Client Alert: Ransomware – COVID-19 & Upgrading Your Defences

Date : March 27, 2020

It's pretty shameful that in the current crisis we're seeing ransomware on the rise. It's even more shameful that organisations involved in fighting the virus seem to be especially at risk. Last year ransomware targeted healthcare more than any other industry, accounting for 29% of total ransomware attacks, according to Beazley's 2020 Breach Briefing report. Recent events suggest that attacks are up as the COVID-19 virus spreads, with criminals working on the theory that an organisation desperate to unlock its data is now more likely to pay.

What techniques are hackers using?

A ransomware attack uses malware that encrypts or otherwise restricts access to computers, system or data by exploiting system vulnerabilities. The attackers demand that the victim pays money (usually in cybercurrency such as Bitcoin) to receive the decryption key or recover access.

The main ways that a ransomware 'payload' can enter an organisation's network are via:

- an attachment to an email (usually framed as something important or "urgent");
- web-browsing;
- remote access and remote control applications; or
- removable media and personally owned devices.

The criminals usually exploit a vulnerability in the operating system or other installed software, which then starts the encryption process.

What's the worst that can happen?

The impact of a ransomware attack can be severe and far-reaching. For the corporate victim, it can mean business disruption, financial loss and reputational damage.

For those whose data has been compromised, this could mean that critical data is rendered inaccessible or disclosed to unauthorised people – in some cases this could include sensitive data.

In terms of data protection law impact, GDPR imposes key requirements relating to security. Controllers must take appropriate technical and organisational measures (TOMs) to keep personal data secure against loss or destruction.

Where a ransomware attack means that an organisation is unable to restore compromised data, this could constitute a breach of GDPR on the basis that appropriate measures have not been taken to keep the data secure.

If a personal data breach has occurred, this will need to be reported by the controller organisation to the relevant data protection regulator(s) (in the U.K. the Information Commissioner's Office (ICO)) within 72 hours, unless the personal data breach is unlikely to result in a risk to individuals. If the personal data breach is likely to result in a *high* risk to individuals, the controller needs to also communicate the breach to individuals whose data has been compromised without undue delay.

It is possible that the incident *may* not amount to a reportable personal data breach *if*:

- a working copy of the data can be restored from back-ups, then the loss of data may not be permanent; and / or
- it can be established that the data being held ransom has not been accessed or misused.

We know that a number of organisations who have suffered a ransomware attack have argued that because the data has not left their systems no data breach has occurred. That's unlikely to be correct. There's detailed

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2016 Cordery. All rights reserved.

guidance on this at an EU level. Individual data protection authorities have issued guidance too for example the ICO's guidance says that even if it can restore data from back-up an organisation "*would still need to look at the circumstances of the case to determine whether or not there were appropriate measures in place which could have prevented the attack from succeeding*".

Organisations that fail to meet their security obligations under the GDPR face high fines as follows:

GDPR Provision	**Requirement**	**Maximum Fines**
Article 5(1)(f) Article 32	For not ensuring that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').	The higher of €20,000,000 and up to 4% of the total worldwide annual turnover of the preceding financial year

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2016 Cordery. All rights reserved.