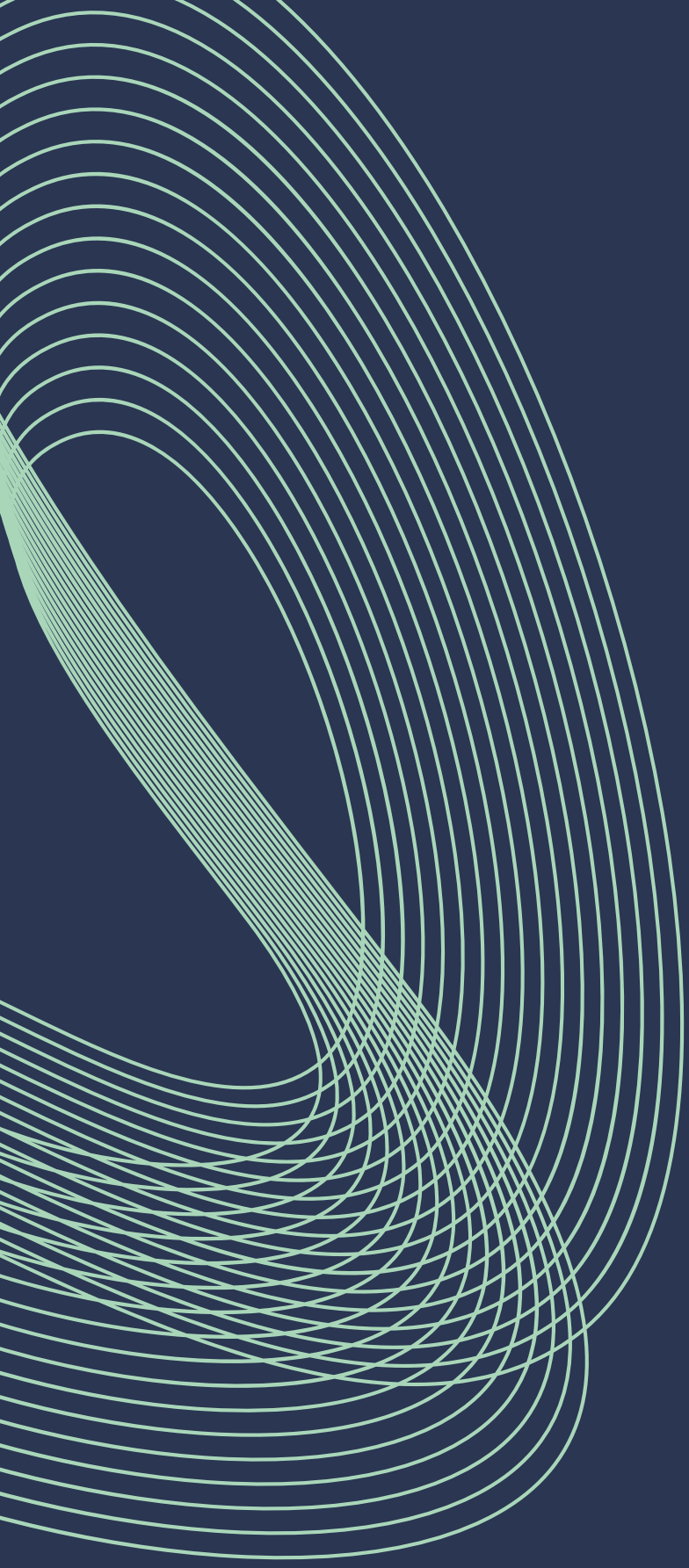
Office of Cyber-Security
& Information Assurance
Cyber-Security Centre for the Isle of Man

CLASSIFICATION: TLP CLEAR

THREAT FOCUS: RANSOMWARE

March 2023



CONTENTS

INTRODUCTION

Recently ransomware has been a hot topic with high-profile attacks on institutions such as Royal Mail bringing wider attention to this ongoing threat. However, ransomware has been a threat for a considerable period: 651 attacks were reported to the UK ICO in 2021 *(1)*, with the actual number of attacks that weren't reported being significantly higher. Indications are that the ransomware threat is continuing to grow as significant financial incentives and an ease of access into the ransomware as a service model provides an attractive proposal to cyber criminals.

'Even with a war raging in Ukraine - the biggest global cyber threat we still face is ransomware'

Lindy Cameron - CEO, National Cyber Security Centre UK

Even though ransomware is not new, technologies evolve and with them so do attacks and vulnerabilities. Organisations must be prepared for a ransomware attack in light of the continuing innovations in ransomware design. In cases where organisations are not prepared, difficult decisions must be made such as whether to pay or not to pay. Both the Manx and UK governments recommend against paying ransoms *(2) (3)*, partly because this money is used to further fuel attacks

This report will provide an overview of current ransomware threats and threat-actors, but as with any threat in cybersecurity the space is constantly evolving and it is best to continue to stay up to date by periodically reviewing a variety of sources.

(1) https://www.insurancetimes.co.uk/news/uk-ransomware-attacks-rise-by-100-in-2021-rpc/1440698.article
(2) https://www.gov.im/news/2022/jul/11/dont-pay-for-ransomware-attacks
(3) https://digitalguardian.com/blog/uk-urges-organizations-not-pay-ransomware-payments

1. RANSOMWARE: OVERVIEW

1.1 Defining Ransomware

Ransomware comprises a variety of techniques, tactics, and procedures used by cybercriminals to achieve their goals. There are various forms of ransomware that can be delivered through multiple vectors, which makes it difficult to encompass ransomware in one definition. Therefore, for the purposes of this report we will be using the ENISA definition as follows:

Ransomware is a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability and confidentiality. (4)

1.2 Ransomware Types

Defining the various types of ransomware can be challenging due to the evolution of the concept, as well as the technical capabilities that ransomware shares with other types of malware. In the past, ransomware typically had a limited focus, such as encryption or locking, which allowed for easy categorisation into simple groups like Encryption Ransomware or Lock-Screen Ransomware. However, the evolution of ransomware means that these categories are no longer adequate to describe the different types of ransomware, as they are no longer restricted to specific actions or targets.

The difficulty in naming ransomware is compounded by the inconsistent naming conventions used by the cybersecurity industry and the assumption that specific types of ransomware are mutually exclusive, for example, that Encryption Ransomware only encrypts files and does not perform any other actions.

(4) https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

1.3 Motivators

Ransomware attacks are primarily carried out for financial gain. Cybercriminals use this type of malware to extort money from victims by demanding a ransom payment in exchange for restoring access to their encrypted files or systems. However, in recent years, there has been an increase in the number of ransomware attacks that are carried out by state-backed actors. These actors, who are typically government-sponsored, use ransomware as a tool to achieve political or strategic objectives.

In addition to financial gain, these actors may also seek to obtain valuable information, disrupt critical infrastructure, or gain leverage in negotiations. State-backed ransomware attacks can be particularly dangerous, as the attackers often have significant resources and advanced capabilities at their disposal. As such, it is essential for individuals and organisations to take steps to protect themselves from all forms of ransomware.

2. RANSOMWARE: DEPLOYMENT

2.1 Initial Access

The first step in a ransomware attack is gaining initial access to the target system. Attackers may use a variety of methods to gain this access, including exploiting software vulnerabilities, stealing credentials, phishing, or using other techniques. However, the current techniques for initial access are often difficult to determine because organisations that are compromised often do not report incidents. This lack of information-sharing can result in reduced knowledge of the techniques being used and consequently an inability to effectively design defences. We encourage any organisation hit by ransomware to report it to OCSIA using our cyber concerns reporting point - all reports are kept strictly confidential.

2.2 Execution

Once initial access is obtained, threat actors may study the target and move laterally within the system to locate assets that can be exploited. This stage can take several weeks, depending on the size and defences of the target. Before executing the ransomware, there is usually a cleaning process to ensure that the ransomware will function correctly. This process may involve disabling security software, stopping databases or other programs that could interfere with the writing of the ransomware, and disabling recovery features such as shadow copies and logs.

The ransomware is then deployed through various means, such as direct deployment or delivery through third-party botnet-based malware mechanisms.

2.3 Threat Actor Objectives

The threats made in ransom demands have also evolved, with new forms of coercion being introduced. In addition to monetary demands, threat actors may threaten to leak data, delete assets, or resell data to competitors. They may also

threaten to launch distributed denial-of-service attacks against the target's infrastructure, increasing the stress and incentive to pay. All of which will only stop after successful negotiation of the ransom payment.

It is important to note that the Isle of Man Information Commissioner should be informed of any ransom demands. The UK ICO has published guidance on what organisations should do in the event of a ransomware attack and also recommends that all incidents should be reported to them (should you be based in the UK).

While monetary demands are still the primary goal of ransomware, there are instances where threat actors may request other forms of payment, such as asking companies to add or remove software features in their products or demanding targets to infect others to obtain free decryption keys. As well as state backed actors looking to disrupt critical national infrastructure.

2.4 Blackmail

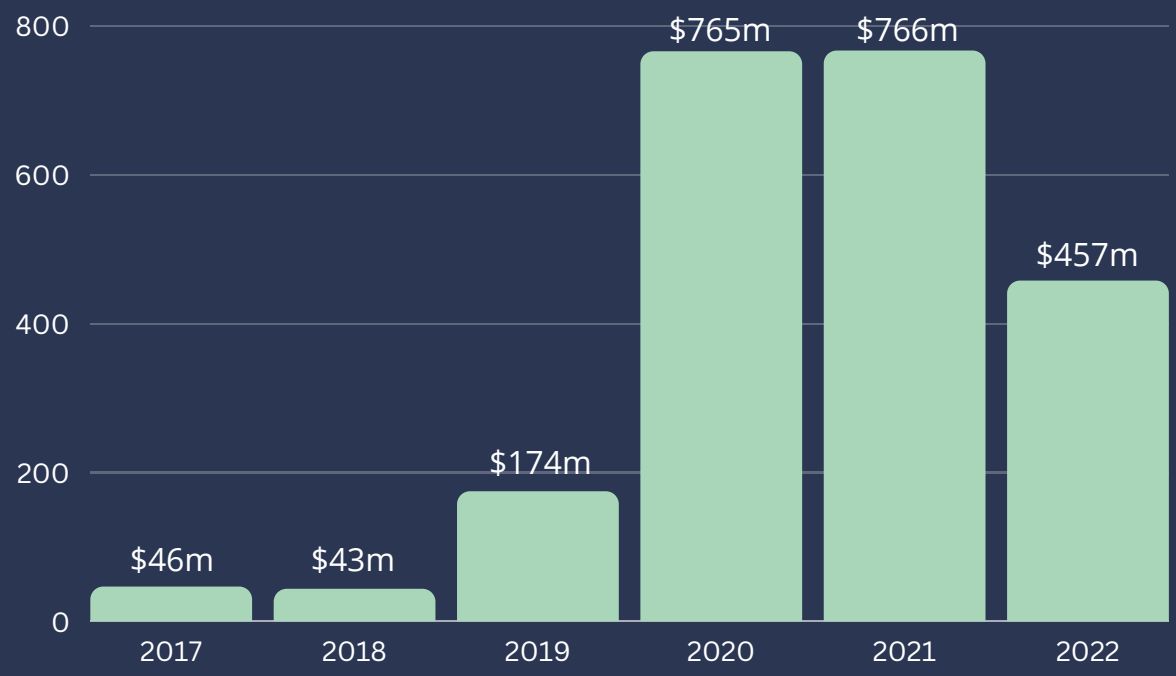
After gaining access to the target's assets, the threat actor will proceed to blackmail the target in exchange for the availability of the assets. This typically involves communication, threat, and demand. Communication is the act of informing the target that their asset is no longer available. The threat is the potential loss or damage that will occur if the demand is not met, and the demand is what the threat actor expects to obtain from the situation.

As ransomware attacks have become more prevalent, the communication of ransom demands has changed from private to public. In the past, ransom notes were displayed on affected systems with instructions on how to pay and communicate with the threat actor to negotiate. However, nowadays, it is common for threat actors to publicly showcase ransom incidents, including information on affected assets, ransom demands, and with a public discrediting of the target. Some threat actors may also coerce not only the target, but also their customers, partners, and interested parties, adding pressure on the target. After a set period of time details might be posted on the dark web and some even host on line auctions for the stolen data.

2.5 Ransom Negotiation

Negotiations regarding ransomware typically occur in private between the targeted organisation or individual and the threat actors. It is important to note that this is not a recommended course of action and OCSIA recommends not engaging with the criminals. Communicating with the criminal confirms they have been successful and could start a countdown timer. The result of these negotiations can have one of two outcomes: the target pays the ransom or they do not. Specialist advice should be sought.

Total value received by ransomware attackers, 2017 - 2022



(5) https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/

Research by chainanalysis showcasing the different values extorted by ransomware attackers, these amounts are not exhaustive and actual totals will be much higher.

3. ATTACK VECTORS

3.1 Vulnerabilities

Ransomware attacks often exploit software vulnerabilities to gain access to a victim's computer system. A vulnerability is a weakness in software that can be exploited by attackers to gain unauthorised access to a system. Attackers can use vulnerabilities in a variety of ways, such as by focusing on unpatched software, tricking users into running malicious software, or gaining access through a compromised third-party service.

One of the most widely known exploits was Follina. Follina is a vulnerability that was discovered in the Microsoft Support Diagnostic Tool and was exploited by attackers to deploy malware. The vulnerability allowed the attackers to execute remote code on the victim's system. Follina has been used to deploy a variety of Malware *(6)*

Another example is the WannaCry ransomware attack that occurred in 2017. The attack targeted a vulnerability in the SMB protocol of Windows called EternalBlue, which was developed by the National Security Agency (NSA) and leaked by a group called Shadow Brokers. The WannaCry ransomware was able to spread rapidly to vulnerable systems and caused widespread disruption to businesses and organisations worldwide *(7)*.

Patching software is critical in preventing these types of attacks. Software vendors regularly release updates that contain security patches to fix vulnerabilities in their software. It is essential to apply these updates as soon as possible to reduce the risk of being targeted by ransomware attacks that exploit vulnerabilities. However, well-prepared an organisation is, sometimes criminals can deploy ransomware through vulnerabilities that have not yet been patched.

(6) https://www.securityweek.com/follina-vulnerability-exploited-deliver-qbot-asyncrat-other-malware/
(7) https://www.mandiant.com/resources/blog/smb-exploited-wannacry-use-of-eternalblue

3.2 Phishing

Phishing is one of the most common ways ransomware is deployed. Attackers send a convincing email that appears legitimate, but it contains a link or attachment that, when clicked, downloads the ransomware onto the victim's computer.

One well-known example of a ransomware attack that was spread through phishing emails is the Locky ransomware. Locky was first discovered in 2016 and was distributed primarily through spam emails that contained malicious Microsoft Word attachments.

The emails were designed to look like legitimate messages, often appearing to come from a reputable company or organisation. The attachment in the email contained a macro that would download when the file was opened and then install the Locky ransomware onto the victim's computer.

Locky quickly became one of the most widespread ransomware threats, infecting hundreds of thousands of computers worldwide and causing significant disruption to businesses and organisations. The attack demonstrated the effectiveness of phishing emails as a means of distributing ransomware, and highlighted the importance of user awareness and education in preventing these types of attacks.

3.3 Supply Chain Attack

Supply chain attacks are an emerging threat that target software developers and suppliers. The goal is to deploy ransomware to a target through a supplier to their customer, this type of attack vector is often used to target critical national infrastructure whose suppliers may lag behind the security measures imposed by themselves.

Attackers hunt for unsecure network protocols, unprotected server infrastructures, and unsafe coding practices. They break in, change source codes, and hide malware in build and update processes.

Because software is built and released by trusted vendors, these apps and updates are signed and certified. In software supply chain attacks, vendors are likely unaware that their apps or updates are infected with malicious code when they're released to the buyer. The ransomware then runs with the same trust and permissions as the app.

One example involves the cyber-espionage group known as Dragonfly (also known as Energetic Bear, Havex, and Crouching Yeti) who have a history of targeting Western energy companies through their suppliers.

In one attack, Dragonfly successfully 'trojanised' legitimate industrial control system (ICS) software. To do so, they first compromised the websites of the ICS software suppliers and replaced legitimate files in their repositories with their own malware infected versions.

Subsequently, when the ICS software was downloaded from the suppliers' websites it would install malware alongside legitimate ICS software. The malware included additional remote access functionalities that could be used to take control of the systems on which it was installed *(8).*

(8) https://www.ncsc.gov.uk/collection/supply-chain-security/third-party-software-providers

4. RANSOMWARE BUSINESS MODELS

Ransomware businesses models have significantly changed with the ransomware groups evolving into business-like structures. Because of this it's useful to categorise attackers into a number of business models.

4.1 Ransomware as a service (RaaS)

A business model known as 'ransomware as a service' (RaaS) involves ransomware operators and affiliates, in which affiliates pay operators to initiate ransomware attacks. The business model is similar to the 'software as a service' (SaaS) model used by legitimate businesses. A RaaS kit may contain bundled deals, user reviews, forums, round-the-clock assistance, and other services that are the same as those provided by reputable SaaS providers. RaaS kits can cost as little as £30 per month.

The real threat of RaaS kits is it allows affiliates lacking the skill or time to develop their own ransomware variant to be up and running quickly and affordably. Allowing inexperienced amateurs to extort unprepared businesses out of significant amounts of money. They are often easy to find on the Dark Web, where they are advertised in the same way that goods are advertised on the legitimate web. The more successful kits are operated on a basis that the purchaser can satisfy the provider that a certain skill set is able to undertake the function so as not to risk their product being picked up and reverse engineered for a fix.

4.2 Group Actors

A single group of threat actors, which is now thought of as the traditional ransomware business model, share, split, and coordinate all the stages of the operation, including selecting the target, vetting the target for vulnerabilities, carrying out the attacks, creating the malware and infection, coordinating the file

encryption keys, negotiating the ransom payment, and collecting the money. The same gang often creates all of their tools, establishes the payment method, and purchases vulnerabilities or the data needed to launch successful assaults.

4.3 State Sponsored Actors

State-sponsored threat actors differ from others because of the differences in motivation. Rather than monetary gain state-sponsored actors are driven by military, commercial, or political objectives. They frequently use hostile cyber operations such as ransomware to acquire sensitive assets for competitive advantage or to damage the national security. To accomplish these goals, state-sponsored threat actors frequently target third-party businesses.

4.4 Individual Actors

Attacks using ransomware were first carried out by individuals or very small organisations. Compared to operations today, these ransomware campaigns were simpler and frequently relied on automated encryption that did not depend on operational collaboration. The development and dissemination of the ransomware were the perpetrators' main concerns. It is exceedingly difficult to determine which groups initially consisted of sole individuals and how long they did so. Individual actors quickly realised that significant labour was needed to deploy a ransomware attack and, therefore, they began organising into small groups.

Individual groups can be identified through their specific skillsets and not just the type of ransom. In some cases they focus on virtual machine platforms, or exclusively operate on windows or MAC, or Android etc..

IN THE NEWS

With the increase in ransomware attacks across all sectors of the economy and public showcasing on the Dark Web, it is to be expected that high-profile targets will receive news coverage.

ROYAL MAIL CYBER ATTACK

On January 11, 2023 Royal Mail reported a cyber attack that caused severe disruption to its systems used for sending mail abroad. The attack affected six Royal Mail sites, including the company's Heathrow Airport distribution centre, and affected its ability to track and trace items sent abroad and prepare mail for dispatch overseas. The attack prompted the company to request that customers stop sending mail abroad owing to expected severe delays.

Subsequent reports on January 12 revealed that the cyber incident was a ransomware attack by the Russian ransomware-as-a-service (RaaS) gang LockBit.

The attack involved printers at the Royal Mail distribution centre in Belfast, Northern Ireland, printing letters from the gang, which claimed responsibility for the disruption and demanded ransom payments. The Cybersecurity news site Bleeping Computer confirmed the involvement of LockBit, stating that it had seen an unredacted version of the ransom letter that included the Tor websites for the LockBit ransomware operation.

Royal Mail, however, has not publicly attributed the attack to LockBit. The company immediately launched an investigation into the incident and worked with the UK's National Cyber Security Centre, Information Commissioner's Office, and National Crime Agency.

THE GUARDIAN RANSOMWARE ATTACK

The Guardian newspaper was hit by a ransomware attack in December 2022 that resulted in unauthorised third-party access to parts of its network. The personal data of UK staff members was accessed, but there is no reason to believe that the personal data of readers and subscribers has been accessed.

The attack was detected on 20 December, and the Information Commissioner's Office and UK police were informed.

Throughout the widely publicised attack the guardian was able to continue normal operations with staff working from home.

Whilst speculation, this could indicate good network segregation by the organisation who have allowed the ransomware not to significantly impact operations. Furthermore this could also reflect on the solid nature of The Guardian's business continuity plans.

YUM BRANDS

Yum Brands, which owns KFC, Pizza Hut and Taco Bell, confirmed that it was hacked in early 2023, resulting in a ransomware attack on some of its information technology systems and the theft of data from its network. The company responded immediately by deploying containment measures, taking certain systems offline, and implementing enhanced monitoring technology.

As a result, roughly 300 locations in the United Kingdom were closed for a day. Yum Brands also engaged cybersecurity and forensics professionals and notified US federal law enforcement, and an ongoing investigation is currently underway.

EDUCATIONAL INSTITUTIONS TARGETED

The hacking group 'Vice City' leaked confidential data from 14 UK schools online after the institutions refused to pay a ransom demand. The documents include sensitive information such as special education needs details, passport scans of pupils, and staff pay scales and contracts. Vice Society has previously targeted education institutions in both the UK and US.

The schools affected by the attack include Durham Johnston Comprehensive School, Mossbourne Federation in London, and St Paul's Catholic College in Sunbury-on-Thames. In October 2022, the Los Angeles Unified School District warned that Vice Society had begun posting data it stole from the institution.

The education sector has been heavily targeted by ransomware in recent years. A report by Sophos found that 56% of lower education institutions and 64% of higher education bodies had been hit by ransomware in the previous year *(9)*. Schools and universities have become a lucrative target for cyber criminals due to factors such as a lack of cybersecurity Investment and vast numbers of devices connecting to their systems.

Experts have warned that education institutions must be prepared to both prevent and respond to ransomware attacks or risk having sensitive data stolen and leaked.

What is particularly worrying is the nature of data stolen by criminal gangs, as schools records will contain significant amounts of special category data.

(9) https://news.sophos.com/en-us/2022/07/12/the-state-of-ransomware-in-education-2022/

ABOUT US

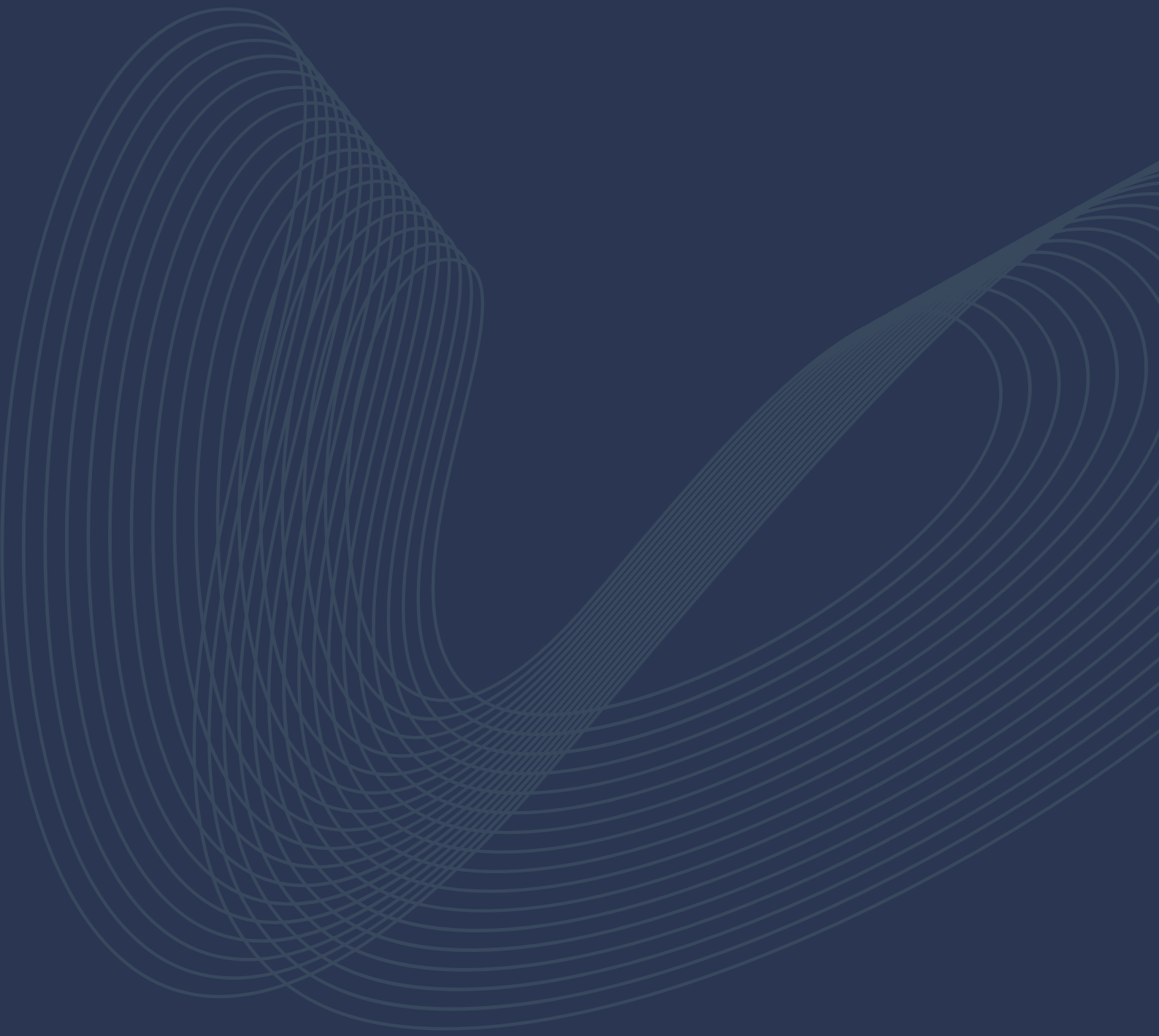
The Office of Cyber-Security & Information Assurance (OCSIA) was established by a Council of Ministers Directive in October 2017.

It acts as the focal point in developing the Island's cyber resilience, working in partnership with private and third sector organisations across the Island alongside the wider population.

The office is committed to supporting Island-residents and businesses by providing practical and targeted advice and guidance. This includes working in partnership with the private sector to improve their cyber resilience and raise awareness about the latest cyber threats affecting our Island.

OCSIA also hosts an annual conference 'CYBERISLE' which is held over the course of one day, and helps business leaders, individuals, community and charitable organisations understand the rapidly changing cyber-security threat landscape.

We would welcome your thoughts on the contents on this document, and if you wish to speak to us please don't hesitate to contact us via cyber@gov.im or through our Cyber Concerns reporting point. All discussions will remain strictly confidential.



Disclaimer

The material in this document is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances. OCSIA accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Open Government Licence

Office of Cyber-Security
& Information Assurance
Cyber-Security Centre for the Isle of Man

www.ocsia.im
cyber@gov.im
01624 685557

Office of Cyber-Security & Information Assurance
2nd Floor
Former Lower Douglas Police Station
Fort Street
Douglas
Isle of Man
IM1 2SR

T: +44 1624 685557

Isle of Man Government
Reiltys Ellan Vannin