Cyber-security: effective incident response – key takeaways

Osborne Clarke's cyber team hosted a cyber security session on effective incident response as part of our 2024 Disputes Week. Osborne Clarke's Nina Lazic, Charlie Wedin and Phil Tansley were joined by Dan Caplin, who leads S-RM's UK incident response team, to discuss key decisions and actions which need to be taken in the immediate aftermath of a cyber-attack to minimise the risk to the business. Below are 5 key takeaways from the session.

1. **Take swift and appropriate action:** The first 48 hours are critical. Your priorities are to **stop the bleed** and to put in place the **right team** to structure the investigation and incident response. The success of your response and recovery will often turn on decisions taken in the immediate hours and days following an attack.
2. **Ransom demands**: Law enforcement discourages payment for policy reasons and the ICO will not take payment to be a mitigating factor when considering enforcement action. However, it is important to consider properly the implications for your business and where the **balance of risks vs benefits** lies. Relevant factors might include your organisation's moral standpoint, insurance cover, reputational impact, the potential harm if data is not decrypted or is published, and whether your organisation is publicly funded. It is also essential to conduct due diligence to ensure that payment does not put you at risk of breaching money laundering, sanctions or funding of terrorism laws.
3. **Notifications to affected data subjects**: Under UK GDPR, data controllers must notify data subjects without undue delay if there is a **high risk** to their rights and freedoms. Ascertaining who the affected individuals are and the extent of data impact can be expensive and time consuming. Consider what information you require in order to carry out an appropriate risk assessment to determine whether a notification obligation exists and establish who should be notified.
4. **PR and communications:** Ensure that your communications are accurate. Reassure stakeholders but avoid making definitive statements until you are certain that the position will not change**. Inconsistent messaging engenders mistrust** and may present challenges in any subsequent regulatory investigations or litigation.
5. **Insurance**: If you have a policy which may cover cyber-attacks, **early notification** to your insurer is key. By starting a prompt and constructive dialogue with your insurer, you can benefit from their expertise, get their buy-in to your strategy and reduce the prospect of disputes over cover down the line.

Preparation is key. Osborne Clarke offers a cyber crisis simulation product tailored to your business so you can ensure that your team is fully prepared to handle an attack. Please contact us for more information.

For urgent advice, please contact us via cyberir@osborneclarke.com.

Key Contacts

Nina Lazic
Partner
T+44 207 105 7400
Nina.lazic@osborneclarke.com

Charlie Wedin
Partner
T +44 117 917 4290
Charlie.wedin@osborneclarke.com

Philip Tansley
Partner
+44 207 105 7041
Philip.tansley@osborneclarke.com