Cyber Security
Strategy

Committee *for*
Home Affairs

Introduction

Cyber security describes the technology, processes and safeguards that are used to protect our networks, computers, programs and data from attack, damage or unauthorised access.

Guernsey is a digitised society and technology drives, or enables, every part of our life from social interaction, through healthcare to education and business.

The transformation brought about by this digitalisation creates new opportunities and regrettably new threats. Our economy, the administration of government and the provision of essential services now rely on the integrity of cyberspace and on the infrastructure, systems and data that support it.

Much of the hardware and software originally developed to facilitate this digital environment has prioritised efficiency, cost and the convenience of the user, but has not always had security designed in from the start. Without protection, hostile states, criminal or terrorist organisations and individuals can exploit the gap between convenience and security. To address this we have developed this Cyber Security Strategy.

The Cyber Security Strategy

Background

We need to make sure that Guernsey continues to be a stable, secure and attractive place to live and do business, including in the rapidly evolving world of increased digitisation, connectivity and with the rapid advances in the availability and use of technology.

Our infrastructure needs to help us do this. We need to:

Make sure that existing legislation, and any legislation we introduce, is fit for purpose, and has appropriate flexibility to respond to evolving threats.

Have the right expertise and capability across the public sector to best respond to threats and embrace evolving opportunities

Raise and promote cyber awareness across government, businesses and individuals.

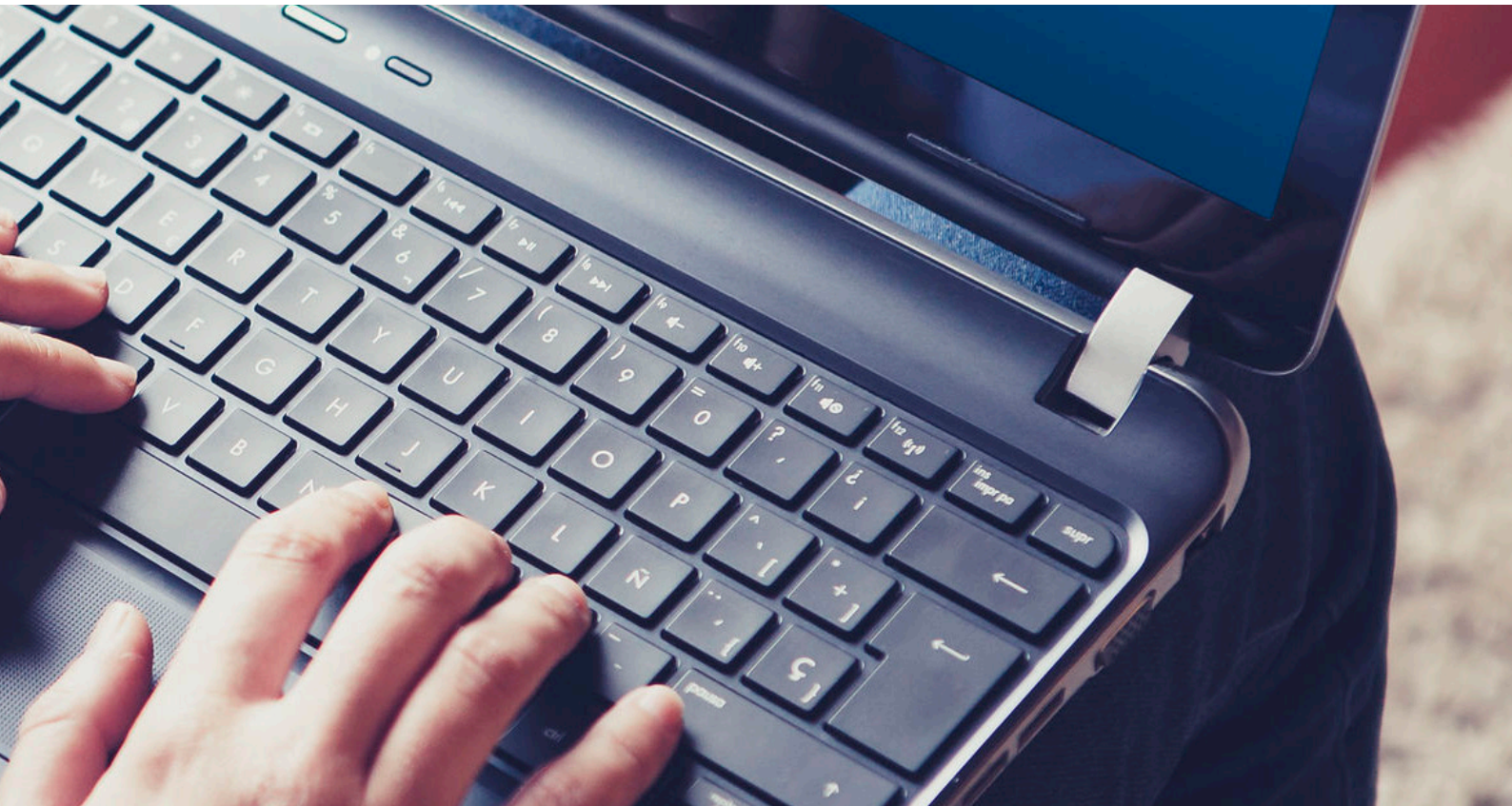
Scope

This Strategy considers the Cyber Environment in three broad areas. These are:

C1 - The Strategic Level – Where a cyber incident may cause serious damage to human welfare on a national level. This could affect the core functioning of Government, have a major impact on our critical national infrastructure or have a significant impact across any of our principal business sectors. A major attack of this nature is characterised by Real World Impact and would require a cross-government response most likely coordinated by the NCSC.

C2 - The Tactical Level – Where a cyber incident has a significant and severe impact on a particular sector but not a national level effect. This could include an attack affecting a specific part of government, a targeted attack on a specific business sector or a discrete part of our critical national infrastructure. The Committee for Home Affairs would coordinate a response to a significant attack of this nature; supported by the NCSC where appropriate.

C3 - The Operational Level – Where a cyber incident has an impact on a discrete group of individuals or businesses. These are likely to be characterised by attacks against an individual, or group of individuals, or a single business. These incidents, the most basic level of routine cyber attacks, do not require formalized ongoing multiagency coordination.



Our Commitment

To ensure that Guernsey citizens, business and Government are as 'safe and secure' going about their legitimate lives in cyber space as they are in the physical environment, we commit to the following:

- Respect the privacy and civil liberties of islanders and ensure our objectives are proportionate and appropriate.
- Work with partners from the UK, Europe, Jersey, across Government and Business to ensure value for money, and learn from the experience and expertise of others.
- Deliver a holistic approach [across Islanders, Business and Government] recognising that there is a wider reputational risk to the jurisdiction of a cyber security incident that cannot be confined to a single business, business sector or part of Government.

Our Strategic Goals

There are eight (8) strategic goals covered in this strategy:

Goal one: Legislation and Regulation

We will provide proportionate Legislation and Regulation to meet the current threat. This will includes the delivery of the new Data Protection (Bailiwick of Guernsey) Law 2017 and review of other related and relevant legislation to ensure it remains fit for purpose.

Goal two: Continuous Assessment

We will establish a framework to continuously assess the threat to Government [including Critical national infrastructure], business and islanders. The threat continues to develop and change with remarkable speed. The threat, and therefore our response, will need to be continuously assessed across Government, Business and Islanders and will require ongoing and continuous assessment.

Goal three: Partners

We will build international cooperation and partnerships with specialist agencies, organisations and businesses from across the UK, the EU and Jersey. We will learn from their expertise, lever their capabilities [where appropriate].

Goal four: Information Sharing

We will establish a framework and capability to confidentially share and report cyber security information across Government, Businesses and Islanders to DETER cyber attacks.

Goal five: Incident Response

We will develop, in partnership, the appropriate incident response capabilities at the strategic, tactical and operational levels to DEFEND from cyber attacks.

Goal six: Standards and Policies

We will set minimum-security standards for Government and Businesses based on international best practice. We will encourage business to adopt these and, in order to protect the wider supply chain in Government, adherence to these standards will be become part of our procurement process.

Goal seven: Law Enforcement

Whilst our response will require support and action from many parts of industry (telecommunications companies and internet service providers) and Government [including but not limited to Education and Trading Standards] we will provide a focus from Law Enforcement as the lead agency for Cyber Security.

Goal eight: Education

We will work with other committees [primarily the Committee for Education Sport and Culture] and our own agencies [primarily Trading Standards] to provide relevant, timely and accurate education on cyber security.

To deliver these strategic goals each has a number of smart objectives that are specific, measureable, achievable, relevant and time-bound. These are:

Aim

Ensure that Guernsey citizens, business and Government are as 'safe and secure' going about their legitimate lives in cyber space as they are in the physical environment.

Strategic Goal	Objective
1. Legislation and Regulation	**1.1** We will deliver new Data Protection (Bailiwick of Guernsey) Law 2017.
	1.2 We will review other relevant laws and bring forward amendments as required.
	1.3 We will enhance the 'Right to be Forgotten' in the Data Protection (Bailiwick of Guernsey) Law 2018 to provide specific protection for Children. In particular we will provide the measures so that islanders can have their social media pre-18 years old 'digital footprint' deleted.
	1.4 We will respond to and handle issues relating to telecoms supply chain security.

2. Continuous Assessment	**2.1** We will conduct annual assessment for Cyber security threats reporting to the Committee for Home Affairs [and other relevant Committees as required].
	2.2 The Chief Information Officer will report, on a monthly basis, to the Policy and Resources Committee, on the Cyber Security issues affecting the States of Guernsey.
3. Partners	**3.1** We will sign a formal Memorandum of Understanding and Cooperation between the UK National Cyber Security Centre (NCSC), Jersey and Guernsey.
	3.2 We will continue to work with the States of Jersey to develop a pan-CI cyber strategy.
	3.3 We will further develop the relationship between Guernsey Law Enforcement and other agencies [such as City of London Police, the NCA, and South West Regional Organised Crime Unit]
	3.4 We will establish a formal Cyber Partnership forum [that will meet on a quarterly basis] to discuss emerging threats, risk and mitigations. This will include [but is not limited to] Government, Law Enforcement, CNI, Business Groups.
4. Information Sharing	**4.1** We will agree access to the UK National Cyber Security Centre (NCSC) Cyber Information Sharing Partnership (CiSP) and gain formal accreditation as a referring agent so we can approve access to the CiSP for businesses, Government entities and other bodies.
	4.2 We will, working with the NCSC, establish a Guernsey [preferably Channel Islands] CiSP to provide a focus for Tactical and Operational Level Threats.
	4.3 Enhance the use of THEMIS as a secure reporting and information dissemination tool for financial cyber crime.

5. Incident Response	**5.1 (C1)** Strategic Level Incident - We will develop the procedures and processes to access and utilize the incident response capabilities of the NCSC in response to a Strategic Level attack.
	5.2 (C2) Tactical Level Incident – We will develop a Guernsey [Preferably Channel Islands] Cyber Incident Response Capability to provide the appropriate resources in response to a Tactical Level Attack.
	5.3 (C3) Operational Level Incident – We will agree the extension of the UK National Firewall over the Bailiwick of Guernsey.
	5.4 (C3) Operational Level Incident – We will further enhance [and encourage the enhancement] the capabilities of Law Enforcement, Telecommunication Companies and Local Internet Service Providers to response to Operational Level Attacks.
	5.5 In addition to our Civil Contingencies activities (or aligned with it), we will conduct an annual Cyber Security exercise to test and assure our measures to meet a Cyber Security Incident.
6. Standards and Policies	**6.1** We will review, and amend if required, the NCSC Cyber Essential, Cyber Essential (Plus) and 10 Steps to Cyber Security policies for use across the Bailiwick of Guernsey. This is in addition to other standards for specialist organisations such as ISO 27001.
	6.2 We will encourage the use and accreditation by businesses of the standards (in 6.1 above). This will include a requirement for businesses tendering for work with the States of Guernsey to meet the appropriate standard.
	6.3 We will direct the Chief Information Officer to review, and update if required, all States of Guernsey internal cyber security policies.
	6.4 The Chief Information Officer, working with the STSB incorporated and non-incorporated trading assets, to assess and report on the cyber resilience of our Critical National Infrastructure.

7. Law Enforcement	**7.1** We will develop the High Tech Crime Unit's capability and capacity to investigate and pursue cyber criminals operating within the Bailiwick.
	7.2 We will develop and maintain effective links with law enforcement partners in other jurisdictions to ensure that cyber criminality which traverses across traditional boundaries on both a national and international scale is combatted collectively.
	7.3 We will enhance and augment local, national and inter-national understanding of 'threat and risk' through engagement with the National Cyber Security Centres 'CiSP', the National Cyber Crime Unit and other such strategic partners.
8. Education	**8.1** The States of Guernsey will develop a new Cyber Security awareness-training course for all public servants.
	8.2 The States of Guernsey will develop specific digital transformation and cyber security training for senior leaders.
	8.3 Law Enforcement will continue to work with national partners and key stake holders to ensure that cyber enabled crime prevention advice is readily available throughout our communities
	8.4 The Bailiwick curriculum will have specific actions to ensure school-children can use the internet responsibly, respectively and safely.

Funding

States of Guernsey funding on cyber security has traditionally focused on internal technical security measures. In order to meet the current and future threat of cyber security this strategy deliberately moves Guernsey from a reactive to a proactive stance. In order to provide value for money to tax payers we have taken the following approach to funding the objectives outlined above:

- **Partnerships –** We will look to establish partnerships to re-use extant capabilities from partners on a no-cost or cost-price basis. For example our MOU with the NCSC will provide access to a range of UK National capabilities that would not be cost-effective for Guernsey to develop on its own. This includes [but is not limited to] Strategic Level Incident Response Capabilities, UK National Firewall, and CiSP Capabilities.
- **Prioritization –** We will look to prioritize work from Law Enforcement and Information Systems and Services (the States of Guernsey internal IT provider) before we ask for new funding.
- **New Capabilities –** Despite partnership and prioritization not all Strategic Goals can be delivered within existing resources. As such a gap analysis has been conducted and a funding bid has been prioritised as part of Capital Portfolio within the Medium Term Financial Plan. A full Business case will need to be developed but in general we will look to be investing in:

    i. C2 - Tactical Level Cyber Incident Response Capability.

    ii. Enhancements to the Internal States of Guernsey Technical Security Measures.

Committee *for* Home Affairs

For more information go to
gov.gg/cybersecurity