Isle of Man
Government
Reiltys Ellan Vannin

Isle of Man

NATIONAL CYBER SECURITY STRATEGY

2018-2022

GD 2018/0029

Contents

CYBER ATTACK

Foreword

Hon. Howard Quayle MHK
Chief Minister

The world is seeing continued threats to cyber security by means of phishing, malware, ransomware and other devious malpractice. In this respect the Island is no different from any other nation. The Isle of Man is an internationally respected and trusted Crown Dependency, with a long history of providing a stable, reliable and secure platform that enables economic prosperity. We must ensure that it remains so. Our reputation for security has become even more significant in this new, digital age. Our Island has an important role to play in the rapidly changing global economy and we have always stepped up and adapted accordingly. As a Government, we are here to support the prosperity of our Island. Our main business sectors operate in the digital world and we must ensure that we stay highly connected and provide an environment where e-commerce is able to operate with minimal constraints, interruptions and insecurities.

Private individuals too must feel confident that all necessary steps are being taken to keep their information and digital lives as secure and protected as possible. My Government fully supports this strategy as it takes us forward. As Chief Minister, in endorsing this strategy, I am determined to see it brought to life for the benefit of the residents of the Island and all those businesses which operate here.

Will Greenhow
Chief Secretary

One of my roles, as head of the Isle of Man Government's Civil Service, is to ensure that the public service continues to transform its services into more efficient, digital ways of working. This was a primary aim of our digital strategy, launched in 2016. We are increasingly dependent on technology in all aspects of our lives and we must ensure that while providing digital services to business and the public they are as safe, secure and reliable as possible.

Our focus is now on the provision and application of cyber security, and this strategy starts us on that vital journey. It requires the Government to ensure that the data it holds is secure and is held in accordance with legislation; it requires that our national infrastructure is protected and resilient; and, in the unfortunate event of an incident, it ensures that we have the appropriate plans and processes in place to rapidly restore operations with minimal disruption. That's why I fully support this strategy and look forward to seeing it in action.

Executive Summary

The Isle of Man has an excellent digital infrastructure. We are able to exploit the benefits that a good network and a well-developed internet service can bring for commerce, for public services and for citizens as individuals. However, these benefits could be put at risk if we do not protect ourselves effectively against cyber-attack. We are already plugged into international efforts to combat cybercrime, including the UK's cyber resilience initiatives. But we cannot always rely on others to defend the Island's commercial resources or protect the personal and financial data of our citizens.

This National Cyber Security Strategy explains what we must do for ourselves. The Government has made it clear that cyber security is one of its top priorities. There will be an initial financial outlay to strengthen our defences and this will be money well spent. The benefits will be enhanced protection for all our residents and the development of new businesses.

The first section of this strategy document explains the nature of the challenges we face. To date the Isle of Man has been fortunate to have faced few cyber-attacks and to have had sufficient resource to defend our systems. However, we are aware of threats, vulnerabilities and risks, which are set out here in detail.

A key aspect of our cyber defences must be to maintain the Island's Critical National Infrastructure. It includes our ports and harbours, our Internet Service Providers, water and sewerage, electricity, gas and oil supplies. The Government will actively support the protection of these systems and capacity for recovery in the event of a cyber-attack.

Emergency Planning and Business Continuity exercises will be adapted to encompass cyber security incidents on a larger scale. The government is also undertaking a detailed analysis of the relevant global legislation and standards for cyberspace, data management and information assurance. It is committed to compliance with international standards that enable our businesses to operate in foreign markets, whilst ensuring that data is secure and protected here on the Island. That will include adopting the EU's General Data Protection Regulation into Manx law by the end of May 2018.

In a statement of strategic intent, this paper declares there can be no excuses for failing to take cyber security seriously. Across the developed world, businesses that did not secure their customers' personal details against theft by hackers have suffered massive reputational damage. The Isle of Man is fortunate to be afforded fundamental levels of protection by the United Kingdom in a number of areas. However, due to the Island's independence and separation from the UK, it falls to us to defend our own digital space.

The strategy sets out four principles for action between 2018 and 2022.

1

Committed leadership by Government to achieve resilience

Through the leadership of the Chief Minister and the Chief Secretary, the Government will ensure the strategy is fully implemented, working together with key partners to provide a solution which meets our national needs.

2

Support for Critical National Infrastructure

In protecting the Island's way of life, its commercial productivity and its economic prosperity, the Government will work across both public and private Critical National Infrastructure (CNI) providers to ensure that services are maintained, are as resilient as is practicable and are able to recover quickly following a cyber-incident.

3

Strong collaboration with business to achieve prosperity

In delivering a cyber-resilient Island, it is essential that Government works alongside businesses and the public mutually and respectfully. The Government will deliver the services and support required whilst ensuring that the rights and values of all are respected. All activities will be undertaken as transparently as possible to ensure all solutions are fully understood.

4

Everyone playing a part in a progressive society

Cyber security and resilience is a shared responsibility. By working together we can ensure that businesses and residents are informed, supported, educated and have the appropriate measures to protect against attacks and have the support to call upon if an incident occurs. By sharing these responsibilities we help to create a society which is well-equipped to deal with the challenges of the future.

Attached to each of these four principles are a series of strategic goals and detailed policy objectives. This builds up into a programme of 27 objectives that will be turned into an action plan over the next three months.

Tracking progress, defining success and tackling the obstacles to delivery will be essential. There will be routine quarterly reporting to the Council of Ministers and Government's Chief Officers' Group to ensure that strategic oversight is maintained and leadership is provided.

An annual review will be undertaken by the Chief Secretary to ensure the strategy, in its entirety, remains relevant and delivering the outputs required at the pace needed.

The document concludes with suggestions for measuring how well the strategy is succeeding and a description of the three aspects of effective cyber security. The watchwords for the Isle of Man will be: Aware, Secure and Resilient.

Introduction

Our society is fully digitally integrated, primarily through the internet and mobile devices. We are fortunate here on the Island to have a network and internet service that is highly developed in comparison with many other locations. Nevertheless, as an independent nation we need to ensure that we apply the right levels of protection and security to the way we operate in the digital environment. We are all aware that cyber-attacks pose a significant risk to the Island's security and safety. There are risks to our infrastructure and to Government data holdings; there are risks to our residents' personal and financial data; and there are risks to our economic stability and prosperity. These threats are always evolving and adapting and we must do our utmost to remain up to date and ready to counter them. The Government's systems and processes are being reviewed continuously to enhance detection and provide better protection, but they need to be constantly adapted, refreshed and renewed to make sure they are giving all of us the protection we need.

This strategy has been developed to address the risks faced by businesses, those in the voluntary sectors, the public sector and residents. We need the implementation to be resilient in maintaining productivity and sustaining the Island's way of life, whilst making the Island the location of choice for business. Its development will be continuous and implementation of the national cyber security programme will take place carefully, step by step. The strategy team have been working hard to develop new structures both inside and outside Government to ensure a collaborative approach to a common threat. These committees and working groups have been designed to find solutions to near-term issues as well as look in to the future to understand what challenges may lie ahead.

This is a long-term programme of major change that needs resources, budget, focused political will and national-level leadership. The Government's competing economic constraints are evident. However, the benefits and opportunities that this strategy can deliver far outweigh the costs. This strategy comprises a number of strands that take account of these external factors and offers levels of protection in line with the evolution of risks and threats.

There are opportunities that will arise for the Island as a whole as the strategy delivers, including cost savings, efficiencies and service improvements. Ultimately, the Island will afford a level of protection for all its residents and support the attraction of new businesses. But there will be an initial outlay to improve, certify and install solutions and services. The Government has made it clear that cyber security is one of its top priorities and that it is to be delivered and implemented as swiftly and efficiently as possible.

We are committed to working in partnership with other nations and with our own industry and businesses. We have an interesting and busy time ahead. This strategy will be of huge benefit to the Island and to everyone who lives and works here.

Richard Wild
Executive Director, Government Technology Services (GTS), Government – Senior Information Risk Owner

The challenge we face

The impact of cybercrime, cyber-attacks and wider cyber-incidents on the Island could be disastrous and have long lasting ramifications. We are all reliant on digital communications with the vast majority of activity underpinning our everyday lives and the way our businesses operate. This is evident as digital business operating from and on the Island grows year on year. Residents are using the internet more and more in support of their lifestyle and consumption of products and services. The risks are variable and the impact can range from minor inconvenience to major disruption. They can't all be removed, but with appropriate measures, systems, processes and technology they can be managed and reduced in probability and impact.

Why do we need a National Cyber-Security Strategy?

Information and data are essential and highly valuable commodities. We need to ensure they are safely, securely and appropriately managed and handled. The digital world impacts all of us in so many ways: how we shop, how power is delivered to our homes and how businesses operate. New technologies are released daily, with items and components that utilise the Internet of Things (IoT). So there is a requirement for Government to do its utmost to make secure the spaces in which we all live and operate.

The Island is interconnected globally across the digital space. This has removed the traditional barriers of physical space and time; it has transcended the legal boundaries of nations; and now digital transactions are almost instantaneous to any part of the world.

To date, the Isle of Man has been fortunate to have faced few cyber-attacks, and to have had sufficient resource to defend our systems. However, with the Government's aspiration to further the Island's economic prosperity and its reach across global markets, we must now review our position on cyber security. We must develop a co-ordinated and tailored approach to those risks and threats that the Island may encounter, and mitigate potential vulnerabilities.

The Island does have well-established Unique Selling Points (USPs), but they remain at risk of loss or erosion in a potentially fickle digital business market. In order to maintain these advantages and meet the ever-growing levels of global data transactions, we must ensure the island is safe, secure, and resilient in cyberspace. The Government sees its priorities as protecting relevant data, sustaining investment and ensuring the continued reliable functioning of information and communication technologies.

What is Cyberspace?

Cyberspace is the digital world in which we operate. It is made up of interconnected networks that enable information to flow globally. It comprises our Information and Communications Technology (ICT) networks, our communications systems and those systems that support our infrastructure. It is essentially the virtual environment that enables interactions between people and machines, including computer networks.

What is Cyber Security?

In delivering Cyber Resilience we need to implement a range of cyber security measures. Some of the most important cyber security measures involve education and awareness. By ensuring that all concerned understand how to mitigate and manage those risks and are aware of the wider issues, we will bring our digital security one step closer.

What is Cyber Resilience?

Cyber Resilience is the ability to protect against and recover from attacks or accidental events that impact our digital world. When ensuring resilience, Government, businesses and residents need to act together. It is not purely about ICT or technical solutions. The human aspects of cyber resilience need consideration and measures should be put in place to ensure everyone understands the risks. Individuals are best placed to protect themselves and others with whom they interact.

What are the associated threats, vulnerabilities and risks?

1. The Threats

The Isle of Man is not impervious to cyber-attack or the threats that are prevalent around the globe. These cyber threats can be delivered by a range of attackers from any location, in any time zone. Their intent may be to disrupt, destroy, deny services and/or extort money. They may, for example, be seeking to obtain commercial proprietary information, commit financial fraud or extort from a chief executive. These attackers have different objectives. For example:

- Cyber Criminals seek financial gain through extortion and ransom, as well as by selling any information they may have acquired on the black market. They target governments, businesses and the public at large using both direct and indirect indiscriminate methods.
- Hacktivists seek to cause damage and disruption to an organisation or body with which they have an issue. Their goal may be to cause extensive reputational and financial harm.
- Nation states (government agencies or their contractors) focus on collecting strategic information for political or economic gain or disrupting industrial facilities in competitive or hostile countries.
- 'Script Kiddies' are the individuals who seek out vulnerabilities and flaws in systems and services. Notionally they are less skilled and not as well-resourced as the more organised criminal actors. However, they have been able to cause significant impact to organisations and public bodies in other nations.
- Cyber Espionage is undertaken by one organisation or person against another to obtain intellectual property illicitly. This could be new technology, accounts data etc. The goal is to obtain competitive advantage or significantly harm the competitor.

2. The vulnerabilities

- Systems Maintenance – IT systems across the public, private and business sectors should be updated and checked regularly and effectively. IT is an expensive commodity and, at times, it may not be financially viable for a company, or family, to replace its IT. However, it is essential that these systems, both new and legacy, are fully updated and all appropriate fixes are applied. The Government, through the Office of Cyber Security and Information Assurance (OCSIA), will provide a focal point for advice and guidance on this area that is accessible and approachable for all.

- Training and Skills - Like the rest of the world, the Isle of Man has a shortage of cyber security resources and skilled operators. This strategy is looking to assess and remedy this as far as is practicably possible. It is our belief that all residents and employees need to have a fundamental awareness of cyber security and, to support this, Government will develop a nationwide cyber awareness campaign to help the Island's residents to understand the fundamentals of staying safe online. Furthermore, it will help business and other sectors to introduce a programme of cyber awareness across their organisations, adopting a methodology of cyber security baselining, similar to that used in the United Kingdom's Cyber Essentials .

- Insider Threat - The human factor is one of the greatest risks to a company and its network. Basic education and training can mitigate most of this potential risk. The insider threat may not be malicious or intended; it may be simply an employee inadvertently plugging in an infected USB stick or sending a misdirected email. In England, the NHS National Data Guardian has warned that staff members tend to ignore precautions that make it harder for them to do their job. Such workarounds are dangerous. Helping staff understand the reasons for the precautions as well as designing worker-friendly solutions will go some way to preventing such dangerous behaviour.

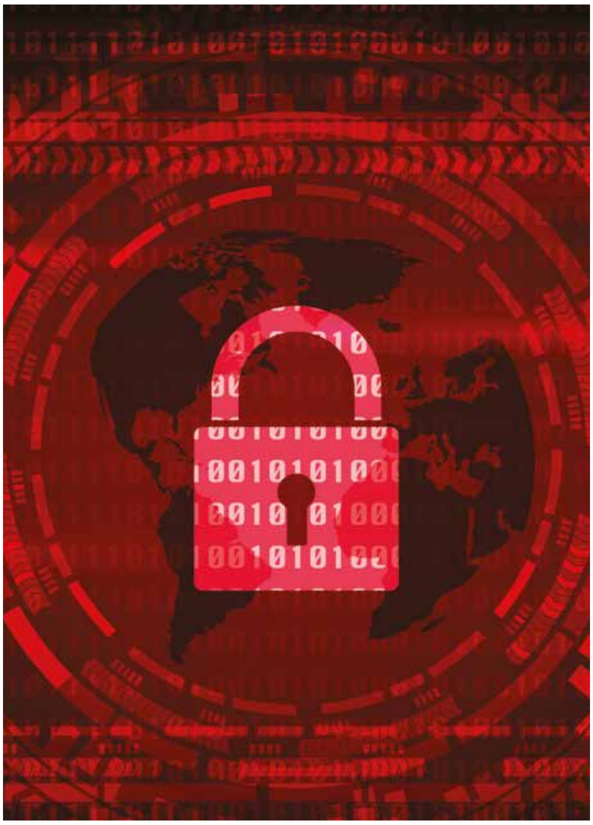
- High Tech Crime - Cyber Crime is a fast moving area of activity that can affect us all. The Government and Isle of Man Constabulary (IOMC) are working together to develop the skills, capabilities and technologies to deliver law enforcement in regard to cybercrime, including online fraud. The IOMC is currently reviewing its capacity and capabilities to counter criminality and illicit activity across the digital domain. As part of this, the Government will undertake a review of associated legislation and guidelines pertinent to the Isle of Man.

- Online Fraud - Currently the City of London Police operates the UK's Online Fraud Portal. This portal serves the whole of the UK and does offer support to Island residents; however it provides limited options for local analysis. IOMC supported by IOM Government is therefore intent on creating an Island-based comparable system that will feed into the City of London Police, but will be primarily focused on Island-based incidents to enable local measures to be applied where applicable. The solution is yet to be determined, but will enable reporting by a variety of means.

3. The risks

The risks to Government are actively managed across all of its operations and in delivery of its services. Cyber risk management is a fundamental part of broader risk management and is integral to the Island's wider resilience capabilities. The Government is looking to manage, reduce and/or mitigate the relevant cyber risks in cooperation with its partners and relevant stakeholders. The main objective is to ensure that Confidentiality, Integrity and Availability (CIA) across the Island's networks are assured and can be quickly restored following an incident, with minimum disruption.

The threats across cyberspace are prevalent and ever changing. So the Government's response must be agile and kept under regular assessment. This requires application of the appropriate controls and adherence to the defined policies, procedures and protocols. By this means we are striving to reduce and manage the extent and ramifications of known and perceived risks.



What are the areas of potential impact?

Critical National Infrastructure (CNI)

The Island's national infrastructure, both publicly and privately owned and/or supplied, is the backbone of our way of life. It includes the ports and harbours, the Internet Service Providers (ISPs), water and sewerage, our electricity supply, domestic gas and oil provision, to name but a few. As a distinct island there is a necessity to protect the full CNI within our shores from cyber-attacks and incidents, maintaining the provision of the services they offer to all.

The backbone of the Island's CNI is made up of large and complex Industrial Control Systems (ICS). They are, for example, embedded within the Island's traffic controls, water filtration, hospital systems, transport network, sewerage, etc. The ICSs enable delivery of essential services through a distributed network, with a number of sub-systems that ensure the processes operate correctly and in a timely manner. These systems are often separated from office-based systems, but can be just as vulnerable. The Government will actively support the protection of these areas and its systems by ensuring cyber risks and issues are mitigated as far as is practicable, contingencies are catered for, and appropriate recovery and remedial activity is developed as part of our national resilience strand of work.

We will work with the non-government entities to ensure the most appropriate and applicable standards and systems are adopted where possible to sustain services and enable expedient recovery following an incident.

Business

As the e-business market, inclusive of e-commerce, develops on the Island, so does the potential for a cyber-attack. The Government is committed to reducing the number of harmful attacks and their impact on the economic and digital sectors. Businesses on the Island need to feel assured that the Government and the Island's Internet Service Providers (ISPs) have done everything possible to secure the networks and services they use in their business activities. The Government is revising and developing its plans to support businesses if they are unfortunate enough to have been a victim of a cyber-attack. Recovery from an attack can be expensive in terms of direct and indirect costs to the business. Unfortunately, awareness of an attack may come sometime after it has started or even finished and the impact may potentially be far worse than initially imagined. Small businesses are just as vulnerable as larger organisations. The Government is determined to provide the same support for Small-to-Medium Enterprises (SMEs) as it does for larger businesses.

In line with the Government's commitment, the Digital Inclusion strategy is helping more people to get online. It will help residents to access training and jobs, social and leisure activities and internet shopping. Being online can also help to address wider social issues and support economic growth. The Government is aligning both the Digital Inclusion and the National Cyber-Security Strategy to ensure that they are complementary.

Reputation

The Isle of Man has a strong business reputation and wishes to maintain and strengthen its reputation as one of the safest places in the world . By ensuring that the Island has a strong cyber-security strategy the Government has committed to ensuring that the Island is a location of choice for companies and the public are secure and aware.

What is Government doing about it?

Business Continuity and Resilience Exercises

The Government has a set of well-developed and established Business Continuity plans. However, as the National Cyber Security Strategy comes into operation, the current plans will need to be adapted to incorporate cyber resilience.

The Isle of Man Government routinely undertakes Emergency Planning and Business Continuity exercises. These exercises will continue in the future. However, they will be adapted to encompass cyber security incidents on a larger scale. Through these exercises, all relevant Government departments and partners will be tested to assess the national response, with Learning from Experience (LfE) protocol adopted whenever necessary. The aim of such exercises is ultimately to maintain states of readiness for key departments and partners,determine any new weaknesses and validate current plans.

Legislation and Standards

In developing the Island's resilience, capacity and capabilities the Government is undertaking a detailed analysis of the relevant global legislation and standards for cyberspace, data management and information assurance. It is committed to meeting the requirements of those regulations and legislative frameworks that enable businesses to operate in foreign markets whilst ensuring data is secure and protected here on the Island.

Underpinning the national strategy are a number of forthcoming EU regulations and directives. The ongoing Brexit negotiations have also been factored into the planning process. The Government has deployed sufficient resource for developing our systems and processes to meet these upcoming events. By the end of May 2018 the Isle of Man Government will honour its commitment, announced by the Chief Minister, to adopt the General Data Protection Regulation (GDPR) into Manx Law. There will be a review of the GDPR's requirements along with an investigation into whether its associated Directives are applicable, namely Network and Information Systems Directive (NISD), Policing and Criminal Justice (PCJ) and the Health and Social Care (H&SC) Directives.

Partnering and unity of approach

The Office of Cyber Security and Information Assurance (OCSIA), as part of the Cabinet Office, will on behalf of Government have responsibility to deliver and manage this strategy with oversight being provided directly by the Chief Secretary and the delegated Member for Cyber.

The Isle of Man national capacity and capabilities are to be developed on a long-term basis. However, accepting that not all things can be achieved independently, the government is ensuring that from the outset and where required, development work will be done in partnership with the United Kingdom's agencies, bodies and organisations to reinforce our own national systems, practices and processes. IOM data and information will remain IOM-owned and managed through properly structured agreements. The Island will benefit further through sharing best practices as a scaled national cyber security solution is delivered.

Digital Government

The Isle of Man Government is currently delivering both its Digital Strategy and Digital Inclusion Strategy, and is keen to develop further the services available over the digital networks. The Digital Strategy has been developed to enable public services to be delivered more expeditiously and more cost effectively. Although the provision of digital services started some time ago, the extent and breadth of online services will develop alongside the advances of the Digital Strategy.

Our Strategic Intent

Aim of the Strategy

There can be no excuses for failing to take cyber-security seriously. Across the developed world, businesses that did not secure their customers' personal details against theft by hackers have suffered massive reputational damage and commercial losses. Individuals know there may be a heavy financial price to pay for divulging passwords and account details. And the scale of the threat is increasing. In May 2017 the WannaCry ransomware attack, which targeted computers running the Microsoft Windows programme, infected more than 230,000 computers in more than 150 countries. It caused disruption in railway systems in Russia and Germany, the phone network in Spain and the NHS in England.

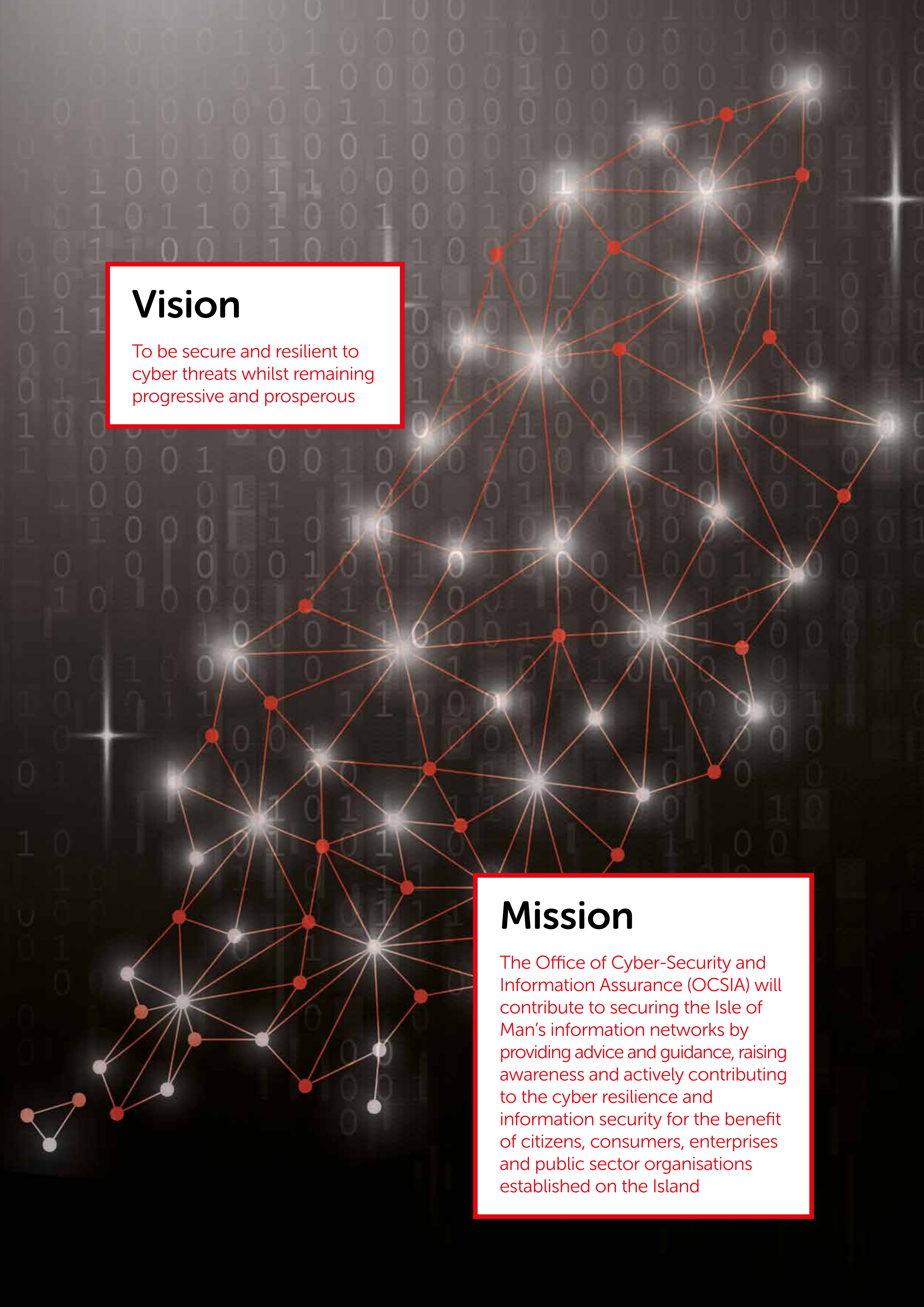
The Isle of Man is small and distinct, but an important player in global economic markets. It is fortunate to be afforded fundamental levels of protection by the United Kingdom in a number of areas, such as defence. However, due to the Island's independence and separation from the United Kingdom, it falls to us on the Island to defend our own digital space.

That is why we need the National Cyber-Security Strategy set out in this document. It has been developed for all residents, all businesses, the third sector and Government. It is a crucial underpinning of our society that will:

- Protect our networks
- Secure the data we hold and use
- Support our economic development
- Counter criminality and illicit activity in the digital environment
- Foster enduring relationships with partners.

The Government is working towards formalising its partnerships with other Crown Dependencies, nations, organisations and academic institutions. For example, the UK National Cyber Security Centre (NCSC) has agreed to work with us on matters of cyber security, and the Isle of Man Government is working towards formalising that arrangement. However, there will still be a requirement for us to maintain a high level of independence to protect our fiscal integrity and economic prosperity. We must develop our own cyber security protection and resilience to minimise the need for external support from partner nations.

The strategy has a clear vision and a strong mission statement, which is explained in greater detail in the rest of this document.

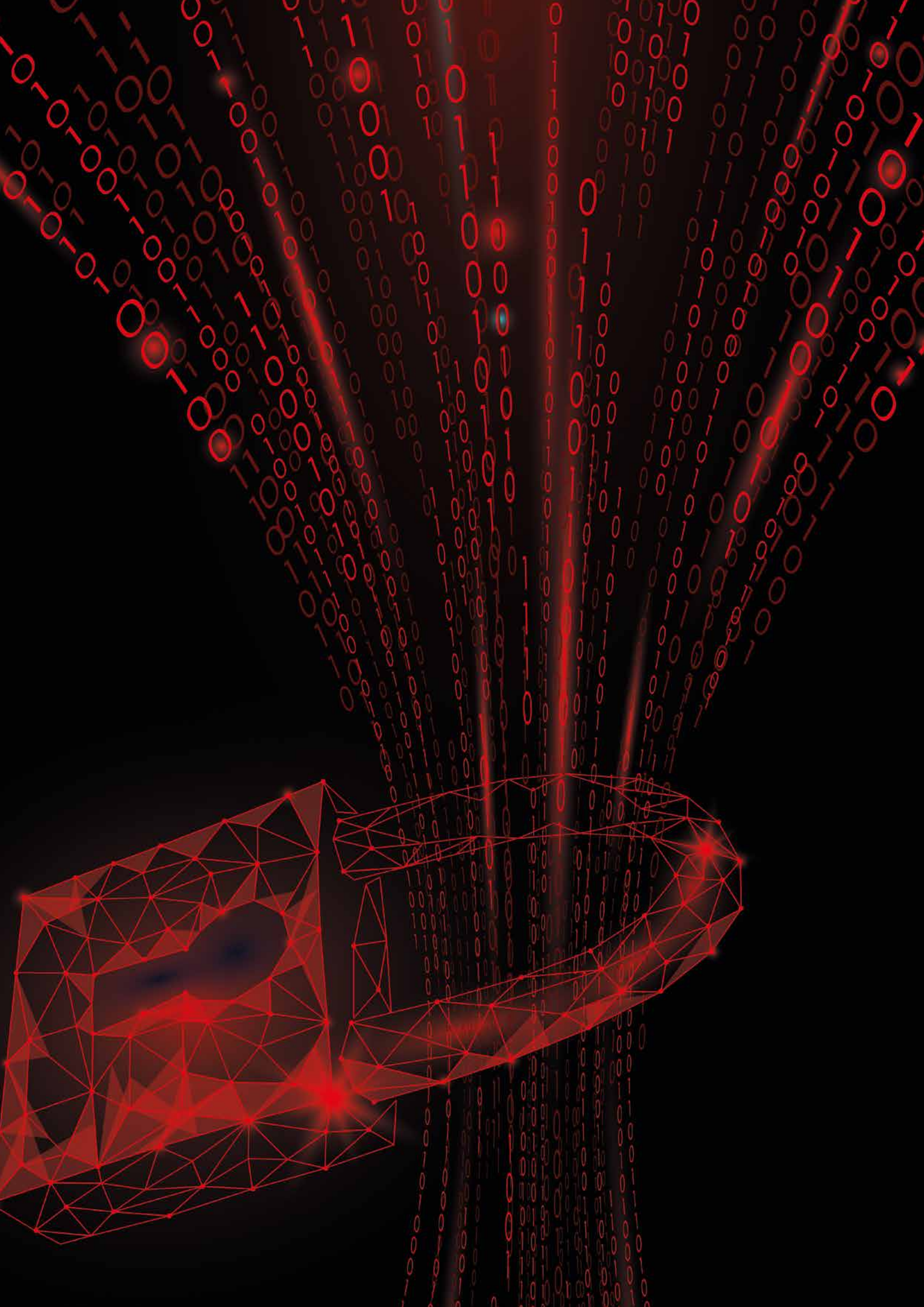


Vision

To be secure and resilient to cyber threats whilst remaining progressive and prosperous

Mission

The Office of Cyber-Security and Information Assurance (OCSIA) will contribute to securing the Isle of Man's information networks by providing advice and guidance, raising awareness and actively contributing to the cyber resilience and information security for the benefit of citizens, consumers, enterprises and public sector organisations established on the Island



Principles, Goals and Objectives

The Isle of Man Government's focus is on providing the Island's residents, its public services and businesses with a safe, secure, resilient and prosperous place to live and operate from. It will do this through the provision of the appropriate systems, processes and measures.

To achieve success we need:

- Committed leadership by Government
- Strong collaboration with business
- Effective action to educate and train everyone in society so that we can all play our part in strengthening cyber security at work and in the home.

This chapter looks at each of these three requirements in turn, setting out the principles we will follow, the strategic goals we have set and the precise objectives that we intend to achieve.

Committed leadership by Government to achieve resilience

Principle:

The Government sees the Island's cyber security and resilience as a top priority. It is a complex area, requiring focussed resources and capabilities. Through strong leadership and governance, the Government will drive progress in support of all on the Island. The Government will work with its partners to ensure the optimal security solution is attained for the Island whilst also developing national innovation and skills.

Strategic goals:

- All Government systems and the data held in them are protected and secure
- All appropriate legislation, standards, and policies are implemented and enforced, with new versions drafted for consultation if required
- Law enforcement agencies on the Island are able to respond effectively to cyber-related criminality
- Enduring multilateral and bilateral relationships enabling collaboration and interaction are established.

Objectives:

- Implement a national capability to detect and defeat high-end threats, whilst utilising partnering agreements /Memorandum(s) of Understanding (MOUs) to reinforce a national capability and capacity
- Enable law enforcement agencies to have access to the skills and capabilities needed to tackle cyber-crime and high-tech crime, undertake cyber forensics, act in support of countering online fraud and have the ability to bolster on-Island skills and resources
- Support the Island's public authorities in the delivery of their services in a secure, resilient and enduring manner that is compliant with the appropriate standards and legislation
- Design and implement a regime of Government information security and risk management with an accountable and competent network of Senior Information Risk Owners (SIROs)
- Strengthen, promote and formalise collaboration with the UK and other international partners
- Support Government, business and public awareness of cyber threats and how to defend, respond and recover
- Bolster and refresh Government contingency planning capacity and skills to expedite recovery from a cyber-incident.

Support for Critical National Infrastructure

Principle:

In protecting the Island's way of life, its commercial productivity and its economic prosperity, the Government will work with providers of Critical National Infrastructure (CNI) in both the public and private sectors to ensure that services are maintained, are as resilient as is practicable and are able to recover swiftly following a cyber-incident.

Strategic goals:

- The Island's CNI is secure and protected
- All appropriate legislation, standards, and policies are implemented and enforced across national infrastructure components, with new versions drafted for consultation if required
- Enduring multilateral and bilateral relationships enabling collaboration and interaction are established specifically related to CNI.

Objectives:

- Ensure the Island's CNI is robust, resilient and able to respond/recover accordingly; develop and formalise partnering with UK, other Crown Dependencies and key International Partners on cyber security and digital domain aspects

- Implement a national capability to detect and defeat high-end threats, whilst utilising partnering agreements /Memorandum(s) of Understanding (MOUs) to reinforce a national capability and capacity across the critical infrastructure on the Island
- Strengthen, promote and formalise collaboration with the UK and other international partners
- Bolster and refresh Government contingency planning capacity and skills to expedite recovery from a cyber-incident across the CNI network, both public and private.

Strong collaboration with business to achieve prosperity

Principle:

In delivering a cyber-resilient Island, it is essential that Government works alongside the business sector. The Government will deliver the services and support required whilst ensuring that the rights and values of all are respected. Furthermore, it will ensure adherence to human rights law, the relevant data protection regulations and other applicable legislation, regulations and standards. Additionally, all activities will be undertaken as transparently as possible to ensure all solutions are fully understood.

Strategic goals:

- The Government, private sector and academia work collaboratively to ensure businesses are secure
- Emerging technologies and the changing digital environment are appraised and changes adopted accordingly.

Objectives:

- Support and develop cyber security research, business and education across the Island
- Promote economic stability through the provision of world class facilities and an environment with freedom to flourish
- Support the protection of national interests and reputation
- Promote investment, research and development in the ICT sector and Island-based cyber capabilities
- Reinforce the wider Digital Strategy and support the Digital Island concept
- Support the Island's development of new markets and technology offers – e.g. Data Businesses, Data Farms, etc
- Reinforce the requirement for Information and Data Assurance across all sectors on the Island
- Support the Island's business community in its ability to tackle financial crime-related activity – money laundering, terrorist financing, etc
- Support the Island based banking community to detect, deter and defend its networks
- Provide a secure cyberspace for business and with business through guidelines, regulation and enforcement
- Strengthen the economic stability, impact and reach of the Isle of Man
- Protect the Island's public and private digital networks in conjunction with the local Internet Service Providers (ISPs).

Everyone playing a part in a progressive society

Principle:

Cyber security and resilience is a shared responsibility, deliverable by all. We are all responsible for our actions and activities online and in the digital space. By working together we can ensure that businesses and residents are informed, supported, educated and have the appropriate measures to protect against attacks and have the support to call upon if an incident occurs. By sharing these responsibilities we help to create a more progressive society.

Strategic goals:

- Plans for the development of national capabilities, capacity and self-reliance in the realm of cyber security through education, training and mentoring are in place
- Support is available to all the residents of the Island, of all ages, through education and outreach, allowing all to be safe and secure online with the appropriate resources if an incident or issue occurs.

Objectives:

- Develop a national programme that encompasses all aspects of cyber security, demystify the area, and instil improved cyber awareness across all sectors and among the public as a whole
- Promote public awareness so people are better able to protect themselves online
- Develop a programme of inclusion on the Island, such as the Cyber Challenge, to enhance digital skills across all generations through community outreach and other programmes
- Develop national cyber skills, knowledge and capability that are able to sustain and meet the market demands.

Government will issue the National Cyber-Security Strategy Action Plan within three months. This Plan will provide more detail on the implementation and progress reporting of the strategy.

Conclusion

It is essential that the Isle of Man Government protects its citizens, businesses and the broader interests of the Isle of Man. This cyber security strategy intends to deliver on the promises made in the Programme for Government and further develop the Island's economic prospects, potential and performance.

Indicators of Progress

Tracking progress, defining success and tackling the obstacles to delivery will be essential. The Office of Cyber Security and Information Assurance (OCSIA) will work, on behalf of the Government, with our partners to align our strategy with theirs. We will also work collaboratively with the Island's business sectors to deliver an efficient and effective strategy.

There will be routine reporting, at least quarterly, to the Council of Ministers and Chief Officers Group to ensure that strategic oversight is maintained and leadership is provided. An annual review will be undertaken by the Chief Secretary to ensure the strategy, in its entirety, remains relevant and delivering the outputs required at the pace needed.

Measures of Success

Knowing if the strategy is delivering successfully is essential to progress and a necessity for both businesses and residents. Through routine review, consultation and surveys, the Government will measure progress and delivery against defined milestones, changing requirements and actions in order to meet any emerging threats and the development of new technologies and ways of working.

We will be successful in delivering the strategy when:

- The Island's businesses are able to operate in a resilient and secure environment, managing their own risks and having sufficient processes in place to deal with them
- The residents of the Isle of Man are informed and aware of the risks of using digital technologies, and are able to report incidents, such as online fraud, and be confident in the support being provided in dealing with them
- E-Government and all public services are managed and delivered in a secure resolute manner by a Government that is cyber aware, cyber-resilient and has the appropriate trained personnel and systems in place
- Businesses and academia prosper on the Island in their research, innovation and collaboration
- E-business continues to grow and operate from the Island, based on a global reputation for cyber-resilience
- Law Enforcement is able to deliver the support and services required in dealing with cybercrime to all on the Island
- The Island's Critical National Infrastructure (CNI) is resilient and secure, but with sufficient recovery plans and processes if an event does occur
- The Government will have in place the services and capabilities to protect and manage the Island's digital space and ultimately support the recovery following an incident.

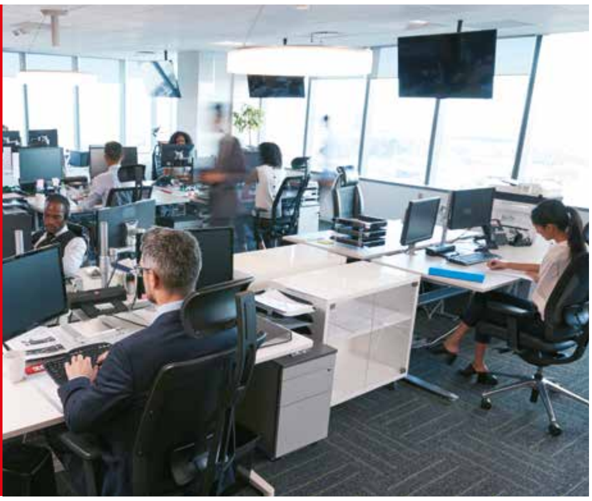
In conclusion, the strategy, through its implementation, will deliver on the following:

Aware

Develop cyber resilience across the Isle of Man government and positively influence the private and third sector entities operating on the Island along with the wider population. Instigate a major transformative programme for delivery through OCSIA designed to test, evaluate and promote cyber security, cyber resilience and information assurance across the Isle of Man.

Secure

Ensure departments, boards, offices and other public authorities as well as businesses and the public are able to deter and defend against cybercrime and other criminal activities by maintaining and sharing pertinent information. Enable the Isle of Man Government to deliver with assurance a level of cyber security that will both protect and deflect nefarious cyber activities to alternate targets. Additionally, the wider Government will be able to respond and recover from a cyber-incident through the coordination of the relevant authorities and bodies.



Resilient

Deliver a network of cyber awareness, implement specialist roles across government able to provide central policy advice, standards, active direction and support to allow the dissemination of knowledge and capability to defend the Island and maximise the safe use of information assets. Government will support the development of the Island’s public and businesses capacity and capability to better defend themselves from cybercrime and fraudulent activities.

Glossary

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.

Cybercrime – refers to a vast array of illegal activities that are implemented via IT systems, including mobile devices. A crime committed with the aid of, or directly involving, a data processing system or computer network. The computer or its data may be the target of the crime or the computer may be the tool with which the crime is committed.

Cybercriminal – an individual who undertakes criminal activities via IT systems and/or mobile devices. Cybercriminals can range from individual, opportunistic criminals, through to highly-skilled and professional groups of computer hackers. Cybercriminals may specialise in:

- Developing malware and selling it to others who go on to launch attacks
- Harvesting data – such as credit card numbers – and selling it to other criminals or they may undertake every stage of an attack, from developing the malware to stealing money from the victim.

Cyber-attack - An attack that involves the unauthorized use, manipulation, interruption or destruction of, or access to, via electronic means, electronic information or the electronic devices or computer systems and networks used to process, transmit or store that information.

Cyber-espionage – the act of spying and illicitly accessing information via IT systems and/or the internet.

Cyber-incident - Any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete or render unavailable any computer network or system resource.

Cyber-security - The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability.

Cyberspace - The electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than three billion people are linked together to exchange ideas, services and friendship.

Cyber-threat - A threat actor, using the internet, who takes advantage of a known vulnerability in a product for the purposes of exploiting a network and the information the network carries.

Chat Rooms - An area on the Internet or other computer network where users can communicate, typically one dedicated to a particular topic.

E-business – (Electronic business) refers to the use of the Web, internet, intranets, extranets or some combination thereof to conduct business. E-business is similar to e-commerce, but it goes beyond the simple buying and selling of products and services online. E-business includes a much wider range of businesses processes, such as supply chain management, electronic order processing and customer relationship management. E-business processes, therefore, can help companies to operate more effectively and efficiently.

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 cyberterrorists 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 Organization, 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.

Malware - Malicious software, known as malware, is an overarching term for software that is designed to infiltrate or damage a computer. Malware's effects can include Denial of Service (DoS), Distributed Denial of Service (DDoS), privilege escalation, keystroke logging, geo-location of smartphones, tablets, laptops and similar devices, and the exploiting social networks.

Phishing – the use of electronic communication (e.g. email) under the guise of a legitimate source to lure a recipient into disclosing sensitive information, e.g. Personal Identifying Data (PID), bank details, etc.

Ransomware - Software that denies you access to your files until you pay a ransom.

Acronyms

CBEST	Bank of England cyber security protocols and guidance
CiSP	Cyber security Information Sharing Partnership
CM	Chief Minister
CNI	Critical National Infrastructure
CO/CabOff	Cabinet Office
CoG	Chief Officers' Group
CoMin	Council of Ministers
CRAB	Cyber Risk Assurance Board
CREST	Council for Registered Ethical Security Tester
CS	Chief Secretary
DGSIRO	Deputy Government Senior Information Risk Owner
DPO	Data Protection Officer
EPC	Emergency Planning Committee
GDPO	Government Data Protection Officer
GDPR	General Data Protection Regulation
GSIRO	Government Senior Information Risk Owner
GTS	Government Technology Services (part of Cabinet Office)
IAM	Information Assurance Manager
IAO	Information Assurance Officer
ICT	Information and Communications Technology
IOMC	Isle of Man Constabulary
IoT	Internet of Things
ISP(s)	Internet Service Provider(s)
LfE	Learning from Experience
MHK	Member of the House of Keys
MOU	Memorandum of Understanding
NCSC	National Cyber Security Centre
NCSS	National Cyber Security Strategy
NISD	Network and Information Systems Directive
OCSIA	Office of Cyber-Security and Information Assurance
SIRO	Senior Information Risk Owner
SME	Small-Medium Enterprise
SOC	Security Operations Centre
USP(s)	Unique Selling Point(s)
WARP	Warnings, Advice and Reporting Point

References

Isle of Man:

Digital Strategy – https://www.gov.im/digitalstrategy

Digital Inclusion Strategy - https://www.gov.im/media/1352205/digital-inclusion-strategy-july-2016.pdf

Programme for Government - https://www.gov.im/about-the-government/government/the-council-of-ministers/programme-for-government/

IOM Information Commissioners Office (ICO) – https://www.inforights.im/

External:

United Kingdom Government Links:

UK Government National Cyber Security Strategy 2016-2021 – https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

UK Government CNI Cyber Apprenticeship Scheme – https://www.gov.uk/guidance/cyber-security-cni-apprenticeships

Centre for the Protection of National Infrastructure (CPNI) – https://www.cpni.gov.uk/

National Cyber Security Centre (NCSC) – https://www.ncsc.gov.uk/

NCSC Cybersecurity Information Sharing Partnership (CISP) – https://www.ncsc.gov.uk/cisp

Warnings, Advice and Reporting Point - https://www.ncsc.gov.uk/articles/what-warp

Other United Kingdom Links:

UK ICO - https://ico.org.uk/

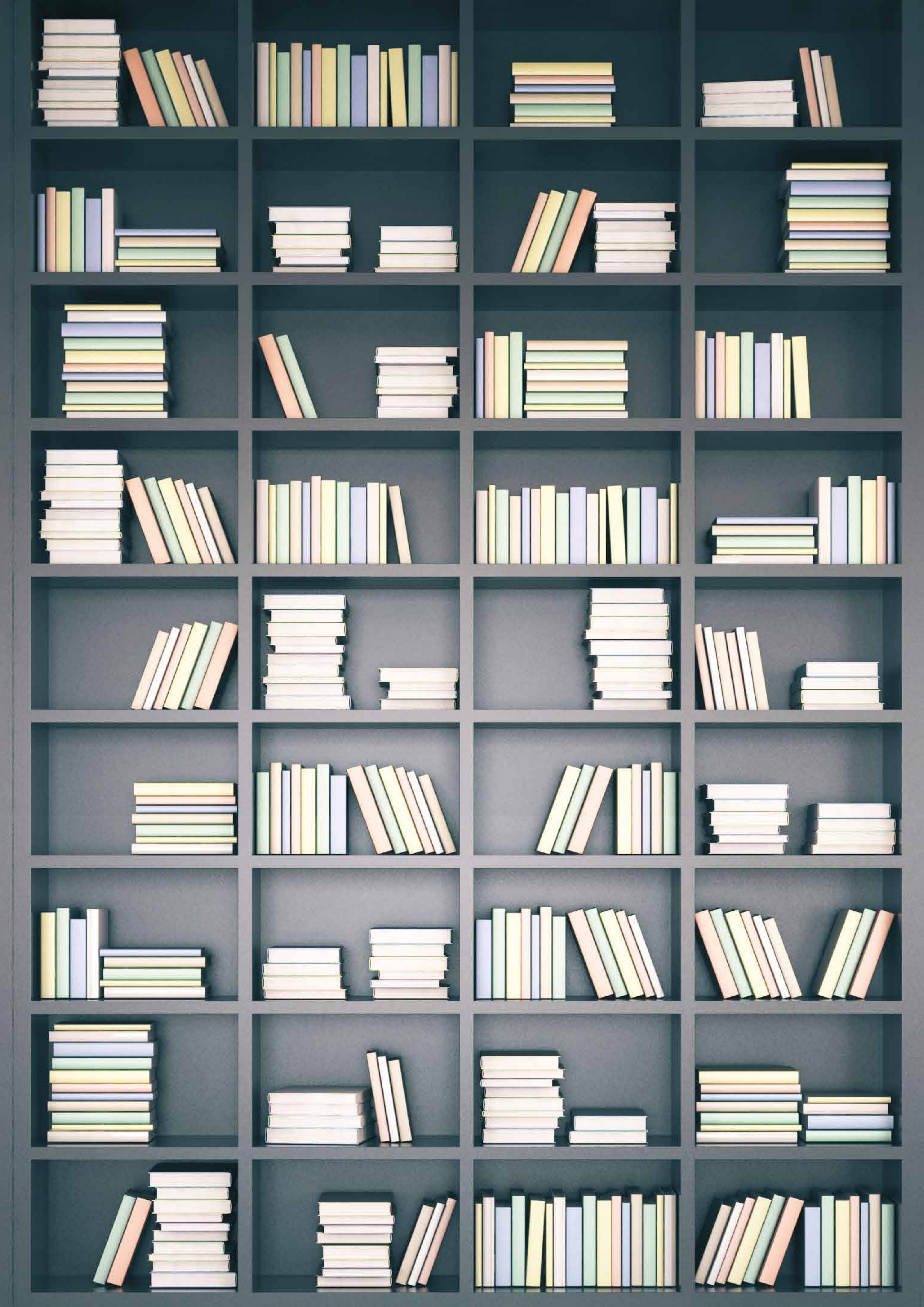
Bank of England CBEST – http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx

Council for Registered Ethical Security Tester (CREST) – http://www.crest-approved.org/

Wider Links:

The European Union Agency for Network and Information Security (ENISA) – https://www.enisa.europa.eu/

National Institute of Standards and Technology (NIST) – https://www.nist.gov/topics/cybersecurity



Isle of Man Government
Reiltys Ellan Vannin

Isle of Man Government point of contact:

Office of Cyber-Security and Information Assurance (OCSIA)
3rd Floor,
Heywood House,
Ridgeway Street,
Douglas
IM1 1EW

ocsia-secretariat@gov.im
+44 1624 685557