BCLP. Client Intelligent

Insights

CYBER SECURITY TRENDS: TIPS FROM RECENT UK ENFORCEMENT - PART 1

Mar 10, 2020

What insights into cyber security norms can organisations glean from the UK ICO's recent enforcement decisions, most of which have been released since the GDPR came into force?

Final fines are still awaited on the UK's largest cyber security incidents since the GDPR, with the initial proposed fines totalling over £280 million. In the meantime, we can distil some of the regulator's expectations from recent decisions – even those under pre-GDPR law show an unmistakable direction of travel.

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: Cover off the cyber basics – they matter even if they didn't cause this incident

Whatever the nature of the cyber incident experienced by an organisation, if the ICO's investigation picks up systemic and wide-ranging failings of security – even if they were not the cause – this is likely to significantly increase the risk and size of a fine.

Typically the basic failings included: missing firewalls, IT systems without proper segregation, failures in patching (e.g. 4 years behind in one case), continued use of unsupported software (e.g. 8 years), inadequate vulnerability scanning, lack of penetration testing and monitoring, improper FTP implementation and failures to log and monitor security incidents. Most recently, the National Cyber Security Centre's Cyber Essentials were referenced in an enforcement decision (4 out of 5 had been missed). These are:

- Secure your Internet connection
- Secure your devices and software
- Control access to your data and services

- Protect from viruses and other malware
- Keep your devices and software up to date

The approach emerging from the regulator seems to be that, since the law requires minimum security standards, poor security can be a contravention of the GDPR and UK legislation even if it has not (yet) caused an actual security breach. This is consistent with the GDPR's accountability principle.

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.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Kate Brimsted

London

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