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

Date : August 18, 2021

We first published this alert in March 2020 and we have updated it to reflect more recent developments

Introduction

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 COVID-19 pandemic seem to be especially at risk. In 2019 ransomware targeted healthcare more than any other industry, accounting for 29% of total ransomware attacks, according to Beazley's 2020 Breach Briefing report. Our experience in handling these attacks suggests that the number of attacks is still rising, with criminals working on the theory that an organisation desperate to unlock its data is now more likely to pay. The recent prolonged attacks on health services in Ireland and New Zealand are just one recent illustration.

But the damage is not just limited to the healthcare sector. The combined effects of COVID-19 + ransomware have already seen at least one victim as Travelex entered into administration in August 2020 after having reportedly paid a ransom to hackers. A rescue package was agreed but with the loss of 1,300 jobs. Regrettably it is likely that Travelex will be just one of many victims.

There are some GDPR-specific terms used in this note which are explained at www.bit.ly/gdprwords.

What techniques are hackers using?

A ransomware attack uses malware that encrypts or otherwise restricts access to computers, systems or data by exploiting system vulnerabilities. The attackers demand that the victim pays money (usually in cryptocurrency such as Bitcoin or Monero) 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;
- what looks to be a voicemail message perhaps via social media;
- remote access and remote control applications (either on the company's own systems or using lateral movement on shared systems); 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. There's a short film on the current state of play with ransomware so you can understand more about it and who is behind these attacks here https://www.corderycompliance.com/cordery-head-to-head-don-smith-ransomware/.

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 some it may mean that they are forced to close.

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. This is because many attacks also come with a threat to release data stolen from the network to try and increase the chances of a ransom being paid.

In terms of data protection law impact, in both the EU and the UK 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. There's an analysis of how GDPR continues to operate both in the EU and the UK here https://bit.ly/brexdpfaq.

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

Often ransomware gangs also take data – either to sell if the ransom demand is not met or to demonstrate to the organisation that they have the data and increase the value of the ransom. In our experience gangs sometimes look for the most sensitive data to sell including passports, health records and personal data relating to the organisation's leadership. Data may also be taken for cybershorting i.e. to move the share price and trade on the value of the organisation.

If a personal data breach has occurred, this will need to be reported by the controller organisation to the relevant DPA(s) (in the UK 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 usually 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
- 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 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 GDPR face high fines as follows:

GDPR Provision	**Requirement**	**Maximum Fines**
Article 5(1)(f)	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 TOMs ('integrity and confidentiality').	The higher of €20,000,000 and up to 4% of the total worldwide annual turnover of the preceding financial year
Article 32		