Safety & Security (15/5/2017)

Web Article
http://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/

The UK’s 19 most infamous data breaches

Software vulnerabilities, lost hard drives and CDs, malicious insiders, poor security - the UK's most important data breaches reveal just how many ways data can be put at risk

By John E Dunn | Apr 10, 2017

Share
Twitter Facebook LinkedIn Google Plus

It's tempting to believe that important data breaches only happen in the US and the figures tend to bear that out – the US accounts for the overwhelming majority of the really big data breaches that have been made public, some of them absolutely vast. But US laws and regulations force organisations to admit to data breaches involving customer, something which is not true in all countries.

In the UK, the most important piece of legislation organisations must worry about is the Data Protection Act and the possibility of fines by the information commissioner (ICO). Below we offer what we believe are the ten most significant data breaches to hit the UK, not in all cases because they were particularly large but because of the type of attack or vulnerability involved or the sensitivity of the data compromised.

Globally, the UK currently ranks a distant second behind the US for data breaches, which is no cause for complacency. Many of the breaches mentioned here happened in the last two years. Undoubtedly, larger and more serious breaches lie ahead.

Infamous data breaches - Wonga (2017)

Payday loan company Wonga has fallen victim to a large data breach that could have hit as many as 245,000 of its customers including bank account numbers and sort codes.

In a customer help page Wonga said it is “urgently working to establish further details and contacting those who we know have been impacted”. Along with the bank account number and sort codes, Wonga believes that full names, email addresses, home addresses, phone numbers, and the last four digits of debit card numbers have also gone amiss. The company thinks passwords are safe but recommends customers change these regardless.

It advises customers notify their banks and request that their accounts are put on alert for unusual activity. But Wonga also states that it believes accounts are now secure and no action is required. At the same time, it recommends being “extra vigilant” across “other accounts and online activity”.

Wonga’s statement finishes: “We take issues of customer data and security extremely seriously. Cyber attacks are, unfortunately, on the rise. While Wonga operates to the highest security standards, these illegal attacks are unfortunately increasingly sophisticated. We sincerely apologise for the inconvenience and concern this has caused.”

Commenting on the attack, James Thompson, regional director for EMEA at authentication company SecureAuth, said that it will serve as a “hefty reminder” to any organisation holding personal and financial data to “continually innovate security and authentication to keep ahead of attackers.”

“Recognising user behaviours that are out of character for an account is key to protecting against actors staying undetected within your network,” Thompson said. “Businesses need to be able to identify and flag deviations in user behaviour.”

Infamous data breaches - Three (2017)

A major breach of Three’s customer upgrade database revealed last November is worse than the network operator initially thought, it was disclosed this week.

The original hack - revealed in November 2016 - occurred when Three’s upgrade database was accessed using an employee login. At the time the company said that no financial information was stolen, but names, phone numbers, addresses and dates of birth were taken.

Three said that of its 9 million customers it believed the data of 133,827 people was compromised.

This week Three said 76,373 more customers had been breached. The investigation is ongoing but the company claimed no further customer breaches are expected.
Commenting on the disclosure, IT security specialist at ESET, Mark James, said: “As always with this type of data breach the focus seems to be on financial information not being

obtained, but when you look at names, addresses, dates of birth and methods of payment, the bank details are the easiest to change.

“The type of information we either would not or could not change is being sold, traded, stored or accessed online by cybercriminals to build a profile of you, the victim. It is then reused much later down the line, often to get more information that can be used either for financial gain or identity theft.”

Infamous data breaches - Sports Direct (2017)

Sportswear retailer Sports Direct failed to tell its entire workforce that they might have had their personal credentials stolen in an internal security breach.

The Register reports that Sports Direct noticed its systems had been compromised in September 2016, but it wasn’t until December that they discovered the data breach – including names, email addresses and phone numbers.
The attacker reportedly gained access through an unpatched content management system running on the open source DNN platform.

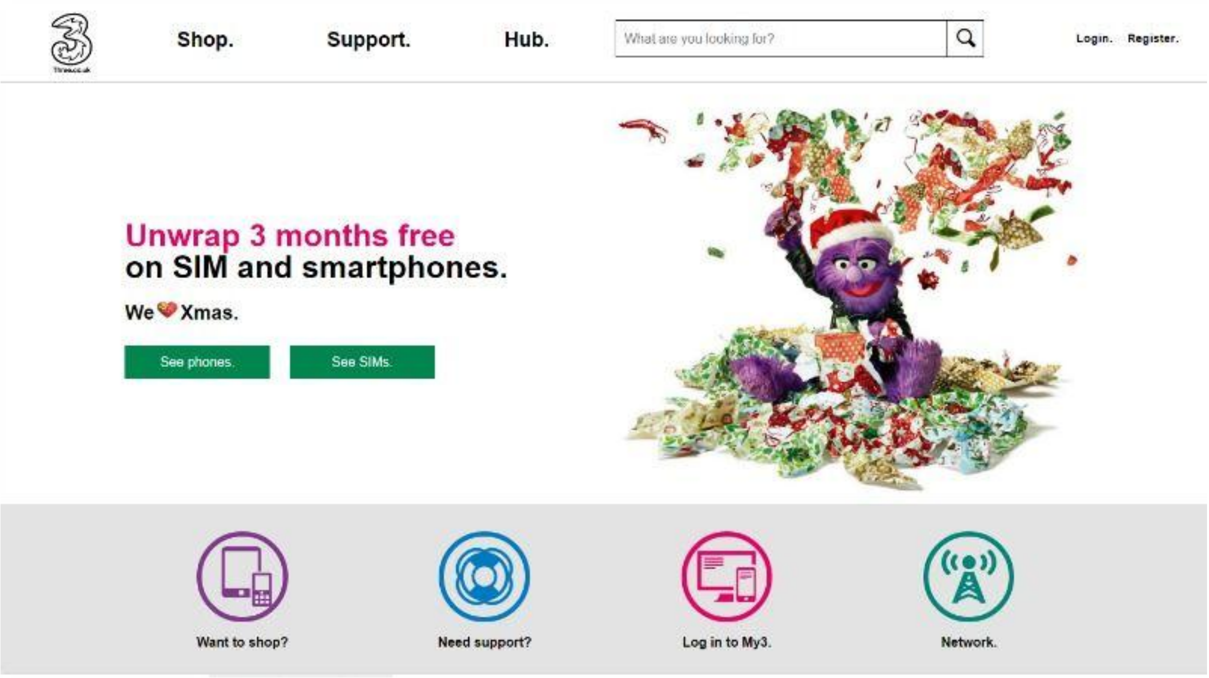
Sports Direct did notify the Information Commissioner’s Office but avoided sharing details of the breach with staff – because there was no evidence that the data had been copied.

Sports Direct did not comment on the breach.

Infamous data breaches - Three Mobile (2016)

Three, one of Britain's largest mobile operators has revealed it has had a major data breach that could put millions of its customers at risk.

According to The Telegraph, hackers accessed Three's customer upgrade database by using an employee login.
Three said that the data accessed did not include any financial information but did say that names, phone numbers, addresses and dates of birth of its customers were obtained.



Unwrap 3 months free
on SIM and smartphones.

We ❤ Xmas.

Since the announcement of the breach (the evening of 17th November), police have arrested three men in connection with the breach.

Infamous data breaches - Tesco Bank (2016)

Late last year, Tesco Bank, the consumer finance wing of the British supermarket giant, froze its online operations – after as many as 20,000 customers had money stolen from their accounts.

Chief executive Benny Higgins said in a statement published on the Tesco Bank website that 40,000 accounts had been compromised – and half of those had money stolen from them. Customers will be able to use their cards for cash withdrawals, direct debit and chip and pin, but will not be able to make online transactions until the situation is under control.
The bank only confirmed that it was subject to criminal activity, and did not describe the attack.

Tesco Bank, which has over seven million customer accounts, has said it will cover any financial costs of the breach. Higgins said: "Any financial loss that results from this fraudulent activity will be borne by the bank. Customers are not at financial risk."

But one customer, Kevin Smith, from Blackpool, told the BBC that he had lost £500 from one of his accounts, while another claimed to have lost £600 and left without emergency funds from the bank.
Adrian Davis, Managing director for EMEA (ISC)2, the independent body for infosec professionals, the breach is evidence of Tesco Bank losing control of operational risk.

"I believe we are at a point where, despite growing awareness of the issues, business leaders are losing control and visibility of core business risk," Davis said. "They have not realised just how much their organisations have changed in the digital age and how this is leaving them vulnerable. They have not treated cyber risk as anything more than an IT problem, and now they, and we, are paying the price."

Infamous data breaches - Sage (2016)

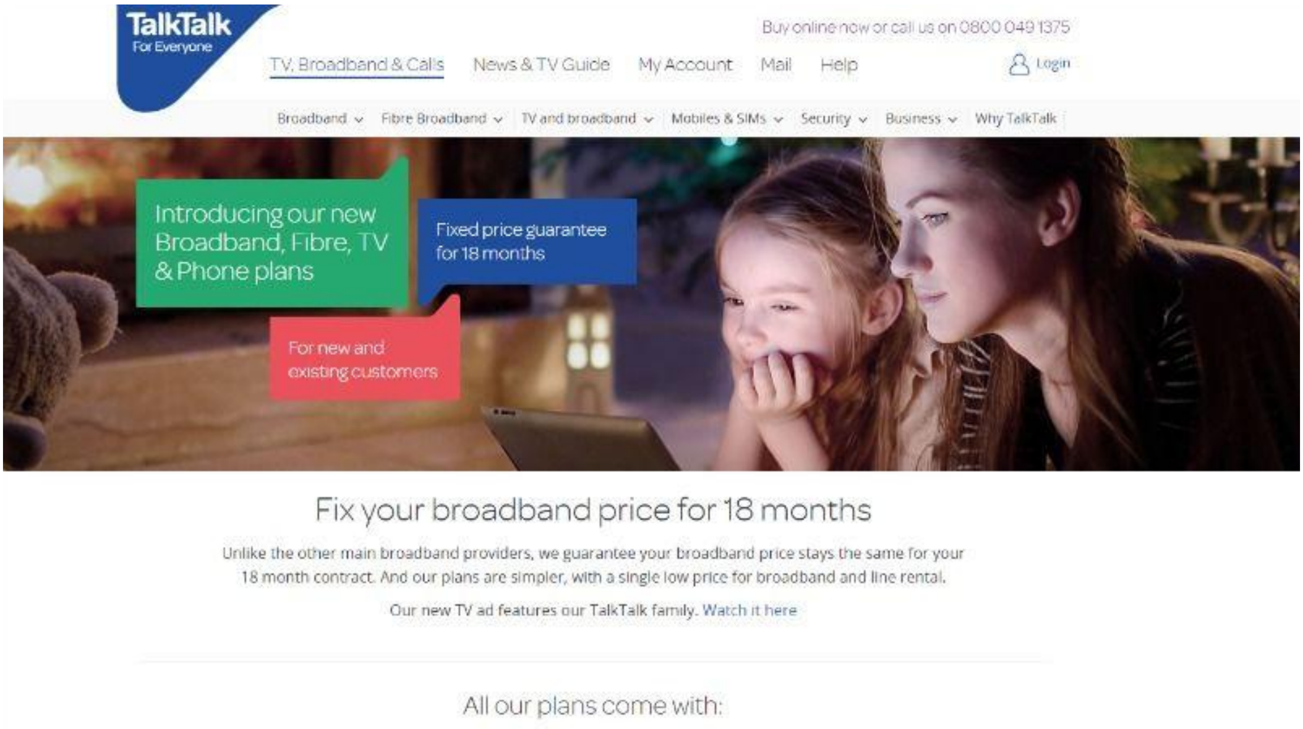
As a FTSE-100 firm, the apparent insider attack admitted by accounting and HR software firm Sage could turn out to be one of the most important in UK data breach history if its scale is confirmed. According to the firm, the employee data of up to 280 UK customers representing a large number of individual users could be at risk. "We are investigating unauthorised access to customer information using an internal login," the firm said in a vague statement that will inevitably re-ignite the contentious issue of insider access.

Infamous data breaches - Kiddicare (2016)

Online child products retailer Kiddicare was forced to admit it had exposed real customer data when testing a new website in 2015. In this case, the mistake was only noticed when customers started receiving suspicious SMS text messages asking them to take an online survey and an investigation eventually uncovered to error. As with many UK breaches, the company played down the fact it had let names, addresses and contact details of up to 800,000 people fall into malevolent hands with the excuse that no credit card data had been compromised (which would have been its liability had it done so).

Infamous data breaches - TalkTalk (2015)

Publicised in October 2015, TalkTalk initially struggled to confirm how many of its four million customers were affected after hackers exploited a reported weakness in the firm's website. TalkTalk CEO Baroness Dido Harding sounded disquietingly vague about the attack's scale when interviewed on TV, and it later transpired that a 'mere' 157,000 personal records had been compromised. Shockingly, the incident was the second (and possibly third) data breach affecting the company in under a year, which could mark it as the moment when dissatisfaction over the rising number of breaches becomes both political and mainstream in the UK.



Buy online now or call us on 0800 049 1375

Fix your broadband price for 18 months

Unlike the other main broadband providers, we guarantee your broadband price stays the same for your 18 month contract. And our plans are simpler, with a single low price for broadband and line rental.

Our new TV ad features our TalkTalk family. Watch it here

All our plans come with:

Infamous data breaches - Moonpig (2015)

Another biggie, a software flaw in the firm's Android app let a researcher access the records of any Moonpig account holder he tried, in theory compromising a total of three million people. As serious, the researcher reported the issue to the firm 18 months before going public in early 2015 after receiving an inadequate response. Significant partly because it involved a mobile app rather than the more common website breach.

Infamous data breaches - Think W3 Limited (2014)

A serious attack in which a hacker was able to get his or her hands on 1,163,996 credit and debit card records from online holiday firm Think W3 by using an SQL injection attack to exploit a weakness on its website. The ICO described the incident as a "staggering lapse" and fined it £150,000.

Infamous data breaches - Mumsnet (2014)

A direct victim of the infamous and widespread Heartbleed SSL software flaw, the compromise allowed hackers to access anything up to 1.5 million user accounts on the hugely popular site, its owners revealed. Although the data inside these accounts was less sensitive than for some of the other accounts, the hack revealed both the potency of big but undiscovered software issues affecting multiple sites and that even big brands could be affected.

Infamous data breaches - Staffordshire University (2014)

A re-run on the lost laptop theme that people assumed had been consigned to history, this time involving 125,000 students and applicants on a computer stolen from a car. But the files had been password-protected said the University, plaintively. That wouldn't have been much of a barrier to the name, address, telephone number and email data.

Included this incident as a reminder that just because times have moved on doesn't mean the old problems go away.

Infamous data breaches - Morrison's supermarket (2014)

An unusual example of the insider attack, the attacker published details of the firm's entire workforce database online, 100,000 employees in all. An employee was eventually arrested for the incident and will presumably come to court at some point which could reveal more details of how the firm's security was bypassed. Inside events are rare but particularly feared because they abuse privileged access that is hard to lock down. Some employees later launched legal action against Morrison's.

Infamous data breaches - Yahoo (2013, 2014)

It seems hard to pin down just one data breach spawning from Yahoo's 22 years in business. Last year appeared to unearth a mammoth lack of security on Yahoo's part with reports uncovering a breach affecting over 500 million Yahoo user accounts during 2014.

Another data breach was reported dating back to 2013, in which an unprecedented 1 billion user accounts were thought to have been affected, creating the largest ever recorded information breach. It's believed that names, email addresses, telephone numbers, security questions (both encrypted and unencrypted) and their answers were exposed during the breach.

Yahoo is now facing numerous lawsuits after being criticised for not disclosing this information sooner, impacting its sale to Verizon, which reduced its bid by $350 million from the initial $4.8 billion price tag.

Most recently, Yahoo revealed this week that 32 million user accounts were compromised in the last two years. The accounts were said to have been accessed using forged cookies which enable an intruder to access an account without its password.

And while it's not a UK-based company, Yahoo has a large number of UK customers, which its data breaches have impacted.

Infamous data breaches - Sony PlayStation Network (2011)

The largest data breach in history at the time, Sony's disastrous 2011 breach saw hackers make off with the customer records of 77 million people relating to its PlayStation Network, including a small number revealing credit card numbers. Apart from downing the company's systems for an extraordinary 23 days, the breach crossed national frontiers, affecting people from all over the world, including the UK. Britain's ICO eventually issued a £250,000 fine for what will go down as the first big data breach to affect people across the globe.

Infamous data breaches - Brighton and Sussex University Hospitals NHS Trust (2010)

The Information Commissioner (ICO) ended up imposing a fine of £325,000 after sensitive patient data of thousands of people was discovered on hard drives sold on eBay. An investigation found that at least 232 de-commissioned drives that should have been deep cleaned and destroyed by a contractor ended up being sold second hand.

Infamous data breaches - T-Mobile (2009)

Sales staff were caught selling customer records to brokers who used the information to market them as their contracts were coming to an end. It was never clear how many records were involved in this murky insider trade but it was believed to run from half a million to millions. Initially the ICO refused to name the firm but was forced to after rival networks said they were not involved, leaving only one name.

In 2011, the two employees involved were fined £73,000 by the courts.

Infamous data breaches - HM Revenue & Customs (2007)

Probably the most infamous large data breach ever to occur in the UK, two CDs containing the records of 25 million child benefit claimant in the UK (including every child in the country) went missing in the post. There was never any indication that these password-protected discs had fallen into the wrong hands but the incident underlined how valuable data was being handled by poorly-trained junior employees.

Infamous data breaches - Nationwide Building Society (2006)

The moment date breaches entered consciousness in the UK, the Nationwide incidentinvolved an unencrypted laptop stolen from a company employee that put at risk the personal data of 11 million savers. The UK's poor disclosure rules made it difficult for outsiders to get information on what had occurred.

The Financial Services Authority (FSA) eventually fined Nationwide £980,000, still the largest sum ever imposed for data loss in the UK, seen at the time as a warning shot for other firms that might have similar incidents. Not everyone noticed.