intelligence to the UK National Cyber-Security Centre (NCSC) and National Crime Agency (NCA) from where actions are taken to block unwanted emails, IP addresses, phone numbers and bogus websites.



6844

emails have been reported since SERS launched in 2020

96%

of respondents* have received a fraudulent email.

*Refers to respondents from our cyber-security awareness survey.

16th August - 13th September 2021.
Issued by the Office of Cyber-Security and Information Assurance.

Case study 3: Social engineering is one of the most used techniques amongst cyber criminals.

A local example saw a senior business leader targeted with a 'phishing' email and an attachment which, when opened, the recipient was encouraged to log in and review the document. The target opened the attachment - which was bogus - and resulted in their online email account being compromised. This compromise led to several emails being sent from the mail account in the victim's name with further bogus attachments whilst at the same time the company's technology team saw large numbers of attempts to brute-force attack other staff members accounts. Whilst we are not aware of any financial loss as a result, several other local businesses also had compromised email services all of which required downtime, disruption and costly technology service interventions.

It was fortunate, in this case, that there was no known loss of funds or business data. It does, however, show just how easy it is for these attacks have an impact and how, as a result of a success in one organisation a number of others can also easily be impacted. In this case the impact, to the best of our knowledge, was in business systems downtime and the cost of the technical resources to remediate the issues.

CyberIsle

In 2019, OCSIA organised their first free for anyone to attend one day cyber conference at the Villa Marina in October, coinciding with internationally recognised Cyber Month.

The conference, called CyberIsle, was supported by businesses through sponsorship or rental of trade stands resulting in the conference being both free to attend and not impacting government budgets. In 2019, the conference attracted over 350 attendees and ran with the theme 'AWARE' intending to raise Island awareness to cyber-issues and how to protect yourself.

The conference was in planning for 2020 when COVID struck. Quickly the conference was evolved into an online collaboration using recorded presentations from government and industry specialists delivering to the theme of SECURE. This time, the online video content was spread over 2 sessions a day from Monday to Friday.

Fortunately, in 2021, the conference was able to proceed as an actual event. Again, the Villa Marina was the venue for the day, and it ran with the theme of being RESILIENT. With an increasing likelihood of some form of cyber-attack occurring for Island residents and businesses, the conference theme was 'not if, but when' a cyber-attack would occur. Over 300 attendees were given examples of attacks and advice on how to reduce the time taken to recover.

Additional to these activities, OCSIA has collaborated with the Police to develop cyber training for staff and officers, established industry sector specific information exchanges for Critical National Infrastructure (CNI IE), Financial Services (FS IE), and Senior Information Risk Officers (SIRO) across central government.

The Island's Strategic Direction

The NCSS has a responsibility to the whole Island which includes government. It is important that the NCSS complements' the other government strategies and delivery is harmonised in the 'One Government' principles of "Our Island Plan".

Our Island Plan

Building a secure, vibrant and sustainable future for our Island

National Cyber-Security Strategy

The NCSS has been reviewed and updated to build on the previous strategy issued in 2018. The NCSS aligns with the Island Plan objective that Island residents and businesses can access support and guidance to help keep them safe online and have access to a secure digital infrastructure.

Isle of Man Government

Our Vision

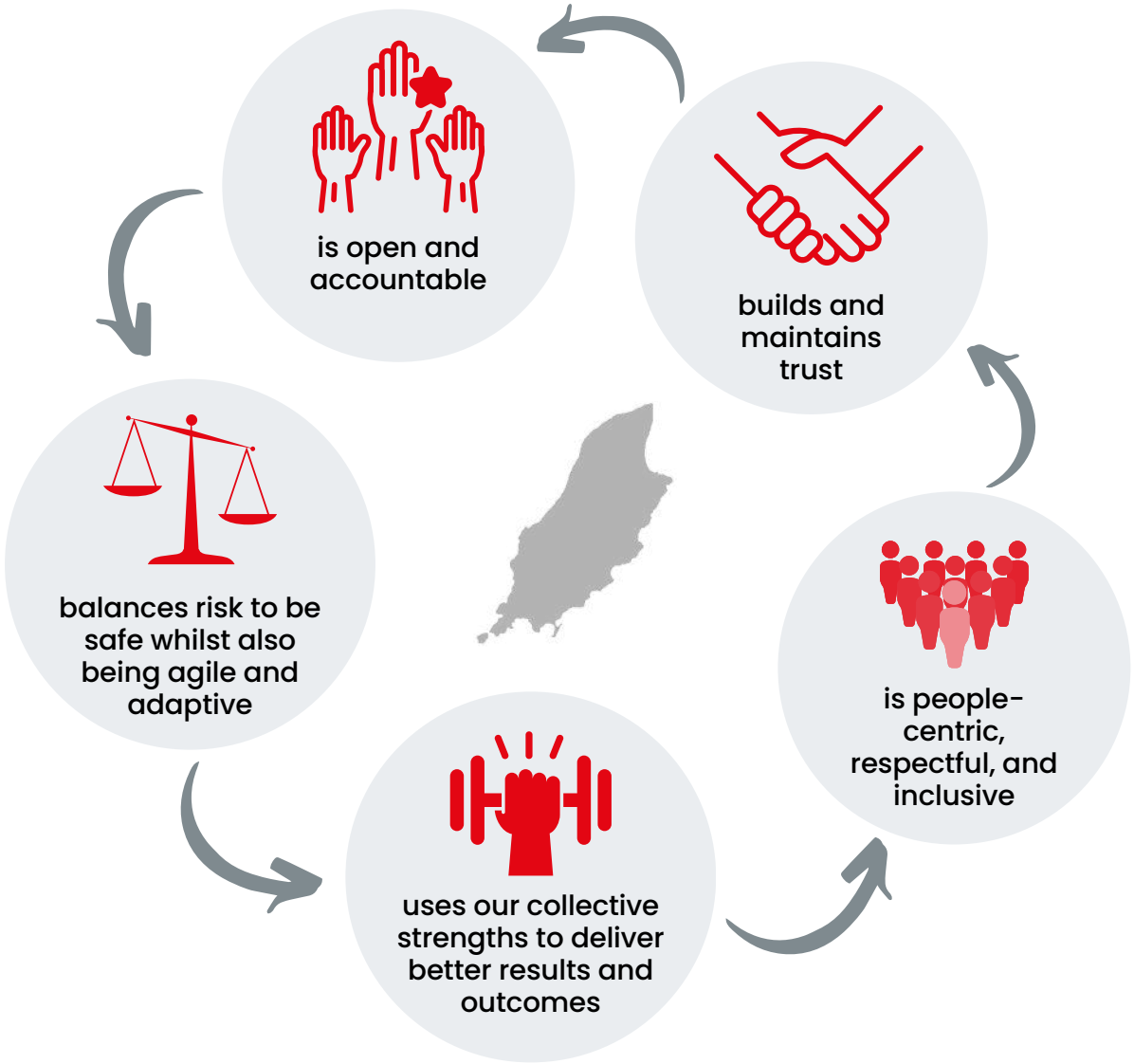
Is the Isle of Man is considered a safe, secure and resilient place in the digital world:

This strategy and its vision are about enabling the Isle of Man to thrive online whilst being safe, secure and resilient. We want the Island's people and businesses to make the most of the opportunities offered by a digitally connected world.

Whilst digital connectivity brings risks, actions can be taken to mitigate or minimise those risks.

Guiding Principles

This strategy establishes five pillars of action to deliver the vision. To do this will require a collaborative approach with all stakeholders, both inside government and across the private sector, working collectively towards the vision and in an approach that -



Cyber-security is not a problem government can fix on its own. We need to work together, to provide a safer digital environment for the Island.

Our Five Priority Areas To Improve Cyber-Security (2022–2027)

There are five priority areas of this strategy, each of which attracts its own actions and areas of activity. These will serve to improve the cyber-security posture of the Island and in turn allow the Isle of Man to operate in a safer and more secure manner in the digital environment. There is no doubt that the cyber-security landscape will continue to evolve driven by new technologies together with new risks and opportunities emerging. Predicting the future in this fast-paced digital environment will not become any easier and this makes the Island's ability to quickly adapt, respond, change and collaborate all the more important.

An annual programme of works will be developed from this strategy. This programme will outline the actions required to deliver to each of these five priority areas, identifying those areas of Island life which need to be involved and collaborate to achieve the annual goals with, where appropriate, lead government departments and theme owners responsible for reporting and delivery of that priority area.

- ☑ Safer & secure citizens in cyber space
- ☑ Resilient & responsive digital Island
- ☑ Education & skills for a safe, secure & resilient digital economy
- ☑ Detect, deter, disrupt & respond to cyber-crime
- ☑ Internationally responsible

☑ Safer & secure citizens in cyber space

If we are to have a safer & secure presence in a digital world we must equip our citizens appropriately and this starts by making them aware of how to use the technologies safely, identify potential risks and to minimise the impact of cyber issues. The work will focus on;

- Building on the work of the previous strategy - providing practical, targeted and regular awareness communications across different parts of society.
- Enhancing the methods of reporting cyber-incidents and the mechanisms from which support can be obtained.
- Continuing to make available and expanding educational tools and support systems to equip citizens to become safe and secure online.
- Increasing efforts to educate the cyber-vulnerable members of society, such as the elderly and children to reduce / prevent victimisation.
- Maximising communication of threats and issues to improve understanding and awareness of the cyber-threats and vulnerabilities impacting society.

☑ Resilient & responsive digital Island

A core activity of cyber-security is to develop an ability to be resilient to cyber-issues and this comes hand in hand with the abilities to identify and respond. The resilience of the Island will depend on the ability to identify the issue and then act promptly and effectively (the response). To react effectively requires the skills and tools. This area of priority expands from building a resilient critical national infrastructure to being able to respond to cyber incidents across the Island.

The wider focus of this priority will include

- Priority protection of the Island's critical national infrastructure (CNI).
- Supporting businesses and society in being protected and resilient against major cyber-incidents.
- Deploying cyber-tools and developing partnerships in the interests of the Island, including national security and law enforcement.
- Supporting CNI sectors and ensuring they take responsibility for the security of their systems and services.
- Improving the information security capability, risk management and resilience of the public sector.

Education & skills to support a safe, secure & resilient digital economy

As the Isle of Man and its economy becomes ever more reliant on digital services and information so an increasing reliance on a cyber-capable workforce, able to prevent, adapt and respond to threats as they develop will be required. This priority area will focus on;

- Developing and delivering an education curriculum that equips our students for employment in a digitally enabled environment and workplace.
- Incentivising and increasing the supply of skilled cyber-security people.
- Supporting the expansion of roles and opportunities in cyber-security .
- Encouraging the growth of the cyber-security industry on Island.
- Supporting industry and professional organisations to promote responsible management of cyber-security across workplaces.
- Promoting the adoption of cyber-security best practices in the workplace.

Detect, deter, disrupt & respond to cyber criminal activity

The criminal elements of society will continue to commit crime and the digital environment is no exception. The evolution of these crimes is likely to impact ever more severely, and the disruption and costs are likely to be proportionate. The Island's response needs to accept this and meet the challenge. The Isle of Man must proactively and collaboratively prevent, investigate, deter and respond to cyber-crime, cyber-enabled crime and terrorist use of the Internet.

Key areas of focus will include

- Preventing cyber-crime particularly against vulnerable groups.
- Increasing support for people affected by cyber-crime.
- Encouraging the reporting of cyber-crime.
- Improving the sharing of information about cyber-crimes.
- Improving information-sharing between law enforcement and the financial sector to reduce victims and impact.
- Seeking to have fit-for-purpose legislation enabling responsible agencies to better manage and respond to cyber-crime.
- Increasing our capability to respond to objectionable material and terrorist activity online.
- Investing in skills, people and resources to combat cyber-crime and cyber-enabled crime.
- Seeking agreement to accede to the Budapest Convention on cyber-crime.

☑ Internationally responsible

The Isle of Man's interests on the global diplomatic stage will be advanced and protected through our relationship with the UK but that does not mean we will be a silent partner. The Island will continue to champion a free, open and secure internet as far as reasonably practicable.

We will respond to unacceptable behaviour in cyberspace, and we will co-operate with others to prevent and deter malicious activity that threatens peace and security.

The Island will seek international engagement on cyber-security issues to -

- Build prioritised partnerships and co-operation at policy and operational levels.
- Prevent, detect, deter and respond to malicious behaviour online.
- Secure our environment and support our international neighbours by strengthening regional capability, confidence, and operational co-operation including law enforcement.
- Contribute to the Island's economic growth.

Glossary

5G technology - 5G is the 5th generation of mobile technology. It is likely to bring higher rates of data transmission, reliability, and connectivity.

Artificial intelligence - A computerised system capable of simulating human decision making and learning, including performing cognitive functions associated with the human mind including learning and language.

Credential harvesting - Collecting legitimate users' usernames and passwords to gain access to target systems, for malicious purposes.

Critical National Infrastructure - Processes, systems, facilities, technologies, networks, assets and services essential to the nation's health, safety, security or economic well-being and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence.

Cyber-attack - Deliberate exploitation of information systems to cause harm.

Cyber-incident - An event, whether intentional or not, that causes adverse consequences to an information system or its data.

Cyber security - Protecting people and their computers, networks, programs and data from unauthorised access, exploitation, or modification.

Cyber-terrorism - refers to the use of the Internet to carry out violent acts that either result in or threaten loss of life or significant bodily harm. The primary objective of cyberterrorism is to achieve political or ideological gains through threats or intimidation.

Cyber-crime - Crimes that are committed through the use of computer systems and are directed at computer systems. Examples include producing malicious software, denial of service attacks, and phishing.

Cyber-enabled crime - Crimes that are assisted, facilitated or escalated in scale by the use of technology. Examples are cyber-enabled fraud and the online distribution of child exploitation material.

Cyberspace - The internet and everything connected to it – the global network of interdependent information systems, telecommunications networks and information technology infrastructures.

Distributed Denial of Service Attack (DDoS) - A cyber-attack that stops users from accessing a service or resource, by overloading that service with requests.

Encryption - The transformation of otherwise readable data into a form that conceals its original meaning, to prevent it from being known or used. Strong encryption is a fundamental element of good cyber security, which is increasingly critical to Isle of Man national security and economic prosperity.

Hacktivists – Despite the absence of 'cyber' in their title, these hacker activists deserve a mention in our glossary. Hacktivists are computer hackers that have aligned themselves with a specific protest organisation or group of activists. Their activities can be similar to those of cyber terrorists or cyber-saboteurs.

Information Communication Technology (ICT) – refers to technologies that provide access to information through telecommunications. It is similar to Information Technology (IT), but focuses primarily on communication technologies. This includes the Internet, wireless networks, cell phones, and other communication media.

Information Security - The preservation, confidentiality, integrity and availability of information; other properties such as authenticity, accountability and non-repudiation may be involved.

Internet Service Provider (ISP) - An Internet Service Provider is a company that provides a service allowing business or personal users to access the internet.

Intellectual Property (IP) - According to the World Intellectual Property Organisation, intellectual property (IP) is a creation of the mind. IP includes inventions, literary and artistic works, designs and symbols, and names and images used in business

Internet of Things (IoT) - The interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data.

Malicious software/ malware - Software designed to infiltrate or damage a computer system. Examples include computer viruses, worms, Trojans, spyware, and adware.

Phishing - Using fraudulent emails to persuade people to reveal confidential information, such as login or banking information.

Quantum Computing - Whereas a classical computer works with ones and zeros, quantum computers have the advantage of using ones, zeros and "superposition's" of ones and zeros. This means they can perform calculations at a far greater rate than classical computers.

Ransomware - A type of malicious software that locks up the files on an information system until a ransom is paid.

Software - The programs used by a computer, as well as other information that it relies on to operate.

Isle of Man Government point of contact:

Office of Cyber-Security and Information Assurance (OCSIA)

2nd Floor
Former Lower Douglas Police Station Fort Street
Douglas
Isle of Man
IM1 2SR

www.ocsia.im
Cyber@gov.im
+44 1624 685557