Cover image:

Data Recovery: Paying Extortionists to Protect Customers Is Not Illegal, But It May Be Risky

24 June 2019 By: Sean Sposito

The popular conversation around ransomware has shifted from detection to remediation. Hospitals, municipalities, and other victims frequently end up paying their extortionists through third parties promising data recovery services. A recent spate of media reports discuss the convenience and dilemmas of giving in to extortion:

- In May, Propublica, a nonprofit news organization dedicated to investigative journalism, reported that vendors who promise ransomware solutions mostly end up negotiating with their clients' extortionists.1
- Earlier in the month, CBS' "60 Minutes" described "why," in the case of ransomware, "the best solution is often paying a ransom."2
- And a Boston Globe Q&A with the author of the Propublica report, in part, put the city of Baltimore's decision not to pay its extortionists demands for 13 bitcoins – roughly $104,000 – into context.3

But what about broader data recovery practices? All of this media coverage has no doubt created internal business questions about both the ethics of paying for decryption keys and the practice of paying cybercriminals in general. These are questions that security executives should be prepared to answer in the elevator, over email, and in meetings.

---

javelinstrategy.com inquiry@javelinstrategy.com 925.225.9100