BCLP. Client Intelligent

Insights

CYBER SECURITY TRENDS: TIPS FROM RECENT UK ENFORCEMENT ACTIVITY – PART 4

Jun 01, 2020

When the regulator has decided to investigate your organisation following a data breach, the remit for the investigation will be wide-ranging and go beyond the narrow circumstances of the breach. Recent decisions shed useful light on the types of internal practices the ICO will look at and take into account when issuing sanctions.

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 FOUR: It matters how and by whom the breach is discovered – control over the messaging will become increasingly challenging and critical

The ICO would usually expect an organisation itself to be the first to know, not least because if it occurs on your own systems and network, early detection is part of good cyber practices. Similarly the GDPR lists as a factor explicitly linked to the risk and size of fine "the manner in which the infringement became known to the regulator". There have been cases where the regulator has been informed by other regulators conducting their own investigation of a company, members of the public, the press and security researchers. These have not been positive for the organisation when the ICO came to determining the appropriate sanction.

Organisations would do well to consider how they can best place themselves in the position where they know early about a cyber incident (or potential incident) and have appropriate control over the notification of the data protection regulator, other regulators, law enforcement, insurers, third parties, individuals, etc. Typically this will form part of the Incident Management Response Policy. This area will become more complex over time with rising numbers of cyber incidents, the development of representative or "class" data breach actions in the UK and the greater interconnectedness of the ecosystem, not least resulting from 5G adoption.

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.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Geraldine Scali

London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483