Learning from others' mistakes: two common security failings in five data breaches

Ali Vaziri, Managing Associate, and Tamsin Hoque, Associate, with Lewis Silkin LLP, mine five Penalty Notices issued in recent years by the UK ICO for insight into how organisations can avoid making the same mistakes

Links to the PNs:

Cathway Pacific www.pdpjournals.com/docs/888104

DSG Retail www.pdpjournals.com/docs/888105

Equifax www.pdpjournals.com/docs/888106

Carphone Warehouse www.pdpjournals.com/docs/888107

Talktalk www.pdpjournals.com/docs/888108

Over a year has passed since news first broke of the UK Information Commissioner's Office intention to fine airline British Airways and hotel chain Marriott £183.4 million and £99 million respectively for their 2018 data breaches. Meanwhile, claimant lawyers backed by litigation funders have wasted no time in launching class actions against each organisation for sums which make even nine figure fines appear relatively restrained.

With BA's Penalty Notice ('PN') hot off the press (see page 2) and whilst we are still awaiting a final outcome on Marriott, now is the time to take stock, drawing on five other relevant examples, of what the GDPR's requirement for organisations to have 'appropriate security' means — especially where those organisations are (to use Elizabeth Denham's characterisation in previous enforcement decisions) "large, well-resourced and established".

The data breaches

Cathay Pacific, February 2020 (£500,000): For a period of approximately 3½ years until May 2018, Cathay Pacific's customers' personal data, including passport numbers, were exposed to attackers. 9.4 million data subjects were affected worldwide, some 111,000 of whom were from the UK. Access was seemingly via an internet-facing server. Cathay Pacific received some 12,000 complaints from customers; the ICO received 2.

DSG Retail, January 2020 (£500,000): Malware installed by an attacker on over 5,000 tills at DSG's Currys PC World and Dixons Travel stores allowed unauthorised access for the nine month period before the attack was detected in April 2018, to over five million payment card details and personal data relating to some 14m people.

Equifax, September 2019 (£500,00): An attack on the credit reference agency's US parent exploited a known and critical vulnerability in a web application framework used by Equifax in its consumer-facing online disputes portal. It resulted in unauthorised access for a 2½ month period ending July 2017 to the personal data of up to 15 million UK citizens. Compromised data for the most part were names and dates of birth, but records also included a large number of other identifiers such as driving licence numbers, as well as credentials.

Carphone Warehouse, January 2018 (£400,000): In July 2015, an attacker entered the system via a WordPress installation using valid credentials which, for 15 days, allowed unauthorised access to the personal data of over 3 million customers (including historic payment card details) and 1,000 employees.

TalkTalk, August 2017 (£400,000): In October 2015, an attacker exfiltrated the personal data of some 156,000 customers (including the bank accounts and sort codes of over 15,000 customers) by exploiting a vulnerability in webpages with access to an underlying database using an SQL injection attack. Those webpages were part of Tiscali's infrastructure, but TalkTalk was not aware of them when it acquired Tiscali's UK operations some years before in 2009.

What is 'appropriate security'?

The GDPR does not prescribe the technical or organisational controls that organisations must have in place to protect personal data — only that they must be appropriate to the level of risk. In making that assessment, organisations are required to take into account the state of technological development, the costs of implementation, the characteristics of the processing, as well as the risks to individuals.

In terms of how those elements come together in the real world, the following passages from the first instance Judge's decision in the Morrisons data breach case — which involved an insider threat — are quite insightful:

"The fact that a degree of security may technologically be achievable, which has not been implemented, does not of itself amount to failure to reach an appropriate standard: an example might be if particular security measures might be introduced which are very costly at the present stage of

development, whereas after a few more years the cost might reduce significantly, as is the case with many new technologies" (paragraph 67).

"I would expect a higher standard to be observed as to the measures appropriate to protect data relating to 100,000 employees than I would expect in respect of a small enterprise employing 6 or 7 workers. Indeed, with economies of scale, measures that might be prohibitively expensive if analysed per head of a small workforce may seem relatively insignificant if spread over the headcount of a large corporate employer. The magnitude of the risk is greater; the cost per head of guarding against it is less" (paragraph 69).

These passages are particularly germane when it comes to organisations who are likely to be "large, well-resourced and established". With that in mind, here are the two failings which were common to all five of the data breaches listed above.

Failing 1: Inadequate software patching

A patch is a set of changes to software designed to update, fix or improve it. Since vulnerabilities in software are always being discovered, closing them through patching before they can be exploited by hackers is, according to the National Cyber Security Centre ('NCSC'), the single most important thing organisations can do to secure their technology.

In all of the fives cases under consideration, the ICO identified that the organisations were not complying with their own patching policies, and in some instances there were no measures in place to check whether software updates and patches were implemented regularly. Particularly of note is the fact that in one case, the organisation had failed to address known IT vulnerabilities, including those that had been identified and reported at a senior level within the organisation.

"Having policies is of little use if they are not observed. Almost all the PNs illustrated a failure, in one regard or another, to comply with the organisation's policies on varied matters such as patching, asset lifecycle, password management and conducting risk assessments. This was also at issue in BA."

Failing 2: Vulnerability scanning

Vulnerability scanning involves using software to inspect computers, networks or applications, and identify known vulnerabilities arising, for example, through misconfiguration.

In these cases, the ICO found that there was a failure to undertake sufficient and/or sufficiently regular system scans, meaning that vulnerabilities were going undetected. In one case, the vulnerability scanning did not even detect the vulnerability despite scanning for it. Also, in some instances either no penetration testing (pen testing is essentially attempting to breach the system's security using the same tools and techniques as an attacker might) was carried out at all, or testing was carried out rarely — in one case, with a gap of 3 years.

The fines

The PNs were all issued under the old regime where the statutory maximum for a 'Level E' rated fine was £500,000 – hence the numbers being relatively modest compared with the maximum sanction available under the GDPR, which is of a far greater order of magnitude.

Although BA was unsuccessful in its submission that a lack of certainty in the new regime means that the Information Commissioner should adopt an approach to fines under the GDPR which is consistent with previous enforcement decisions under the Data Protection Act 1998 (including by imposing the previous cap), these PNs remain relevant given that when it comes to security, the obligations are similar. They also evidence an upward trajectory in the level of fines, and increased willingness of the regulator to come down harder on errant organisations.

Until BA's jumbo penalty notice landed in October 2020, only one other PN had been issued under the GDPR: £275,000 to online pharmacy, Doorstep Dispensaree, in respect of security failings. With BA and Marriott as the guinea pigs, and with one now down and the other to go, it is still relatively early days when it comes to understanding how the Information Commissioner will in practice apply her sanctioning powers. The 114-page BA penalty notice does, however, certainly give some helpful insight into her reasoning when considering whether to impose a penalty, and in calculating the appropriate amount with regard to the matters listed in Article 83(1) and (2) GDPR, as well as the application of the 5 step approach set out in her Regulatory Action Policy ('RAP', copy at www.pdpjournals.com/docs/888109).

What should organisations be doing?

The PNs referred to above provide an opportunity for organisations to learn from others' mistakes when it comes to security — especially where the controls that organisations have failed to put in place are ones which the ICO deems basic, commonplace security measures. When it comes to determining the amount of any administrative penalty, such failures were previously taken into account as an aggravating feature. Hence, for example, the Information Commissioner listing as an 'aggravating feature' in Cathay Pacific's case the fact that the airline had "failed to satisfy no

(Continued on page 14)

(Continued from page 13)

less than four out of the five National Cyber Security Centre's basic Cyber Essentials". In BA's case, although the Information Commissioner determined as part of her assessment at step 2 of the RAP that the nature of the failures were of "serious concern" — not least because there were multiple measures which, in her view, BA could have put in place which would have prevented or mitigated the attack — she did not note any relevant aggravating factors at step 3. Keep in mind, however, that when listing indicative examples of aggravating factors, the RAP includes "the state and nature of any protective or preventative measures and technology available, including by design". A failure to put in place basic, commonplace security measures could well fall under this head with an inflationary effect.

As we have seen above, despite being "large, well-resourced and established", when it comes to inadequate software patching and vulnerability scanning/pen testing, organisation after organisation have repeated the same mistake. This is nothing new, hence the ICO issuing a report back in 2014 in which (amongst others) the two common failings addressed above were highlighted. Indeed, pen testing was also touched on in the BA penalty notice, with the Information Commissioner observing: "had more rigorous testing been performed, or had internal penetration tests been performed … many of the problems identified within this decision are likely to have been detected and appropriately addressed."

The Information Commissioner was also keen to emphasise in the BA penalty notice that a company of BA's size and profile is expected to be aware that it is likely to be targeted by attackers, sophisticated or otherwise. Further, she rejected the suggestion that the attacker(s) were primarily responsible for the GDPR breaches — the breaches related to BA's failures to put in place appropriate security, and those failures were exposed by the attack.

Additional lessons

While we wait to see what further insights can be gleaned from the Marriott penalty notice, in the spirit of 'lessons learnt', here are some additional thoughts:

When it comes to security, 'doing the basics' does not necessarily equate to being easy to do in practice: Patching, for example, can be notoriously difficult to apply, even impossible in some instances.

Most security incidents are not the product of zero-day vulnerability exploits (i.e. attacks that exploit a weakness before a fix become available) — they are relatively simple attacks: That is why the NCSC's Cyber Essentials framework, with its five basic security controls, is a useful baseline for organisations to protect themselves against a wide variety of common online threats, irrespective of size or sector. Although many large organisations will be mature enough in their security posture such that their controls go far beyond the framework's requirements, Cyber Essentials is the base set of technical controls now expected by the ICO.

In terms of the ICO's particular expectations when it comes to security, its recently launched Accountability Framework lists ways to meet them and includes (unsurprisingly) regularly running vulnerability scans and having access to/acting on updates on technical vulnerabilities e.g. vendor alerts or patches: Many of the organisations referred to above shared other basic failings such as inadequate anti-virus protection and poor password management practices. Indeed, hardcoded passwords stored unencrypted in plain text were a vulnerability exploited by BA's attacker(s).

Accountability is a key data protection principle, and we know that policies are an important way to demonstrate compliance: Having policies is, however, of little use if they are not observed. Almost all the PNs illustrated a failure, in one regard or another, to comply with the organisation's policies on varied matters such as patching, asset lifecycle, password management and conducting risk assessments.

This was also at issue in BA's case: departing from a policy decision that all remote network access would be protected by multi-factor authentication, enabled the attacker to access BA's network using the login credentials BA had provided for the use of an employee of a third party supplier. The departure was seemingly based on a dated risk assessment which could not be located.

On the subject of risk assessments, these are another key accountability tool under the GDPR: Two of the PNs evidenced failures to assess risk: one in relation to the security arrangements of the data recipient; and another in relation to a third party with system access. If risk has not been assessed (either properly or at all), it cannot be mitigated through controls. This is crucial when it comes to vendors, as they are very often the weakest link, as further evidenced by the BA breach which was caused by a supply chain attack. Frameworks such as Cyber Essentials are a useful default minimum standard to be required by organisations of their supply chains when assessing risk, so at least there is some degree of assurance about their ability to prevent some of the more basic online attacks.

Buying a new business or thinking of merging? Make sure the risks have been properly assessed, which involves doing appropriate due diligence. In TalkTalk's case, the vulnerability which was eventually exploited came with legacy IT architecture it acquired along with Tiscali. It would seem that in Marriott's case, the same is likely to be true. According to the ICO, Starwood hotels group's systems were compromised in 2014 and Marriott failed to undertake sufficient due diligence when it subsequently bought the group in 2016.

A further 'sanction' — class actions

Whilst organisations have traditionally focused on the risk of regulatory ac-

tion (especially financial penalties) for security failings, the spectre of class actions has raised the stakes. In the cases of BA and Marriott, following her investigations, the Information Commissioner observed in 2019 that BA had "poor security arrangements" and that "Marriott failed to undertake sufficient due diligence...and should also have done more to secure its systems." Those observations were sufficient encouragement for a group litigation order and a representative action respectively where, taking the formula of multiplying the anticipated award to a single claimant by the number of claimants, estimates of damages dwarf any administrative penalty (actual or intended).

It is not surprising, therefore, that the Information Commissioner noted in the BA penalty notice that "BA does not admit liability for breach of the GDPR". More so given her finding —which BA will doubtless have found most unhelpful — that "it is likely that many of these individuals will, depending on their circumstances, have suffered anxiety and distress as a result of the disclosure of their personal information … to an unknown individual or individuals". Whilst the Information Commissioner did not comment on BA's assertion that "claimant law firms will, for entirely self-serving purposes, use the word 'distress' very liberally, essentially with the aim of garnering thousands of potential claimants on no-win- no-fee agreement", BA's concern about class actions is palpable.

Conclusion

Although BA might take some comfort from the fact that the Information Commissioner seemingly resiled from using turnover as the primary metric to calculate the fine (that change in approach accounting for the bulk of the 90% reduction on the Notice of Intent — mitigations and COVID having a relatively limited deflationary effect), the spectre of class actions means that its woes are far from over.

"Always try to learn from other people's mistakes, not your own — it is much cheaper that way." In the spirit of the US election, this 2013 social media post by the incumbent President is apposite given the often huge direct and indirect costs of data breaches which, as the Information Commissioner has now made clear, cannot be claimed as a mitigating factor when it comes to calculating the amount of any PN. So although the threat landscape is ever-changing, and (to use Ms Denham's words) "sophisticated cyber attacks on global businesses are commonplace", there is every incentive for organisations now to revisit controls in place with a particular focus on areas where it is possible to learn from others' mistakes.

Ali Vaziri and Tamsin Hoque
Lewis Silkin LLP
Ali.Vaziri@lewissilkin.com
Tamsin.hoque@lewissilkin.com