CYBER SECURITY: THE EVOLVING NATURE OF A DIRECTOR'S DUTY

WRITTEN BY TINA ASGARIAN, LAUREN MCLEOD & ROBERT SHEPHERD

31 AUGUST 2017

In the fourth of Compliance Matters' series of regulatory columns by experts in Guernsey's legal sector, Mourant Ozannes Partner Robert Shephard, Senior Associate Tina Asgarian and Associate Lauren McLeod discuss the ever-more relevant issue of cyber risk and the role of directors in making sure their business is secure for outside threats.

Many companies that operate in Guernsey's financial sector hold their most valuable assets in digital form. Threats to their business are therefore evolving daily. This year, many businesses have seen the re-emergence of "old school" IT attacks such as ransomware, while others are experiencing (and telling regulators about) new and innovative attacks. In some cases, there have been reports of attackers destroying back-ups, leaving companies with little choice but to pay up or lose their data.

As long as cyber-crime continues to pay, Guernsey's financial sector will continue to be at risk. As the tools at the disposal of cyber-criminals grow in sophistication, board members at banks, fund firms and other financial institutions must change their agenda to ensure that they understand and are able to deal with the threats that face their organisations.

The risks for companies have been been the subject of many books already, but the risk for directors who are struggling to get the basics right is uncharted territory. This is worrisome because any failure on their part to prepare properly for a cyber-attack by following recommended guidelines might land them in personal trouble with the law and with regulators.

The evolving jobs and obligations of executives and NEDs

The purpose of this article is to glace at the changing landscape of directors' duties and the issues that directors may have to consider before the gap between criminal capability and a company's ability to defend itself becomes unbridgeable.

Let us first examine the main duties that every director has. 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. The substance of the duties carried out by the individual are of sole importance here.

The director's relationship with his company (and indeed this applies to anyone who discharges the function of a director, regardless of whether he has the title of director) is primarily a fiduciary relationship of trust. Directors owe a duty to act in the best interests of the company and in good faith and honesty. If they fail in these duties, they may incur personal liability.

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 duties and obligations towards the regulator.

Over the next 18 months, the law relating to cyber-security and data loss is going to change. Although the main obligations and duties that a director owes to the company will not change, the terms of reference are evolving as fast as cyber-threats are. Cyber-security can no longer be seen as issue merely for IT departments and a problem about which directors need not worry. Many companies have employed a chief information officer (CIO) to

oversee the implementation of appropriate security measures or to establish a committee to assess the risk and guard against potential threats, but delegation without supervision or control may not be enough to protect a director from personal liability.

Back to basics

In the aftermath of a cyberattack, the investigator will begin by gauging the worth of the information risk management regime that the directors have set up to protect the company. He might look at:

- the type of network security and the frequency with which the company tests and monitors it;
- anti-malware software;
- staff training;
- security policies, including home and mobile working policies and access to removable data; and
- the incident response plan that is in place.

Most directors lack the skills and experience to assess their companies' security risks themselves but the regulator expects them to recruit appropriate talent, such as a CIO, to manage their cyber-security risk. If directors merely delegate tasks down the chain of command without keeping an eye on things and without knowing where the company's weaknesses lie, or without knowing the basics of 'good cyber-hygiene,' they could be held to be failing to act with reasonable care, skill and diligence.

Every director has a continuing obligation to acquire and maintain a good enough knowledge and understanding of the company’s business to be able to perform his directoral duties properly. In the context of cyber-security, this does not require him to know the underlying policies word-for-word, but he should be aware of the information risk management system. He should also know the strategies his firm has evolved and the reasoning behind them.

Even though Guernsey is outside the UK, its directors ought to look at HM Government's "10 steps to cyber-security." These steps concern the protection of information as a board-level responsibility; basic security controls to ward off the most common cyber attacks; risk management regimes; secure configuration; network security; privileges for users and how to manage them; education and 'awareness' for users; incident management; the prevention of malware; monitoring; removable media controls; and home and mobile working.

Effective management ought to be coupled with good basic controls and directors should test and question the resultant policies. They should ask, where necessary, what "third-party standards" they meet, find out whether anyone has tested the safeguards to look for weaknesses and ensure that the systems and protocols are acceptable for the company's insurance policy. A director is better placed than the CIO or his team of information experts to spot the areas of the business (perhaps data, money or intellectual property) that are more likely to be exposed to an attack and should therefore benefit from more protection.

Things that directors are good at

Although nobody expects them to be good at "tech talk", directors ought to know how they are going to react to an attack, whom they should inform and what actions to take. They should also think about how the board is going to discuss confidential, legal or litigation-related advice in board meetings after the event. While doing this they ought to think about reports prepared for the board that assess the company's exposure. All this might add to the company's obligation to disclose information to the regulators.

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 the need to consider whether force majeure clauses [which free the parties from liability or obligation when an extraordinary event prevents them from fulfilling their obligations] should be inserted into standard contacts.

Directors ought to ensure that someone is monitoring the company's insurance policies as a matter of routine; the company must have adequate cover in the event of a cyber-attack. Alongside the company's need for insurance, directors should not disregard their own 'directors and officers' ('D&O') policies and related indemnities. As regulatory investigations become more commonplace, directors would be well-advised to check the level and extent of their cover to include this.

These, then, are some examples of how a director's duty to act in the best interest of his company is becoming more onerous. He is not, however, expected to prepare for every eventuality. It is unlikely that he will fail in his duties and obligations by a mere error of judgement. However, if he fails to take reasonable action and recognise that his duties extend to ensuring that his company is as prepared as it can be for a cyber-attack (in view of its size, resources and weaknesses) then he may be exposing himself to personal liability, regulatory sanctions and, in an extreme case, criminal liability for breaches under section 515 Guernsey Companies Law.

The Guernsey Financial Services Commission

If the company is a licensed company, then directors will need to be aware of their duties to the regulator. The GFSC is able to take action if a director fails to discharge their regulatory duties 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 the law of data protection

Section 61 Data Protection (Guernsey) Law 2001 states unequivocally that directors may be liable if an offence has been committed with a director's consent or connivance or due to his neglect, and that he may be punished accordingly.

On 25 May 2018, the European Union's General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) will come into force in the UK. This will impose severe penalties for non-compliance, being the higher of 20 million euros or 4% of a company's worldwide turnover. The States of Guernsey have voted to enshrine the GDPR in island law with the implementation date set for May 2018. Compliance with the GDPR and other legislative changes which affect the way in which data is stored and secured will rest with each financial firm's board. Directors will be obliged to keep an eye on legal developments and ensure that every system meets their requirements. The board will also have to take a risk-based approach to governance.

Although, as the recent 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. A major data breach involving a large number of data subjects could give rise to legal action, even if they have suffered no financial loss.

Limiting the risk

Each business' risks, budgets and weaknesses differ from those of the next. There is no one-size-fits-all solution to their troubles. Whether a director has acted in breach of his duties to his company ultimately depends on the facts of each individual case; however, directors who act reasonably and pro-actively to make their companies take technical and operational steps to prevent and minimise the likelihood of cyber-attacks are bound to have gone a long way to ensuring that they have discharged their duties.

Directors might wish to take at least the following practical steps.

- Employ (or engage) a dedicated cybersecurity expert who is qualified to brief and train the board of directors regularly.
- Formulate a robust cybersecurity policy and do so carefully. Ensure that someone is monitoring and reviewing it constantly. Make it part of the firm's "corporate governance" regime and make a note every time someone considers the policy and takes action.
- Ensure that the company has adequate insurance and that the board of directors understands the extent and limits of the policy.
- Set up contingency measures to take during and after an attack and be prepared to respond to an attack with a detailed plan that someone has tested.

An original version of this article was first published in Compliance Matters, August 2017.