Samuel Zizzo

1 December 2024

Should Companies Be Allowed to Pay Ransomware?

In 2023, cybercriminals embezzled over $20 billion across the globe. This shocking amount of money extorted over the internet has left many businesses—primarily the main targets of these attacks—paralyzed. Many companies and their systems are critical to the American network and infrastructure. Once a system is compromised, few options are available to the victims other than paying the ransom. This is because, as soon as law enforcement becomes involved, all fate of the data falls directly to the authorities, and in nearly all cases goes cold for the victim. Therefore, companies should be allowed to pay these cyber ransoms as a last resort to restore critical data, taking into consideration the devastating impacts of allowing these systems to be crippled for an extended period. By not paying, a company almost guarantees losing all stored data, which further illustrates why companies should continue to be allowed to pay cyber ransoms.

The debate over whether to pay ransoms is further complicated by the substantial financial and reputational costs associated with data breaches. For instance, data breaches not only lead to immediate financial losses but also long-term reputational damage that can significantly affect customer trust and corporate value. Companies face not only the loss of immediate operational data but also potential breaches involving sensitive customer information which could lead to litigation and regulatory fines. The argument for allowing ransom payments is supported by the notion that it can be the lesser of two evils, especially in cases where the lost data comprises critical intellectual property or sensitive personal information that could potentially save lives or prevent further financial ruin.

Ransomware is encryption, locking any data with a security key. Ransomware can be executed on a small scale, for example, an individual in Florida blackmailing someone in Georgia on his home computer, prompting the person in Georgia to pay a certain sum of money (predominantly cryptocurrency because it is easiest for the attacker to remain anonymous) to get access to his computer back. Unfortunately, this attack is more commonly executed on a larger scale against Linux servers by groups of hackers on large business models like CNA Financial, which is one of the largest insurance firms in the U.S. that was a recent victim of a ransomware attack and negotiated their way down strategically from $60M to $40M with the Russian hacking group named "Phoenix." Companies like CNA have extremely sensitive and important customer information that would be devastating for the company and their customers to have leaked by an attacker. And risking obtaining their data back with the authorities could end up with a bigger loss of money for the organization. According to Grimes, an accredited cybersecurity author, "Law enforcement has the legal right to do many things, potentially against your wishes, if they want, such as seize assets, investigate people, forbid transactions, etc. When you invite law enforcement to get involved in your cybersecurity incident, you are inviting a risk that they could force a particular decision not wanted by the victim or their organization" (Grimes 112). This statement clearly explains how involving law enforcement in a ransomware investigation could be detrimental to a company and its customers. Companies are required to report and avoid paying ransomware if it is executed by certain groups of people; this has been made a federal law by OFAC's Enforcement Guidelines and states that there is a "presumption of denial," which means that a company would have to ask a lawyer what guidelines to follow if they were a victim of a cyber-attack by one of the groups stated in OFAC's Enforcement Guidelines. This shows that the government has implemented procedures for companies to follow if they were

victims of a cyber-attack, and this makes it difficult in some circumstances for companies to obtain their data and not break any federal cyber laws.

Although companies have set up backups for their data and used anti-ransomware software, nothing online is 100% secure from attacks, and data backups are still vulnerable to ransomware attacks unless they are stored completely separately from the main data architecture. Unless a company has a completely secure off-site data backup center or a secure cloud data center that is autonomous from the company, you can pretty much bet they will lose all their customers' data if their systems get compromised. Although losing data doesn't sound extremely abhorrent initially; to put it in perspective, NIH's N3C Database currently stores approximately 6.3 million health records in the US. All health records include sensitive patient information that can be used to save lives. The inability to access this data at any moment could be an extremely detrimental reality if preventative thought is not taken by the victim before attacks happen. Williams states, "Non-payment may not be an affordable option for companies that could face financial ruin if they don't pay up—and quickly" (Williams NA). This statement argues that not paying can leave some companies in financial ruin. It also supports my statement on how extremely important and dependent most companies are on secure data storage systems.

The argument of whether we should allow companies to pay ransomware to recover data has been a rising question in the cybersecurity industry. Many stances have been taken on the subject. Many variables play into the question. There are various attackers, from various countries, with which we have various relations and political standings. This makes it hard for companies and cybersecurity professionals to reach a consensus on the main question. Although many critics argue that paying cyber ransom fuels an endless cycle of cybercrime and only rewards the attackers for their efforts, there is nothing that companies can do in a situation like

that but pay or lose their data altogether. Although it seems crazy to just hand money over like that, it is often the best strategy to recover data in a worst-case scenario data loss situation.

Cybercriminals have been working long and hard to maintain their presence in the ransomware sector, and every day cyber-attacks grow increasingly more malignant with the integration of artificial intelligence in recent ransom scripts. This means that companies need to take direct action to prevent these attacks from happening at the same scale that the attackers are. Although many people are against paying criminals for very understandable and agreeable reasons, companies should still be legally and socially allowed to pay cyber ransoms without repercussion because, at the end of the day, the companies need to stop at nothing to best protect a large percent of America's data. If companies follow the correct standards for protecting their business and planning for ransomware attacks, then nothing should ever be a surprise, and data should always be able to be restored.

Works Cited:

Williams, Clive. “Cybercrime: Why Many Choose to Pay the Ransom.” *The Australian*, 14 Nov. 2022. Gale In Context: Opposing Viewpoints, https://link.gale.com/apps/doc/A726553029. Accessed 5 Nov. 2024.

Grimes, Roger A. *Ransomware Protection Playbook*. John Wiley & Sons, Incorporated, 2024. Adobe Digital Editions, p. 112.

Lemnitzer, Jan. “Ransomware Gangs Are Running Riot – Paying Them off Doesn’t Help.” *Gale Opposing Viewpoints Online Collection*, Gale, 2024, https://link.gale.com/apps/doc. Accessed 1 Dec. 2024.

“The Ransomware Dilemma.” *MIT Sloan Management Review*, June 2022, p. 13. Gale In Context: Opposing Viewpoints, https://link.gale.com/apps/doc/A734809644/OVIC. Accessed 1 Dec. 2024.