MACFARLANES

DIRECTORS - WHAT ARE YOUR CYBER-SECURITY RESPONSIBILITIES?

BACKGROUND

Media reporting of successful cyber attacks on the likes of Sony, Target, Anthem and the Office of Personnel Management in the US, together with the considerable cyber-risk awareness campaigns undertaken by the UK Government, mean that the subject has been well-publicised. But for those who have no background in technology, where should you begin so as to act effectively for the company, as well as to ensure that you have discharged your director's duties?

The Companies Act 2006 introduced an objective test which measures you, as a Company Director, against the standard of "*a reasonably diligent person with… the general knowledge, skill and experience that may reasonably be expected of a person carrying out the functions carried out by the director in relation to the company…".* This sits alongside a subjective test as to the knowledge, skill and experience that you actually have.

There are several points to note from this. Directors:

- have a duty to keep themselves informed as to issues which should be in their contemplation;
- are unlikely to be held liable for errors of business judgement;
- may be held to be negligent if they do not take professional or expert advice; and
- are entitled to rely on others to whom functions are reasonably delegated. However that reliance cannot be unquestioning and you will retain a residual duty of supervision and control. This means that you must know (i) that there are means of monitoring any delegated role and (ii) the business well enough to understand any warning signs generated.

WHAT DO YOU NEED TO DO?

Where, therefore, do you start if you know nothing about it? Cyber-security is a topic which needs close attention from the board, albeit that any reaction to the risk assessment must be proportionate.

Firstly ensure that there is a person, or better still, a team assembled (comprising at least IT, operations and legal) to whom the cyber-risk assessment function can be delegated. You can then start to question that team. There is a large volume of information on cyber-risks available, and to distil it into a digestible summary risks omitting important considerations. Such an assessment can only ever be specific to your business but the following non-exhaustive list will help:

Have we undertaken an analysis of cyber-risks to the business and its staff?

- What is it that our business owns which others might want? Is it data, money, IP, or are we undertaking activities which might attract some form of public criticism? Within those categories, are there any items of particular value, the protection of which should be prioritised?
- Who might wish to cause us harm? Former or departing employees, competitors, social activists, criminals (theft or ransom) or at a more macro level, foreign organisations or nation states?

What form of cyber-security programme and set of policies do we have in place?

- Have we adopted any third party standards in our business e.g. ISO 27001?
- Have we taken into account e.g. the considerations identified in the UK Government's guide 10 Steps to Cyber Security in putting together our programme?
- What would be our immediate reaction to any hack? Who would be informed and what actions would we take?

What technology (IT security) measures do we have in place?

- How do we monitor our networks for attack? How often are we updating our perimeter security and what is our "patch" management policy (updates from suppliers to guard against known technology risks and weaknesses)?
- What firewalls and malware detection software do we have in place?
- User access – who has authority to access our network? Is it just employees and what level of internal segregation is there? Are certain areas of the system protected or off-limits? Who has overall control of the system and who holds the passwords?
- If any non-employees have access to our system, have they been adequately vetted and what contractual terms are they bound by to ensure they are controlled? Do our contracts with relevant third parties adequately deal with information security and cyber-risk?
- How often do we engage third parties to undertake penetration or vulnerability testing on our systems to assess vulnerabilities? How do we react to the results of those tests?

Staff education

- What have we done to educate our staff on cyber-security issues and the role they can play to combat those threats? In particular, what do they know about the threat posed by spam email, social media and the dangers of a casual approach to personal IT security?
- Do our employment policies and procedures support such training and place responsibilities on relevant personnel appropriately?

How often is all of the above reviewed?

- Threats to your business clearly need to be kept under active consideration, even if changes to your cyber-risk programme are less frequent. The discussion need not be held at every meeting but you do need to ensure that the risk assessment phase of your cyber-programme is regularly on the board agenda in order to ensure that your obligations are properly fulfilled.

There are further tests to satisfy which arise in the context of laws aside from the Companies Act, but at a generic level, a business which reacts positively to directors setting the scope of the assessment described above will have gone a long way to minimising liability in the event of a cyber-breach. Working from the principle that no business is immune to a breach of some kind, it is critical that a business implements appropriate technical and organisational measures to counter unauthorised access to its networks and data. This is in essence the standard required by relevant applicable legislation (including the current UK Data Protection Act, drafts of the EU Data Protection Regulation, the proposed EU "Cybersecurity" Directive and the current UK Communications Act). It may also be difficult to suggest that a director who has satisfied him/herself as to the company's position in relation to the matters described in this note will have failed to discharge his common law duty of care so as to be at risk of liability for negligence.

CONTACT DETAILS
If you would like further information or specific advice please contact:

RUPERT CASEY
PARTNER
DD: +44 (0)20 7849 2256
rupert.casey@macfarlanes.com

JULY 2015

MACFARLANES LLP
20 CURSITOR STREET LONDON EC4A 1LT

T: +44 (0)20 7831 9222 F: +44 (0)20 7831 9607 DX 138 Chancery Lane www.macfarlanes.com

This note is intended to provide general information about some recent and anticipated developments which may be of interest.
It is not intended to be comprehensive nor to provide any specific legal advice and should not be acted or relied upon as doing so. Professional advice appropriate to the specific situation should always be obtained.

Macfarlanes LLP is a limited liability partnership registered in England with number OC334406. Its registered office and principal place of business are at 20 Cursitor Street, London EC4A 1LT.
The firm is not authorised under the Financial Services and Markets Act 2000, but is able in certain circumstances to offer a limited range of investment services to clients because it is authorised and regulated by the Solicitors Regulation Authority.
It can provide these investment services if they are an incidental part of the professional services it has been engaged to provide. © Macfarlanes July 2015