CASE STUDY

Pritchetts

ASSESSING THE NATURE OF A DATA BREACH AND NAVIGATING BREACH-REPORTING REGULATIONS

Challenge

Our client identified a possible phishing incident (where a nefarious organisation seeks to gain access to your system by seemingly innocent requests for usernames and passwords). One of the client's employees had clicked a link in an innocuous-looking email and then entered their username and password, allowing access to sensitive staff information. Our client asked us to walk them through the process of managing their data breach response, and help them to decide whether to notify the Information Commissioner's Office ("**ICO**") of the breach.

The big problem in terms of whether to notify the ICO was that the client **could not prove that no personal data had been accessed**, so they **could not prove that there was no risk to individuals from the data breach**. However, perhaps a bigger problem facing them was time. As with all personal data breaches under the GDPR's regime, the clock had started ticking from the moment that the company became aware of the possible breach. In this case, the time limit of 72 hours would have been reached less than 24 hours from when we were called.

Solution

We had previously drafted a data breach policy for our client following a wide-scale data protection audit across their group of companies. We therefore supported our client to perform an initial data breach investigation by using this policy and to document their findings.

Part of our support involved helping our client to analyse the requirements for reporting a data breach to the ICO and to individuals, and to decide whether this was required in this situation. It was decided that an initial report should be made to the ICO while the client carried out more detailed investigations into the incident. As part of our response, we helped our client to identify that they needed improved IT systems and audit trails, which would enable the client to interrogate their systems themselves. This would, in turn, enable them to prove or disprove in a shorter timeframe whether access had been allowed to sensitive data, and whether that data had been used, removed, etc.

(continued…)

Legal directory extract

"Stephanie's legal knowledge regarding data protection is as good as it comes among solicitors. She is excellent at quickly identifying the commercial issues for the client, focusing her legal skills on achieving the best outcome and avoiding distractions."

Quoted in **The Legal 500 UK 2021**

Solution (continued)

We introduced our client to forensic IT experts to help them to identify at a technical level what the breach had been and what technical steps they needed to take to avoid future incidents. In addition, our client engaged us on a separate matter to carry out specific data protection training sessions for staff across the business who used data intensively in their roles. This training included a short section on data security, reminding staff of the dangers of social engineering and phishing, among other issues. This data protection training completed the organisation's wider technical data security training programme.

Impact

Appropriate handling of data breach situations is critical for data protection compliance. Not only can the ICO impose large fines for non-compliance, but there is also the potentially catastrophic risk to reputation and customer confidence, which can severely damage a business's bottom line. Careful handling of data breach situations is also important to help prevent claims against the organisation from affected individuals, which can irreparably damage an organisation's brand and reputation.

We helped our client to realise that they needed to update their systems so that they could avoid any similar scenarios in future where they found themselves unable to demonstrate that there had, in fact, been no risk from a data breach. Among other benefits, this would circumvent the need to send a preliminary report to the ICO, with all the potential risk of a follow-up investigation!