SLAUGHTER AND MAY

Who’s next after TalkTalk?

Frequently Asked Questions on Cyber Risk

“Fraud threat to millions of TalkTalk customers”

“TalkTalk cyber-attack: website hit by ‘significant’ breach”

These are just two of the many alarming and uncomfortable headlines that Dido Harding, TalkTalk Chief Executive, and her many millions of customers woke up to on 23rd October. They are the type of headlines that no senior executive would like to see about their company, nor its customers whose personal data it is processing.

Our clients have been approaching us with increasing frequency in recent months for advice on cyber risk, and an appropriate legal and regulatory response to that risk. We have collated in this briefing the following commonly asked questions, together with some summary answers:

1. What level of cyber security does a company need?
2. Given recent cyber attacks, should a board be reviewing cyber risks?
3. Should every board have a cyber security expert?
4. Do organisations need internal and/or external experts, consultants and/or auditors to assess and review cyber readiness?
5. Can a company benchmark what others are doing in this area?
6. If a cyber attack is suspected or happens, who needs to be informed?
7. If your company is the victim of a malicious cyber attack, would it still be held responsible for the implications?
8. Is insurance against cyber security risk available?
9. What steps should companies be taking in relation to their suppliers?

In response to the challenges for our corporate clients posed by cyber risks, we have created a cross-stream Cyber Group, with experts from our corporate, financial services, technology, data protection, financing and dispute resolution streams. For more information on the support we can offer to your organisation, or if you require specific cyber advice, please contact:

Frances Murphy, Corporate
T +44 (0)20 7090 3158
E frances.murphy@slaughterandmay.com

Rob Sumroy, Technology and Data
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

Ben Kingsley, Financial Institutions
T +44 (0)20 7090 3169
E ben.kingsley@slaughterandmay.com

Jonathan Cotton, Disputes and Investigations
T +44 (0)20 7090 4090
E jonathan.cotton@slaughterandmay.com

1. What level of cyber security does a company need?

There can be no ‘one size fits all’ approach to security: it depends on the type of information a company holds and the threats it faces as an organisation.

This is explicitly recognised, from a data protection perspective, by both the law, which requires organisations to put in place “appropriate technical and organisational measures” (which will vary from case to case), and the European Regulators – for example in the UK, the ICO advises organisations to adopt a “risk-based approach” to deciding the appropriate level of security.

That said, there is a significant amount of available guidance, and some ‘market standards’ are emerging. Examples include the emphasis on encryption of personal data and the adoption of recognised security standards, including PCI/DSS where payment card details are stored and processed, ISO 27001, a certification which many customers expect their IT suppliers to have, and the UK Cyber Essentials scheme, which the Government mandates for suppliers providing certain services to the public sector.

One of the more uncomfortable media questions faced by TalkTalk Chief Executive Baroness Harding related to encryption and her inability to confirm if all of the data lost was encrypted. The inquiry into cyber security and the protection of personal data online, launched by the Commons Select Committee for Culture, Media and Sport following the latest TalkTalk attack, also includes a request for views on the ‘nature, role and importance of encryption in protecting personal data’. There is clear guidance from the UK and European data protection regulators that organisations should ‘encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen’. However, encryption on its own may be insufficient in the face of a cyber breach, and is a good example of the fact that there is no ‘silver bullet’ to solving the cyber issue. The loss of encrypted data may still cause concern, for example where an account which can access thedata in an unencrypted form, or the relevant encryption key, is itself compromised, or where there has been insufficient back-up of the lost data.

Maintaining appropriate measures and technology to achieve cyber security is clearly an essential component in the effective management of cyber risk. However, it is important to remember that this comprises only part of the solution; establishing an appropriate cyber risk framework is about much more than implementing up-to-date technology. Key to managing your organisation’s cyber risk is the development and implementation of an effective, holistic enterprise-wide strategic approach to cyber.

2. Given recent cyber attacks, should a board be reviewing cyber risks?

Cyber security is vital for the continued success and growth of business. It therefore needs and deserves regular consideration at board level. It should, like any other significant risk, be included in the risk register, meaning that the risk, or its separate components, should be assessed and reviewed on a regular basis, taking into account the evolving likelihood and impact.

By failing to implement robust risk and crisis management protocols, directors may expose themselves and their companies to significant legal risks, including potential breaches of directors’ duties, corporate governance and disclosure obligations, as well as financial and reputational risks.

It is therefore imperative that your directors implement a robust and proactive cyber security policy, combined with a disciplined and rigorous board oversight process, appropriate to your company. Delegation of the day-to-day management of cyber security does not, of itself, prevent directors from fulfilling their duties of management and oversight, but directors cannot abdicate their responsibility to manage significant risks, which are likely to include cyber risk.

3. Should every board have a cyber security expert?

There is no objectively correct board profile from a cyber security perspective. The standard to which the directors will be held in respect of the management of cyber risk will depend on the value of the company's digital assets and the extent to which the company relies on online systems.

Whilst still relatively few companies have a board level seat dedicated to someone with relevant expertise, there does appear to be a distinctive trend in this direction, with cyber and technology expertise being sought in selection of non-executive directors.

Even if your company does not have an expert on the board, prudent oversight requires that such expertise is present at a suitably senior level within the organisation.

Although it is now good practice to appoint one person – either on the board or at an appropriate senior management level – with responsibility for cyber, your directors cannot abdicate their responsibility for cyber security. In order to act in a way that promotes the success of the company and demonstrates reasonable care, skill and diligence, all directors must show an active and informed engagement with the company's cyber security profile and risk mitigation.

4. Do organisations need internal and/or external experts, consultants and/or auditors to assess and review cyber readiness?

Given the growing significance of cyber risk, it would be prudent, at a minimum, for an organisation to include cyber security in its annual internal audit.

The extent to which additional input of external experts, consultants and/or auditors is required will vary depending on the nature of your organisation, your relative exposure to cyber risk and your internal expertise.

In any event, your board should regularly assess whether such external input would be necessary or appropriate in light of the evolving risk landscape. Unless the risk is low and/or the internal expertise is (and remains) strong, some degree of external input on aspects of the cyber risk framework, policies, protocols and/or training programme is likely to help your directors when considering whether they have exercised reasonable care, skill and diligence in respect of cyber security.

5. Can a company benchmark what others are doing in this area?

It is important that your organisation does seek to benchmark itself against both your competitors and the market-leaders from a cyber security perspective, as this will be a key consideration when assessing whether your organisation has implemented appropriate security measures and/or adopted a suitably risk-adjusted approach.

Whilst there is not, at present, a huge amount of publicly available information about current practice, there are increasing expectations that companies should collaborate with one another (as well as with regulators, including the FCA and the ICO, and government agencies) to share information and intelligence on cyber security threats and mitigation techniques.

The Cyber-Security Information Sharing Partnership offers a platform for secure online collaboration where companies can exchange information to help strengthen their cyber security.

The results from studies and inquiries may also provide some useful information. For example, the Commons Select Committee for Culture, Media and Sport has launched an inquiry into cyber security following TalkTalk's latest breach. It is seeking views on a number of areas including the robustness of measures taken by ISPs and telecoms providers to maintain the security of their customer's personal data, the level of investment being made to ensure their systems remain secure and anticipate future threats, and the role and importance of encryption in protecting personal data. The deadline for written submissions is 23 November 2015.

Separately, most industry and trade bodies have cyber security high on their agendas, and law firms, insurers, consultants and other advisors are beginning to convene round tables and other events at which best practice and experience can be shared.

6. If a cyber attack is suspected or happens, who needs to be informed?

Companies are often reluctant to admit that they have been hacked for fear of potential reputational damage, loss of customers, litigation and because the disclosure in itself could expose technological weaknesses and increase their vulnerability. However, we strongly advise all companies to develop breach notification strategies, in anticipation of cyber breaches – for regulatory, legal, contractual or reputational reasons, some scope of notification is likely to be necessary. It is far better to implement a properly considered strategy than to have to consider the difficult notification issues in the midst of an actual attack.

As with all material issues affecting your company, from a legal and regulatory perspective, it is unlikely that complete non-disclosure of a material cyber attack, or delays in that disclosure, would be an acceptable option. Regulators in the financial services and telecoms sectors in particular require serious data or system breaches to be notified. Your company may need to inform law enforcement agencies, and may have contractual obligations to promptly notify corporate customers. UK listed companies will also need to consider whether the cyber attack constitutes inside information requiring announcement; share price movements following the limited number of such announcements made to date suggest that the markets have indeed regarded those particular cyber attacks as price sensitive.

Data breaches often, although not always, involve some form of personal data (bank account details, for example). While there is currently no general legal obligation in the UK to report data breaches, there are some sector specific legal and regulatory requirements. The ICO has also issued detailed guidance confirming that it believes "serious" personal data breaches (for example involving a large volume of data loss) should be brought to its attention. The ICO has publicly criticised TalkTalk for taking more than 24 hours to notify the ICO of the recent cyber attack, on the basis that this may have prevented the ICO from helping consumers to mitigate the breach.

Reporting to the ICO will not automatically result in the breach becoming public – the ICO has confirmed that it does not see it as its responsibility to publicise breaches notified to it that are not already in the public domain. However, it may recommend that the reporting company does so and, if the breach leads to regulatory action, the ICO does tend to publicise any regulatory action it takes.

7. If your company is the victim of a malicious cyber attack, would it still be held responsible for the implications?

It is acknowledged that no organisation can protect against any and all cyber attacks. As a result, your company will not be responsible on a strict liability basis for a cyber breach. Defences are available; for example, in a data protection context, your company would look to avoid liability by establishing that it had appropriate technical and organisational measures in place.

Having said that, there is no defence in being the victim of a criminal act. Once attacked, your company will need to show that it had in place an effective strategy and has taken (and is continuing to take) appropriate steps to address and mitigate the risk. It is not possible for you to ‘outsource’ your risk (for example to your IT outsource provider) – it is your company’s responsibility to ensure your suppliers have appropriate security measures in place and to monitor this.

Unless your company establishes appropriate technical and organisational measures to protect the personal data you process, you are leaving yourself open to claims from individual data subjects even though your company is the direct victim of a malicious cyber attack. As a result of the recent Vidal-Hall judgement, it is now clear data subjects no longer need to prove they have suffered damage from a data breach, but would instead be able to claim monetary compensation through the courts simply for the distress they have suffered. Recent reports suggest Morrisons supermarket chain is to be sued by 2,000 of its employees following last year’s data security breach in which their personal details were leaked by a disgruntled former employee, with distress suffered purportedly forming the basis of their claims.

8. Is insurance against cyber security risk available?

It is, but within Europe it is not yet widely used, and certainly less common than in the US. Despite the cyber security risks to which organisations are exposed, the UK Government has suggested that only 2 percent of large businesses have specialised cyber insurance in place and only 10 percent of large businesses have any cover at all (either on a standalone basis or in other policies). However, the cyber environment is a dynamic one and there is now an increased focus on cyber insurance as a way of managing and mitigating cyber risk. The mandatory data breach notification obligations imposed on many companies in the US are seen as the main driver behind the greater uptake in specific cyber insurance policies on that side of the Atlantic; however it also explains the narrow scope of those US cyber policies aimed primarily at losses flowing from the breach notification.

Although cyber security insurance can be a valuable tool, cyber insurance policies will not provide total protection. Reputational damage, for example, is a key area which would likely not be covered by cyber security insurance because of the difficulties in quantifying and proving such loss.

Transferring or mitigating cyber security risks by way of insurance or by other means will only be possible if the key risks are known and quantified. Brokers are therefore advising all companies to undertake a cyber risk identification and quantification exercise, and to discuss with their brokers the types of risk they face, and the different ways in which those risks can be mitigated. Many brokers suggest money is better invested in risk mitigation activities (including improving systems, policies and strategies around cyber) than in specific and expensive cyber insurance policies.

You should also assess whether, and to what extent, you are already protected by existing insurance policies. For example, policies which relate to commercial property and business interruption, professional indemnity insurance or general liability may provide some cover against cyber security risks. However, there are many misconceptions about the level of cover that traditional policies provide and, as cyber risk has become more significant, some insurance companies have taken the decision to exclude cyber security from traditional policies, in particular those relating to business interruption.

9. What steps should companies be taking in relation to their suppliers?

Some high-profile cyber attacks, such as the attacks in the US against major retail chain Target have taken advantage of supplier vulnerability. It is therefore important that your organisation regularly assesses its supply chain from a cyber risk perspective. This will include performing due diligence on, and agreeing appropriate contractual protections with, new suppliers.

Your organisation should review its existing supply chain to check, for example, that:

- your suppliers have robust security measures in place, adhere to agreed standards (such as ISO 27001 / Cyber Essentials) which are adopted in such a way as to cover all relevant risks and that they are obliged to maintain and update their adherence as standards evolve;

- your suppliers are contractually obliged to inform you of (and to take steps to rectify) any known or suspected cyber breaches;

- you have the ability to audit your supplier's compliance with the cyber-related contractual obligations; and

- your suppliers are contractually liable (and able to pay) for any losses arising from a cyber breach and/ or have sufficient insurance or parent company guarantees in place. It is worth considering whether 'traditional' liability clauses in IT contracts, which will often exclude or cap the types of losses you would most likely suffer as a result of a cyber breach (for example loss of data) are now fit for purpose for your material supplier contracts in this era of increased cyber risk.

This material is for general information only and is not intended to provide legal advice.
For further information, please speak to your usual Slaughter and May contact.

November 2015