BCLP. Client Intelligent

**Insights**

# CYBER SECURITY TRENDS: TIPS FROM RECENT UK ENFORCEMENT ACTIVITY – PART 6

Jul 20, 2020

From the ICO's standpoint, the steps you elect to take post-breach and the speed with which you implement them are key. Demonstrating readiness to learn lessons from a breach incident by making investments in post-breach security measures is an important factor in the assessment of sanctions (both pre and post GDPR). Whilst final fines are still pending for the most significant cyber security incidents to have occurred since the GDPR, recent ICO enforcement decisions provide useful illustrations of the expectations the ICO has from a cyber security standpoint.

## 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: Attend to post-breach mitigation quickly

Significant post-incident investment in cyber security tends to be judged positively when the regulator is determining the size of any fine. There are no signs from the ICO's decisions so far that this could be seen negatively, e.g. as an indication that the organisation admits past inadequacies (though this could be fact specific). In future, the positive activity (and obligation) of mitigating potential harm from a cyber incident might need to be judged against the statutory aggravating behaviour of gaining financial benefit from an infringing activity (e.g. through under investment in cyber security). This is not currently the case.

## TIP: Non-statutory security standards may be applied: third party, the regulator's guidance, your own policies

Cyber security incidents which are "personal data breaches" under the GDPR do not inevitably result from failures to meet the statutory "appropriate" security measures. But this will usually be the case in practice.

Looking at fines for pre-GDPR security failures, and whether the organisation had put in place the required appropriate technical and organisational security measures, the ICO has taken into account

- ignoring the ICO's own security guidance for organisations (e.g. in relation to the mis-configuration of an FTP sharing arrangement);
- whether PCI-DSS standards had been met (the incident involved a large number of payment cards);
- the UK National Cyber Security Centre's basic 5 Cyber Essentials;
- the organisation's own security policies (e.g. in relation to management of domain administered accounts and user access rights, not documenting exceptions to encrypting back-ups, failure to conduct risk assessment of third party access);
- failing to patch a CVE (common vulnerability exploit) for a prolonged period (10 years).

We are still at an early stage in the maturity of the GDPR and the related UK legislation; as the codes of conduct and certification schemes anticipated in the legislation mature, we can expect a proliferation of even more standards for security requirements and therefore a complexity in the frameworks against which organisations may be judged.

### 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


---