GUERNSEY CYBER SECURITY REVIEW

EXECUTIVE SUMMARY

FOREWORD

I am delighted that the States of Guernsey has completed a detailed cyber-security review which looks at government, businesses and individuals. Guernsey is part of a global economy and a highly connected world. Having a clear understanding of the threats, challenges, risks and opportunities that we face provides us with the evidence needed to deliver two of the key requirements of government - to ensure the safety and security of our community, and to build our economy.

Stability and security are the cornerstones of our quality of life and our economic competitiveness. One of the unique qualities of Guernsey is that our community experiences a very low level of crime, and we go about our day to day lives without the concerns of many other jurisdictions. However the computers and digital infrastructure that enable that also mean that we are potentially connected to many who, regretfully, would do us harm.

Safety and security of islanders is always paramount in my mind. This review will enable us to fully understand the threat, so that we can further develop our comprehensive and flexible approach to deal with it. Whether it is law enforcement, trading standards, government or telecommunications and IT firms, we will continue to work together to reduce the cyber-risk so that we are as safe as possible on-line. We will protect the safety and security that are part of our everyday lives.

Businesses will always be a target for cyber-criminals who have attacked companies across the banking, entertainment, telecommunications and retail sectors. Guernsey prides itself as a trusted jurisdiction, and we must ensure we remain so in the interconnected digital world. We will take risks seriously - and take appropriate steps to mitigate these risks. But through our government economic development plan, and through forums such as the joint business and government Fintech and Digital Oversight Group, we can use the cyber-review to turn these threats into opportunities. This, in turn, will enhance our offering to the existing finance sector and developing sectors that can differentiate us and provide another reason that Guernsey is a great place to do business.

Guernsey is internationally renowned as a trusted jurisdiction. This cyber-review will enable us to strengthen that trust.

Deputy Jonathan Le Tocq
Chief Minister of Guernsey/Premier Ministre de Guernsey

BALANCING OPPORTUNITY AND RISK IN CYBER SPACE

Guernsey has long had a tradition of successfully leveraging its unique geography, legal status and entrepreneurial skills to punch above its weight in the development of new products, services, and markets. The States' success in banking and fiduciary services has been extended more recently into areas such as specialist insurance, financial technology and e-gaming. Recognising the opportunities, the States have made digital government and promotion of a digital economy a central feature of their economic and social development plans.

The 2014 Economic Development Plan affirms that "one area of major focus will be the development of Guernsey's digital capability – both in terms of infrastructure on the Island and the development of islanders' digital skills". At the same time, the States are moving to embrace e-government initiatives that promise to transform the provision of services for islanders.

However, Government, businesses and islanders are becoming increasingly aware of the risks of the move into cyber-space. Threats to cyber security are increasing daily as criminals and hostile states exploit weaknesses, while vulnerabilities are also growing in an era of pervasive and always-on Internet connectivity. At the same time, rising public awareness of privacy and security issues increases the expectation by islanders and consumers that their information will be protected.

Guernsey is no stranger to dealing with 'traditional' risks such as fraud. However islanders have tended to see serious criminal, terrorist or nation state threats as being distant from their everyday concerns. Unfortunately, just as with any other nation state, the States of Guernsey's ability to control its digital borders, to police and regulate businesses, and to protect its population has been eroded in the digital age. To date, known cases of criminal attack, accidental outage and cyber-espionage have been manageable and have not seriously affected the States' reputation or wellbeing. That said, Guernsey's hard-won reputation as a trusted place to do sensitive business could easily be forfeit if there were to be a large-scale cyber security failure. Public loss of financial client customer data; release of sensitive personal records; or a significant incident of fraud, cyber-extortion or sustained denial of service attack could at a stroke set back progress.

Governments and businesses worldwide are responding to cyber-risks by developing national strategies and risk management processes, reforming legislation and regulation, building cyber security capabilities and raising public awareness. Guernsey has made a good start. Government and the private sector have begun to work together on the issue; companies and Government have adopted risk management approaches; and industry has responded with a growing array of cyber security products. However, for Guernsey to succeed in its ambitious digital vision, it must seize the opportunity now to build security into the design of its digital economy and e-government offering. This review provides the opportunity for the States to put in place the required building blocks that will secure the future of the Island's cyber-space and enable Guernsey to win competitive advantage by being seen as a safe place to do digital business.

TRENDS IN CYBER THREATS

The States of Guernsey understand that the threats in cyber space and the online digital world are real and cannot be wished away or ignored. They recognise that cyber threats will continue to grow as technology becomes ever more pervasive and integrated into our daily lives. The Guernsey Cyber Security Strategy therefore must ensure it takes account of the trends that impact all users in the digital world. Emerging trends point to the potential for a more challenging online environment for those that are unaware or unprepared.

The following trends pose threats to the island community:

- Rapid technological advances, multiplying opportunities for hostile actors.
- Increasingly innovative development of malware and its methods of delivery. More disruptive tools will be shared by adversaries through online marketplaces.
- Hacker tools and techniques that are currently rare will become commonplace.
- Advanced state threat actors will keep innovating and new state actors will emerge.
- Disruptive terrorist cyber-attacks on critical infrastructure or sensitive data centres are likely to multiply as the capability level of extremist groups matures.
- Cyber-crime will significantly increase as more services move online and criminals, operating remotely, exploit new opportunities for fraud and theft.
- Guernsey's position as a leading international financial centre is certain to attract continued attention as an attractive target for exploitation.
- Guernsey's legacy ICT systems will be upgraded to include greater interconnectivity and mobility, potentially making them more vulnerable to attack.
- National systems will aggregate increasing amounts of data. The resulting 'big data' will be an attractive target for attack and will require increased protection.

To counter these threat trends, cyber-defences must be strengthened faster than attackers can innovate. The risk of being caught and brought to justice must be made greater than the lucrative rewards cyber criminals currently enjoy. Vulnerabilities need to be closed down – without new ones being introduced – and a step-change in public awareness and security culture must be achieved.

AN OPPORTUNITY FOR MARKET DIFFERENTIATION

In addition to protecting its digital economy and Government from threats, a strong cyber security environment can provide a market advantage for Guernsey. Although a number of other countries are ahead in their investments in digitisation, building a reputation as a safe, secure and private place to do business could allow Guernsey to leapfrog other jurisdictions that lack this brand value. With the right investments in policies, structures, education and infrastructure, Guernsey can become both a thought- and market-leader in cyber-education, cyber-defence, data privacy and digital security. This is especially true in areas such as innovative financial technologies.

CYBER SECURITY REVIEW

In 2015, the States of Guernsey commissioned the Ascot Barclay Group (ABG), a Guernsey-based cyber security company to conduct a detailed assessment of the cyber maturity level of the island across Government, Businesses and Islanders.

The Guernsey Cyber Security Review consulted over 250 Islanders via one-on-one interviews, workshops and surveys across both public and private sectors as well as the general island population.

The review used ABG's *Cyber Maturity Framework*™ (CMF) which evaluated the maturity of governance, legal, cultural and educational factors in Guernsey's ecosystem. This assessment was laid against a detailed threat and risk assessment, informed by interactive workshops with States of Guernsey Government departments, Law Enforcement, Critical National Infrastructure organisations as well as Business stakeholders to generate a Gap Analysis that highlighted priority areas that needed to be addressed. This analysis generated various options for different policy approaches. The remainder of this document represents an executive summary of the results of this exercise and highlights proposed actions and priorities for the States of Guernsey.

STRATEGIC GOALS

Guernsey has three primary goals when it comes to Cyber Security and the digital economy:

1. Secure Guernsey's cyber space for Government, business and Islanders
2. Maximise opportunities for market differentiation
3. Support and enable current and future businesses in the digital space

ACTION PLAN

To achieve these goals, Guernsey should focus on the following areas:

1. Improving the skills base of islanders
2. Investing in cyber awareness and essentials
3. Setting up Island CERT
4. Facilitating information sharing
5. Building Guernsey as a base for cyber business

1. SKILLS BASE

Individuals and organisations can invest considerable time and money in deploying or reinforcing IT systems but without proper human resource development, vulnerabilities will remain. Reinforcing the human dimension of cyber security offers a relatively quick, efficient and cost effective approach towards making Guernsey a safe and digitally secure island for years to come.

Action points:

- **Policy Council**
  - Distribute cyber-hygiene Standard Operating Procedures (SOPs) and recommendations, reinforced by awareness training for all Ministers, civil servants, staff and the relevant supply chain across government departments.
  - Identify any potential weak links in the infrastructure that may offer adversaries the opportunity for exploitation. Communicate the message that one major or significant breach is all it takes to cause substantive economic, reputational or structural damage.
  - Implement an accepted standard or bench mark to reduce risk across all Government entities.
- **Commerce & Employment**
  - Sponsor workshops for private sector to improve board-level understanding of cyber security across Guernsey private sector. Target Non-Executive Directors as well.
  - Deliver or commission practical cyber-hygiene clinics to strengthen the resilience of smaller and mid-sized businesses on the island and of larger organisations where assistance from international headquarters is lacking or deemed ineffective.

2. CYBER AWARENESS AND ESSENTIALS

There is general consensus across the island community that cyber-risks can be avoided or reduced simply by raising awareness. Our analysis shows however that the level of cyber security awareness is still relatively low and needs to be improved across Government, businesses and the island community in general. Within Government, training and awareness on cyber security requires more strategic attention, not only for the induction of new staff but also for existing ministers, deputies and staff members who, like all of us Islanders, require periodic refreshes on their knowledge of new cyber threats. In smaller businesses, threat awareness levels are also generally lower than in larger businesses. Recent island-based initiatives show what can be done with limited investment. The Scams Campaign helped promote awareness among consumers, and cyber security events have reached many key business people at limited cost. Both businesses and the States now need to focus more intently on cyber-awareness and the implementation of essential cyber-hygiene.

Action points:

- **Education Department**
  - Include e-Safety and cyber security education and training.
- **Trading Standards / Skills Guernsey**
  - Continue to run ad-hoc campaigns on timely topics to educate islanders on cyber awareness issues, measuring reach and impact to improve delivery over time.

  - Develop and distribute an interactive game to learn more about the safe use of the internet and as an additional means of communicating new threats.

- **FinTech and Digital Oversight Group (FDOG)**
  - Develop and pilot a Cyber Security Kitemark jointly with private sector and run a pilot in key industries.
  - Sponsor and accredit independent assessors to certify businesses with the Guernsey Cyber Security Kitemark.
- **Police and Security Services**
  - Collaborate in the strengthening of capabilities to identify and prosecute cyber crimes and fraud in order to stay ahead of emerging threats.

3. ISLAND CERT

Developing a Computer / Cyber Emergency Response Team ('CERT-Guernsey' or 'Island CERT') would help place Guernsey at the centre of threat intelligence sharing in a manner optimised for island communities. This could be offered as a States of Guernsey paid service to other island communities (and British Overseas Territories) or else run as a shared service co-managed by the Crown Dependencies of Guernsey, Jersey and Isle of Man.

Action points:

- **Policy Council**
  - Create a Cyber / Computer Emergency Response Team (CERT) on-island responsible for threat collation & analysis, informing government policy and strategy, managing the government security operations centre (GSOC), as well as managing any necessary remedial or action against threats to Guernsey's islanders, businesses and Government.
  - Explore opportunities to serve neighbouring jurisdictions (Jersey, Isle of Man and beyond)

4. INFORMATION SHARING

Guernsey's legal system has responded promptly to cyber risk by passing new laws to tackle modern day threats and challenges. That being said, cyber-crime remains difficult to detect and trace let alone prosecute. Organisations suffer cyber-events which for commercial reasons they do not wish to share with or report to the authorities. As a result, much cyber-crime goes unreported and frauds or attacks strike other uninformed victims and cause damage that could have been prevented. Enhancing information exchange between businesses and law enforcement agencies is therefore vital if Guernsey is to respond adequately to incidents and ensure the protection of the States' cyber-space.

Action points:

- **Policy Council**
  - Create an anonymous incident reporting system connecting islanders and industry with the Guernsey Island CERT so that information may be shared safely and securely whilst protecting the anonymity of the source.
  - Create and maintain a low-cost online threat information feed to inform islanders and businesses of current cyber threats and mitigation measures to better respond to cyber threats.

  - Consider following the lead of other jurisdictions that are introducing compulsory breach disclosure to ensure the containment of particular threats. Disclosure could be managed sympathetically and kept anonymous. For example, it could be limited to a verbal information share between senior executives within Island-based organisations and specific named individuals representing the interests of the States and all who operate, live and work in Guernsey.

5. GUERNSEY AS A BASE FOR CYBER BUSINESS

With the deployment of a CERT on-island and the development of skills and awareness training across all sectors, Guernsey would position itself well to become a cyber business market leader now and in the future. The island already has promising projects that can be leveraged in this direction.

Action points:

- **FinTech and Digital Oversight Group (FDOG)**
  - Support the Digital Greenhouse project as a cultural space for cyber awareness training, professional cyber security education, eGov services testing, and domestic cyber security technology and services display.
- **Guernsey Training Agency (GTA)**
  - Promote a Cyber Education Centre of Excellence in partnership with bodies like Coventry University's MBA in cyber-security. The Centre would help provide specialist training and cyber security scholarships.

STATES OF GUERNSEY

Commissioned by States of Guernsey