BCLP. Client Intelligent

Insights

CYBER SECURITY TRENDS : TIPS FROM RECENT UK ENFORCEMENT ACTIVITY – PART 2

Mar 20, 2020

In this part of our briefing series, we cover how prior regulatory enforcement action affects the assessment of sanctions and some pitfalls associated with undertaking internal security audits.

Who is this relevant for?

For our Cyber Security Trends we reviewed recent findings to provide easy to use tips. Cyber incidents are sector and geography agnostic. These briefings draw on UK adjudications but are relevant for a GDPR-focus outside the UK and highlight cyber security trends more generally.

TIP: Prior enforcement and unaddressed problems can increase the sanction risk from a later breach

Any prior enforcement action or past shortcomings identified by the regulator and not addressed ahead of a cyber incident will be aggravating factors when it comes to the chance and size of a fine. This is not surprising and is specified in the GDPR. Organisations should prioritise known issues, focussing on those likely to pose the greatest potential security risk.

TIP: Your own security audits may work against you

We are seeing the ICO scrutinising then relying on adverse findings from a company's own security assessments. This can also extend to third party, e.g. customer audits conducted and any connected to third party standards, such as PCI-DSS (where the organisation has little choice or control over the process).

With this in mind, organisations may wish to consider how they engage in future information security and cyber audits and, in particular, whether they can take place under the protection of legal privilege (confidentiality alone is unlikely to be a sufficient bar from producing a report to the ICO, if requested).

What sanctions apply?

In the UK the ICO can fine up to 4% of annual global turnover or £17,500,000 whichever is higher. There are related powers to compel actions to be taken, information to be provided and to conduct on site assessments and interviews.

Brexit Postscript

Once the UK has finally left the EU at the end of 2020, organisations impacted by cyber security breaches face an increased risk of multiple fines and enforcement actions for the same incident. This is because the UK ICO will no longer participate in the GDPR cooperative "one stop shop" mechanism alongside its European counterparts.

As the UK's ICO is the one of the largest and best-resourced data protection authorities in Europe, with a proven track record of enforcement, companies with pan-European operations cannot afford to take their eye off the UK.

The author leads the UK Data Privacy and Cyber Security practice at BCLP. She can be contacted on kate.brimsted@bclplaw.com. *Earlier parts in the series can be accessed here.*

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Kate Brimsted

London

kate.brimsted@bclplaw.com
+44 (0) 20 3400 3207

should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.