CYBER SECURITY TEAMWORK

Keiron Dalton *explains how greater collaboration between banks and authorities is crucial to winning the cyber security battle*

It goes without saying that cyber security is one of the great technological challenges of our time. Cyber fraud has become a lucrative global business for those perpetrating the attacks, and businesses face a constant struggle to keep up with the rapidly expanding skillsets of hackers. Symantec's *Internet Security Threat Report 2017* aptly summed up the state of play: in 2016, there were 357 million new malware variants, an increase of two million on 2015. For ransomware in particular, 98 new malware families appeared in 2016, which represented an increase of 227 percent on the previous year. With such figures in mind, it is imperative that organisations stay on their toes as far as cyber crime is concerned.

FINANCIAL SERVICES FIRMS ARE FAILING TO REPORT DATA BREACHES IN GOOD TIME

The cyber security spotlight is being shone even more brightly on banks and financial institutions, for the obvious reason that they guard the fortunes of the majority of the world's businesses and consumers. With this in mind, and the fact that the financial world is consequently a preferred target for hackers, it would be sensible to assume that banks and similar organisations would inform the authorities whenever they fall victim to a successful cyber attack.

However, Megan Butler, a Director at the Financial Conduct Authority (FCA), recently made the claim that financial services firms are actually failing to report data breaches in good time. Whether this is accidental or deliberate, it has the potential to be extremely damaging for the wider banking and financial sector, as transparency is key in the battle against cyber crime.

The findings of the FCA point to a key issue that needs to be addressed: a lack of collaboration between financial institutions and authorities when it comes to data breach reporting. If we are to gain the upper hand in this seemingly never-ending conflict with cyber criminals, this situation needs to change, and soon.

According to the FCA, the number of attacks reported to the regulator has increased from five in 2014, to 49 over the course of 2016. Of these, ransomware is said to be becoming the weapon of choice for hackers, and now makes up around 17 percent of the reported incidents. This close-to-tenfold increase at least provides some indication of the growing scale of the problem.

However, given the number of attacks that are inevitably carried out on the industry on a daily basis, the reported figure of 49 incidents over the course of an entire year looks somewhat unrealistic, with the real amount likely being much higher than this.

There are a few logical reasons why a bank might choose to keep a data breach under wraps. The financial and reputational impact of a successful cyber attack can be particularly severe, and picking up the pieces can take a considerable amount of time if information is released into the public domain. Organisations could also justify remaining quiet so as not to alert hackers to further flaws in their systems before they have had adequate time to patch them up.

FAILURE TO REPORT

Despite the reasons a bank or financial institution may give, hiding a data breach from the authorities should not be considered a positive course of action. For a start, failing to report such an incident makes it more likely that an organisation will be considered liable under security breach notification rules. Even more pertinent, however, is the impact that a cover up can have on security in the wider industry in general. If a bank uncovers a threat, it may learn how to address it and mitigate against the same thing happening in future, but the financial community outside of that one institution will not be able to put a similar security framework in place. Essentially, this is playing into the hands of hackers, and is something that must change.

If the fight against financial fraud is to be strengthened, greatly increased transparency between institutions and the appropriate authorities is critical. This means that both parties need to work together and be more proactive in protecting their customers' data and money, and work to build the relationships they share as they tackle this growing issue. In the case of the banking industry this is especially crucial.

A current example of collaboration across the financial services industry lies in the Open Banking standard, which has only recently been implemented. Designed to increase competition and the amount of choice available to consumers, the regulation compels banks to share certain customer data, so that rivals can tailor their offerings to suit the needs of customers more accurately.

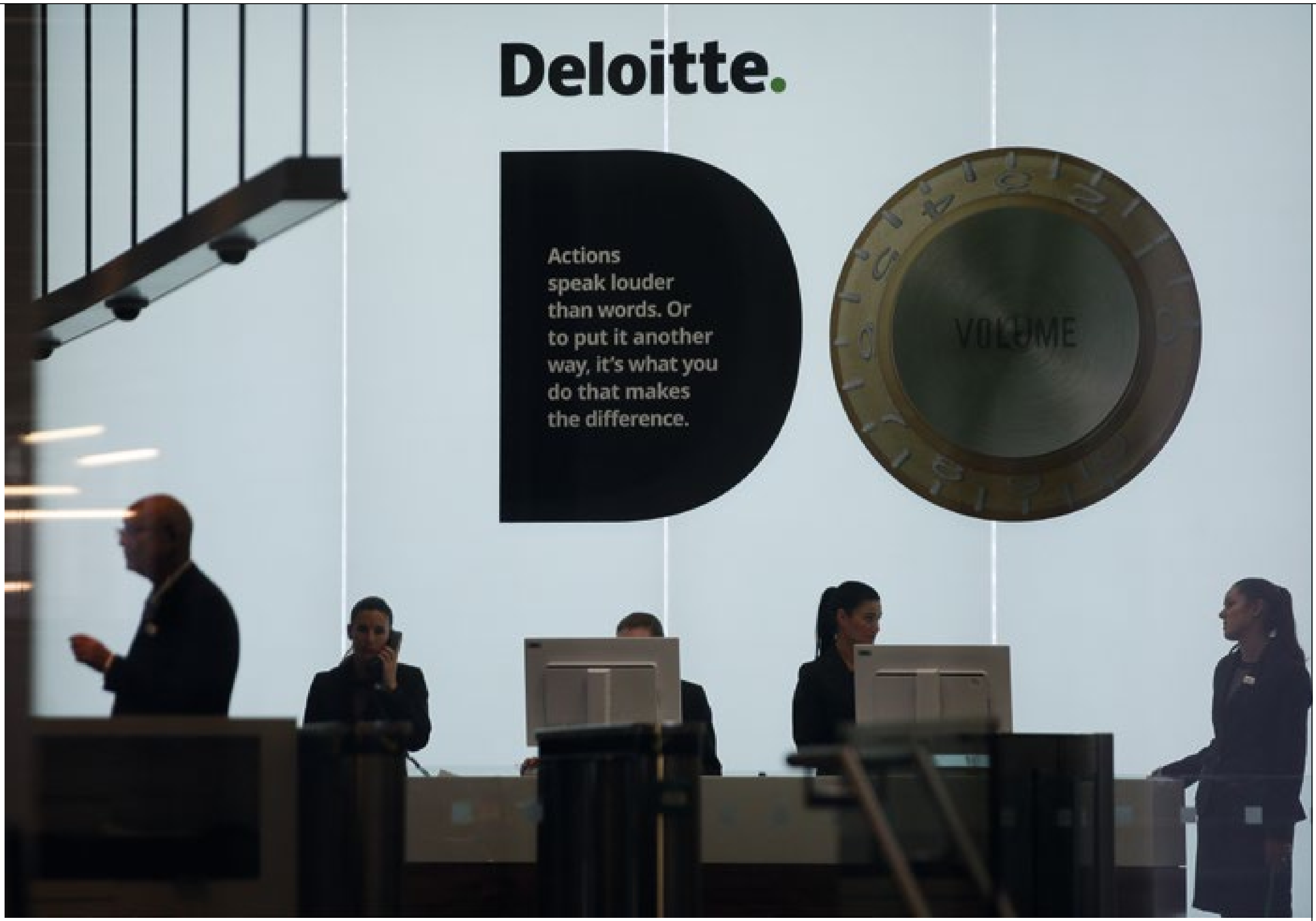
COLLABORATION IS KEY

While Open Banking is still very much in its infancy as a live standard, the fact that it has been brought into place underlines how this level of collaboration is very much a possibility. With this in mind, a similar approach to data breach reporting could work wonders. After all, if we can be open to improving business and boosting savings for customers, why is the industry not doing the same to improve security of the public's money?

This renewed spirit of collaboration should also include banks working closely with mobile network operators, as mobile has become the favoured platform for many customers. Banks and telephone companies often have access to the data showing how people use their networks, in particular how a certain customer behaves, and what is considered 'normal' or within a predictable pattern for that individual. Being able to quickly differentiate between normal and suspicious behaviour will become increasingly important for banks as they adhere to Know Your Customer practices, and will reduce the risk of false positives when suspicious patterns are flagged. For this to become the norm, it is vital that financial institutions, mobile companies and authorities make more of an effort to be open about how they share information.

So how can financial institutions and the appropriate authorities create this more reciprocal,

▶


Deloitte.
Actions speak louder than words. Or to put it another way, it's what you do that makes the difference.
VOLUME

Deloitte claimed that "very few" of its clients were affected by a hack after a news report said systems of blue-chip clients had been breached

Picture credit: Getty

harmonious relationship? As in many aspects of modern life, technology has the power to be a great enabler in this situation. Sophisticated fraud detection and multi-factor authentication software – such as divert detection and location checks to verify the identity of banking customers – can encourage the development of greater transparency by making it much easier for financial institutions to accurately detect and report on a data breach, as well as deal with any damage before it becomes so serious that an organisation is tempted to keep it under wraps.

PURSUIT OF GREATER SECURITY

Ultimately though, all of this can only be possible if both parties are willing to compromise. From a bank's perspective, it is of paramount importance that at least some element of competitiveness is put to one side, in aid of the pursuit of greater security for customers. At the same time, authorities need to make sure that they are as sympathetic as possible to the challenges that financial services organisations face, and ensure that frameworks are in place that enable breaches to be reported with ease, and without fear of severe regulatory repercussions. If this can be achieved, the end result is a win-win situation for both parties, and ultimately for the customers themselves.

The issue of cyber fraud in the financial world will not be resolved overnight. The threat landscape continues to evolve at considerable pace, so banks and other financial institutions need to do everything in their power to stay one step ahead. Evidently, key to this pursuit is ensuring that an organisation's cyber security defences are watertight, and that internal security teams adopt a proactive approach to weeding out flaws and vulnerabilities in their systems.

However, it is also unrealistic to expect systems to be completely invulnerable to malicious intrusions, especially given the skills possessed by modern hackers. With this in mind, openness is essential when things go wrong, regardless of how embarrassing or financially damaging a data breach may be. Banks and similar institutions may look upon regulators and authorities with a degree of suspicion, but ultimately, the two parties share a common goal: ensuring that rules designed to keep customers safe are followed.

> CYBER SECURITY IS ONE OF THE GREAT TECHNOLOGICAL CHALLENGES OF OUR TIME

At the end of the day, banks need to realise that authorities aren't out there purely to punish them for mistakes they make. At the same time, regulators perhaps have a role to play in dispelling this image, by communicating their plans and intentions as clearly as possible, and playing their part in fostering more productive relationships.

By keeping this common goal in mind, there is every chance that this emphasis on greater transparency will become a long-lasting philosophy, and the security of customer data can be safeguarded for the long term ●

Keiron Dalton is responsible for the global strategic direction of Aspect Software's Verify mobile identity service. He possesses a wealth of experience of IT innovation, with mobile security being his key area of expertise.

TESCO Bank
Free cash withdrawals
We won't charge you for taking your cash out when you use your debit card
RBS
CASHLINE
Free cash withdrawals
We won't charge you for taking your cash out when you use your debit card
RBS
CASHLINE

In 2016, around 20,000 customers had money stolen from their accounts after Tesco Bank was hit by hackers

Picture credit: Getty