Victim of a cyber-attack? Key Considerations from DACB's Cyber Team

Published 27 May 2021

Cyber-attacks are becoming increasingly prevalent within our digital society. Here is a quick guide to the key considerations your organisation should think about should you fall victim to a data breach.

1. Pre attack: Have a breach management plan

A breach management plan will set out key information and actions to help your organisation detect and respond to a cyber-attack in a fast and yet carefully coordinated manner. A good plan should set out details such as the technical measures, policies and processes for employees to follow. Your plan should also include details of the individual nominated to deal with the organisation's data breaches (your data protection officer). This is crucial as valuable time can be wasted following an attack if employees struggle to identify the correct person and strategy to deal with the breach.

A clear breach management plan will allow you to easily move on to the next stage of dealing with a cyber-attack.

2. During the attack: Notification requirements

The notification requirements following a cyber-attack are set out in the GDPR. In the UK, the key body to notify is the ICO and any data subjects impacted by a loss of personal data.

Notifying the ICO

The ICO should be notified of a personal data breach no later than 72 hours of an organisation becoming aware of it. The threshold is that there should be a "reasonable degree of certainty that a breach occurred." If you are not sure, then you can take time to follow up with further investigations. However, the preference is to generally give information that is available within the 72 hour window and then to update the ICO as more information is discovered.

The ICO encourages data controllers to provide as much detail as possible when reporting a data breach to avoid extra information being requested. Where a notification to the ICO is not made within 72 hours, it should be accompanied by reasons for the delay.

Notifying individuals

It is important to consider whether any data subjects need to be notified about the data breach. The threshold is higher for notifying individuals than for the notification to the ICO. An organisation is under an obligation to notify individuals where there is likely to be a high risk to the rights and freedoms of individuals. For instance if you know that personal data such as individual's banking information and identity documents were impacted by the data breach, you may decide to notify those individuals in order for them to take the necessary steps to protect themselves from identify / financial fraud. This notification is to be made without undue delay.

Breach logs

In addition to the notification requirements, you should keep a log of any breach suffered by your organisation. A breach log should be kept regardless of whether you notify the ICO or not. It should include the following information:

1. What happened;
2. How and why it happened;
3. What steps you took to mitigate the risk; and
4. Whether you need to notify the ICO. If you are not notifying the ICO then also state the reasoning behind this.

3. Post attack: Learning from mistakes

Every organisation should learn from mistakes and 'near misses'. You should consider what went wrong and any measures that could be taken to prevent a similar event occurring in the future. Identify trends, staff training needs and / or gaps in processes. Overall, prevention is key!

Data protection should be included in your organisations' audits. A good report will show action taken promptly, what actions

were taken to protect individuals, the cause of the breach, steps taken to prevent it occurring again and the general measures and compliance.

A key way to guard against future cyber-attacks is to invest in staff training. 25% of all breaches received by the ICO during Q4 2020-21 were through inadvertent disclosure – data emailed or posted to the incorrect recipient. The remainder were phishing incidents and ransomware.

DAC Beachcroft's Data Risk Specialists Response provide clients with a comprehensive breach management service, with the flexibility to respond to any type of breach, from the loss of a single paper file to the targeted theft of thousands of electronic personal data records by hackers. If you are current suffering from a cyber-attack and require some assistance, contact us at datarisk@dacbeachcroft.com or call **+44 (0)800 302 9215** to find out more about how we could help your business.

Authors

DAC BEACHCROFT