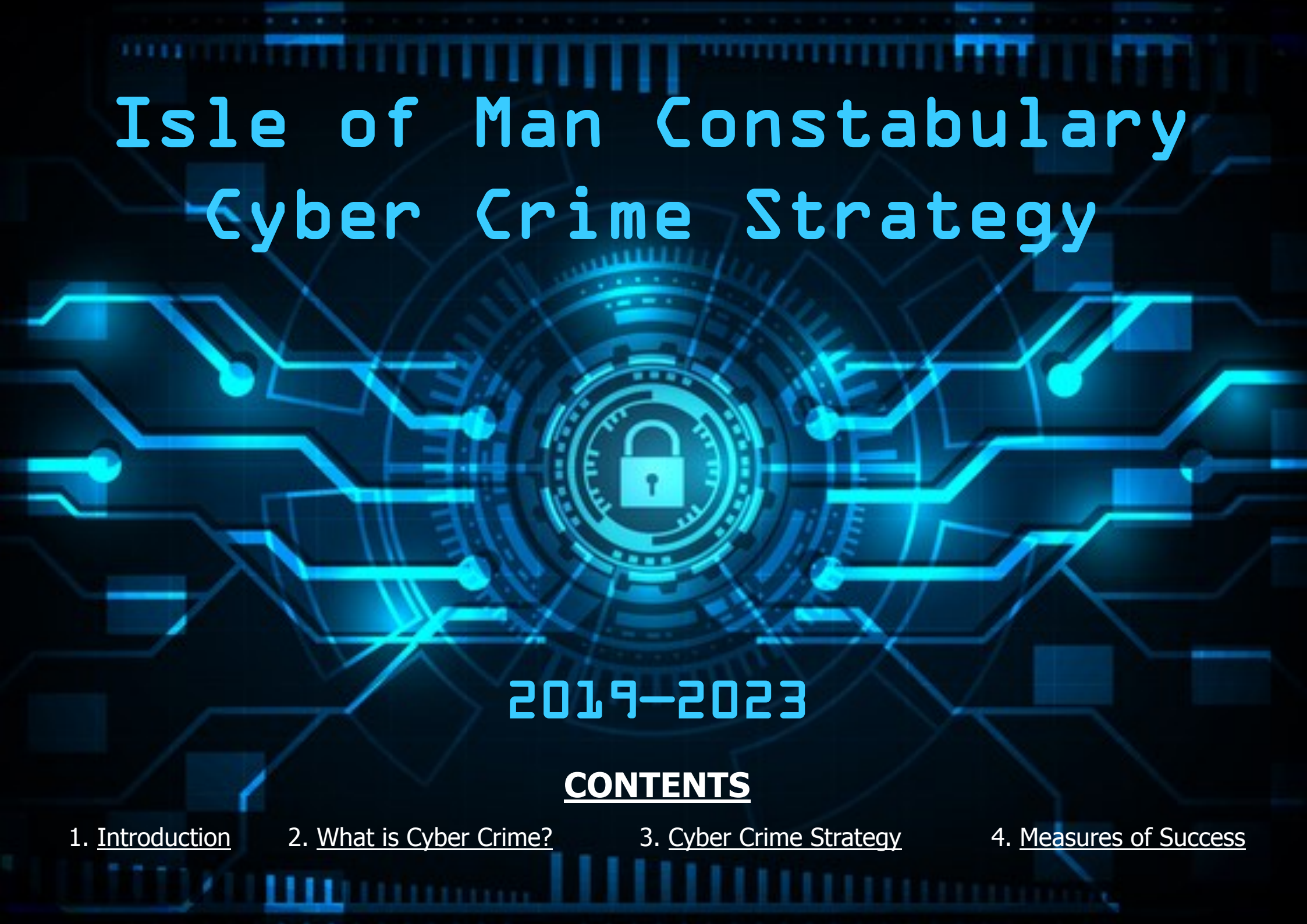
Isle of Man Constabulary Cyber Crime Strategy



2019–2023

CONTENTS

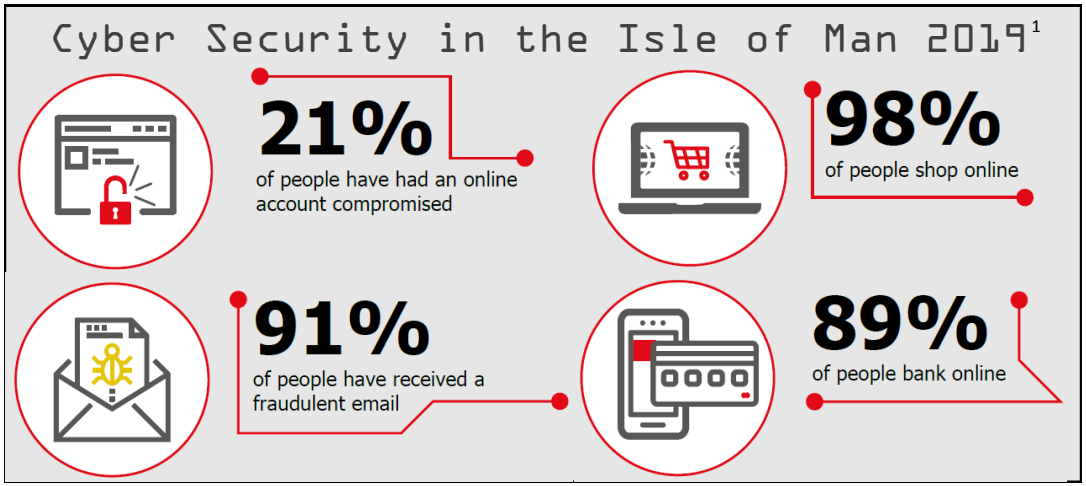
1. Introduction

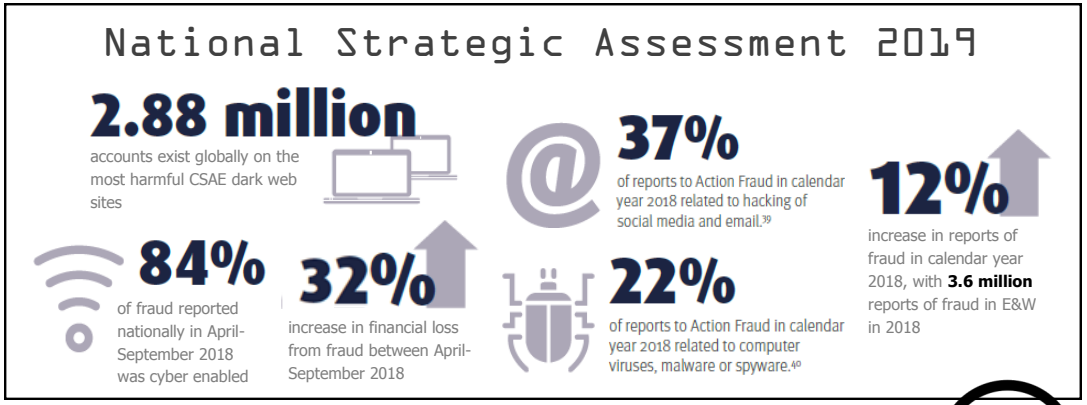
The Isle of Man Constabulary aims to make the Isle of Man the safest small island. We are committed to reducing crime and protecting victims and the vulnerable.

This strategy sets out our aims underpinned by prevention and explains how we will minimise the impact within our community. Prevention is embedded at the heart of the strategy and is a primary aim of all our strategic and operational objectives. The strategy sets out our priorities, at the heart of which lies prevention. Stopping people from falling victim to cybercrime is our intention.

The methodologies of cyber crime are varied and so too are the potential victims, who span a broad spectrum of the population including both businesses and individuals.

We live in a digital age and the landscape of crime and offending is changing rapidly. Despite rises locally in fraud scams, phishing and malware, the threat and risk to the Isle of Man and the delivery of Policing in this area is somewhat unknown, which is why understanding our demand is so important. This in turn will inform all other areas of the strategy and help us to deliver it.



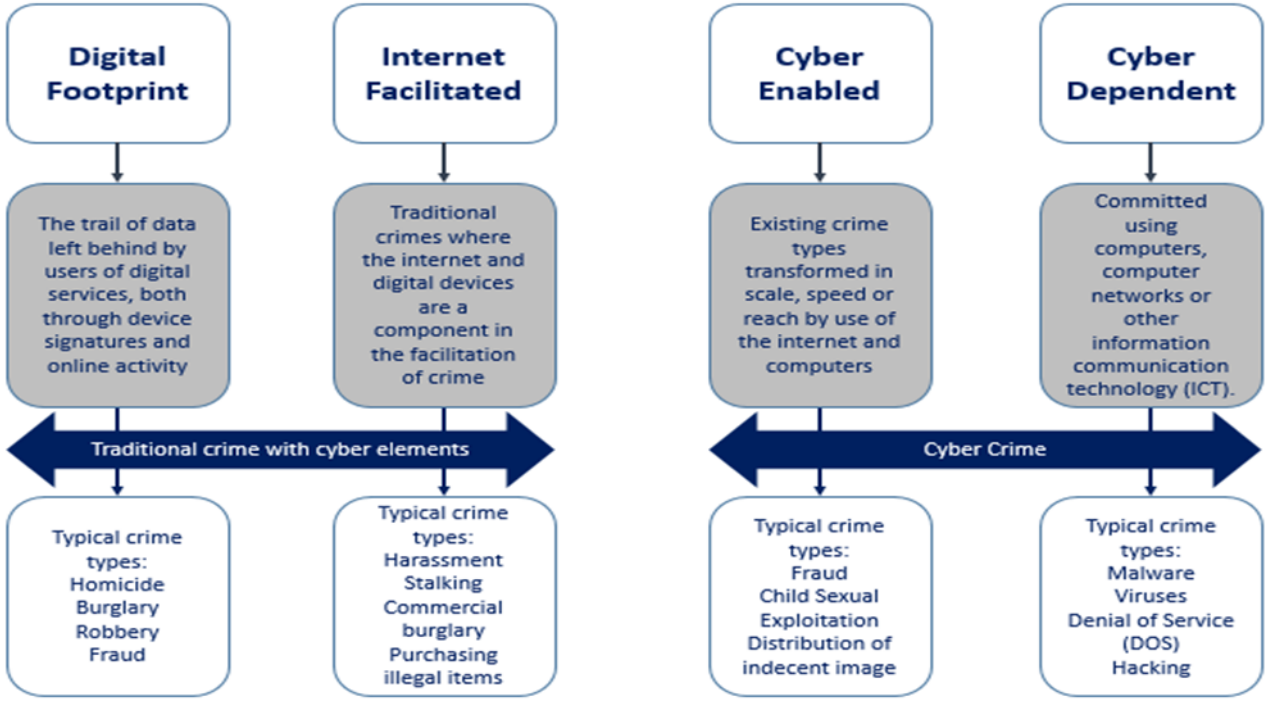


1. Based on data from Isle of Man Government cyber security awareness survey (15 April - 3 May 2019, 649 responses). Issued by the Isle of Man Government, Office of Cyber Security and Information Assurance.

2. What is Cyber Crime?

Cyber crime is any offence which is committed through, or enabled by the use of technology, whether or not the offence is predicated solely on the technological element or whether the technology merely assists the perpetrator in the commission of the offence.

Cyber crime continues to rise and it is becoming increasingly difficult to separate these offences from more traditional crimes. Similarly, technological advances of email and mobile devices have increased the potential for offending in this way, not to mention making it harder for the offenders to be identified as they can commit offences from anywhere in the world.



3. Cyber Strategy Aims

GOVERNANCE AND POLICY

Build an Infrastructure that is fit for purpose across the spectrum of investigating and tackling cyber crime

DEMAND

Understand the threat and risks we face from cyber crime, creating an environment to better inform the demand on IOMC

CAPABILITY

Enhance the force capability to react to digital and cyber crime threats, creating resilience to the risks posed by cyber criminals

PREVENT

Make prevention the heart of the strategy; by understanding the threats, increasing our capability, working with partners and developing our people.

PEOPLE

Invest in our people to grow and expand our capability to deal with increasingly complex crimes

PARTNERSHIPS

Seek innovative ways to create new public and private collaborative opportunities

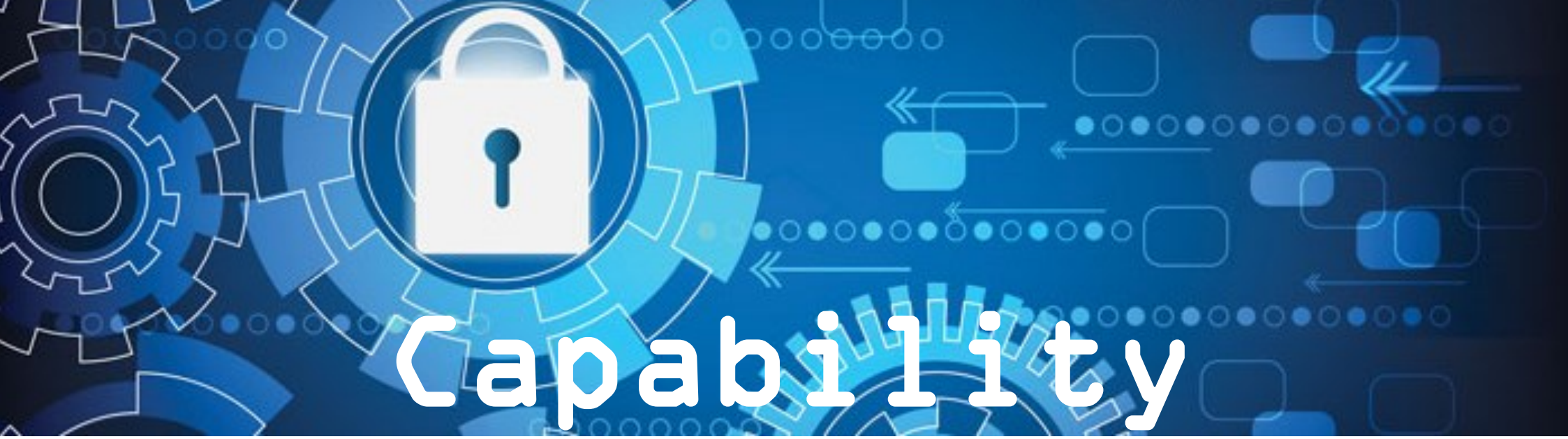
Prevent

- ⇒ Identify the risk of harm and protect the vulnerable in the digital world
- ⇒ Create ways through people and technology to develop better intelligence gathering
- ⇒ Signposting self help and prevention information, making this a key component of IOMC website
- ⇒ Promote digital and cyber information sharing
- ⇒ Raise public awareness through media and other key opportunities for communication
- ⇒ Engage in outreach with OCSIA* and other key partners to drive prevention across the Isle of Man

*Office of Cyber Security and Information Assurance.

Demand

- ⇒ Use new systems and processes to capture local activity and provide a local reporting pathway
- ⇒ Understand our demand:
  - ◊ Identify how cyber crime is committed on the Isle of Man
  - ◊ Identify the impact of cyber crime on the Isle of Man
  - ◊ Understand the threats and risks to the Isle of Man, along with our vulnerabilities
- ⇒ Use understanding of demand to inform an effective and efficient police response and drive prevention
- ⇒ Identify national threats of cyber criminality and links to serious and organised crime groups
- ⇒ Identify risks posed at a National and International level



Capability

- ⇒ Create resilience with an omni-competent team of cyber crime specialists
- ⇒ Ensure specialists are equipped with the right technology
- ⇒ Ensure that cyber capability is employed within serious and other complex crime investigations
- ⇒ Enhance specialist capabilities and specialist support within all relevant investigations
- ⇒ Develop clear response pathways in line with the Islands main cyber & digital threats
- ⇒ Develop a more comprehensive approach to cyber crime proactive policing
- ⇒ Promote an environment to enhance capability and outcomes through digital specialists, knowledge and volunteers

People

- Upskill the Isle of Man Constabulary workforce to be more digitally savvy
  - Develop blended learning to enhance the digital skills of the workforce
  - Seek wider opportunities to provide training and CPD
  - Ensure that Neighbourhood Officers have the skill set to tackle cyber crime within the community and drive prevention
- Recruit and build a larger Cyber digital team that meets demand
- Ensure our people have the right knowledge, skills and tools for the job
- Increase the use of volunteers and develop cyber specialists
- Ensure that training is at the forefront of supervisory planning

Partnerships

- ⇒ Build partnership and collaboration opportunities to enhance the overall strategic aims
- ⇒ Create partnerships with the North West Regional Crime Unit (NWROCU)
- ⇒ Build partnerships for mutual assistance through the National Cyber Security Centre
- ⇒ Capitalise on opportunities for digital investigators of the future through the private sector and the University College IOM
- ⇒ Ensure the Isle of Man Constabulary has access to the best practice and innovative skills promoted through the CoP within the UK
- ⇒ Develop closer collaboration between the IOMC and OCSIA to understand threats and drive prevention
- ⇒ Better collaboration with Action Fraud and access to informative data

4. Measures of Success

PREVENT	Able to identify the vulnerable	Fewer victims of cyber crime	Improved public satisfaction	Bemchmark against July 2019 OCSIA Cyber Survey
DEMAND	Threats and Risks are identified	Informed future strategic planning	Identified risks to the IOM and any links to serious and organised crime	The demand picture is used to inform tasking
CAPABILITY	ISO 17025 or equivalent performance framework	Access to sufficient technical equipment	Increased officer capability with technology	Supporting investigations in relation to drug and cash seizures.
PEOPLE	Increase in the number of cyber trained investigators	Volume of training increased and governance around it	Contribution by Digital Volunteers and IOM University students	Our people are able to access additional digital resources
PARTNERSHIPS	Agreed formal collaboration with NW ROCU	Clear pathways to NCCU	Increase the types of support available to IOMC Investigators	Increased support and collaboration from the private sector