ARTICLE

APPLEBY

CYBERSECURITY IN THE ISLE OF MAN

by Andrew Webb and James Dean

July 2017

In recent months many major companies across a diverse range of industries have been the victims of hacking. Unlike previous hacks in the past such as the Mossack Fonseca release of confidential information these are financially motivated through the use of Ransomware. This is why it has never been more important for businesses to have full understanding of the requirements imposed on them by law to prevent financial and reputational loss to their business. Not only will a business suffer but individuals in that company, such as directors, may have criminal proceedings brought against them and could be subject to fines. This article will provide you with a quick overview of the cybersecurity legislation in place on the Isle of Man.

TYPES OF THREATS

Historically the most common form of hacking is Phishing where a hacker will target an individual and through the use of either spam emails or fake websites attempt to trick them into providing their personal details such as bank details or personal passwords. In the past few months the threat of hacking has been growing at an alarming rate and hackers are deploying various new methods. They are deliberately targeting businesses that may potentially have overlooked their cybersecurity due to lack of threat in the past.

As mentioned Ransomware has now been drawn into the public eye through many public attacks and due to the South Korean web provider Nayana paying out about $1 million in Bitcoins to the hackers. This may only further encourage others to pursue this potentially lucrative method. Ransomware is when software is maliciously deployed onto a computer that blocks access to data until a ransom is paid. In more elaborate attacks this can be combined with other hacking tools advertising a method preventing or removing the Ransomware in question, which in turn is malware software that causes further harm once downloaded.

OUTLINE OF THE LEGAL FRAMEWORK

In the Isle of Man at present there is no comprehensive piece of cybersecurity legislation, instead a number of different statues govern cybersecurity.

Data Protection Act 2002 (the DPA)

Regulates the storage of information and imposes obligations to protect personal data collected by a company through security measures under the Seventh Principle of the DPA. A breach of the obligation to keep data secure gives rise to potential criminal sanctions and/or financial penalties enforced by the Isle of Man Information Commissioner (the **Commissioner**).

Computer Security Act 1992 (the CSA)

The CSA criminalises the interference with computers without authority, including where the intention is to commit other crimes by means of accessing computers, altering computer programs or producing 'hacking tools'. Offences under the CSA are not limited to the offenders being present in the Isle of Man.

WHO IS RESPONSIBLE FOR CYBERSECURITY

Any business requiring a licence under the Financial Services Act 2008 will be under the regulatory surveillance of the Financial Services Authority (the **Authority**). The Financial Services Rulebook (the **Rulebook**) as published by the Authority to provide guidance for regulated businesses makes it clear that any serious or significant incident involving data loss, financial loss, and disruption to services or denial of services should be disclosed to the Authority. It would be good practice for a company to not only inform the Authority of actual breaches of network security but also prevented breaches. Additionally the Authority has published specific regulatory guidance on cybersecurity highlighting the risks and to draw businesses attention to the legal and regulatory provisions.

SHARING OF INFORMATION

One of the biggest areas that any business will have to strengthen is the improvement of its data lineage techniques in order to have a comprehensive understanding as to who holds what data, the time they are in possession of the data and more importantly what security do the holders of the data have in place.

The Eighth Principle of the DPA relates to how personal data is shared and transferred and requires any data that is sent off island to be done so only to territories which guarantee an appropriate level of protection for the data and its subject. Similarly, the standards of the General Data Protection Regulation (the **GDPR**) will have to be met if information is to be transferred outside of the EU. Approved codes of conduct and certifications will likely be the mechanism used to prove satisfactory status under GDPR (which will be in effect from 25 May 2018).

FUTURE DEVELOPMENT

The Directive on Security of Network and Information Systems (the **Directive**), which is seen as the first comprehensive piece of EU legislation on cybersecurity was approved by the European Parliament in 2016. Member States will have to implement the Directive into their national laws by 2018. Some security provisions in the Directive overlap with the GDPR, which the Isle of Man has indicated it will elect to adopt. But it remains to be seen if the Isle of Man will implement the Directive.

The GDPR establishes one single set of rules across Europe so that there is no longer a discrepancy amongst member states. Whilst the Isle of Man is not a member state it is deemed a third country under the GDPR. Therefore in order to obtain adequacy finding which will allow personal data to travel in and out of the EU to a

third country (such as the Isle of Man) and vice versa it will need to comply with the GDPR. All Isle of Man businesses carrying on business with member states will need to comply with the GDPR by 25 May 2018.

These new regulations extend the security coverage and provide the Commissioner with extended powers and fines. Regular review and testing of the cyber security measures will also be required. With large scale and sophisticated cyber-attacks becoming increasingly regular it is not surprising that the GDPR strengthens the requirement for organisations to implement the appropriate technological and organisational cybersecurity measures. The GDPR looks to equate organisational and managerial responsibility for cybersecurity with technological precautions.

With the current rate of new technological developments and the hackers adaptability to exploit them it is imperative that companies review their legislative compliance and take urgent steps to rectify any potential breaches.

This article has been written by:

Isle of Man
Andrew webb
Counsel
awebb@applebyglobal.com

Isle of Man
James Dean
Trainee
jdean@applebyglobal.com

Andrew Webb is Counsel in the Corporate Department at Appleby. A copy of this article is available on the firm's web site at applebyglobal.com