Weil

November 2015

Alert

Cyber Security: Lessons to be learned from TalkTalk

By Barry Fishley and Simon Taylor

The highly publicised cyber security attack on TalkTalk provides a timely reminder of the prevalence of cyber security issues and the need for organisations to continue to review and, if necessary, update measures which could reduce the chances of a successful attack or mitigate its effects.

The legal risks arising from data security breaches have increased as it is no longer necessary to prove financial loss in order to claim compensation for distress. In addition, a recent court decision to allow employees to bring a class action against supermarket chain Morrisons for a data security breach may be the start of a trend. Finally, the draft Data Protection Regulation will increase sanctions for serious data breaches to a maximum fine of 2 percent of worldwide turnover.

Key considerations include:

- Ensuring there is full senior management engagement on the issue and periodic updates to the board;
- Identifying the most critical data, the jurisdiction in which it is physically located and the impact on the business in the event of a breach - resources should be appropriately focused on the biggest areas of risk;
- Appraising and upgrading IT policies and procedures (e.g. IT monitoring and employee IT security policies) and ensuring there is employee awareness and training;
- Compliance with legal and regulatory frameworks including Data Protection Act requirements to ensure that appropriate technical and organisational measures are taken against unauthorised use, loss or destruction of personal data;
- Considering and adopting industry standards: various industry standards offer recommendations and an objective measure of commitment to cyber security. For example, BSI ISO/IEC 27001 is an internationally-recognised security standard which is particularly useful on account of its risk-based approach;
- Having a response plan to be implemented in the event of a security breach and ensuring the plan identifies the responsibilities of key stakeholders in the relevant business areas. For example IT, HR, legal, communications

and compliance. The plan should dovetail with business continuity/disaster recovery plans and also cover communications with customers, employees (which should typically include FAQs), notifications to any applicable regulatory bodies (such as the Information Commissioner's Office) and a media/PR plan;

- Assessing the levels of security surrounding third party access, such as remote hosting;
- Undertaking appropriate due diligence of suppliers to ensure they are operating in line with leading industry standards. For example, a number of UK IT suppliers have self-certified under the UK's Cyber Essentials Scheme;
- Undertaking frequent penetration testing of IT systems and seeking to encrypt personal data as much as possible (which, from reports, appears to be one of the issues with the TalkTalk attack); and
- Reviewing the insurance position. Organisations should consider if their insurance is specific enough to cover cyber attacks. Either basic policies covering third party claims resulting from data breach, or more comprehensive policies that cover other losses (e.g. reimbursing cost of customer notifications) should be in place.

If an organisation does fall victim to a major cyber attack, a rapid, considered and comprehensive response is critical to mitigate the reputational and legal impact of the incident:

- **Stick to the plan.** If a cyber attack response plan has been adopted, it should be implemented immediately. An unfocussed response is likely to significantly augment the impact of the cyber attack;
- **Mobilise the response team.** Remember that cyber security is not just an IT concern. As mentioned above, the response plan should have already identified key stakeholders to oversee its implementation. If data which is the subject of the hack is hosted by external vendors, those vendors will also form an important part of the response team;
- **Contact your insurers.** As with any insurance, immediate and full disclosure is necessary.
- **Assess and make safe.** Assess the type and scope of the cyber security incident. Act rapidly in conjunction with the IT function and IT suppliers to identify and seek to eliminate the security vulnerability which permitted hackers to access your networks, and take steps to ensure business continuity as far as possible by, among other things, implementing disaster recovery/business continuity plans;
- **Own the narrative.** If the attack is already in the public domain, reputational impact can be mitigated by the prompt issuance of a statement from a senior representative setting out the known facts whilst the attack remains under investigation internally. The initial statement should be followed by regular updates. For example, the CEO of TalkTalk was put forward to explain the circumstances and impact of the recent cyber attack – this provided reassurance to customers and the market that the incident was being treated with appropriate seriousness at the most senior level;
- **Engage with customers.** Consumer-facing businesses should contact customers whose personal data may have been compromised, describing the types of data compromised and a process by which customers can determine if their data has been accessed and how they can best protect themselves going forward. Where payment card data has been stolen, some organisations have offered free credit monitoring to affected customers. As mentioned above, the risks of claims are increasing, so there is a need to be circumspect with any customer notification;
- **Inform and work with regulators.** Although it may not be a strict legal requirement, consider notifying the Information Commissioner's Office if personal data is involved. However, before doing so it is critical to ensure the notification is as detailed as possible and that it identifies actions which will reduce the risk of the incident re occurring; and
- **Learn from your mistakes.** In the longer term, a review of the circumstances which led to the cyber attack will enable an organisation to assess the improvements to cyber security management that are required to mitigate against the risk of

recurrence. It is not possible for an organisation to achieve complete immunity from a cyber attack, but it is very easy to criticise an organisation where a known risk or vulnerability facilitates a cyber attack (this was one of the criticisms levelled against TalkTalk). It is important that cyber security measures are kept dynamic and under review to respond to the ever-changing nature of online threats, with corresponding updates to any response plan.

If you have questions concerning the contents of this Alert, or would like more information about cyber security, please speak to your regular contact at Weil, or to:

Barry Fishley (London)	barry.fishley@weil.com	+44 20 7903 1410
Simon Taylor (London)	simon.taylor@weil.com	+44 20 7903 1141

©2015 Weil, Gotshal & Manges. All rights reserved. Quotation with attribution is permitted. This publication is provided for general information purposes only and is not intended to cover every aspect of structured finance for the featured jurisdictions. The information in this publication does not constitute the legal or other professional advice of Weil, Gotshal & Manges. The views expressed in this publication reflect those of the authors and are not necessarily the views of Weil, Gotshal & Manges or of its clients.

The contents of this publication may contain attorney advertising under the laws of various states. Prior results do not guarantee a similar outcome. If you require specific legal advice then please contact any of the lawyers listed above.

The firm is not authorised under the Financial Services and Markets Act 2000 but we are able, in certain circumstances, to offer a limited range of investment services to clients because we are authorised and regulated by the Solicitors Regulation Authority. We can provide these investment services if they are an incidental part of the professional services we have been engaged to provide.

We currently hold your contact details, which we use to send you information about events, publications and services provided by the firm that may be of interest to you. We only use your details for marketing and other internal administration purposes. If you would prefer not to receive publications or mailings from us, if your contact details are incorrect or if you would like to add a colleague to our mailing list, please log on to www.weil.com/weil/subscribe.html, or send an email to subscriptions@weil.com.