



Data Privacy Detective Podcast – Episode 69: Negotiating with Digital Kidnappers

Jul 28, 2021

Categories:

[Blogs](#)

[Podcast](#)

[Technology Blog](#)

Authors:

[Joseph J. Dehner](#)

[William T. Repasky](#)

Ransomware. It's in the headlines. It's digital organized crime across borders.

When an organization's IT system freezes with its data locked by a ransomware gang, what happens? Ransom is demanded, and ransom often gets paid. But how does this work?

In this podcast episode, [Bill Repasky](#), attorney with Frost Brown Todd LLC, shares key insights on the process of negotiating with ransomware criminals. They want payment in cryptocurrency. Victims want their data and systems restored. This becomes a business transaction. But not a typical one.

Ransomware strikes in 2021 involve highly sophisticated criminal syndicates. To them it's about the money. When they strike a target and freeze the organization's ability to operate an IT system, they reveal their digital identity and dictate how to send a ransom payment. The target may be willing to pay – but should do so only after negotiations to ensure that the payment will accomplish two essential objectives – (1) providing a decryption key to unlock the encrypted data and restore the IT system's operation; and (2) ensuring that the data has not been taken (exfiltrated) by the criminals, or if it has, to have it returned with no copies kept by the criminals. The victim organization should check before making payment to be certain it does not violate U.S. sanctions laws by paying a group or person listed on the OFAC list. See [Specially Designated Nationals And Blocked Persons List \(SDN\) Human Readable Lists | U.S. Department of the Treasury](#).

Successful conclusion of a ransomware attack requires expertise, patience, and insight. Learn how it's done, pitfalls to avoid, lessons from past victims.

If you have ideas for more interviews or stories, please email info@thedataprivacydetective.com.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.