SLAUGHTER AND MAY

Here be dragons

First steps for a corporate navigating the unsure waters of a data breach†

November 2017

Increasingly, we see headlines that another corporate has experienced a data breach. Recent examples include HBO, which experienced the leak of an episode of its hit fantasy drama Game of Thrones, as well as Sony, where hackers gained possession of internal e-mail traffic as well as unreleased movies.

But situations where a large amount of seemingly innocuous personal information has been exfiltrated can do equal potential damage to a corporate, with a number of potentially harmful customer relation and regulatory results. In point of fact, at the time of writing, the credit monitoring company Equifax has been criticised for a data breach that includes the personal information of up to 143 million customers, with reports that a lawsuit against it for up to $70 billion is being prepared.

Key points

Corporates faced with a potential data breach should act quickly to assess potential legal action and to contact potentially affected customers.

Corporates should keep regulators informed and up-to-date with developments in their internal investigations.

Corporates can take precautionary action now to lessen the impact of any future data breach.

These high profile examples relate to US companies. This article looks closer to home, and focuses on what steps a corporate based in the UK can take in the following days and weeks to safeguard its position, when faced with evidence that it has been subject to a data breach.

Investigation – first steps

Notification of the potential breach may come in a variety of ways. In a recent case for TalkTalk, the potential breach came to light when the company started to receive complaints from customers that they were receiving a number of scam calls. In other examples, such as the HBO hack, the perpetrators of the breach may have made this information publicly available (or offer it for sale) for the purposes of blackmail or self-enrichment.

At this point, it is important for a corporate to move quickly to establish whether its data has indeed been exfiltrated. This will involve engaging fully with its internal IT team, and, depending on the scale of the breach, considering bringing in external information security experts as soon as possible. Of course, if information is publicly available, then it will be relatively straightforward to compare this information with data held internally to see if the report of a breach is accurate.

Litigation

One of the first steps for a corporate to take is to consider legal proceedings to secure an injunction to restrain the perpetrators of the breach from taking further action with its data, whether this consists of offering it for sale or releasing further information publicly.

† This article first appeared in the November 2017 edition of Butterworths Journal of International Banking and Financial Law.

If news of the data breach is not yet public, a corporate may also wish to consider applying to the court to have the injunction hearing (and any further proceedings) held on a confidential basis. Particular care should then be taken by the corporate not to supply any information in any confidential schedules to a third party adviser during the course of its investigation.

It is likely that, at the early stage in any investigation at which an injunction should be considered, full details of the individuals who exfiltrated the data will not be available. In this event, it is possible to apply for an injunction on a general and anonymous basis against the perpetrators of the data breach. This process is sometimes referred to as obtaining a 'John Doe' or 'Persons Unknown' injunction - but if the identities of the hackers are subsequently discovered, they can be joined individually to the action by later application to the court.

If successful, corporates may consider providing a copy of the injunction to media organisations to ensure that they are bound by its terms, should there be a concern of private information, or customer personal data, being published.

As the identities of the perpetrators are likely to be unknown at the time this step is taken, this will by necessity be an ex parte injunction, with the attendant duty on the corporate to make full and frank disclosure to the court of the circumstances surrounding the breach. Indeed, given the broad sanction that the court is being asked to approve in the event of a 'Persons Unknown' injunction, it is particularly important for the corporate's legal team and advisers to bear in mind this duty of disclosure to the Court.

Customer communications

An important point for every corporate in this situation is the need to keep customers engaged and informed through the process. There is a balance to be struck here, between informing customers as soon as possible that their personal data may have been exfiltrated from the company, and not alarming customers unnecessarily before fuller details emerge of what information, if any, has been subject to the data breach. Moreover, once any set of customers is informed, it should be expected that news of the data breach will become public in an expedited timeframe.

Corporates should look to put into place a robust system for dealing with customer complaints and enquiries. This could classify the type of customer complaint, as well as have available a template response which can be tailored and built on to address the customer's specific concern. If the data breach has affected a large number of customers, then the corporate should consider hiring additional staff to deal with customer queries at the point at which customers are informed of the incident.

It has become standard practice to offer some form of credit protection for customers who are worried about their personal information being abused. In this context, it is worth noting that Equifax has been criticised for tying the offer of credit protection to limiting its liability for the breach – so it may be worth offering the protection without further conditions being placed on the customer.

Regulation

An important consideration for a corporate which suffers a potential data breach is notification of regulators. The Information Commissioner's Office, the authority established to uphold information rights in the UK, recommends that it is notified of any serious breach of personal data. Certainly, where the volume or the sensitivity of the data lost is high, it is recommended that the ICO is informed of the breach as soon as is possible. Note that it is not necessary to wait to have built up a 'full picture' of the breach before making an initial notification – it is sensible to notify the ICO early in the investigation, and then keep the ICO updated regularly as the corporate's investigation uncovers more details.

The ICO has the power to levy a monetary penalty where it feels that corporates have not

sufficiently protected the personal data they control. This power is not a paper tiger; in the TalkTalk case mentioned above, the ICO recently fined the company £100,000 for the personal data breach it suffered.

Corporates should also consider whether there is a need to notify any further regulators, whether in the UK or globally. This will be a fact-based decision relating to how the corporate is authorised to do business, and where the affected customers reside.

It may be that a corporate will have to devote resources to dealing with queries from different regulators across the world, each of whom will have differing areas of interest according to their own priorities as well as the kind of data affected in their own jurisdiction. It is important to take advice on aligning responses to regulators, to ensure that there is consistency and no inequality in the information provided to each.

It should also be noted that the position on informing the ICO will change next year. From 25 May 2018, the General Data Protection Regulation will make it mandatory to notify the ICO of a personal data breach without undue delay (72 hours where feasible), unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. If a corporate does not comply with this regulation in general, large fines (of up to 2% of annual worldwide turnover) can be levied.

Engagement with Police

Where data is intentionally taken, there is likely to be a criminal element to the breach, and corporates should accordingly make a report to the police. A report to Action Fraud, the UK's national cybercrime reporting centre, should be considered, in addition to any report to the relevant local police force.

The police will ask for information relevant to the crime to be preserved. Though it is likely that any such information is being preserved already as part of the corporate's internal response to the breach, it is important to ensure that sources of data requested by the police have been secured.

Further information will usually be requested, such as witness statements from employees at the corporate and an 'Impact Statement for Business' which details any adverse effect on the corporate as a whole. As a result, the corporate should be prepared to dedicate management time to deal with these queries, as well as put in place a more junior team to liaise directly with the police on any further queries they have.

One immediate benefit of this course of action is that the corporate will be able to stay informed by the police of the progress in their own investigation where it is appropriate for them to do so. As the police have certain powers not available to the corporate (e.g. search-and-seizure and tracking powers), it is likely that these areas of their investigation will move more quickly than the corporate's own.

Preventative measures

Corporates should ensure that databases are kept up to date, and that they are aware of what personal data is stored in which locations in relation to separate groups of customers. In the event that one of these systems is breached, this will ensure that the compromised material is kept to a minimum, as well as ensure that the corporate has a clear idea of which group of customers is affected.

Corporates should regularly review internal as well as external security measures. While often care is taken to prevent unauthorised access to external parties, there is also a danger posed by employees, or other contractors, who may have access to a corporate's premises, taking information externally though unauthorised to do so. The ISO guidelines on internal document security are a good place from which to draw internal guidelines.

To help prevent an external breach, it may be advisable to get an independent IT adviser to 'stress-test' your system, using methods such as

penetration testing, to see whether there are any potential vulnerabilities.

Conclusions

- Take sensible measures and contact potentially affected customers quickly.
- Keep regulators abreast of developments.
- Conduct your own internal investigation as quickly as possible, and engage any legal or technical advisers who can assist.
- Report the matter to, and keep in touch with, the police. Check in with them if there are any issues they want to investigate themselves in the first instance.
- Take steps now to review your internal information storage procedures, to ensure that if a data breach occurs, you are well prepared to deal with it efficiently.

Mohan Rao
Associate
T +44 (0)20 7090 3827
E mohan.rao@slaughterandmay.com