Professional SECURITY Magazine

Inquiry into online data security

10TH NOVEMBER 2015

The Culture, Media and Sport Committee has launched an inquiry into online data protection and cyber security after the recent data breach in October 2015 affecting about 160,000 of TalkTalk's customers, writes Pulina Whitaker, pictured, of the law firm Morgan Lewis.

It has been reported that credit and debit card information and personal identifying information of TalkTalk's customers, such as their names, dates of birth and email addresses, have been accessed by the perpetrator. It has also been reported that TalkTalk had previously suffered two other data breaches in the last year. The inquiry will look at the TalkTalk data breaches, the most recent one of which is currently the subject of a criminal investigation, and also look at telecoms' and internet service providers' obligations to keep personal data of its customers secure. A deadline for written submissions to the inquiry is November 23, 2015.

Data protection obligations

All "data controllers", such as mobile operators and telecoms operators, have obligations to their customers to have in place adequate technical and organisational measures to keep personal data secure. Such measures often include encryption of personal data as well as having in place boundary firewalls, malware protection and patch management software. The Government launched its voluntary Cyber Essentials scheme in 2014 allowing organisations to apply for one of two levels of cyber security badge certification:

- Cyber Essentials – this requires organisations to complete a self-assessment questionnaire (which is marked by an independent external body); or
- Cyber Essentials Plus – this requires the organisation's systems to be tested by an independent external body.

Although voluntary, the Government is intending to encourage organisations to be more proactive about cyber security in the face of increasingly sophisticated cyber-attacks. The key cyber threats facing organisations are:

- State-sponsored hackers
- Organised criminals
- Hacktavists
- Organisations and
- Current or former employees.

Cyber security professionals view the chance of a business becoming a victim or a repeated victim of a cyber-attack as almost inevitable and, therefore, all organisations should review regularly their cyber security measures as the threat landscape evolves.

New data protection laws

The proposed new Network and Information Security Directive (the "Directive") sets out cyber security obligations for certain market operators and information system providers. The legislation is still in draft form but is expected to be finalised later this year or in early 2016, along with the proposed General Data Protection Regulation (the "Regulation") which reinforces obligations on data controllers to have secure systems to protect personal data.

Data breach notifications

Some European countries have current obligations to notify data protection authorities about personal data breaches. In the UK, only some organisations such as Internet service providers and telecommunications operators must notify the UK data protection authority within 24 hours of a breach. Under the Regulation, as currently drafted, data controllers will have to notify the data protection authority about a breach involving personal data within 72 hours and, in certain circumstances, notify the affected individuals without undue delay. There are parallel obligations on market operators to notify the authorities without undue delay under the Directive, although Internet service providers may have different timing obligations (these proposals are still being discussed). In some instances, individuals whose personal information has been compromised may or should also be notified.

Continual review

The Government's Cyber Essentials Scheme is a useful starting point for organisations who are only recently, or who have not started, to consider cybersecurity risks to their businesses. Cybersecurity professionals view the chances of businesses becoming victims of a cyber-attack as being almost inevitable. The Cyber Essentials badge certification does not provide a clean bill of health but just confirmation that the organisation's cybersecurity measures are satisfactory at the time the assessment is conducted. It crucial that organisations continually review the risks their businesses face, including the structure and make-up of their workforce, geographical operations and the sensitive nature of their business information. Cybersecurity measures should be reviewed and updated accordingly.

The Government recommends that organisations with badge certifications re-certify at least once a year to retain the badge. Additionally, there are other cybersecurity standards that organisations can consider implementing, such as ISO 27001, the family of standards helping organizations keep information assets secure. Using this family of standards helps organisations manage the security of assets such as financial information, intellectual property, employee details or information entrusted to them by third parties.

This article was originally published in

Professional Security Magazine.

The online version can be found here.