You've been ransomed. Now what?

Digital Asset Redemption

Make sure everyone your team is on the same page to avoid common pitfalls in the early stages of a ransomware attack.

✖ DON'T:

✖ ENGAGE DIRECTLY WITHOUT EXPERTISE
This can escalate risks, compromise negotiations, and delay resolution.

✖ PAY THE RANSOM IMMEDIATELY
Besides paying too much, you could risk insurance complications, violating sanctions, or not getting your data back.

✖ IGNORE YOUR LEGAL OBLIGATIONS
Ignoring legal obligations or regulatory requirements on data protection, privacy, and incident reporting can result in penalties.

✖ NEGOTIATE WITHOUT A PLAN
Get a clear strategy, predetermined objectives, and an understanding of the organization's limitations before negotiations begin.

✖ UNDERESTIMATE THE THREAT
Underestimating the severity or impact of the attack can lead to delays in response efforts and exacerbate the situation.

✖ PROVIDE SENSITIVE INFORMATION
This can further jeopardize your recovery and data privacy.

✔ DO:

ENGAGE INCIDENT RESPONSE TEAMS
These teams are trained in crisis response and willl triage the situation.

ASSESS THE SITUATION
Evaluate the extent of the attack, scope of the breach, impact on operations, and criticality of the affected systems.

CONSULT LEGAL AND LAW ENFORCEMENT
Seek guidance from legal counsel and involve law enforcement to understand the legal implications 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 in case negotiations fail or the ransom is not paid.

ESTABLISH PROTOCOLS
Keep internal stakeholders informed to ensure coordinated decision-making and response efforts.

Need immediate help? We're here 24/7. digitalassetredemption.com/support