SEPTEMBER 2017

mourant

UPDATE

# Cyber security: the evolving nature of a director's duty

Update prepared by Tina Asgarian (Senior Associate, Guernsey)

With the increasing frequency of cyber-attacks, failing to properly prepare for a cyber-attack could leave directors exposed to personal liability. This update considers the changing landscape of directors' duties and outlines some of the issues directors may need to think about before the gap between criminal culpability and a company's ability to defend itself becomes insurmountable.

For many companies operating within Guernsey's financial sector, their most valuable assets are held in digital format and the threats to their business are evolving. This year many businesses have seen the re-emergence of previously seen attacks such as ransomware, whilst others are reporting new and innovative attacks. In some cases there have been reports of attackers destroying back-ups, leaving companies with little choice but to consider paying up or lose their data. As long as cybercrime continues to pay, the Guernsey financial sector will continue to be at risk and as the tools at the disposal of cybercriminals grow in sophistication, board members should ensure that they understand and are able to deal with the threats which face their company. The risks for companies have been well documented. However, the risk for directors who struggle to get the basics right is uncharted territory, and a failure to prepare properly for a cyber-attack and implement recommended guidelines could leave directors exposed to personal liability.

## The evolving role and obligations of directors and non-executive directors

In order to consider how and why directors' duties are changing (including their exposure to personal liability) it is useful to briefly revisit a director's core duties. A director's relationship with the company (and indeed any individual who discharges the function of a director regardless of whether they have the title[1]) is primarily a fiduciary relationship. Directors owe a duty to act in the best interests of the company, in good faith and honestly and a breach of these duties may result in personal liability on the part of the director. In discharging their duties, directors should always consider whether they are: acting in the best interest of the company and promoting its success; exercising independent judgment; exercising reasonable care, skill and diligence; and avoiding conflicts of interest. Alongside these fundamental duties, directors should also be mindful of their obligations towards the regulator.

Over the next 18 months, the legal framework relating to cybersecurity and data loss is set to change. Whilst the core obligations and duties which a director owes to the company have not changed, the terms of reference are evolving fast. Cybersecurity can no longer be seen as an 'IT issue' and a problem which directors do not need to worry about. Many companies have employed a Chief Information Officer (CIO) to oversee the implementation of appropriate security measures or established a committee to assess the risk and guard against potential threats, but delegation without supervision or control may not be sufficient to prevent a director from personal liability.

[1] In Guernsey, duties owed by 'directors' apply to non-executive directors, alternate directors, and shadow directors. In other words, to any person occupying the position of director by whatever name called. What is important is the substance of the duties carried out by the individual.

## Back to basics

In the aftermath of a cyber-attack, the first port of call for an investigation will be to look at what risk management regime the directors implemented to protect the company. This may include:

- the type of network security and how often it is tested and monitored
- anti-malware software
- staff training
- security policies including home and mobile working policies and access to removable data, and
- the incident response plan in place.

Most directors will not have the skills or experience to assess the company's security risk but directors will be expected to recruit appropriate talent, such as a CIO, to manage the cybersecurity risk. Being able to distinguish between the delivery of IT and information security is an important corporate governance step. Simply delegating tasks down the chain without oversight and without understanding where the company's vulnerabilities lie could be construed as failing to act with reasonable care, skill and diligence.

A director has a continuing obligation to acquire and maintain a sufficient knowledge and understanding of the company's business to be able properly to perform the duties of a director. In the context of cybersecurity, this does not require a director to know the underlying policies word-for-word, but they should be aware of the information risk management system and what strategies have been implemented and why. Directors are advised to review and consider the UK Government's 10 steps to cyber security[2] to better understand the threats which their firms might face. Effective management needs to be coupled with good basic controls and directors should test and question the policies. They should ask, where necessary, what third party standards they meet, whether the safeguards are tested to assess vulnerabilities and ensure that the systems and protocols do not fall short of the company's insurance policy requirements. A director may be better placed than the CIO or its team of information experts to understand which areas of the business are more likely to be exposed to an attack (for example data or intellectual property) and therefore which areas should be prioritised for protection.

Directors need to know how they will react to an attack, who should be informed and what actions to take. Directors should also consider how the board will discuss confidential, legal or litigation advice in board meetings after the event, consideration of which will extend to reports prepared for the board assessing the company's potential exposure, which in the event of litigation may fall within a company's disclosure obligations.

Other examples may include the need to review standard contracts to see if the parties can rely on a data breach as grounds for early termination and consider whether force majeure clauses should be inserted into standard contacts.

Insurance policies should be routinely monitored to ensure that the company has adequate cover in the event of a cyber-attack. Alongside the company's insurance needs, directors should not forget their own D&O policies and related indemnities. As regulatory investigations become more commonplace, directors would be advised to check the level and extent of their cover to ensure that they have adequate insurance cover in place.

The above are some examples of how a director's duty to act in the best interest of the company needs to evolve, but directors will not be expected to prepare for every eventuality. It is unlikely that their duties and obligations will be breached by a mere error of judgement. However, if they fail to take reasonable action and recognise that the duties they owe extend to ensuring the company is as prepared as it can be for a cyber-attack (ie, given its size, resources, vulnerabilities etc) then they may be exposing themselves to personal liability, regulatory sanction and, in an extreme case, criminal liability for breaches under section 515 of the Guernsey Companies Law.

[2] https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/NCSC%2010%20Steps%20To%20Cyber%20Security%20NCSC.pdf

## The Guernsey Financial Services Commission (the GFSC)

If the company is a licensed company, then directors will need to be aware of their obligations to the regulator. The GFSC is able to take action if a director fails to discharge their regulatory obligations including issuing public statements, disqualification orders and personal financial penalties. Recent public statements demonstrate the seriousness with which the GFSC takes breaches and the levels of fines that can be imposed on directors. In the event of an inspection, directors should be prepared to demonstrate how they have assessed the risks to the company, and the ways in which this was monitored and controlled. Procedures and policies will need to be carefully documented, periodically reviewed, and above all directors will be expected to demonstrate that they have effective oversight and control of the measures they have implemented.

## Developments in Data Protection Law

Section 61 of the Data Protection (Guernsey) Law 2001 provides that directors may be liable where an offence has been committed with a director's consent, connivance or due to their neglect, and may be punished accordingly. On 25 May 2018, the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) will come into force in the UK. The GDPR will impose severe penalties for non-compliance (up to 20 million euros or four per cent of a company's worldwide turnover). The States of Guernsey have confirmed that the GDPR will be incorporated into local law with the aim to be ready for implementation in May 2018. Compliance with the GDPR and other legislative changes which affect the way in which data is stored and secured will rest with the board. Directors will need to monitor developments and changes to the applicable legislative regimes and ensure that every system meets these requirements. The board will need to adopt a risk based approach to governance.

In addition, a major data breach involving a large number of data subjects could give rise to legal action, whether or not financial loss has been suffered. As the recent English case of *Google v Vidal-Hall and others* [2015] EWCA Civ 311 demonstrates, it is not just the regulators that companies need to be concerned about. In this case, three individuals brought claims in England against US based Google Inc for misuse of private information and breach of the English Data Protection Act 1998.

## Limiting the risk

Each business will have different levels of risk, varying budgets and vulnerabilities, and there is no one-fit solution. Whether a director has acted in breach of the duties owed to the company ultimately depends on the facts of each individual case; however, directors who act reasonably and pro-actively to ensure that their company implements technical and operational measures to prevent and minimise the likelihood of a cyber-attack will have gone a long way to ensuring that they have discharged their duties.

As a minimum, directors may wish to take the following practical steps:

- Employ (or engage) a dedicated cybersecurity expert, a person qualified to brief and train the board of directors regularly.
- Carefully formulate a robust policy on cybersecurity which is constantly monitored and reviewed, forming part of the governance framework, and record all consideration and action taken.
- Ensure the company has adequate insurance and that the board of directors understand the extent and limits of the policy.
- Agree contingency measures for during and after an attack and be prepared to respond to an attack with a detailed plan which has been tested.

## Contacts

Tina Asgarian
Senior Associate, Guernsey
+44 1481 731 447
tina.asgarian@mourant.com



[Document Reference]