Bristows

Taking the hackers to court

Why injunctions should be part of your cyber response playbook

Picture this: you're an executive facing a nightmare cyber attack scenario. An email has just hit your inbox from an unknown perpetrator claiming to have hacked your systems and stolen data. They are demanding a ransom: if you fail to pay, you risk seeing your data sold to the highest bidder or exposed to the world.

If your company is one of the lucky ones with a cyber incident response plan already in place (only **55% of medium-sized businesses** and **73% of large companies** have one currently[1]), you are likely launching it into overdrive. There is suddenly a lot to do in a very small space of time and taking the hacker to court may not be high on your list of priorities.

In this paper, we consider how securing various court orders can form an invaluable part of your co-ordinated incident response strategy, and one which has the potential to pay dividends further down the line.

Bristows

Interim injunctions in a cyber context – why bother?

An interim injunction involves an urgent application to the court seeking provisional measures before trial – normally compelling someone to either do something or stop doing something. It is only granted in the context of legal proceedings where there is a risk of harm that cannot be adequately compensated with damages later.

You might be thinking: *Why would I waste time getting a court order against an anonymous cybercriminal who's probably overseas and unlikely to care about UK law?*

Yet plenty of organisations have gone down this legal route after being hacked. Here are some examples of cyber victims who've taken their attackers to court and secured injunctions:

hcrg Care Group

A healthcare organisation
February 2025[2]

ucu University and College Union

A professional association in the education sector
August 2024[3]

ArmstrongWatson® Accountants, Business & Financial Advisers

An accountancy firm
March 2023[4]

PENDRAGON

A national automotive retailer
October 2022[5]

Ince

An international law firm
March 2022[6]

XXX

An anonymous company
March 2022[7]

4 NEW SQUARE CHAMBERS

A barristers' chambers
June 2021[8]

PML

An anonymous UK company
February 2018[9]

CLARKSONS

A global shipping provider
November 2017[10]

Bristows

Key features – what order to seek and why

Each of the above organisations experienced unauthorised access to their IT systems from an unknown perpetrator, had a significant amount of data stolen and were the victims of a ransom demand, with the threat of publication and/or selling the data to malicious third parties if they failed to make payment.

On the next few pages, we break down the main features of the court orders that were sought and explain why they may be worth pursuing:

1. Non-disclosure order/order for delivery-up of stolen data

What is it? Generally, orders sought in these cyber attack scenarios involve: (i) a prohibitory injunction prohibiting the publication of the stolen data; and (ii) a mandatory injunction requiring the hacker to deliver up and/or delete the data.

Why bother? The hacker will be in contempt of court if he publishes or fails to return the stolen data. Although this is unlikely to deter the hacker himself from carrying out his threats, the court order will also be a powerful tool in relation to third parties, including the platforms or providers hosting the stolen data. Any third party that has notice of an injunction (e.g. prohibiting publication) and knowingly aids or abets the breach of its provisions (e.g. by continuing to host the data or make it publicly available) could also be pursued for contempt of court. These parties are more likely to take proactive steps to remove the material once you have secured the order and alerted them to the violation.

Example: In *PML*, once the order was granted, PML was able to identify the websites hosting the stolen documents and serve the order on them. In response, the hosting companies blocked access to the documents or deleted them altogether. These steps had a significant impact in helping to contain the breach by minimising the time the documents were publicly available.

Bristows

Key features – what order to seek and why

Main features of the court orders that were sought and why they may be worth pursuing:

2. Without notice/ex-parte

What is it? In cyber attack scenarios, injunction applications are generally brought "without notice" and "ex-parte", meaning the hacker is not informed of the application and is not given the opportunity to attend the hearing. Because of the potential injustice caused by this, the party making the application will need to have a strong enough case and good reasons for not providing notice.

Why bother? Cyber victims will not want to alert the hacker of their intention to seek an injunction as this could trigger the immediate publication of the data or other threats being carried out.

Example: The courts agree that in hacker/blackmail scenarios a "without notice" application is justified and is therefore the standard course in these applications. For example, in *Armstrong*, the court found there was a real risk that notice would trigger the misuse or publication of the data in an attempt to deprive the application of any substantive or practical effect.

Bristows

Key features – what order to seek and why

Main features of the court orders that were sought and why they may be worth pursuing:

3. Action against "persons unknown" and service out of jurisdiction

What is it? Instead of a named defendant, the application will be brought against "persons unknown". The application is also likely to feature a request that the court allows for service out of jurisdiction, allowing the order to be served on the hacker by alternative means.

Why bother? These are necessary measures to get around the hurdles created by not knowing the identity of the hacker or his address for service.

Example: Applications against "persons unknown" are routine in cyber attack scenarios but the court will need to be satisfied that the definition of "persons unknown" is sufficiently clear to identify those who are included and those who are not. When seeking service out of jurisdiction, it is commonplace to ask to use the method that the hacker has used to communicate with you, although this may change over time. In *HCRG Care*, HCRG was granted permission to upload the order via the web portal which the hacker had provided as a means of contacting him (which included a facility for uploading documents). When the upload facility was removed by the hacker, HCRG instead sent an email to the web portal with a link to a filesharing site where the order was available. The hacker then disabled the chat function entirely, prompting HCRG to serve later court documents by email instead and seeking a retrospective amendment to the alternative service provisions in the order.

Bristows

Key features – what order to seek and why

Main features of the court orders that were sought and why they may be worth pursuing:

4. Private hearings and restrictions on court documents

What is it? The applicant will often request that the hearing to determine the application be held in private and that certain restrictions are placed on third parties being able to obtain court documents relating to the hearing. As this is an exception to the principle of open justice, private hearings will only be justified in certain circumstances.

Why bother? Private hearings will allow cyber victims greater control over what information is made public about the attack and when. This can be particularly important where the hearing is held very soon after the attack occurred and the organisation does not want sensitive details, such as how the hacker breached its systems or what steps it has taken to track down the data or the hacker, in the public domain before it has a chance to act on them.

Example: In *Ince Group*, the court agreed that a public hearing would defeat the interests which Ince Group was seeking to protect. A private hearing was necessary to ensure that efforts to trace the hacker were not hampered and third parties were not encouraged to search for the stolen data. Ince Group also requested and was granted an order that copies of the documents on the court file would only be provided to any third parties if they first made an application, which placed further protections against information getting into the wrong hands.

Bristows

Key features – what order to seek and why

Main features of the court orders that were sought and why they may be worth pursuing:

5. Anonymity

What is it? This allows the victim of the cyber attack to remain anonymous so their name will not be used in any public documents, including the judgment.

Why bother? Although many organisations will be keen to prevent potentially embarrassing details of them falling victim to a cyber attack being made public, the mere risk of an organisation suffering negative commercial or reputational consequences is not generally a sufficient reason to make an anonymity order.

Example: In *XXX*, the company was a technology provider in relation to highly classified projects of national significance. It established that much of the stolen data was security sensitive, highly classified and protected by the Official Secrets Act 1989. The court agreed that this data would be of interest to several categories of persons with potentially malicious intent, including hostile nation states, organised criminal groups and terrorist organisations. In these circumstances, it was appropriate for the company to remain anonymous.

Bristows

Key features – what order to seek and why

Main features of the court orders that were sought and why they may be worth pursuing:

6. Injunctions against third parties

What is it? As well as seeking orders from the court directed at the hacker himself, there may be circumstances where it would also be helpful to seek injunctions from third parties that may have information relevant to the cyber attack such as the identity of the hacker or the location of the stolen data. These third parties could include banks or crypto exchanges (where money has been stolen or changed hands) or the providers of websites or servers where the stolen data is being stored or hosted. Injunctions in this context may include Norwich Pharmacal Orders, freezing orders and/or mandatory injunctions requiring the deletion of relevant data.

Why bother? Ultimately, where it has been possible to trace and/or recover the stolen data, this will prove the most effective means of successfully containing the incident and neutralising the threat of the hacker. Securing the stolen data through third party injunctions or using court orders to ascertain the identity of the hacker will complement any injunctive relief sought against the hacker and further enhance the cyber victim's breach response narrative.

Example: In *PML*, the company had been able to trace the stolen data to a cached website hosted by a company in another European jurisdiction. PML therefore applied for and obtained a court order in that jurisdiction directed at the European server requiring it to block access to the cached website. This order was served on the European server at the same time as the injunction order was served on the hacker and was complied with shortly after.

Bristows

When to seek the injunction – timing is everything

Once you have decided that seeking an injunction will be part of your strategic response to the cyber attack, you will also need to carefully consider when best to bring the application and how this fits with the rest of your incident response.

In particular, you will need to weigh up the following factors:

1. **Urgency:** Applications are made on an urgent basis and you will therefore need to show that you acted quickly, without unreasonable delay. In some circumstances, this could be within a matter of days from being alerted to the attack.

2. **The hacker's timings:** You will also need to ensure you take action before publication of the stolen data takes place. These timings will often be dictated by the hacker, who will likely have provided a short a deadline to pay the ransom by. Consider trying to buy time from the hacker if needed – in *PML*, the company was able to negotiate a two week extension, during which time it was able to make significant advances in tracking the data and preparing its containment strategy.

3. **Team stood up:** Once the order is granted, the "cat will be out of the bag": the hacker will know that you have involved the courts and do not intent to meet his demands. This will almost certainly result in the immediate publication of the stolen data. You will therefore need to make sure that you have a team and process already in place for dealing with the fall-out, including identifying where the data has been published and serving the order on the companies involved to secure the swift take-down of the material.

4. **Comms strategy:** Unless you have been able to secure an anonymity order, then going to court will also trigger awareness of the cyber attack to the general public. You will want to ensure you already have your communications strategy in place which will deal with public statements, proactive communications to key clients and dealing with queries from the press and other interested groups.

5. **Regulatory update:** You will also want to ensure that any information that is made public through the hearing is consistent with the information you have provided to regulators (such as the ICO). You will want to consider providing a proactive update to the regulator if additional information has been made available during the hearing which did not form part of your initial notification.

Bristows

What next? Proceedings following an interim injunction

As interim injunctions are only intended to offer temporary relief pending trial, once you have taken the step of seeking an interim injunction you are also committed to commencing proceedings against the hacker (at the same time as or shortly after seeking the interim injunction). The following factors will be relevant in this context:

The claim: The claim will likely be framed as a breach of confidence claim as the hacker has accessed, retained and/or disclosed information which ought to have remained private and confidential.

The remedy: The remedy sought will likely be permanent injunctive relief, both to restrain use and disclosure of the information and to require deletion or delivery up of the information.

Maintaining interim injunction until proceedings determined: At the initial hearing the court will likely set a return date at which it will assess whether the interim injunction should remain in place while proceedings progress. This return hearing is often considered on the papers, meaning that neither party is required to attend court.

Closing out proceedings: The court will typically want to know how you intend to 'close out' the proceedings given that the hacker is very unlikely ever to participate. It is therefore generally necessary to apply either for default judgment or summary judgment. There are tactical differences associated with both of these options so the exact route will depend on your priorities. For example, default judgment can be cheaper and was therefore the route taken for many of the cyber victims mentioned above. Summary judgment on the other hand may be preferable if there is a chance the judgment would need to be enforced in foreign jurisdictions (and was sought by *XXX* for this reason).

Bristows

Wider impact – insurance, reputation and regulatory action

In addition to the use cases described above, taking court action sends a clear message that you are not paying up or giving in to the hacker's threats – you are fighting back. Not only is this an important factor in dissuading cybercriminals from continuing the attack or from staging future attacks, it is also likely to be relevant to how the incident is treated or perceived by your cyber insurer (if relevant), regulators and the court of public opinion.

Insurers:
Seeking legal remedies in the form of injunctions may be one of the requirements under your cyber insurance policy, although it is more likely to constitute 'advice' from your insurer rather than a requirement.

The ICO:
Although the ICO does not have a stated position on seeking injunctions following a cyber attack, it does expect you to take reasonable steps to safeguard the stolen data. The ICO is also clear that paying the hacker's ransom is not a safeguarding measure and does not protect individuals whose data has been affected.

Clients/customers/business partners/the broader public:
With cyber attacks becoming ever more prevalent, few (if any) organisations will be able to completely protect themselves against an attack occurring in the first place. Your clients, customers, commercial partners and the broader public will therefore be less concerned about the fact the breach occurred and more concerned about how quickly and effectively you acted in the aftermath to respond to the threat and protect their interests.

The proactive steps involved in seeking an injunction and enforcing it against third parties following the court order will demonstrate that you have taken the incident seriously and responded appropriately to protect the information against unauthorised publication. Supported with other measures that will undoubtably form part of your broader strategy, obtaining injunctive relief signals a robust and competent response to the incident. This can help to convince regulators not to take enforcement action and can further frame how the incident is reported in the press, ensuring that your breach-nightmare doesn't also become a PR-nightmare.

Bristows

How Bristows can help

At Bristows, our experienced data protection team works hand-in-hand with our seasoned litigators. We can help you consider your options in a data breach scenario – including guiding you through the menu of options and complexities around securing an injunction at the right time for your organisation.

If you would like any advice or further information regarding the use of injunctions in a cyber attack context, please do get in touch with us.

Key contacts

Marc Dautlich
Partner
Data protection, privacy & cyber
View profile

Freya Ollerearnshaw
Senior Associate
Commercial disputes
View profile

Quick links:

Cyber & data breaches

Meet the cyber team

Meet the litigation team

Bristows

Bristows LLP
100 Victoria Embankment
London EC4Y 0DH
T +44 20 7400 8000

Bristows LLP
Avenue des Arts 56
1000 Bruxelles
Belgium
T +32 2 801 1391

Bristows (Ireland) LLP
18 - 20 Merrion St Upper
Dublin 2 D02 XH98
Ireland
T +35312707755

Bristows.com

[1] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches survey-2024#chapter-3-approaches-to-cyber-security
[2] *HCRG Care Ltd v Persons Unknown* [2025] EWHC 794 (KB)
[3] *University and College Union v Person(s) Unknown* [2024] EWHC 2998 (KB)
[4] *Armstrong Watson LLP v Persons Unknown* [2023] EWHC 762 (KB)
[5] *Pendragon v Persons Unknown* [2022] EWHC 2985 (QB)
[6] *Ince Group Plc v Person(s) Unknown* [2022] EWHC 808 (QB)
[7] *XXX v Persons Unknown Queen's Bench Division* [2022] EWHC 1578 (QB) 12 Apr 2022
[8] *New Square Limited v Person or Persons Unknown (unreported)*
[9] *PML v Persons Unknown* [2018] EWHC 838 (QB)
[10] *Clarkson Plc v Persons Unknown* [2018] EWHC 417 (QB)