Client Update
UK Telco Fined for Cyber Breach: Lessons Learned

LONDON
Jane Shvets
jshvets@debevoise.com

Saqib Alam
saqibalam@debevoise.com

Robert Maddox
rmaddox@debevoise.com

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

James J. Pastore
jjpastore@debevoise.com

WASHINGTON, D.C.
Luke Dembosky
ldembosky@debevoise.com

NOTE: This article first appeared on the StrategicRISK website on 17 October 2016.

On 30 September 2016, the UK's Information Commissioner's Office ("ICO") fined TalkTalk Telecom Group plc a record £400,000 for data security failings that allowed a hacker to access almost 157,000 customers' personal information last year. The monetary penalty serves as an opportunity for companies to reassess their cybersecurity risk profile—particularly in the context of mergers, acquisitions and post-M&A integration—and ensure that their systems and controls meet regulators' latest expectations.

WHAT WENT WRONG?

In 2009, TalkTalk, the UK TV, broadband and telecoms provider, acquired the UK operations of the Italian telecoms operator, Tiscali. Unknown to TalkTalk, Tiscali had legacy webpages that allowed access to a customer database and which remained accessible via the internet post-acquisition.

The database was stored on an outdated version of MySQL, affected by a software bug for which a fix had been available since 2012. In October 2015, a hacker exploited this vulnerability on three legacy Tiscali webpages to access the database. The hacker acquired almost 157,000 customers' personal data such as their names, addresses, dates of birth, telephone numbers, email addresses and financial information.

The ICO fined TalkTalk for two breaches of the UK Data Protection Act 1998: First, for failing to take appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data. Second, for keeping customers' data for longer than was necessary for the purposes it had been collected.

While the ICO found that TalkTalk had not deliberately breached its obligations, its failings still represented a "serious oversight" which led the ICO to issue a record breaking £400,000 fine.

LESSONS LEARNED

The TalkTalk penalty is a timely reminder of the global trend of increasing regulatory scrutiny of businesses' cybersecurity posture. Companies can learn from TalkTalk's experience to better protect themselves. The following takeaways from the TalkTalk penalty notice may be helpful.

First, (re)identify your information architecture. Companies should know what data they hold and where and how. This is not a one-off task; companies should constantly monitor changes which may affect their data security requirements. By apparently failing to audit Tiscali's webpages either during pre-acquisition due diligence or following acquisition in 2009, TalkTalk left the door open for hackers six years later.

Businesses may, therefore, wish to identify ahead of time situations that might require a non-routine reassessment of their data architecture, such as acquiring another company, changing data hosting arrangements or retiring old IT systems.

Second, adopt tailored and proportionate protections. Not all data should necessarily be treated equally. Companies are well advised to determine which data assets are most critical, not only to the company itself, but also to its customers. For instance, the ICO said TalkTalk ought reasonably to have known that failing to adequately protect the database could cause substantial damage to those whose data was stored on it.

A proportionate protection framework may enable a company to deploy resources where they are needed most and to use cybersecurity budgets more efficiently. In TalkTalk's case, the ICO emphasised that the fact that the customer database contained financial information heightened the need for robust technical and organisational safeguards. It found that TalkTalk overlooked the need to ensure that it had robust measures in place to protect such data, despite having the financial and staffing resources available to do so. Companies may, therefore, wish to differentiate between the types of data they hold, how each category is protected and how long each is kept to help minimise cybersecurity risk efficiently and in a risk-based manner.

Third, be proactive. While cyber threats are often asymmetric (you cannot control a hacker), businesses should consider whether they have adequate systems and controls in place which allow them to identify and monitor suspicious activity and discover vulnerabilities. This ranges from the high tech

(e.g., periodic penetration testing and real time data monitoring) to routine housekeeping (e.g., enforcement of document retention policies that call for periodic purging of older data). The ICO penalised TalkTalk for not updating its database software to address a known vulnerability, in what it called an "ongoing contravention". It is therefore important that companies have ways to systematically pre-empt, identify and quickly resolve these sorts of issues.

Fourth, be ready to respond and remediate. Regulators do not expect perfection. Companies may, however, be cast as a villain, rather than a victim, if they are not prepared to deal with an attack quickly, effectively and transparently, with a focus on protection of consumers. The ICO recognised that TalkTalk had been the subject of a criminal attack as a mitigating factor in its decision to fine the company. The ICO also recognised, as mitigating factors, that TalkTalk took substantial remedial action, notifying affected customers and offering 12 months of free credit monitoring.

Companies generally are better placed to deal with a breach if they have a carefully crafted incident response plan in place ahead of time. By pre-emptively thinking about how and who will deal with incidents of varying degrees of severity, businesses can respond more quickly and more effectively when they arise. For example, knowing in advance what information you will need to give regulators, customers and the press (and who will give it) may help a business channel scarce resources in a time of crisis.

THE FUTURE

With regulators' ever-increasing focus on cybersecurity showing no signs of abating, companies should act now to ensure they have a robust framework to address cybersecurity risk. While some may see the TalkTalk fine as relatively lenient, the EU General Data Protection Regulation, which comes into force in May 2018, brings with it increased penalties of up to the greater of €20 million or 4% of global annual turnover for the preceding financial year.

Companies are likely, therefore, only to see the cost of noncompliance increase in the future. If applied to TalkTalk, for example, the new EU regime could have resulted in a monetary penalty of more than £50 million, far exceeding the maximum £500,000 penalty it could have received at present. Businesses may, therefore, wish to act now, rather than pay the tariff later.

* * *

Please do not hesitate to contact us with any questions.