Freedom of Information: Paying Ransom to Cyberthieves

Adapted from the writings of Dayan Yitzhak Grossman

May 27, 2021

On May 7, Colonial Pipeline, an oil pipeline system that carries gasoline and jet fuel, suffered a ransomware cyberattack—the largest cyberattack on an oil infrastructure target in the history of the United States—that impacted computerized equipment managing the pipeline. Colonial Pipeline paid the ransom (75 bitcoin, worth $4.4 million) within hours. Colonial's CEO Joseph Blount explained that he authorized the ransom payment because executives were unsure how badly the cyberattack had breached its systems or how long it would take to bring the pipeline back:

> I know that's a highly controversial decision…I didn't make it lightly. I will admit that I wasn't comfortable seeing money go out the door to people like this.[1]

Redeeming captives for "more than their value"

The Mishnah declares that we do not redeem (human) captives for "more than their value,"[2] and the Gemara gives two reason for the prohibition:

1. To avoid excessively burdening the community.
2. To avoid incentivizing additional seizures.

Most *poskim* accept the latter reason as normative,[3] although some consider the matter unresolved.[4]

Does the Mishnah's prohibition apply to paying ransom to cyberattackers?

Voluntary redemption

The Gemara explains that a point of divergence between the two rationales is where an individual voluntarily offers an excessive ransom for his relative: The former rationale does not apply, but the latter does.[5]

A business paying a ransom for the decryption of its data is presumably considered voluntary payment, insofar as management is acting in the interests of the shareholders, as their fiduciaries. The same would apply to a governmental agency ransoming its own data, if it considers this to be in the best interests of the public. It would seem, then, that the former rationale is not applicable, while the latter might be, if the concern for the incentivization of kidnapping can be extended to the incentivization of ransomware attacks.

Data are not people

While there has been a great deal of halachic discussion about the parameters of the Mishnah's prohibition and its application to various modern scenarios (particularly those involving political terrorism), these scenarios have all involved human captives (usually living ones, and occasionally their remains); I am not aware of any discussion of paying ransoms for the decryption of data.

On the one hand, perhaps the concern for the incentivization of crime does not apply, since cyberattacks are not as terrible as kidnappings. Although

ransomware attacks on hospitals have been linked to deaths,[6] these links are tenuous and indirect, and it seems difficult to argue that halacha would consider such attacks to be the equivalent of kidnapping, given that halacha treats captivity as a fate worse than death by natural causes, death by the sword, and death by famine![7]

But on the other hand, given the relative ease with which such attacks can be perpetrated; the global reach of cyberattackers; the deep, society-wide vulnerability to such attacks; and the very real possibility of future attacks causing grave societal harm, including death, it can easily be argued that it is indeed imperative to avoid incentivizing such attacks.

Ransoming oneself

Tosafos maintains that even the latter rationale applies only to the ransoming of others, but one is always permitted to ransom oneself, since *Chazal* never forbade someone from giving up whatever he has to save his life;[8] this position is codified in the Shulchan Aruch. It can be argued, then, that according to either rationale of the prohibition, a business is still entitled to pay whatever ransom it wants on its own behalf. Perhaps, though, this dispensation is only when one's very life is at stake (as per the language of Tosafos) and does not extend to paying ransom to avoid nonlethal harm.

The value of data

A final consideration in the application of the Mishnah's prohibition to ransomware attacks is that the prohibition is only against redeeming captives for "more than their value." In the original context of human captives, one interpretation of the "value" of a captive is his value on the slave market, and if there is no local slave market, we estimate his value to a slaver who would transport him to a locale where there is such a market.[9] Others interpret the "value" in light of the need to avoid incentivizing future seizures, and understand that the problem is with overvaluing Jews relative to non-Jews, since this will cause kidnappers to specifically target Jews, but there is apparently no prohibition against paying even excessive ransoms in general.[10]

With respect to the former definition of value in the classic sense of worth in the market, much has been written about the business value of data, from the various perspectives of legitimate businesses,[11] subjects of the data,[12] and the criminal underworld.[13] Depending on the nature of the data in question and which perspective is adopted, it will be more or less feasible to arrive at a concrete valuation of a particular collection of data. According to the latter perspective, paying ransom to cyberattackers would be generally permitted, except for where this would engender the perception that Jews and their businesses are especially attractive targets.

[1]Collin Eaton. Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom. The Wall Street Journal. https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers

-a-4-4-million-ransom-11621435636.
[2]Gittin 45a.
[3]Yad Hachazakah *Hilchos Matnos Aniyim* 8:12; Radvaz ibid.; Kesef Mishneh ibid.; Ramban and Rashba to Gittin ibid.; Shulchan Aruch Y.D. 252:4.
[4] Ran ibid. Cf. Shu"t Bnei Vanim *cheilek* 1 *siman* 43 *os* 2 pg. 150 for an exhaustive list of the opinions of the *Rishonim* on this question.
[5]Gittin ibid. and Rashi there.
[6]William Ralston. The untold story of a cyberattack, a hospital and a dying woman. Wired UK.
https://www.wired.co.uk/article/ransomware-hospital-death-germany;
Nsikan Akpan. Ransomware and data breaches linked to uptick in fatal heart attacks. PBS Newshour.
https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks;
Brian Krebs. Study: Ransomware, Data Breaches at Hospitals tied to Uptick in Fatal Heart Attacks. Krebs on Security.
https://krebsonsecurity.com/2019/11/study-ransomware-data-breaches-at-hospitals-tied-to-uptick-in-fatal-heart-attacks/.
[7]Bava Basra 8b.
[8]Tosafos ibid. s.v. *Delo legarvu velaisu* (alluding to Iyov 2:4).
[9]Shu"t Maharam Lublin *siman* 15.
[10]Shu"t HaRadvaz *cheilek* 1 *siman* 40. Cf. Pis'chei Teshuvah ibid. *s.k.* 5, and Bnei Vanim ibid. at length.
[11]The world's most valuable resource is no longer oil, but data. The Economist.
https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data;
Data Valuation—What is Your Data Worth and How do You Value it? Open Data Science.
https://medium.com/@ODSC/data-valuation-what-is-your-data-worth-and-how-do-you-value-it-b0a15c64e516.
[12]Hanna Kozlowska. How much is your data worth? Quartz.
https://qz.com/1655610/how-can-you-measure-the-worth-of-your-data/.
Pauline Glikman Nicolas Glady. What's The Value Of Your Data? TechCrunch.
https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/.
[13]Brian Krebs. How Much Is Your Identity Worth? Krebs on Security.
https://krebsonsecurity.com/2011/11/how-much-is-your-identity-worth/.
Brian Krebs. How Much is Your Gmail Worth? Krebs on Security.
https://krebsonsecurity.com/2013/06/how-much-is-your-gmail-worth/.