NOVEMBER 2015

blackfoot

BLACKFOOT NEWSFLASH

TALK TALK DATA BREACH
What are the implications for personal data?

What happened?

Telecoms operator Talk Talk confirmed on Thursday 22 October that the personal details of up to four million customers may have been lost in a data breach. Initially, it was not known exactly what data had been stolen, whether it had been encrypted or how many customers were affected.

Hackers reportedly contacted Talk Talk demanding a £80,000 ransom in Bitcoin not to publish customer data, according to cybersecurity blogger Brian Krebs. The company allegedly suffered a distributed denial of service (DDoS) attack, which distracted attention from the exfiltration of data via an SQL injection attack.

Talk Talk subsequently confirmed that their website not core systems was attacked. They did not store complete card account numbers in the clear on their website. Talk Talk confirmed that any bank account details accessed would be similar to those provided when writing a cheque or requesting a bank transfer (bank account and sort code). Talk Talk account passwords had not been accessed, and the company offered to provide free credit monitoring for 12 months to all customers via a third party.

On Monday 26 October, a 15-year-old boy from Northern Ireland was arrested in connection with the hack. He was subsequently released on police bail.

Personal data: the new low-hanging fruit

This latest data security breach may be the start of what was predicted at the beginning of 2015. Criminals are moving beyond card data and are increasingly targeting personally identifiable information (PII).

When compared to card data, PII can be monetised in more ways and for longer. PII currently fetches around three times as much as card data when sold on underground forums. It is also frequently stored unencrypted, making it more accessible to criminals.

As addressed in the Autumn 2015 *Blackfoot Quarterly* newsletter, some businesses may be taking a financial decision on how or whether to protect customer data, based on the size of the fine if data is lost, stolen or misused. Fines for loss of card data are limitless. However, fines from the Information Commissioner's Office (ICO) for the loss of PII are currently capped at £500,000.

At Blackfoot, we believe such an approach fails to consider the fully-loaded costs of a data breach. This includes lost revenue, productivity and ability to trade. There are also legal, technical and forensic costs, plus remediation and recovery costs. Last, and by no means least, is the cost to a company's brand and reputation. This includes loss of customer trust and potentially commercial contracts.

This time it's personal…

A number of factors are pushing the safeguarding of personal data up the corporate agenda. We discussed many of these at our recent Blackfoot Customer Day. For example:

- The new **EU General Data Protection Regulation (GDPR)** includes provisions around mandatory breach notifications for the loss of personal data, an increased fine schedule and the appointment of a data protection officer. The final text of the Regulation is expected at the end of 2015. If passed by European legislators, the GDPR will become law in the UK within two years. Provisions currently being discussed include giving national data protection authorities powers to fine companies up to €100 million or five per cent of global turnover in the event of a data breach.

- The **UK Consumer Protection Act 2015**, which came into effect on 01 October 2015, gives consumers similar rights around digital content as they have for physical goods. It also introduces the 'opt out' principle for class actions. This aligns the UK with the US system for class actions. Everyone affected is automatically a member of the class that is suing, rather than having to 'opt in' to the action or bring a claim in their own name. The 'opt out' principle is currently only available for competition or price fixing claims, although it could be rolled out to other areas in the future, including data loss.

- The **US EMV chip liability shift** on 01 October 2015 could cause a shift in criminal behaviour towards less secure targets. As counterfeit card payment fraud becomes more difficult to perpetrate in the face-to-face environment worldwide, criminals could increasingly turn their attention to less secure remote channels (e.g. e-commerce, mail order and telephone order) and personal data, which is less securely stored.

- The ICO may pursue **regulatory action** against companies who do not use encryption software to protect data. This ICO briefing note was issued following a spate of laptop thefts where personal data was stored but not encrypted.

Blackfoot recommendations

We recommend our clients to:

Consider personal data in parallel with the handling of sensitive card data, and ensure workstreams to manage data are aligned.

Audit the personal data they store on their websites, irrespective of whether such sites are transactional e-commerce websites.

Review their data protection policies. This is with particular regard to the encryption of personal data and whether security controls are in place and of sufficient maturity. (Naturally the concept of personal data applies to current and former customers, employees and so on).

Devise a mix of controls to prevent, detect, respond and recover from a data security incident. The effectiveness of any risk management approach comes through a balance of controls pertinent to their business.

Check their e-commerce applications, especially if they are not handling and storing sensitive card data. If card processing is outsourced, the level of security around personal data stored on a website could be weak. And we see such applications as being particularly vulnerable to attack.

For more information

To find out more about the implications of handling personal data within your organisation, please contact your Blackfoot account manager.

blackfoot

Blackfoot UK Limited
Tel: 0845 805 2409
E-mail: info@blackfootuk.com
Web: www.blackfootuk.com

ADVISE >
ASSESS >
ASSURE >