National Cyber Security Centre

Ransomware:
What you need to know

Ransomware remains a major cyber threat to the UK. This infographic, produced for senior staff in both **small** and **large organisations**, re-iterates the ongoing threat from ransomware, and reminds business leaders that applying NCSC guidance will lessen the impact of 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 data and services.

These attacks may also generate high-profile public and media interest, especially if sensitive data stolen during the attack is published online. 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 computer may become locked, or the data on it may be stolen, deleted or encrypted (so you can't use it).

Most ransomware tries to spread to other devices on your network, so your entire organisation could lose access to crucial services or data.

Criminals will usually make contact using an untraceable email address (or an anonymous web page) to demand payment promising to unlock your computer and/or access your data. Payment is invariably demanded in a cryptocurrency such as Bitcoin.

They may threaten to publish your sensitive data online if payment is not made in time.

Where to get more help?

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

- Mitigating malware and ransomware attacks: guidance for technical staff 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 understanding the threat from ransomware will mean they can have constructive meetings with their technical experts.

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

Ensure you are implementing the NCSC's guidance on mitigating ransomware. The guidance 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 if vulnerable services or early signs of cyber attacks (including ransomware) have been detected on your network.

Ensure you have an incident management plan that meets the unique challenges of ransomware attacks. You should think in terms of 'when' (rather than 'if') you experience a cyber incident.

Should you pay the ransom?

The UK government strongly advises **against** paying ransoms to criminals. If you do:

- there is no guarantee that you will get access to your computer, data or systems
- your organisation will still be infected
- you will be paying criminal groups
- you're more likely to be targeted in the future