Insurance Times

10 March 2020 | By Clare Ruel

High-profile data breaches pushes cyber insurance up agenda

More needs to be done by large corporates to ensure that client and customer data is protected

Two major security breaches broke last week pushing cyber insurance to the top of the agenda.
Last week Boots suspended all payments via its Advantage card for a short period of time after a security breach attempt to break into customer accounts using stolen passwords.

Advantage card customers can use their loyalty card points to pay for items in store or online as the points have an equivalent cash value.

This suspension measure was used as an extra precaution to protect customers.

The incident affected 1% of the company's Advantage card holders (150,000 people) in a bid to steal reward points which can be spent in store or online.

A spokesperson for Boots said: "We can confirm we have written to a small number of our customers to tell them that we have seen fraudulent attempts to access boots.com accounts.

"This was after our IT security team spotted unusual activity on a number of Boots Advantage card accounts, including attempts to access and spend Boots Advantage Card points.

"These attempts can be successful if people use the same email and password details on multiple accounts. We would like to reassure our customers that these details were not obtained from Boots. We are aware that other organisations may be impacted too."

Boots is writing to its customers and said it will replace points in the instance that they have been used fraudulently.

And hot on the heels of this also on 5 March Virgin Media's database containing phone numbers, addresses and email addresses suffered a data breach due to being "incorrectly configured" which allowed for unauthorised access, its chief executive Lutz Schüler said in a statement online. It affected 900, 000 people which is 15% of its customer base.

Meanwhile on the 2 March Tesco issued new Clubcard's to 600,000 account holders after discovering a security issue.

Although its Clubcard accounts were not hacked, Tesco said that it was a precautionary measure.
It follows the FCA being hit by a data breach recently exposing 1,600 people's details with Eldon's Arron Banks being one of them.

Not mandatory
Eva Berg-Winters, chief executive and co-founder at cyber MGA Bewica told *Insurance Times* that cyber insurance cover is not mandatory for store cards.

"It's important to note that Boots has not actually been hacked. They have noticed hackers using client credentials (ie: login, password) to use boots points for their own benefit.

"Using breached credentials is one of the most common forms of attack. Our own data on UK SMEs shows that one in three business email accounts has been in a data breach with the password stolen as well.

"It is human nature to reuse passwords - our data very much shows that as well. Obviously, hackers try those credentials on sites to see if they can get access. As was the case with boots."

No monetary losses
Matt Honea, director of cybersecurity at Guidewire said: "Unfortunately, these types of attacks are getting more common, and users should understand that they need to use unique passwords across websites to protect themselves."

He told *Insurance Times*: "It is worth noting that in this [Boots] case is not a data breach at all.

"If there are no monetary losses, then there can be no cyber insurance claim, but it will depend on how they categorise "Boots points" and what the [sterling] conversion equates to."

This is because the majority of the cyber insurance today is purchased by corporations rather than individuals, he continued.

"There is however a growing number of personal lines policies available for individuals looking to protect themselves from cyber-attacks.

"Typically, these policies will cover the loss of funds resulting from a social engineering attack, where for example an individual has been persuaded to hand over their bank account details to a hacker.

"However, in most cases these policies will not cover the loss of funds should the financial services institution be hacked themselves.

"Instead it would be the bank themselves responsible for reimbursing any lost funds. This same general rule would most likely apply for the loss of loyalty card points," Honea added.

Robust data management
Meanwhile, the Virgin data breach is "one long line of cyber incidents where confidential personal information was accidentally made available online" Honea continued.

"In fact over the last few years the majority of data breach insurance claims have come from accidental release of records rather than malicious hackers breaking into an organisation.

"This demonstrates the importance of businesses having robust data management processes and ensuring they are applied at all times.

“Regulations such as GDPR have driven the business community to make this a board-level issue – but this incident highlights that more needs to be done by large corporates to ensure client data is secured appropriately.

“Accidental human misconfigurations are a key component of data breaches.

“Large companies need to invest in education, training, and verification procedures to ensure that critical systems that access data have at least two checks in place, similar to that of two factor authentication that is more common today.”

In August 2018, Superdrug’s online customers were targeted by hackers who swiped the personal details such as names, addresses, date of birth and phone numbers of 386 accounts and holding the health and beauty high street retailer to ransom.

Untraceable currency

But Michael Reitblat, chief executive and co-founder of Forter highlighted that reward points are a “currency as valuable and untraceable as cash”.

“Fraudsters can sell the loyalty account’s PII, or directly access accounts to redeem valuable reward points and coupons for themselves.

“Suspending loyalty accounts causes massive inconvenience to consumers who miss out on their benefits, however temporary.

“Fraudulent activity in these accounts can negatively impact the customer experience, causing serious damage to brand reputation, and significant monetary losses to merchants.”

In light of the recent high-profile breaches he said that they demonstrated the growing underground market for loyalty program account data.

“It is becoming increasingly apparent that loyalty program accounts are low hanging fruit for fraudsters, with loyalty programme fraud rising 89% year on year,” he said.

Meanwhile Adam French, consumer rights expert at Which? added: “This data breach has exposed the data of almost a million Virgin Media customers and whilst no financial details or passwords were included, those customers are likely to be worried.

“It is vital that Virgin Media continues to provide clear information on what has happened.

“For anyone concerned they could be affected – it’s good practice to update your password after a data breach. Also, be wary of emails regarding the breach, as scammers may try and take advantage of it.”

Subscribers read more

Cyber criminals go phishing using Coronavirus outbreak to swipe data