5 Takeaways from the Carphone Warehouse Breach

The Carphone Warehouse breach is the biggest so far announced in the post GDPR era.

What are the salient points to note from this breach?

1. 6 million records accessed
2. NCSC, ICO, FCA investigating
3. 3 million records accessed in 2015 breach
4. Cyber security risk identified by board in last FY report
5. If GDPR applies, maximum fine of £420m could apply

A recently announced massive cyber attack at Dixons Carphone Warehouse has resulted in significant unauthorised access to millions of records including personal data. It appears that two breaches occurred which resulted in;

- 6 million customer records being stolen including 5.9 million payment card details
- 1.2 million customer records including name, address, email

In January Carphone Warehouse were fined £400,000 for a breach that occurred in 2015 when 3m customer records (including personal details) and 1,000 employee records were stolen.

Dixons say the breach was only discovered in the week leading up to the announcement and it actually occurred in the July 2017. Under the Data Protection Act they would be liable to a maximum fine of £500,000. Under the new GDPR regulation the fine could rise to a maximum of £420m based on last years' global turnover of £10.5bn.

In their most recent report, Dixons identified information security as a risk and their potential vulnerability to malware and cyber attacks. They identified potential consequences that could include reputational damage, reduced cash flow, financial penalties, reduced revenue and profitability, loss of competitive advantage. Dixons did appear however to be heading in the right direction to manage the risk ensuring senior management oversight including a Strategic Improvement Plan and increased investments targeted at managing the information/cyber security risk.

The independent regulator the ICO is investigating the current breach along with the FCA and NCSC. The ICO has said it is yet to determine whether GDPR or the 1998 Data Protection regulations will apply.

The NCSC is working on how the breach has impacted UK citizens and what measures can be taken to prevent such a breach re-occurring. They have also published guidance on what to do for people who think they have been affected by the breach.

The CEO Alex Baldock has apologised saying that they have fallen short of expected standards. He confirmed that they have called in cyber experts to investigate as well as relevant authorities and the unauthorised access has now been blocked.

Anyone affected or concerned about their personal data being accessed and how it could be used should contact Action Fraud.

The breach came to light as a result of a massive attempt to compromise the cards in a card processing system, this means that someone tried to use the card details to take unauthorised payments.

Dixons shares fell 6% following the announcement of the breach.

Useful Resources

GDPR Readiness Test [Checklist]

GDPR 12 Step to take NOW [Infographic]

9 Steps to Implement a Security Management Tool [eBook]