National Cyber Security Centre

Ransomware:
What you need to know

Ransomware is the biggest cyber threat to the UK today. Since 2019, the NCSC has observed a steady growth in ransomware incidents, affecting UK organisations of all sizes. This infographic re-iterates the ongoing threat from ransomware, and reminds business leaders that **applying** NCSC guidance can drive greater cyber resilience against these types of attack.

What is the threat from ransomware?

Ransomware attacks can be massively disruptive to organisations, with victims requiring a significant amount of time (and money) to recover critical services and deliver against customer demand.

They may also generate high-profile public and media interest, especially if sensitive data stolen during the attack is published. This can expose your organisation to long-term reputational damage.

Ransomware attacks are becoming both **more frequent** and **more sophisticated**. The NCSC believes that ransomware will remain a major threat to the UK for the next one to two years.

Ransomware is a board-level responsibility. All business leaders should ensure it's on their risk agenda.

What is ransomware, and how does it work?

Ransomware is malicious software ('malware') that prevents you from accessing your computer, or the data stored on it.

During a ransomware attack, your data is normally encrypted (so that you can't use it) or it may be stolen. The attackers may even threaten to publish your sensitive data online.

Attackers usually send a ransom note demanding payment to recover encrypted data, often using an anonymous email address. They will typically request payment in the form of a cryptocurrency.

Most ransomware is 'enterprise-wide', meaning it's not just one user or one device that is affected, but the whole network.

Where to get more help

The following NCSC advice and guidance contains the most up-to-date ransomware mitigations:

- **Mitigating malware and ransomware attacks: guidance for system owners on how to defend against malware and ransomware attacks**
- **The rise of ransomware blog: a more detailed look at how ransomware threats are evolving**
- **Ransomware - what board members should know: a blog explaining the basics of ransomware for non-technical audiences (includes key ransomware questions that board members should ask their cyber security staff)**

What should business leaders be doing?

Business leaders don't need to be cyber security experts, but knowing the basics of how ransomware works will mean they can have constructive conversations with their technical experts about the threat.

Make sure ransomware is high on your board's agenda. Cyber security is a board-level responsibility, and business leaders should be asking *specifically* about ransomware.

Ensure that the NCSC's guidance on ransomware is being implemented within your organisations. The guidance (listed below left) includes practical steps that organisations of all sizes can take to increase their resilience against ransomware attacks.

Register for the NCSC's free Early Warning Service, which can warn you if vulnerable services or early signs of cyber attacks (including ransomware) have been detected on your network.