National Cyber Security Centre
a part of GCHQ

Guidance for organisations considering payment in ransomware incidents

ABI

British Insurance Brokers' Association

IUA OF LONDON
INTERNATIONAL UNDERWRITING ASSOCIATION

This guidance has been jointly developed by the insurance industry bodies ABI, BIBA, IUA and the NCSC. It is for organisations experiencing a ransomware attack and the partner organisations supporting them.

It aims to minimise the overall impact of a ransomware incident on an organisation and help reduce:

- disruption and cost to businesses
- the number of ransoms paid by UK ransomware victims
- the size of ransoms where victims choose to pay

The NCSC and the insurance industry bodies recommend victim organisations review the following guidance before paying a ransom to a criminal group.

This guidance is general in nature and does not override specific laws and regulations that may apply. The ultimate decision whether to pay the ransom is with the victim.

Being prepared for any incident is key and will help lessen the impact if one happens. The NCSC offers comprehensive guidance, including how to develop an incident management capability and prevent ransomware in the first place.

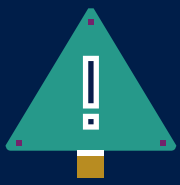
Background context

Ransomware is the key cyber threat facing UK organisations. In a ransomware attack, a cyber criminal group gains unauthorised access to an organisation's network and uses malware to encrypt files and prevent access to data and devices. The criminals then demand a ransom, usually in a cryptocurrency, in exchange for a decryption key to decrypt files and restore systems.

Victims of ransomware also increasingly face an extortion threat, where the attacking cyber criminal group threatens to publish or sell stolen data unless a ransom is paid. But following payment, a victim may discover the attacker has lied about deleting the data and look to sell it to other criminals for profit, or repeat the threat of releasing it months, or even years, after the incident.

Things to consider

Don't panic



In the immediate aftermath, a ransomware attack can feel overwhelming. Ransomware actors know the tactics to use to pressure organisations into making quick decisions. But slowing down to review the options will improve decision-making and lead to a better outcome.

Review alternatives, including not paying

Decisions about payment should be informed by a comprehensive understanding – as much as is possible – of the impact of the incident. Cyber criminals will try to convince you that payment is the only way to recover. It can take time to check your options. You might have viable backups, or there may be unexpected ways to help recover systems and data, partially or fully. You may even be able to access decryption keys through third parties, such as law enforcement, who make them freely available.

Record your decision-making

Maintaining a careful record of the incident response, decisions made, actions taken and data captured (or missing) is important for post-incident reviews, lessons learned or presenting evidence to a regulator. During an incident, it is sensible to record decision-making offline, or on systems that are not impacted by the incident.

Where possible, consult experts

Objective external experts such as insurers, the NCSC, law enforcement or cyber incident response (CIR) companies familiar with ransomware incidents can improve the quality of your decision-making. The NCSC website includes a list of CIR companies recommended by the NCSC. Insurance providers will often provide recommended CIR companies.

If you have cyber insurance, you should report the attack to your insurer or broker. There will be a number to call, or an app, that is also available out of hours. If you outsource your IT network, you should engage your IT provider.

Involve the right people across the organisation in decisions, including technical staff

Few scenarios will engage senior business owners and decision-makers as quickly as deciding whether to pay a ransom, but make sure the options aren't presented prematurely and that you provide the strongest possible evidence base.

Assess the impact

Decisions about payment should be informed by an understanding of the impact on your business.

- **Business operations:** Where you have put in place workarounds to manage disruption, you will need to determine how long they can be sustained. .
- **Data:** In almost all ransomware incidents, cyber criminals now also steal data and you cannot trust a promise to delete it once a ransom is paid. You should carry out an assessment to determine what data was compromised and how sensitive it is. Consider taking legal advice and whether you need to make a disclosure to the Information Commissioner's Office (ICO). You should also evaluate the risks to life, vulnerable groups or national security, if data were published. You may want to verify, to the best of your ability, that any claims about the nature and amount of data stolen are true.
- **Financial:** You can conduct a cost analysis of your different options. Balancing costs against other impacts will be a key determining factor in your decision. Costs incurred may include business disruption, security improvement work, staff overtime, legal expenses or regulatory penalties. The sum paid to the criminal group is also typically negotiable.

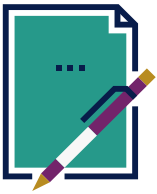
Investigate the root cause of the incident to avoid a repeat attack

Making a payment without clarifying the original source for the compromise, and then taking appropriate mitigation actions, leaves your organisation open to further incidents. Some ransomware attackers may offer to disclose how you were compromised, but don't take this at face value and instead seek to independently validate how it happened.

Be aware that payment does not guarantee access to your devices or data

Even where a decryption key is acquired, it's unlikely to result in an immediate return to business as usual, particularly for large organisations. Running a decryption key across complex networks can take time. If a victim organisation has access to both backups and a decryptor, it may prove quicker to use backups.

Consider the correct legal and regulatory practice around payment



There are legal and regulatory considerations for UK organisations to consider before paying a ransom. Payments may not be lawful, for example, if a ransom payment is made to an entity or area sanctioned by the UK.

You should also take into account the relevant local laws and regulations applicable to all the jurisdictions in which you operate – for example, if you are a parent company operating in the UK with subsidiaries elsewhere, where both are impacted by the attack.

Know that paying a ransom does not fulfil your regulatory obligations

The ICO is clear that it doesn't consider a payment to criminals who have attacked a system as a risk mitigation – and that it wouldn't reduce the amount of any penalty.

Report the incident to UK authorities

Organisations experiencing a ransomware attack can report it, as reporting an incident to the UK authorities will help support victims. The UK government's incident signposting service will help you understand which organisations to notify.

The NCSC works on incidents of national significance and where this is the case, a victim will benefit from engaging with the NCSC because:

- the NCSC can help manage a victim's engagement with the rest of government, allowing the affected organisation to focus on the incident response
- the NCSC may share unique information and insight that will help the victim and their insurance or CIR provider, where there is one, to understand and manage the incident
- it may result in a more favourable regulatory response, including a lower fine from the ICO