GUIDANCE FOR ORGANISATIONS DURING RANSOMWARE INCIDENTS

Originally published by Counter Ransomware Initiative (CRI).

Cover Statement

1. Members[1] of the Counter Ransomware Initiative1 are joining together, alongside insurance bodies[2] to issue guidance for organizations experiencing a ransomware attack and partner organizations supporting them.
2. Acceding to ransom payment demands fuels the ransomware business model, and 2023 was the worst year on record for ransomware payments globally (Chainalysis).
3. Ransomware is a complex and transnational problem that requires strong international collaboration to address. At the 3rd CRI Summit in 2023, the CRI issued a joint statement that strongly discouraged anyone from paying a ransomware demand. This statement recognized that paying a ransom to ransomware actors:
    - Does not guarantee the end of an incident, or the removal of malicious software from your systems,
    - Provides incentives for criminals to continue and expand their activities,
    - Provides funds that criminal actors can use for illicit activity, and
    - Does not guarantee you will get your data back.
4. This guidance is non-binding in nature and does not override specific laws and regulations that may apply across CRI member jurisdictions.
5. When organizations become victims of a ransomware attack, deciding whether to pay a ransom or not can be a difficult decision to make. The CRI has put together guidance for organizations facing a ransomware incident. This guidance provides a holistic overview of the steps organizations should explore before considering paying a ransomware criminal, including examining the potential negative consequences of paying a ransomware criminal.

[1] Albania, Argentina, Australia, Bahrain, Bulgaria, Canada, Chad, Colombia, Costa Rica, Denmark, ECOWAS Commission, France, Germany, Greece, INTERPOL, Ireland, Israel, Japan, Kenya, Lithuania, Mexico, Moldova, the Netherlands, New Zealand, Nigeria, Philippines, Republic of Korea, Romania, Rwanda, Sierra Leone, Singapore, Slovakia, Slovenia, Spain, Switzerland, United Arab Emirates, United Kingdom, United States, Uruguay, Vanuatu, Vietnam.

[2] American Property Casualty Insurance Association, Association of British Insurers, British Insurance Brokers' Association, Dutch Association of Insurers, Insurance Council of Australia, Insurance Council of New Zealand, International Underwriting Association, MSIG Asia Pte Ltd, Singapore Reinsurers' Association, Swiss Insurance Association.

6. This guidance aims to minimize the overall impact of a ransomware incident on an organization and help reduce:
    - Disruption and cost to businesses.
    - The number of ransoms paid by ransomware victims.
    - The size of ransoms where victims choose to pay.
7. Cyber insurance can be an important risk management practice. CRI members recognize the important role that cyber insurance can play in helping to build resilience to cyber attacks, including through supporting the companies they insure to improve their protective measures. CRI members and insurance industry bodies will collaborate to deepen the important role the commercial cyber insurance industry plays to strengthen and support organizations' resilience against ransomware.
8. CRI members and insurance industry bodies recommend victim organizations review the following guidance before ultimately considering whether to make a ransomware payment to a cyber criminal group.

Guidance for organizations during a ransomware incident

1. Organizations are encouraged to make preparation, as part of their business continuity plan, and develop and implement their policies, procedures, frameworks, and communications plans in advance of any ransomware incident.

Consider the correct legal and regulatory environment around payment

2. There are legal and regulatory considerations for organizations to consider before paying a ransom which experts can provide access to advice on. Cyber insurers can also direct victims towards legal counsel who can provide advice.
3. Payments may not be lawful in certain circumstances, for example, if a ransom payment is made to a sanctioned entity.

Reporting the incident to the authorities

4. Reporting incidents to the authorities at the earliest opportunity can support victims. Such reporting will allow the authorities to provide the necessary advice and support to victims, in turn strengthening their resilience and preventing future ransomware incidents. Timely reporting of attacks and any payment made is also necessary for the authorities such as law enforcement to conduct effective investigations, compile evidence for any future disruption of ransomware actor activities, and to improve the authorities'

overall understanding of ransomware criminal operations to better support future victims, and possibly stop future attacks, including through apprehension and prosecution of those responsible and seizure and disruption of their infrastructure and services.

Evaluate all options

5. In the immediate aftermath, a ransomware attack can feel overwhelming. Ransomware actors know the tactics to use to pressure organizations into making quick decisions. But slowing down to review the options available could improve decision-making and lead to a better outcome.
6. Due diligence, reasonable collection of information and analysis of the potential harms, should be a component of every organization's incident response and recovery plans. Due diligence can provide the following benefits:
    - Assurance that key pieces of information or evidence, will not be missed.
    - Clear, data-backed rationale behind decisions.
    - Ability to meet any relevant domestic legal requirements, such as incident reporting.

Where possible, consult experts

7. External experts such as insurers, national technical authorities, law enforcement or cyber incident response (CIR) companies familiar with ransomware incidents can improve the quality of decision-making. Insurance providers will often provide recommended CIR companies to assist organizations. If organizations have cyber insurance, they should comply with the reporting provisions of the insurance policy. 3 Review alternatives to paying ransom
8. As a general approach, organizations are strongly discouraged from making payment, in line with the joint statement issued at the 3rd CRI Summit in 2023.
9. While the CRI statement strongly discourages organizations from making payments, in accordance with local laws and regulations, there may be occasions where a victim may ultimately consider paying a ransom.
10. Decisions about payment should be informed by a comprehensive understanding – as much as is possible – of the impact of the incident and whether payment is likely to change that outcome or not. Cyber criminals will try to convince victims that payment is the only way to recover, despite the downsides of paying ransoms.

Gather relevant information to assess the impact and legal obligations

We recommend that organizations consider the following

11. Take time to consider the technical situation, including availability of back-ups, alternative sources for decryption keys, time estimate for restoring functionality once decryption keys are obtained. Some of these tools may be available from cybersecurity firms, law enforcement agencies, or other commercially available or open-source tools.

12. Put in place workarounds to manage business disruption, and determine how long these workarounds can be sustained. When reviewing the organizational impact, organizations need to assess its system functionality, impact to business operations, impact to customers and employees (including indirect impact on the supply chain where applicable), and the likelihood of further data exfiltration.

Assess the impact of the incident

13. Taking steps to assess the impact of the incident helps organizations to be better prepared and for insurance coverage discussions. It is important to note that some costs – notification to impacted individuals, regulatory penalties related to safeguarding data and others – may already be incurred as a result of data exfiltration during the ransomware incident, regardless of whether the information is ultimately leaked. The impact of these costs should therefore be considered separately from the determination of whether to pay. Considerations may include:
    - Examining what insurance coverage you may have.
    - Estimating the revenue loss from business interruption, security improvement work, staff overtime, legal expenses or regulatory penalties.
    - Identifying any potentially stolen data or intellectual property and estimate the potential damage to the organization, customers and clients if applicable, from any stolen data being released.

14. Finally, in many ransomware incidents, cyber criminals now also steal data. Therefore, victims should not trust a promise to delete the stolen data once a ransom is paid. It is good practice for organizations to carry out an assessment to determine what data was compromised and how sensitive it is. Legal advice is helpful to ensure compliance with laws and regulations, and with regard to reporting to and seeking assistance from the relevant authority. Organizations should also evaluate the risks to life,

personal data or national security, if data were published. We recommend verifying that any claims about the nature and amount of data stolen are true.

Record your decision-making

15. 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.
16. The goals of this process are to create an auditable trail for decisions; develop succinct explanations for decisions; and reduce the likelihood of another successful attack.
17. These efforts may look different in different jurisdictions, as regulatory processes, legal systems, and internal organizational requirements vary.

Involve the necessary stakeholders across the organization in decisions, including technical staff and senior decision makers

18. Few scenarios will engage senior business owners and decision-makers as quickly as deciding whether to pay a ransom. However, organizations should make sure the options are not presented prematurely and that the strongest possible evidence base is provided.

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

19. Even where a decryption key is acquired, it’s unlikely to result in an immediate return to business as usual. Running a decryption key across complex networks can take time. If a victim organization has access to both backups and a decrypt or, it may prove quicker to use backups.
20. It is important to keep in mind that making payments and acquiring the decryption key may not guarantee the end of the incident. A victim should not presume that a compromised system that has been restored—either from a back-up copy or after using a decryption key—is secure. A back-up copy may also have been compromised, and malicious actors may have ensured that a system restored from an encryption key remains vulnerable to future exploitation.
21. It is also important to consider that the malicious actors may not fulfil promises to delete stolen data and that you will be unlikely to have

Post incident evaluation: Investigate the root cause of the incident and make the necessary preparations to avoid a repeat attack.

22. Making a payment without clarifying the original source for the compromise, and then taking appropriate mitigation actions, leaves an organization open to further incidents. Organizations should seek to independently validate how the compromise happened and remediate any flaws.

23. Organizations should also assess if the initial breach and associated vulnerabilities have been remediated. Assessing how the compromise happened would help organizations to strengthen their defenses against future ransomware attacks. This includes implementing prevention and risk-mitigation measures such as credential management, network segregation and segmentation and having offline/disconnected back-ups.

Source: Counter Ransomware Initiative (CRI)