BCLP. Client Intelligent

Insights

RANSOMWARE – WHY PAYING UP EARNS NO CREDIT WITH THE UK'S DATA PROTECTION AUTHORITY AND OTHERS

Aug 22, 2022

In a joint letter this summer, the UK's data protection regulator (the ICO) and the UK's National Cyber Security Centre (the NCSC) sought to convey some key messages to the legal profession relevant to advising clients experiencing a ransomware incident. The NCSC's view is that ransomware is currently the biggest cyber threat facing the United Kingdom and there has been an increase in ransomware attacks and sums paid out to criminals in recent months.

The letter is insightful because it addresses a number of common misconceptions about responding to ransomware attacks. The ICO also took the opportunity to clarify its expectations for organisations faced with responding to a cyber-attack of this kind. This is significant because the ICO is empowered under data protection legislation to impose fines of up to GBP 17,500,000 or 4% of annual global turnover and historically the highest fines have been issued for security fallings impacting personal data.

The ICO and NCSC reinforce the message that paying a ransom should **not** be viewed by an organisation as a reasonable step to take in order to protect data. The UK GDPR's requirement to take appropriate technical and organisational measures to keep personal information secure (and to restore information in the event of an information security incident) does not mandate payment of a ransom according to the ICO.

In fact, the ICO has gone further and confirmed that payment of a ransom:

- will **not** be seen by the ICO as an appropriate means to protect or restore the stolen data
- will **not** be viewed as "mitigation" and therefore
- will **not** result in a lower penalty by the ICO should it undertake an investigation - "*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*".

Instead, where an organisation has fallen victim to a ransomware attack, the ICO will recognise mitigation of risk if the organisation has taken steps to understand fully what has happened and learned from it and, where appropriate, has reported the incident to the ICO, the NCSC, law enforcement (via Action Fraud), and can evidence that it has taken advice from, or can demonstrate compliance with, appropriate NCSC guidance and support.

Triage steps when facing a ransomware attack

- Refer to the ICO's updated ransomware guidance (one case study specifically discusses ransom payments)
- Consider the need to report the incident to the ICO as a "personal data breach"
- Consider engaging experienced cybersecurity professionals to assess the likelihood / extent of data exfiltration
- Consider reporting the incident to the NCSC – this operates a ransomware hub where it gathers all its relevant resources together on the topic – and to Action Fraud
- Check the status of your most recent offline backup of your most important files and data
- Check your insurance cover – some policies will cover expenses related to a ransomware attack, such as employment of a security specialist or storage of data at a third party location (or even payment of the ransom itself).

The ransomware threat landscape beyond the UK

In the EU, the European Union Agency for Cyber Security (ENISA) assessed ransomware as the prime threat in its most recent threat landscape report and published further information about the scale of the ransomware issue and an indication of the level of payment of ransoms: "*Between May 2021 and June 2022 about 10 terabytes of data were stolen each month by ransomware threat actors. 58.2% of the data stolen included employees' personal data. ...For 94.2% of incidents, [it is unknown] whether the company paid the ransom or not. However, when the negotiation fails, the attackers usually expose and make the data available on their webpages. This is what happens in general and is a reality for 37.88% of incidents.*" This led ENISA to conclude that over that period ***"the remaining 62.12% of companies either came to an agreement with the attackers or found another solution."***

In February 2022 a Joint Cybersecurity Advisory was issued by cyber security agencies in the U.S. (the FBI and CISA), the UK (the NCSC) and Australia (the ACSC), stating "***cybersecurity authorities in the United States, Australia, and the United Kingdom strongly discourage paying a ransom to criminal actors.*** *Criminal activity is motivated by financial gain, so paying a ransom may embolden adversaries to target additional organizations (or re-target the same organization) or encourage*

*cyber criminals to engage in the distribution of ransomware. Paying the ransom also does not guarantee that a victim's files will be recovered. Additionally, reducing the financial gain of ransomware threat actors will help disrupt the ransomware criminal business model***".**

Where a ransom is paid, there may be additional obligations to report the fact to a responsible regulator, such as the requirement for critical infrastructure entities to report certain cybersecurity incidents and ransom payments to the Cybersecurity and Infrastructure Security Agency (CISA) within a matter of hours. Our briefing on the U.S federal Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) is here.

The clear message is that paying ransoms is strongly discouraged. The issues are well known - there is no guarantee the victim will get the decryption key and it likely incentivises further criminal behaviour. Indeed, there has been "ransomware-as-a service" for around 10 years. The ICO also notes in its recently-updated ransomware guidance that, even if a ransom was to be paid, an organisation must still treat the data as compromised (data could have been exfiltrated during the attack) and take the appropriate actions. An organisation would still need to consider how to mitigate risks to individuals even in cases where the fee had been paid and the data has been "unlocked". Aside from this, in certain circumstances, a payment to cyber criminals could have sanctions implications, or require consideration of anti-terrorism legislation. All of these factors combine to render the paying of cyber ransoms an even more unattractive proposition.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Kate Brimsted

London

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

Geraldine Scali

London

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

Anna Blest

London

anna.blest@bclplaw.com
+44 (0) 20 3400 4475