Ransomware - Key Takeaways - Pinsent Masons

October 2021

1. **Staff & training** - Simple human error is often a key feature in cyber attacks. Limit the potential damage through systems and controls. Think about regular training, restricted administrator accounts, minimum password limits, password rotation, multi-factor authentication, network segregation and of course, back-ups.

2. **Incident response plan** – take some of the pressure out of a cyber incident by having a plan in place setting out who your co-ordination team internally are, as well as the key stakeholders you need to contact externally – legal, forensics, PR, insurance. Make sure the plan is accessible even when your systems are encrypted. Pinsent Masons' product, Cyturion, is a cloud based response tool which can help.

3. **Legal considerations** – UK GDPR dictates when a personal data breach must be reported to the ICO. This should happen within 72 hours of becoming aware. Notification to the individuals impacted is also needed if they are at "high risk". Pinsent Masons can support you in conducting a thorough risk assessment and advise whether the relevant thresholds for reporting having been met.

4. **Engage with the threat actor?** – This is a complicated question. Your business may have a position on whether it fits with its purpose or culture to engage. Conversely, business continuity may mean you do not have the luxury of choice. In the UK, it is not presently illegal to pay a ransom, however, detailed due diligence must be conducted, to consider the risk of sanctions, proceeds of crime, money laundering and funding terrorism offences.

5. **Law enforcement –** Engaging with law enforcement can be a delicate balance. Whilst there may be circumstances in which it is necessary to report an incident to law enforcement, your business will want to focus on getting systems back up and running. Careful consideration therefore needs to be given to when and how you engage with law enforcement, and consider to what end.

Pinsent Masons has a dedicated 24/7 call centre, that allows you to connect to an expert immediately to help you through your cyber crises and determine what steps should be taken.
+44 20 7741 6127