07 July 2022

RE: The legal profession and its role in supporting a safer UK online.

We are writing to ask for your assistance in sharing some key messages with the legal profession in England and Wales to assist them in better advising their clients who may have suffered a cybersecurity incident.

In recent months, we have seen an increase in the number of ransomware attacks and ransom amounts being paid and we are aware that legal advisers are often retained to advise clients who have fallen victim to ransomware on how to respond and whether to pay. It has been suggested to us that a belief persists that payment of a ransom may protect the stolen data and/or result in a lower penalty by the ICO should it undertake an investigation. We would like to be clear that this is not the case.

Law Enforcement does not encourage, endorse nor condone the payment of ransoms. While payments are not usually unlawful, payers should be mindful of how relevant sanctions regimes (particularly those related to Russia) – and their associated public guidance - may change that position. More importantly, payment incentivises further harmful behaviour by malicious actors and does not guarantee decryption of networks or return of stolen data. UK data protection law requires organisations to take appropriate technical and organisational measures to keep personal information secure and to restore information in the event of an information security incident. As regulator, the ICO recognises in setting its response and any penalty level the actions taken to mitigate the risk of harm to individuals involved in a data breach. For the avoidance of doubt the ICO does not consider the payment of monies to criminals who have attacked a system as mitigating the risk to individuals and this will not reduce any penalties incurred through ICO enforcement action.

Where the ICO will recognise mitigation of risk is where organisations have taken steps to fully understand what has happened and learn from it, and, where appropriate, they have raised their incident with the NCSC, reported to Law Enforcement via Action Fraud, and can evidence that they have taken advice from or can demonstrate compliance with appropriate NCSC guidance and support.

The cost of cyber crime is estimated to be in the billions. The Economic and Social Costs of Crime report estimated an overall cost of £1.1bn from computer misuse incidents against individuals in England and Wales in the 2015/16 financial year. However, this is a partial estimate only. Crucially, this does not include the cost to businesses which are thought to bear the majority of the cyber crime costs, meaning the true cost from cyber crime will be much higher.

As the regulator of the security principle the ICO has recently published its updated ransomware guidance[1]. This sets out an up-to-date view of the common ransomware compliance issues including what you should do if you receive an offer to make a payment. The NCSC website has a ransomware hub[2] which sets out all its guidance in one place.

In the event of a ransomware attack, there may be a regulatory requirement to report to the ICO as the data regulator whereas NCSC – as the technical authority on cyber security – provides support and incident response to mitigate harm and learn broader cyber security lessons. The NCSC works with organisations to ensure they have understood how they came to be a victim of ransomware, have understood the cyber security implications and taken steps to

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ransomware-and-data-protection-compliance/#scenario-7
[2] https://www.ncsc.gov.uk/ransomware/home

protect themselves from similar incidents. Neither the NCSC nor Law Enforcement share information on incidents with any regulators without permission from the affected organisation. However, the ICO, the NCSC and Law Enforcement continue to work together – sharing information on strategic trends – to ensure we are making the UK a safer place to be online.

The National Crime Agency (NCA) lead the Law Enforcement response to ransomware and work closely with the National Police Chiefs Council (NPCC), Regional Organised Crime Units and Local Police forces to investigate offenders and deliver services to support victims of ransomware. These include Cyber Resilience Centres across the country which provide support to the smallest businesses to help them understand their cyber security requirements and the necessary steps they need to take to fulfil obligations under UKGDPR and DPA 18.

We are keen to engage and work with you, and, through you the profession, to ensure there is understanding and clarity about the cyber security standards we expect organisations to follow when they have been a victim of a cyber attack. This engagement is already well supported by the Insurance Trust Group and we welcome the collaboration between the NCSC, Law Society and Bar Council on the recent Cybersecurity questionnaire for the sector.

If it would be helpful to meet to discuss how we might collaborate further on this we would be pleased to do so. Please contact Scott C at NCSC and he can work with your teams to make the necessary arrangements.

Yours sincerely

John Edwards

UK Information Commissioner
Information Commissioner's Office

Lindy Cameron

Chief Executive Officer
National Cyber Security Centre