Article

Apr 2025

To Pay or Not to Pay – Ransomware, the question too many businesses are facing

Imagine coming back to your house and finding that the locks have been changed and all of your possessions are for sale on the front lawn for all your neighbours to see, this is the awful reality that more and more businesses are facing in this digital age as ransomware continues to terrorise businesses.



Damon Brooker
Information Security Consultant
Email damon.brooker@waterstons.com

Ransomware is a form of malware that locks you out of your IT systems and demands payment, but also increasingly steals a copy of your data for blackmail purposes. It has evolved into a relentless daily threat that businesses must be prepared for in the current cyber climate. The NCSC has stated that "Ransomware attacks continue to pose the most immediate and disruptive threat to our critical national infrastructure (CNI)" [1] and home office reported that over 50% of businesses have experienced some form of cyber security breach or attack in the last 12 months [2]. These attacks have devastating consequences, as shown by the attack on Synnovis which impacted thousands of procedures and appointments across six NHS trusts [3].

In an effort to start counteracting malicious threat actors, the home office has announced a public consultation seeking views on three proposals aimed at striking a significant blow to the ransomware business model [4].

Proposals

1. **Targeted ban on ransomware payments**

This proposal aims to extend the UK government's principle that central government departs cannot make ransomware payments to additionally include all organisations within the UK public sector, CNI and potentially essential suppliers to these sectors from making a payment to cyber criminals in response to a ransomware incident.

The primary aim is to remove the financial incentive which drives criminal gangs to target essential agencies and infrastructure, as successful payments provide further resourcing for future attacks [5]. The Home Office is seeking to achieve the right balance of effective and proportionate measures to encourage compliance with the proposed ban, ranging from criminal or civil penalties for non-compliance by ransomware victims, especially where a payment is made after the victim has been told it has to be blocked.

2. **A new ransomware payment prevention regime**

The proposal aims to increase the National Crime Agency's awareness of live attacks and criminal ransom demands by requiring any victim of ransomware (including organisations and/or individuals not covered by the proposed ban set out in Proposal 1) to engage with the authorities and report their intention to make a ransomware payment before paying over any money to the threat actor responsible.

This would allow the potential victim to receive support and guidence, including discussion of non-payment resolution options and the authorities to review the proposed payment to understand if the ransom has links to criminal gangs and other criminal activity.

3. A ransomware incident reporting regime

The proposal is collecting viewpoints on if all ransomware incidents should be reported or if only organisations and individuals meeting a certain threshold should report incidents. The reporting would require potential victims to submit an initial report within 72 hours and a full report within 28 days to the relevant parts of the government.

This increased reporting would fill the current avoidable gap in government intelligence allowing the scale and source of ransomware attacks to be better understood. This information can then be used to guide and support the UK's National Crime Agency and partners to focus resources on specific groups that cause the most significant impact to the UK economy, such as Operation Cronos which targeted infamous group Lockbit [7], to infiltrate and disrupt their operations.

What Can You Do?

Paying the ransom should be avoided at all costs for a few reasons, the NCSC's current guidance is "law enforcement does not encourage, endorse nor condone the payment" [8], it encourages the cycle of crime, there are no guarantees you will get access to your data, it places a target on your back for next time and there are ethical implications of where the money goes from the payments.

Waterstons' advice is to never engage with cyber criminals and seek the support of cyber professionals or those provided by your insurer. However, where technical controls have failed and adversaries have been able to encrypt and steal critical business assets, that businesses may have to consider the possibility of paying out in an attempt to restore operations as fast as possible.

1. Cyber Controls

Prevention of ransomware by implementing appropriate cyber controls is essential to protecting your business against having to experience this distressing situation. This includes firewalls, SOC monitoring, web filtering and immutable offsite backups which provide the critical last line of defence allowing organisations to restore operations. Governance frameworks such as Cyber Essentials provide great sources for identifying gaps within your organisation and the NCSC reports that "Organisations which have Cyber Essentials are 92% less likely to put a claim on their cyber insurance than those who don't" [1].

2. Get involved in the conversation

Consultations such as these are likely to be used as the basis for drafting future legislation and requirements for both individuals and organisations to comply with when dealing with a ransomware attack. It is imperative that you get involved and make sure your voice is heard to ensure the UK takes the correct steps going forward to address this pressing issue that is facing all of us.

3. Establish key partnerships

Partnerships provide businesses with the ability to share key expertise and close known gaps in capability to ensure your organisation has taken the necessary precautions to protect itself. These partnerships can provide the essential support needed during incidents by sharing resources when needed to avoid committing to costly inhouse solutions.

To find out more about the services Waterston's offer, visit Cyber Security Services - Waterstons UK

References

[1] NCSC "NCSC Annual Review 2024" NCSC Annual Review 2024

[2] UK Government "Cyber security breach survey 2024" Cyber security breaches survey 2024 - GOV.UK

[3] BBC "NHS confirms patient data stolen in cyber attack" NHS England confirm patient data stolen in cyber attack - BBC News

[4] NCSC "Your say proposals to counter ransomware" New proposals to counter ransomware: Have your say - NCSC.GOV.UK

[5] Brammer Z. "Mapping the Ransomware Payment Ecosystem: A comprehensive visualization of the process and participants" Mapping the Ransomware Ecosystem

[6] UK Gov "Consultation Document Proposals" Consultation ransomware

[7] EUROPOL "Law enforcement disrupt world's biggest ransomware operation" Law enforcement disrupt world's biggest ransomware operation | Europol

[8] NCSC "A guide to ransomware" A guide to ransomware - NCSC.GOV.UK