The top 5 legal considerations for a cyber incident

The way in which you manage the fallout from a cyber incident can be critical to your business.

At DUAL, we encourage organisations to be proactive with their incident response plan, which lays out the guidelines for responding to a cyber incident. One key workstream is the legal and regulatory implications.

One of our breach response panel law firms, Clyde & Co LLP, has set out the top five legal considerations following a cyber incident:

1 Legal privilege

- **What is privilege?** The concept of legal privilege applies to legal advice prepared by a lawyer for his/her client, and any communications prepared for the dominant purpose of bringing or defending legal proceedings.
- **Why is it important?** It preserves the confidentiality of communications and documents that are obtained or created in the course of an investigation into a cyber incident. This means that such communications or documents are not disclosable in investigations and proceedings arising from the incident.
- **How can you protect legal privilege?** Legal counsel must be instructed at the outset of an incident and other third-party vendors should be instructed through legal counsel.

2 Legal and regulatory obligations

- **What types of legislation might be triggered?** Civil laws, predominantly data protection and privacy legislation, and sector specific legislation. Criminal laws, some of which require the management of an organisation to report a crime it has knowledge of.
- **What are the obligations to notify?** Organisations may need to notify law enforcement, regulators and/or data subjects in multiple jurisdictions within strict time frames, failing which they may be subject to large monetary fines and/or third-party claims.
- **Have thresholds for notification been reached?** Many laws have a threshold for notification only where the compromise of the data is likely to cause harm or serious harm to the data subjects (or similar wording). Organisations will have to assess the extent to which any thresholds may have been reached in the impacted jurisdictions.

3 Contractual obligations

- **What are your contractual obligations?** An organisation will need to check what its contractual obligations are to customers and suppliers to see whether any contracts contain requirements to notify the other party of a cyber incident; or, if its systems are down and business operations are impacted, it might breach service level requirements to its customers and may need to notify them accordingly.
- **Has a third party breached its contractual obligations to you?** It is also worth considering whether any third party may have been involved in the incident and/or been responsible. If so, you may need to put those third parties on notice of a potential claim against them.

4 Ransom negotiations and payments

- **Are they legal?** There is no general legal prohibition in most Middle East jurisdictions on negotiation with cyber criminals or the payment of ransoms. However, organisations must carry out appropriate due diligence to ensure that they would not be in breach of any anti-money laundering, terrorist financing or sanctions laws in making a ransom payment.
- **What else should be considered before paying a ransom?** Although it may not be illegal to pay a ransom, there are other risks involved. For example, the risk of double extortion if the threat actor remains in the organisation's systems; the risk that, even if the ransom is paid, the threat actor may not erase the data and may proceed with publishing it or selling it to a third party; and the risk that the organisation may be perceived as an easy target for other cybercriminals.

5 Communications

- **What do you need to consider from a legal perspective?** Communications in public domain must be worded carefully and with the potential for future regulatory investigations and third-party litigation in mind. It is best to stick to the bare facts and do not elaborate unnecessarily or try to put a positive spin on communications. It is also important to bear in mind that any communications with the threat actor could end up in the public domain and could be used by third parties to mount a claim against the organisation.

DUAL | CLYDE&CO

Helping you do more

One Creechurch Place, London EC3A 5AF

dualinsurance.com