ProCircular℠
SECURITY. PRIVACY. TRUST.

Ransomware: When do I pay?

A discussion of the criteria for analyzing the risks and a model for decision making.

Plain and simple, data ransoming is on the rise.

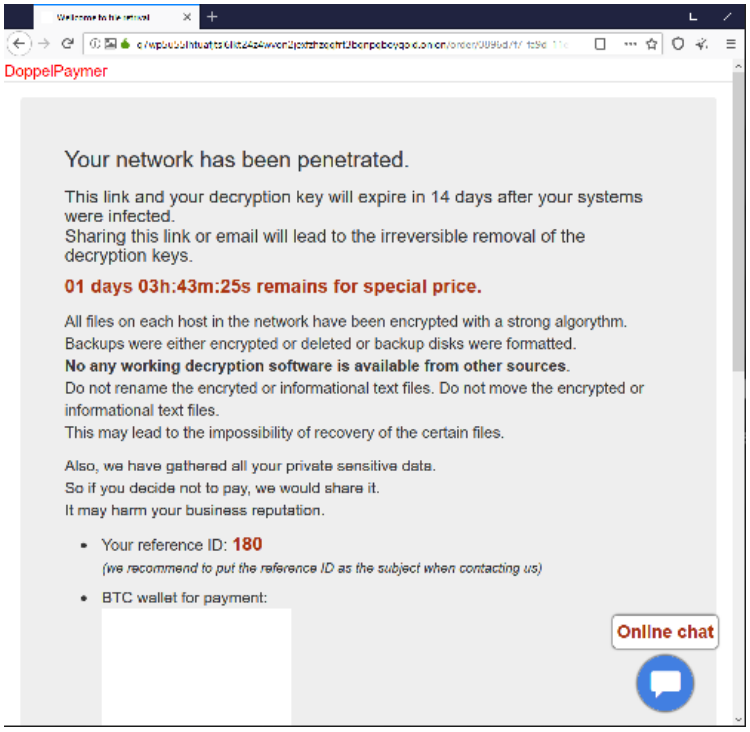
Most of us never consider the possibility that we may become victims of a ransom scenario in our lifetimes. Cyber attacks are a relatively new threat that is evolving rapidly. As this growth continues, more and more parties find themselves at the receiving end of a ransom message. Their organizational or personal data is held hostage while a clock ticks down to fuel their anxiety.

Traditionally, negotiation with any hostage-taker has been considered a dead loss. Common wisdom suggests it will only embolden bad actors and increase the number of incidents. There is a natural tendency to extend this philosophy to data ransoming as well; but with the increasing number of threats and the *extraordinary* cost of downtime in an online world, we can no longer afford to take this hardline stance.

Contrary to our predisposed reaction, paying out against ransomware must be considered alongside the other options available amid a data breach incident.

Like any other business decision, the issue of *whether* to pay is a risk calculus with several variables to inform your approach. In addition to the fiscal implications, there is also an important ethical argument to consider. Nonetheless, reviewing *all* available options should be a part of any risk-related decision.

This document may not answer the “Should I pay?” question for your specific organization or scenario, but it provides guidelines that allow you to assess your relative risk and choose more wisely.



ProCircular
SECURITY. PRIVACY. TRUST.
2451 Oakdale Blvd. Coralville, IA 52241
www.procircular.com | solutions@procircular.com
844-95-SECUR

History & Today

"Do NOT negotiate with terrorists."

We have heard this mantra from politicians and law enforcement for decades, seen it depicted in pop media, and generally accept it as truth.

This logic developed in an era where international terrorism was extraordinarily risky to both the terrorist and the target. Hijacking an airliner required significant investment in planning, training, and coordination on the part of the terrorist. The impact on the target and resulting outrage was even greater (Baum, 2016).

In the modern world of cybersecurity and asymmetric threats, however, these rules may no longer apply.

Unlike the hostage scenarios that spawned this logic, a lone hacker in a bedroom in Ukraine can upend the online business of *millions* of people transacting *billions* of dollars. An internet connection, a laptop, a copy of the most recent freeware phishing tools, and an afternoon are the only investments necessary to cause devastation. It can be argued that never in human history has a single person had such capacity to dramatically disrupt the lives of so many others with relatively *minimal personal risk*.

As a result of increased accessibility and reduced risk, the number of attacks of this type is higher than at any point in history. In just the first three quarters of 2019, there were roughly 7.2 billion malware attacks and 151.9 million ransomware attacks (Sonicwall, Inc., 2019).

Ransomware attacks are typically carried out using a Trojan, a malicious file disguised as a legitimate one, that the user is tricked into downloading or opening when it arrives as an email attachment. Once opened, the infected computer encrypts its own files then hunts for other systems on the network to do the same. Modern versions of these malware include software crafted by the NSA and are highly virulent once inside a private network (SentinelOne, Inc., 2019).

Harmful tools like these are freely available on the dark web and, therefore, they are a constant threat and ongoing problem. They enable hackers of various stripes to hold people and organizations hostage with little effort.

Consider the Variables

In a data ransom scenario, there is much to consider when evaluating potential options. Applying a game-theoretical model can be an excellent way to expose the relevant variables and make a rational decision. In "A Game-theoretical model of Ransomware," Nicholas Caporusso lays out a prescient list of primary variables to consider (Caporusso N., 2019):

Financial:

- The *actual* value of the data encrypted
- The cost of downtime/opportunity cost to victim
- The ransom amount requested

Operational:

- The victim's ability to pay the ransom
- The victim's ability to restore the affected data

Situational:

- The trust level in the attacker

ProCircular SECURITY. PRIVACY. TRUST.
2451 Oakdale Blvd. Coralville, IA 52241
www.procircular.com | solutions@procircular.com
844-95-SECUR

- The credibility of the threat posed by the attacker
- The reputational risk of paying the ransom
- Your principles and ethics

Financial Considerations:

The cost of a breach

As in any Business Continuity or Disaster Recovery scenario, it makes sense to evaluate the relative cost of downtime. There are a host of costs to consider in your estimation and many detailed articles have been written on the subject. Among them, you should assess:

The actual value of the data encrypted

While having your data encrypted can be a traumatic event, it is advantageous to keep a cool head and look at the information that was *actually* affected. If the infiltration was limited to a few workstations that can be easily reimaged with no financial or critical operational data stolen, it is less attractive to pay even a modest ransom.

The cost of downtime/opportunity cost to victim

Considering the cost of operational downtime should be a part of any standard business-continuity planning process. In lieu of that level of formality, consider how much it costs to have affected employees unable to work, the impact of not being able to ship or deliver your products and services, or the inability to collect or receive payment. Summing those approximate values can be an easy, offhand way to determine the net cost per hour of the affected systems.

One of the largest costs associated with ransomware or any sort of cybersecurity incident is the *opportunity* cost. The analysis of which often requires an all-hands-on-deck approach and the destruction of which can last several weeks or even years. Keep in mind, for every moment your team spends thinking about the threat's impact, they are *not* executing on the plans previously made for growth or improvement.

In most organizations, everyone will want to participate in the "save the day" efforts, disrupting their productivity and negatively impacting planned goals and growth. While not easily calculated, opportunity cost must be considered on a timeline. Look one month ahead, have you failed to meet proposed improvements or deadlines because resources were reallocated to recovery efforts? What would be the cost of that impact across multiple departments?

The ransom amount requested

The amount of the ransom requested is another important variable. While a ransom of $1,000 is considered fairly standard in the consumer realm, ransom amounts in the corporate world can be hundreds of thousands, if not millions of dollars (Masarah Paquet-Clouston, 2019).

Comparing the ransom amount to the costs incurred from non-payment is a critical part of this risk calculation. For example, the city of Atlanta was originally asked to pay $52,000 on the Sunday *preceding* the week that was covered so heavily by the media. Once the media became involved, so did the FBI. The story dominated the national stage and the hacker would not have taken *any* amount of money to release the data.

This modest payment of $52,000 could have saved Atlanta tens or hundreds of millions of dollars in recovery costs, excluding the cost of the municipal downtime and the impact to millions of affected taxpayers.

ProCircular
SECURITY. PRIVACY. TRUST.
2451 Oakdale Blvd. Coralville, IA 52241
www.procircular.com | solutions@procircular.com
844-95-SECUR

Operational Considerations:

The victim's ability to pay the ransom

Another factor to consider is the victim's ability to actually pay the ransom.

Threat actors are not handing off briefcases of cash in underground locations, they use a digital currency that is extremely difficult to trace, usually Bitcoin. For the novice user, purchasing Bitcoin and transferring payment to another account can be a daunting effort. It can take multiple days to get the right amount of money into the right places. This process can often exceed the hacker's set time limit. The more professional threat actors will honor this time limit and simply leave your data permanently encrypted.

To be proactive, determine whether or not paying ransomware may be a viable option in the future, then establish a cryptocurrency account *before you need it*. ProCircular recommends Paxful.com as an easy-to-use Bitcoin account, with many different payment options available.

The victim's ability to restore the affected data

The condition of your data—and more importantly, your backups—is probably the most critical criteria in your decision-making process. If you have the capacity to restore data on affected systems, or simply reimage those impacted machines without business interruption, you are well ahead of the game and should probably never consider paying a ransom. Many organizations have invested thousands of dollars in their backup and disaster recovery programs. A credible ransomware attack is an example of when those investments will pay off.

If your backups have also been encrypted (or do not exist), your options are greatly reduced. ProCircular encounters situations where an organization's entire online footprint has been encrypted; they are simply unable to operate without the decryption keys. Solutions can be very limited, particularly for small businesses, due to the prevalence of ransomware. Threat actors know when they have you up against a wall, especially if they personally accessed your system and know the limited scope of your enterprise.

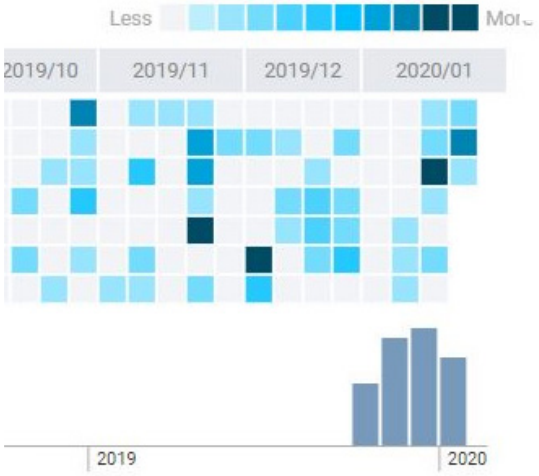
Situational:

The trust level in the attacker – Will they keep their word?

In any adversarial situation, it is important to understand your opponent. There are a variety of ways to accomplish this when dealing with ransomware. Although the number of people sending out ransomware is almost impossible to calculate, the more serious and professional ransomware criminals are relatively easy to identify.

Examine their transaction history

One of your first moves should be looking at past Bitcoin transactions from the address to which the attacker is asking you to transfer funds. As shown in the images below, the threat actor using Bitcoin account number 3PAcw8CxQsbg1KUafsA3cxvHGvVRFoeZfB has extensive history receiving Bitcoin payments in the last three months.



ProCircular
SECURITY. PRIVACY. TRUST.
2451 Oakdale Blvd. Coralville, IA 52241
www.procircular.com | solutions@procircular.com
844-95-SECUR

This attacker has received sixty-three payments since October 2019. Considering an exchange rate of $8654.7 per bitcoin, they have received approximately $220,000 in a matter of months. With further research, we were able to determine that the average Bitcoin payment for this account was roughly $10,000. In this instance, the attacker asked for a Bitcoin payment of $15,000, so we knew they were working within their usual range and not demanding a wildly different ransom.

Based on the frequency and consistency of these transactions, we judged this actor as a professional ransomware specialist, not some "fly-by-night" occasional hacker. This knowledge increases the likelihood that they will return the decryption keys upon payment. In an adverse aerial situation, it works to their advantage to have *you* believe that paying the ransom will lead to your desired outcome.

Additionally, compiling what you know about the hacker can be informative as well. Often these negotiations occur over chat or email. Keeping an eye on *when* they are responsive can reveal which time zone from which they are working. For example, if you are in the central time zone and the hacker is unresponsive after 4:00 pm but responsive again at 3:00 am, you can reasonably assume they are in an EU time zone.

Paying close attention to their style of writing can also be revealing. While the currency is typically discussed in dollars or bitcoin, simple things like the difference between "$100" and "100$" may reveal where they operate (Various, 2011). French-speaking countries and former colonies typically place the currency symbol after the amount. While this may not necessarily speak to the reliability of the hacker, it can help you know more about your opponent.

Examine the malware threat

You should also examine the nature of the malware itself. The dark web offers plentiful options for an individual to purchase the tools necessary to start a ransomware campaign. Fortunately, run-of-the-mill tools are easily detected by modern filters and endpoint protection. The more advanced applications, particularly those designed for a specific environment, are strong indicators of the complexity and capability of the attacker. Just like the ransomware transaction history, quality malware can indicate the attacker is more likely to deliver the keys once payment has been made.

The reputational risk of paying the ransom

It would be foolish not to consider the potential damage to an organization's brand in the face of a publicized breach.

This is significantly less relevant than it used to be, as more and more seemingly secure organizations have been hacked or held for ransom. That said, the impact on individual customers' perceptions of the organization can still be severe. Accounting firms go out of business, banks are inundated with phone calls, and the cost of notifications skyrockets for organizations that have deep relationships with clients based on implicit or explicit trust. Simply stated, the more important *trust* is to your organization, the *greater* the reputational risk from a ransomware outbreak.

Most professional ransomware organizations prefer to fly under the radar and may only brag about a victory in very small circles to avoid being arrested. They are primarily motivated by money, not bragging rights. Compared to the negative publicity of a large data breach or loss, it may be worth paying a ransom for that reason alone.

Your Principles and Ethics

No paper on ransomware would be complete without a discussion of the moral implications of paying off a hacker. These are just two examples of arguments for and against negotiation with terrorists (Benyamin, 2018).

"Negotiating with terrorists undermines rule of law."

Terrorists are criminals, period. The tactics utilized by terrorist organizations and organized crime families, particularly drug cartels, are basically interchangeable. Murder, extortion, kidnapping, drug trafficking, rape, and the innumerable other acts committed by terrorists are already codified by law as criminal acts. Touting some purported grievance as the reason for these crimes does not excuse them.

Societies ruled by law expect their governments to pursue justice. Just as we would not negotiate with John Gotti or El Chapo over the nature of their crimes, we should not negotiate with terrorists in response to theirs. There is a solid argument to be made that payment will only encourage future attacks. There is a chance that, even after paying the attacker, you may not receive the encryption keys, leaving you out in the cold. There is also a chance that the hacker will give you the keys but their established access within your network will lead to additional payment demands in the future.

There is also concern about what, and whom, your payment is inevitably funding. You need your data back so you pay the ransomware. Did you just inadvertently finance a coup d'état, organized crime, or Al Qaeda's next terrorist training camp?

With no sure way to know, the moral implications in this regard can be simply too great to overcome.

"Negotiating with terrorists is preferable to the alternatives."

Terrorists are nothing if not persistent. FARC guerillas made Columbia's jungles untraversable for three decades. Al Qaeda has been operating since (gulp) 1988 and they may be stronger than ever before; not to mention ISIS. The threat to public security is real, present, and potentially long-term. Governments must, therefore, weigh the cost of non-negotiation (such as indiscriminate bombings, the kidnapping and torture of innocents, or biological warfare) against potential gains of peace to be won through negotiation.

Non-negotiation can also eventually mean confrontation through violence. The only problem is that this kind of warfare is asymmetrical and generally more costly for governments than it is for terrorist groups. For instance, in 2011, it was estimated that America's "War on Terror" had cost $1 trillion. In 2018, that number has risen to $5.6 trillion. Thus, negotiations with terrorists may actually *benefit* national economic and security interests.

In the realm of data ransoming, however, the stakes are considerably lower. After an objective analysis of the threat actor's tools and credibility, the benefit of negotiating and paying a ransom may significantly outweigh the cost and impact of accepting the breach as a total operational loss. Therefore, it is worth keeping it as an option in the right circumstances.

Applying Game Theory

In this paper, we will not delve too deeply into the game theory behind the decision-making process. Instead, we use a preexisting model from a published work (Caporusso N., 2019).
We have taken a simple, weighted approach based on our own experience to develop a calculus that can inform your decision making.

	Weighting		
Criteria	H	M	L
How valuable are these data to your operation?	5	3	1
How high is the cost of the related downtime?	5	3	1
How would you describe the amount being demanded?	2	3	5
How able are you to pay the ransom?	1	3	5
How likely is it that you can restore from backup?	-15	-7.5	5
How likely is it that you'll get the decription key? (trust level in attacker)	5	4	1
How credible is the threat posed by the attacker?	5	3	2
What is the potential reputational damage?	4	2	1
In princible, how comfortable are you paying a hacker?	5	3	-10

In this model, we have taken the criteria described above and built a system that weighs each metric by 3 different levels: high, medium, or low. A risk score is assessed for each of the criteria based on the state of the organization and the nature of the incident. For example, if the data that has been affected is highly valuable to your organization, ranked as a high, 5 points are added to the overall risk score. Conversely, if you are staunchly against paying a hacker in principle, there is a serious negative impact on that risk score that reduces the recommendation.

Risk Rating:	22	49%
The higher the number, the greater the rationale for paying the ransomware		

The result is a risk rating in which the higher the value, the greater the rationale for paying the ransom. While imperfect, ProCircular believes that this quantitative approach to risk analysis has never been applied to ransomware before.

Conclusion

Like most decisions in life, resolving a ransomware attack is not a simple "yes" or "no" question. There are numerous financial, operational, and situational variables to take into account. Our opinion is that we should never rule out an option until we have had a chance to thoroughly consider them.

With a careful analysis of the risks and a little bit of soul searching, you will make more informed decisions and find the solution that best fits your organization's needs and specific threat scenario.

ProCircular
SECURITY. PRIVACY. TRUST.
2451 Oakdale Blvd. Coralville, IA 52241
www.procircular.com | solutions@procircular.com
844-95-SECUR

Bibliography

Baum, P. (2016). *Violence in the Skies: A History of Aircraft Hijacking and Bombing.* Paris: Summersdale Publishers Ltd.

Benyamin, C. (2018). *Should we negotiate with terrorists?* Retrieved from The Perspective: https://www.theperspective.com/debates/politics/should-we-negotiate-with-terrorists/

Caporusso N., C. S. (2019). A Game-Theoretical Model of Ransomware. *In: Ahram T., Nicholson D. (eds) Advances in Human Factors in Cybersecurity. AHFE 2018. Advances in Intelligent Systems and Computing* (pp. 4-10). Springer, Cham.

Masarah Paquet-Clouston, B. H. (2019). Ransomware payments in the Bitcoin ecosystem. *Journal of Cybersecurity*, Volume 5, Issue 1.

SentinelOne, Inc. (2019, May 27). *ETERNALBLUE | THE NSA-DEVELOPED EXPLOIT THAT JUST WON'T DIE.* Retrieved from sentinelone.com: https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/

Sonicwall, Inc. (2019, October 22). *SONICWALL SEES DRAMATIC JUMP IN IOT MALWARE, ENCRYPTED THREATS, WEB APP ATTACKS THROUGH THIRD QUARTER.* Retrieved from sonicwall.com: https://www.sonicwall.com/news/dramatic-jump-in-iot-malware-encrypted-threats-web-app-attacks-third-quarter/

Various. (2011, Feb 4). *What is the difference between 20$ and $20?* Retrieved from Stack Exchange: https://english.stackexchange.com/questions/11326/what-is-the-difference-between-20-and-20

ProCircular SECURITY. PRIVACY. TRUST.

2451 Oakdale Blvd. Coralville, IA 52241
www.procircular.com | solutions@procircular.com

844-95-SECUR