Appendix 1

Bermudan Government Cyber Attack 2023

On 20 September, five weeks after a cyberattack on the government's IT systems, the Bermudan 'Royal Gazette' has reported that public services are still not fully restored following September's cyber-attack.

For several days following the attack, government staff had no access to email and the Government's main switchboard was unavailable. Communication with the public often had to be arranged though social media and through the use of mobile phones, including a supposed increase in the use of WhatsApp and Gmail.

A report on cybersecurity published in September 2019 highlighted shortcomings in the country's cyber security posture sand called for urgent actions to protect its cyberspace.

Colonial Pipeline Ransomware 2021

On May 7th 2021, the Colonial Pipeline that provides gasoline and jet fuel to the South-eastern US was subject to a ransomware attack, impacting the computerised equipment managing the pipeline. The attackers asked for 75 Bitcoin (then equal to $4.4 million) to provide the government with the tool required to restore the system. Under FBI instruction, the ransom was paid to the attackers, who are believed to belong to the DarkSide group, and upon receipt they provided the decryption tool required for restoration.

The provided tool was able to restore the system, but the processing time was long, leading to the pipeline being down until May 12th. After 4 days of shutdown, fuel shortages began to occur, due to panic buying over fears of a long-term shutdown. Multiple flights were disrupted, with flight schedules changed, due to the fuel shortage. Following the attack, the price of fuel rose to over $3/gallon after the attack, which was the highest it had been since 2014.

Vodafone Portugal 2022

On February 7th Vodafone was targeted by a cyberattack that lead to the temporary disruption of critical services, and wide scale reputational damage. Misinformation about the attack spread quickly due to the geopolitical environment during a time of cyberattacks and public unrest.

The effect of the attack was that Vodaphone Portugal's network was taken down, and was only restored to full capacity 4 days later. Vodafone Portugal Chief Executive deplored the attackers for "[shutting down] schools, hospitals, firefighters, companies, families… the lives of millions of Portuguese"

Appendix 1 (continued)

Irish Health Service Executive Ransomware 2021

On May 14th 2021 the Irish Health Service Executive (HSE) suffered from a major ransomware attack, causing all IT systems to be shut down.

The attackers are still unknown, but presumed to be the Russian criminal group WizardSpider. The attackers launched the attack through an email containing a malicious Microsoft Excel file on March 16th, which when downloaded gave the attackers access to the HSE systems. This access continued to grow over the following weeks.

8 weeks after the initial infection the Conti ransomware was detonated, leading to the compromise and abuse of several high privilege accounts, the compromise of a significant number of servers, and the exfiltration of data, before moving laterally to statutory and voluntary hospitals.

Following the identification of the malware, the HSE shutdown all IT systems and access to the National Healthcare Network. The ransomware cyber-attack had a significant impact on hospital appointments across the country, with many appointments cancelled including all outpatient and radiology services. Several hospitals described situations where they could not access electronic systems and records and had to rely on paper records, with significant disruption to routine appointments, including maternity check-ups and scans.