You've been ransomed. Now what?!

First: Take a deep breath. We're on our way to help.

Next: Use this guide to make sure everyone on your team is on the same page while avoiding common pitfalls in the early stages of a ransomware attack.

DON'T:

Engage Directly Without Expertise

Refrain from engaging with threat actors directly without the guidance of cybersecurity experts, legal advisors, and law enforcement authorities, as this can escalate risks and compromise negotiations.

Pay the Ransom Immediately

Avoid rushing to pay the ransom without fully understanding the situation, assessing other options, and considering the potential consequences of rewarding criminal behavior.

Ignore Your Legal Obligations

Do not disregard legal obligations or regulatory requirements related to data protection, privacy, and incident reporting when responding to a ransomware attack, as this can result in legal liabilities and penalties.

Negotiate Without a Plan

Resist entering negotiations without a clear strategy, predetermined objectives, and an understanding of the organization's limitations, as this can lead to unfavorable outcomes or unnecessary compromises.

Promise Immediate Payment

Avoid making promises or commitments to threat actors regarding payment or compliance with their demands before evaluating the situation and consulting with relevant stakeholders.

Underestimate the Threat

Refrain from underestimating the severity or impact of the ransomware attack, as this can lead to delays in response efforts and exacerbate the situation.

Provide Sensitive Information

Avoid disclosing sensitive information or sharing credentials with threat actors during negotiations, as this can further jeopardize cybersecurity and data privacy.

DO:

Assess the Situation

Evaluate the extent of the ransomware attack, including the scope of the data breach, potential impact on operations, and criticality of the affected systems.

Engage Incident Response Teams

Consult cybersecurity professionals and incident response teams to analyze the attack, identify vulnerabilities, and devise strategies for mitigation and recovery.

Consult Legal and Law Enforcement

Seek guidance from legal counsel and involve law enforcement agencies, such as the FBI or local authorities, to understand the legal implications and potential consequences of negotiating with threat actors.

Assess Potential Value

Begin to determine acceptable ransom amounts and negotiating terms by attempting to quantify the value of data stolen or encrypted.

Evaluate Backup Data

Determine if critical data is backed up and stored securely to prevent further loss in case negotiations fail or the ransom is not paid.

Establish Protocols

Keep internal stakeholders informed about the situation, including executives, IT staff, legal advisors, and relevant department heads, to ensure coordinated decision-making and response efforts.

Digital Asset Redemption