Law in cyberspace

With the significant rise in data breaches and cyber incidents in the past few years, organisations are becoming increasingly aware of the risks that cyber attacks pose to their business. Cybersecurity threats are now a board-level issue. David Varney and Isaac Bedi examine the legal obligations that organisations should be considering when a cyber attack occurs

When sophisticated cyber-attacks do occur, organisations often focus their attention on instructing third party IT providers to remedy and rectify the breach. They neglect to approach their lawyers to assist them with ensuring that they comply with their legal obligations in respect of any data breach.

As well as the importance of obtaining legal advice at the earliest stages of an attack, it is also important to have in place a well-planned and rehearsed cybersecurity readiness programme.

Key considerations

Clearly, the key concern for organisations which suffer a cyber attack is the restoration of their systems and the recovery of any data lost. To that extent, unless organisations have internal teams who can deal with an attack it is critical for them to have an arrangement in place with a third-party IT provider and to instruct them as soon as possible upon discovery of an attack.

However, organisations should also ensure that in conjunction with their immediate IT response, they contact their lawyers to assist with ensuring compliance with their legal obligations, such as:

- The compliance obligations associated with paying any ransom to the attackers
- The obligation to notify regulators, such as notifying the ICO within 72 hours where any personal data is involved in the attack
- Any contractual obligations to notify their insurers of the attack
- The obligation to notify data subjects of the attack where there is a high likelihood of a risk to their rights and freedoms
- Any contractual obligation to notify third party suppliers or customers of the attack

It is important to remember that failure to notify any insurer within the required timeframe will often result in any coverage for cyber insurance being invalidated. Similarly, any failure to notify third party suppliers or customers may result in a breach of contract, entitling those third parties to terminate any agreement and potentially claim damages as a result.

The advantage of instructing lawyers as part of the immediate response in the aftermath of a data breach is that they can consider all the above issues from the outset and scan the horizon for any issues in the breach response strategy that may create problems or complications for the organisation in the future and once the immediate impact of the breach has been resolved. These issues might include any claims brought by individuals or customers as a result of the cyberattack or any claims the organisations may wish to bring against third parties who may have some responsibility for the breach, such as a third-party IT provider who has failed to protect against a cyber attack.

David Varney

Most importantly, instructing lawyers at the outset of an attack means that the organisation can benefit from the legal privilege that communication between clients and their lawyers is afforded. In particular, where a third-party IT provider is being instructed to investigate the root cause of an attack, having lawyers instruct the provider on the organisation's behalf will mean that any report produced may be subject to legal privilege, allowing the organisation to retain control over this information and who this is disclosed to, which will be of significant benefit to the organisation should any claims be brought against it as a result of the attack, or indeed should they wish to bring any claim themselves against any third party who may be responsible for it.

Key takeaways and implications

Ultimately, an organisation's response to any cyber attack should ensure that it prioritises its legal obligations in respect of a breach alongside its cyber response. Ensuring that lawyers are on hand at the earliest stages of the breach will allow organisations to ensure they remain compliant with their legal, contractual and regulatory obligations throughout. ❐

by David Varney is a partner, and Isaac Bedi is a solicitor, in the technology team at independent UK law firm Burges Salmon. Burges Salmon has worked with partners from across the cybersecurity industry to assemble a team of experts who can address issues arising from a data breach or cybersecurity attack, including digital forensics support.
www.burges-salmon.com