Cyber crime: court-assisted breach containment

Ali Vaziri, Senior Associate at Lewis Silkin LLP, explores how the courts can help contain a confidentiality breach in the light of recent cases involving organisations that have been hacked, had data stolen, and are then blackmailed

Prevention is better than cure. But cyber incidents happen, even in organisations with an "optimised" level of maturity where security is "baked in" rather than "bolted on"; and when incidents do occur, fear of publicity should not dissuade organisations from asking the courts for help when they have been hacked, had data stolen, and are then blackmailed.

There are a range of orders which the English courts are willing to make against anonymous hackers to contain a confidentiality breach. Even if those orders are ignored, they can still be useful, for instance, when it comes to securing the removal of stolen data from other hosts/publishers, both in England and abroad.

The dreaded email

The email every organisation dreads (or should dread) receiving:

"… your company's servers are hacked. … Proof of my words attached below (some files which I could not ever possibly have) … you have two possible options:

(1) To pay. I delete all the data … and we forget about each other, forever.

(2) Not to pay. … I publish all information in public. I think you will understand what happens next: the shares of the company will collapse; the company's credibility will be undermined; all contracts, documents, databases and all internal correspondence of the company – everything is going to be public. .... Its going to be the dead end for the reputation of your company."

To pay or not to pay?

The attacker has given you only two options. To pay or not to pay - both options are unpalatable.

So what do you do? Answer: put your incident response plan into action. That plan will ideally have been well-rehearsed by all members of your incident response team, with scenarios involving common attack vectors.

Simply having a plan and a team in place will not dictate the strategy, or provide step-by-step instructions on how to handle an incident (after all, incidents can occur in countless ways). The plan and the team are, however, vital in ensuring the effectiveness, efficiency and consistency of your organisation's response. Those controls will empower the incident lead to draw on the expertise, judgement and abilities of team members, both internal and external, to take the response in whichever direction seems necessary or most desirable.

Some organisations have been known to pay up, trust the criminals to do as promised, and leave it at that. Others are reported to have tracked down the bad actors, got them to sign non-disclosure agreements, disguised the payment as part of a legitimate "bug bounty" programme and, having buried the body (or millions of bodies, as the case may be) hoped that no one finds out.

Leaving aside ethics, let alone laws on breach notification, neither of these approaches look good when the news does eventually surface. Both of these options also leave affected individuals at risk of harm, and unable to take steps to protect themselves. In the context of the widely reported increased penalties under the General Data Protection Regulation ('GDPR'), it is also worth keeping in mind that the UK regulator has expressly referred to deliberate concealment of a breach as being the sort of behaviour that could attract higher fines.

But pre-GDPR, organisations rarely notified regulators, let alone those affected, unless there was a real chance they were going to be found out. Investigations and sanctions from regulators, litigation with data subjects, brand damage, a tumbling share price – there has been every incentive to encourage firms to try to sweep a breach under the carpet.

The blackmailers' leverage

It is precisely this potential for pain and embarrassment that blackmailers leverage to their advantage to bend victims to their will. But the tides might be turning.

Organisations – no doubt prompted by

the GDPR – have been spending time and money investing in data privacy compliance programmes, and beefing up security. So regulatory scrutiny is perhaps not quite the concern it once was for many.

Further, recent government figures from April 2018 suggest that more than two thirds of large businesses have suffered a cyber breach or attack in the past 12 months, making them no longer the exception, but the norm. There is an increased recognition that no organisation is immune.

In that context, data breaches might seem to be losing the stigma they once had; and with it, the levers traditionally used by blackmailers also lose some of their effectiveness.

A third option: the courts

The widespread nature of cyber attacks, and the consequent reduction in corporate 'shame' which results, may go some way to towards explaining why, in recent months, the Media and Communications List at the High Court has seen organisations who have suffered such attacks boldly resisting the two options presented to them by anonymous blackmailers.

Instead, some businesses are choosing a third option: going to the courts and seeking interim non-disclosure orders ('INDOs') to restrain threatened breaches of confidence by hackers, as well as orders for the delivery-up or destruction of the stolen data.

Claimants are also asking for orders requiring the anonymous blackmailers to identify themselves (i.e. self-identification orders).

PML and Clarkson: examples of court-assisted breach containment

INDOs and self-identification orders were sought by claimants in two recent cases:

(1) PML v Person(s) Unknown (responsible for demanding money from the Claimant on 27 February 2018) [2018] EWHC 838 (QB); and *(2) Clarkson PLC v Person or Persons Unknown who has or have appropriated, obtained and/or may publish information unlawfully obtained from the Claimant's IT systems [2018] EWHC 417 (QB*).

In February of this year, an organisation called "PML" (not its real name) was secretly hacked and a very large amount of data was stolen. Three of PML's directors were sent the email at the start of this piece (which went on to demand £300,000 in Bitcoin).

PML asked the court for anonymity and got it (hence the claimant company only being referred to as PML).

Although a derogation from open justice, anonymity protects blackmail victims and is an important legal policy. The court has previously held that its procedures must be adapted to ensure that blackmailers are not encouraged or assisted, and that victims are not deterred from seeking justice.

In addition to anonymity, the hearings were conducted in private. This was justified because police investigations were under way, and the court needed to know sensitive information about the data stolen, as well as what the hacker did to obtain the data. The court file was also sealed to prevent access to documents which might otherwise defeat the injunction and anonymity order.

A few months before PML, Clarkson PLC (a FTSE 250 company) responded somewhat differently to a blackmail attempt, but still sought help from the courts. Rather than seek anonymity, it issued a public statement confirming that its security systems had been breached but that it would not be held to ransom by criminals.

The statement anticipated that the hackers might release some data, but asserted that its lawyers were on standby to take all necessary steps to preserve the confidentiality in the information. True to that statement, Clarkson sought and was granted an INDO which led to a default judgment and final order for an injunction.

> ***"some businesses are choosing a third option: going to the courts and seeking interim non-disclosure orders ('INDOs') to restrain threatened breaches of confidence by hackers, as well as orders for the delivery-up or destruction of the stolen data"***

Assessing risk in a data breach

On becoming aware of a breach involving personal data, organisations should immediately start assessing the likely resulting risk. That assessment will help the business to take effective steps, not just to contain and address the breach, but also to determine what (if any) data protection notifications are required. Both the severity of the potential impact on individuals, and the likelihood of that impact occurring, will need to be considered.

A second public statement issued by Clarkson some time after the default judgment was handed down gives some insight into the circumstances of the breach, and therefore of the factors which are likely to have been considered in its own risk assessment.

We now know that access to Clarkson's computer systems was via a single and isolated user account, and for a sustained period of just over five months. Individuals potentially affected were based in a number of jurisdictions, including in the USA, and many sensitive categories of personal data

(Continued on page 8)

(Continued from page 7)

were potentially affected.

To illustrate, the categories of data listed by Clarkson were said to include: "date of birth, contact information, criminal conviction information, ethnicity, medical information, religion, login information, signature, tax information, insurance information, informal reference, national insurance number, passport information, social security number, visa/travel information, CV/resume, driver's license/vehicle identification information, seafarer information, bank account information, payment card information, financial information, address information and/or information concerning minors."

Interestingly, Clarkson has claimed that as a result of its "investigation and legal measures" it was able to "successfully trace and recover" the copy of the data that was illegally taken from its systems. It is not clear what those "legal measures" were. It is possible (albeit unlikely) that once served with the INDO, the bad actor was prompted to identify itself and deliver up the data, though some might be sceptical on that point.

In any event, and notwithstanding its apparently successful recovery of the stolen data, Clarkson decided to notify potentially affected individuals, even though such notification is mandated by the GDPR only where a breach is likely to result in a *high* risk to the individuals concerned. The notification was said to be in "an abundance of caution".

Whilst nothing was said of the numbers of records affected, Clarkson's decision is not altogether unexpected given what it has revealed about the nature and sensitivity of the personal data affected, as well as the severity of impact on individuals (which included children) – and, in particular, the potential for identity theft or fraud.

> ***"In this new era of accountability, an order is also an important document you can hold up to the world to show that you are doing everything in your power to mitigate the potential impact of a cyber breach on those individuals affected. This could help, not just in your dealings with relevant regulators, but also in the civil courts – not to mention in the court of public opinion"***

The list featured special category and criminal conviction data. There, Article 29 Working Party's WP250 guidelines tell us physical, material or non-material damage should be considered *likely* to occur.

The fact that the breach was the result of malicious intent (rather than an error or mistake) is also a factor that increases the likelihood of the stolen data being used in harmful way, since that was the initial purpose of the breach.

These factors are likely to have been reflected in Clarkson's risk assessment and, therefore, in its decision to notify individuals. Had Clarkson been unable to ascertain exactly what had happened to the data between it being stolen and being recovered (including who had accessed it), then that too would undoubtedly have been a relevant factor.

As an aside, there is nothing like a data breach to provide a new-found appreciation, when it comes to risk, of many seemingly less relevant GDPR principles such as data minimisation (i.e. "don't collect what you don't need") and storage limitation (i.e. "don't keep it if you don't need it"). After all, you cannot destroy, lose, alter, disclose or give access to something your organisation does not have in the first place.

How can the courts help in practice?

Orders made in *Clarkson* and in *PML* illustrate a pragmatism and willingness to intervene on the part of the courts, where hackers blackmail organisations. Consider asking for the specific help of the courts in the following ways:

- unable to identify the hackers? Ask for an order requiring them to identify themselves.
- concerned about the hackers' intentions? Ask for an interim non-disclosure order.
- worried about being identified publicly as a blackmail victim? Ask for anonymity, hearings in private, and for the court file to be sealed.
- reluctant to disclose the full case? If you are worried about sensitive information in the claim papers being disclosed to/misused by the hackers, ask to wait until they identify themselves.
- no idea where the hackers are based? Ask for permission to serve out of jurisdiction.
- no address for service? Ask for alternative service by whatever means were used to communicate with you, such as email (as was the case in *Clarkson* and *PML*) or text message (see *NPV v (1) QEL (2) ZED (person unknown allegedly trying to blackmail the Claimant) [2018] EWHC 703 (QB*) – a recent non-cyber blackmail case).
- want to keep costs down? If the hacker fails to engage (as is almost inevitable), ask for your default judgment application to be determined on paper instead of at

another hearing.

- how long to get an order? You should be able to get in front of a judge within a matter of hours (though in *PML*, having immediately reported the matter to the police, the claimant stalled the blackmailer for a number of weeks before applying to the court).

Why bother with the courts?

It would seem that Clarkson's INDO contributed in some way to its successful recovery of the stolen data. We do not know whether PML was able to do the same.

But as many will be quick to point out, in most cases the reality is that:

- a court order is unlikely to deter hackers from making disclosures of the stolen data;
- a self-identification order is just as unlikely to prompt hackers to identify themselves when ordered; and
- disobeying an order might be a contempt of court, but hackers will already have committed a string of other criminal offences.

So why would an organisation bother with the expense and inconvenience of legal proceedings?

The (other) benefits of an order

Even if INDOs do not prompt blackmailers to return stolen data, they can still be a useful tool when it comes to preventing further dissemination of those data by publishers or hosts – even if the publishers or hosts are in other territories. The chief reason for this is that orders of the English High Court are generally respected internationally.

So whilst making the stolen data inaccessible might be a question of 'whack-a-mole' in the short term, an order can pay off as it makes for a much more effective mallet whenever and wherever those data pop up. In *PML*, various companies hosting the stolen documents blocked access to them or deleted them when served with the injunction. The reality is that hackers are likely to get bored before you do, and inevitably their focus will at some point shift to other softer targets who are more likely to cave into their demands.

In this new era of accountability, an order is also an important document you can hold up to the world to show that you are doing everything in your power to mitigate the potential impact of a cyber breach on those individuals affected. This could help, not just in your dealings with relevant regulators, but also in the civil courts – not to mention in the court of public opinion.

Court orders are not always going to be appropriate in confidentiality breaches. But paying off hackers does not guarantee the outcome hoping to be achieved. It encourages further attacks, and may send a message to the wider criminal fraternity that your organisation is a worthwhile target. There is, therefore, some comfort in knowing that the options presented by attackers are not the only ones available to your organisation, and that you can wrestle back some control of the situation with the courts' help.

Ali Vaziri

Lewis Silkin LLP

ali.vaziri@lewissilkin.com