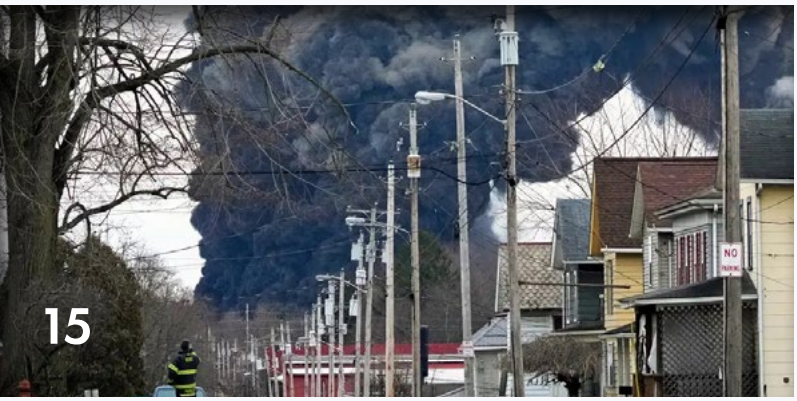
INTERNATIONAL ASSOCIATION OF CLAIM PROFESSIONALS

DECLARATIONS

2022-2023 YEAR IN REVIEW

CONTENT

2022 - 2023



FEATURES

CONTENT

Editors
Beth Diamond
John Parsley

Publisher
Catherine Kalaydjian

Designer
Teresa Ku

TO PAY OR NOT TO PAY – RANSOMWARE'S TOUGHEST QUESTION

By:
Theodore J. Kobus III, Partner and Chair, Digital Assets and Data Management Practice Group
Eric B. Gyasi, Counsel
Thomas I. Moran II, Associate

Ransomware remains a persistent and significant threat to businesses, organizations, and municipalities. With increasing frequency, threat actors faced with security measures are evolving sophisticated countermeasures to evade detection and successfully encrypt the victim's data. With a ransom note in hand and encrypted systems, victim organizations face a difficult decision – "to pay or not to pay?" The two primary reasons for a ransomware payment are for receipt of the decryption key or to prevent publication of exfiltrated data. This article begins with an overview of how ransomware occurs, factors organizations must weigh in deciding the appropriateness of payment, and the implication of this decision.

Anatomy of a Ransomware Attack

Deployment

A ransomware incident begins when a threat actor gains unauthorized access to a network. This occurs in several ways, ranging from a user clicking on a link in a phishing email, to exploitation of a public-facing remote desktop protocol, an unpatched software update, or misconfiguration of security settings. After gaining access, the threat actor conducts network reconnaissance to understand network architecture, potentially determine the location of critical and sensitive company data for exfiltration, and creation of persistence mechanisms or "back doors" to have alternate access into the environment. As the threat actor completes data exfiltration, the threat actor then denotes the ransomware executable as widely as possible and leaves a ransom note to the victim. The ransom note usually provides a link to a chat portal on the dark web where the threat actor waits for negotiations to begin.

Containment and Recovery

Upon discovery, organizations should take steps to mitigate the impact of the incident. The steps generally include disconnecting the organization's network from all external connection; initiating a forensic investigation to understand the vulnerability exploited, means of access, and range of threat actor lateral movement; and deploying a monitored endpoint detection and response solution to detect and quarantine any persistent threats to the environment. Prior to security incidents, organizations often fail to account for the length of time it takes to restore an organization's network from backup files. The answers to each of these questions, taken together, will impact the viability of the backups and the ability for the organization to restore from backups.

What makes ransomware attacks difficult to manage for organizations is that such attacks require executives to make far-impacting decisions, in an accelerated timescale, with limited information. One way to gain information during a ransomware attack is to contact the threat actor. Engaging with a threat actor is beneficial whether or not a payment will ultimately be made. First, answers from the threat actor can help guide the forensic investigation. Forensic investigations are reverse re-creation of a crime scene – in many instances the words of the threat actor help shed light on the exploited vulnerability. Second, connecting with the threat actor and requesting "proof of life" helps the organization determine the type of exfiltrated data and which parts of the network may be affected. Understanding the data that was stolen will help organizations assess their legal risk, business risk, and ultimately, whether a ransom payment should be made. Next, connecting with the threat actor begins the process of obtaining a decryption key – should one be needed to accelerate the recovery and rebuild process. Organizations need time to determine whether or not restoring from a backup is possible and practical. And, engaging with the threat actor helps the victim company assert more control. If the threat actor is ignored, they will do whatever is necessary to gain your attention, often by contacting executives, board members, employees, and other stakeholders.

Assemble Incident Response Team

Many organizations as part of their cybersecurity protocols deploy and maintain defensive software across their network. With defensive software and tools in place, often, organizations receive alerts early when suspicious or unauthorized activity is detected on the network. The difficult aspect, like much of 21st century life, is assessing the voluminous quantity of daily data and alerts which often means signals and alerts are missed. When an organization's security apparatus notices suspicious or unauthorized activity, organizations should implement their incident response plan as appropriate. A properly drafted incident response plan will guide the organization to engage cybersecurity counsel to initiate a coordinated incident response process. Counsel can then engage a cybersecurity investigation firm on the organization's behalf to conduct a privileged forensic investigation and negotiate with the threat actor.

Is Payment to the Threat Actor Needed

In most situations, organizations consider making ransom payment to obtain a decryption key or to prevent the publication of data. On the other hand, organizations will consider not making a ransom

payment because of the cost (even with insurance reimbursement), perceived reputational impact, potential sanctions liability, and general corporate philosophy against engaging with threat actors. Time is a critical piece of leverage both parties are attempting to gain in ransomware attack. For the threat actor, a poorly-prepared organization has very little time for which their business can withstand the business impact. For a well-prepared organization, paying a ransom immediately or shortly after an attack is not an imperative. The longer the organization can wait, the greater the payment "discount." In short, the direct impact to business revenue – in the immediate aftermath and the medium term – is a key driver in the discussion and decision to pay for a decryption key.

Taken together, the question of payment to a threat actor is a dynamic decision, which requires an analysis of the following key factors:

- **Operational Impact** – assessing the impact of the incident on your network's capacity and organization's operations;
- **Identity** – the identity and behavior of the threat actor;
- **Ransom Demand** – price of the ransom demand;
- **Recovery timeframe** – recovery timeframe with or without a decryption key; and
- **Sensitivity** – importance/sensitivity of the data taken or encrypted during the incident.

While the analytical framework remains the same, no two organizations are alike. The unique fact-specific circumstances of each situation will weigh differently as an organization contemplates a ransomware payment decision. In addition, organizations that are successful with this analysis utilize the expertise of a cross functional teams across their enterprise to assess, develop, and complete this analysis.

Crucially, an organization must also determine if payment is feasible. Payment is possible where the threat actor is not subject to sanctions or other regulatory restrictions by the United States Treasury's Office of Foreign Asset Control ("OFAC"). Still, ransom demands are once again increasing to the point where a payment is not justified. An unemotional approach to negotiations should be taken while carefully considering the various data points.

Assessing Operational Impact

A ransomware attack attempts to encrypt the highest possible percentage of a network. In some cases, the attack succeeds in encrypting one hundred percent of a network environment, while in other attacks it is a lower percentage. Similarly, in some incidents, key systems are locked down while in other matters the systems are not as critical, Determining if a decryption key is needed and how urgently it is needed is dependent on the operational impact to the victim organization. If business-critical backups are viable and restoration is possible with limited interruption, then the organization may be able to continue to conduct business through the restoration process, making the key less valuable. If business-critical systems and the respective backups for each such system are encrypted, this increases the urgency for a decryption key and decreases the leverage an organization has in negotiating with the threat actor.

Additionally, engaging with the threat actor early in the incident, as mentioned above, may provide the victim organization with additional information needed to determine the full scope of data involved in the incident. As part of negotiations, the threat actor may provide a file tree, which lists the data purportedly taken from the network. If an organization receives a file tree early in the process, the organization can review the files listed and determine the importance, from a reputationally and operationally, of the claimed exfiltrated data from the network.

What is the identity of the threat actor?

When legal counsel engages a third-party firm to conduct negotiations, those negotiations can provide additional color, context, and insight into the ransomware group and its tactics. While most groups name themselves in the initial ransom letter, there may still be more complexity in determining which threat actor is responsible for the incident or if an affiliate of the group of the identified threat actor is actually involved. It is important to understand this nuanced point. Some ransomware groups license their malware to individual actors or groups who use the ransomware

Most Commonly Observed Ransomware Variants in Q1 2023

Rank	Ransomware Type	Market Share %	Change in Ranking from Q4 2022
1	BlackCat	12.6%	+2
2	Black Basta	11.8%	-
2	Royal	11.8%	+2
3	Hive	7.1%	-2
4	Lockbit 3.0	6.3%	+3
5	Phobos	4.7%	-
5	BianLian	4.7%	New in Top Variants
6	Play Ransomware	3.9%	New in Top Variants

Market Share of the Ransomware attacks

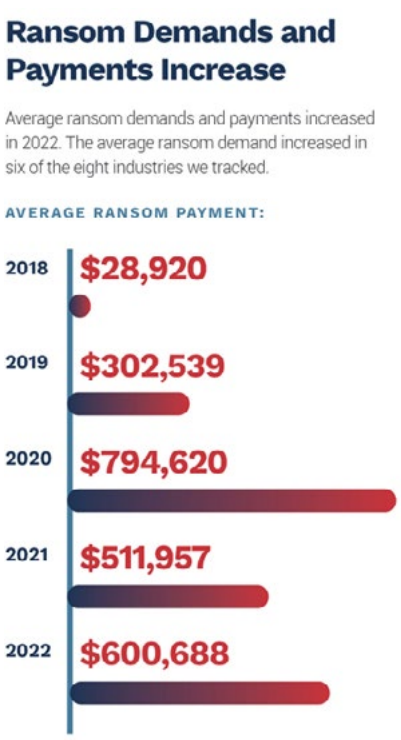
and are only loosely affiliated with the variant. These actors may be less predictable, less reliable, and may be more volatile. However, some groups are structured more like corporations and rely heavily on their reputation to make good on their promises, thus resulting in more efficient, predictable, and even-keel negotiations.

Developing an understanding of the threat group faced by an organization will help determine how quickly negotiations progress and if the threat actor is likely to provide the agreed-upon deliverables upon payment. As an example, the Hive ransomware group was well known for its volatile behavior – oftentimes calling employees or clients of a victim organization to spread the word about the incident and raise alarm that sensitive data has been exfiltrated from the network. While Hive's behavior was unnerving, and a source of anxiety for an organization, it also may have disincentivized the victim organization from providing payment to prevent the publication of data – as Hive already reported the incident to third parties.

Most importantly, organizations need confidence that the agreed-upon deliverables will materialize; the deliverables usually include a decryption key, proof of deletion, a promise not to attack again, and in some instances an overview of how the threat actor gained access to the environment. Note, paying a ransom to avoid publication does not pobviate the need to comply with breach notification laws. If a threat group has a reputation for re-extorting victims, i.e., demanding more money after payment has already been made, then organizations need to assess its risk tolerance in reaching a decision.

Can We Afford This?

Perhaps too obvious a point is that ransom demands can only be paid in instances where the organization can afford a payment. It is not unusual for organizations to rely on insurance dollars to reimburse an organization for their ransom payments. Depending on the organization's insurance policy, funds are set aside specifically for ransom payments, or the payments drawn from the overall pool of coverage dollars. Other work streams which may affect the overall money available include legal analysis, a forensic investigation, threat actor negotiations, and restoration assistance. Additionally, if insurance is unavailable or exceeded, organizations may also pull from their reserves or operational budget to complete a payment.



Ransom demands can sometimes be prohibitively expensive as threat groups may think they have hit a different, larger organization, or they have misread a document stolen from the environment which suggests that revenue is greater than it is. In these situations, negotiations with the threat actor will need to focus on obtaining a drastically reduced demand, which is sometimes achievable with certain threat groups. However, the negotiation process always takes time, and there are risks and benefits associated with extended ransom negotiations; below is a detailed discussion of this aspect.

How Long Will This Take?

Organizations With Substantial Operational Impact

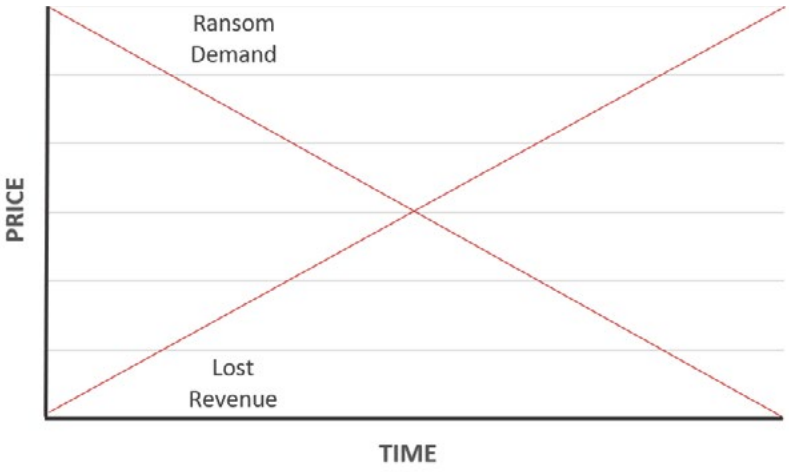
A difficult truth about ransomware negotiations is that achieving a substantial reduction in price takes time – usually at least a week. This is especially difficult when the victim organization is fully encrypted or is inoperable as a result of the event, as everyday potential revenue and profits are lost.

In these situations, the organization first needs to determine, as a baseline, if it can afford the initial ransom demand. If the initial demand is, for lack of a better term, affordable, and a decryption key is needed for restoration, then the organization may be inclined to conclude negotiations quickly in order to receive a decryption key. If, however, the initial ransom demand is beyond the organization's budget, or willingness, to pay, then the organization will need additional time to achieve a reduction in price that the organization to afford.

Ransomware Timeline

Year	Demand to Payment	Demand to Payment for Payments <$1M	Demand to Payment for Payments > $1M	Encryption to Restoration
2020 Average	8 Days	7.4 Days	9.2 Days	13 Days
2021 Average	11.1 Days	13 Days	9.8 Days	12.2 Days
2022 Average	14.2 Days	14 Days	14.9 Days	12.7 Days
2022 Median	11 Days	11 Days	15 Days	8 Days

As an example, the illustration included here shows time as the X-Axis and price as the Y-Axis. At some point, assuming that the operational impact to the organization is significant, the cost associated with lost revenue will become greater than the cost of obtaining a decryption key. Early in the negotiation process, organizations should work to determine when that date will occur in order to achieve an affordable settlement in advance of the revenue loss exceeding the demand.



Organizations with Limited Operational Impact

In instances where businesses can continue critical operations, even only on a limited basis, during the negotiation process, additional time creates leverage to substantially reduced ransom demand. Because the organization can continue operations during the negotiation process, the date in which the cost of the ransom demand will exceed the lost revenue is pushed several days (or even weeks) later than if it had not been able to conduct business during the negotiation process.

How Sensitive is the Data Involved?

While restoring business operations is usually the primary consideration for making payment to the threat actor, some organizations are inclined to pay to prevent the publication of sensitive information. For instance, if the file tree provided by the threat actor indicates that the exfiltrated data taken from the network includes proprietary information undercutting the organization's advantage with competitors if it where to be made public, the rationale for payment increases materially. As a hypothetical example, if an organization had a trade secret stolen, such as a secret formula for a soft drink, the inclination would likely be to take the steps needed (including ransom payment) to mitigate the chances of publishment. Depending on the jurisdiction of a litigation matter following the breach, organizations may also consider the potential to affirmatively assert that the organization made payment to avoid public disclosure. It is meaningful to note threat actor "publication" often occurs in the deep and dark web. Loosely defined, deep and dark web refers to the unindexed portion of the internet where navigation is difficult and access to criminal forums, websites, and chatrooms are governed through special admission and passwords. In short, even when a threat actor does publish exfiltrated data in the deep and dark web, the unindexed and password access nature of the deep and dark web makes regular and easy access difficult.

Still, the "proof of deletion" provided by threat actors is often just a screenshot of data deletion from a folder. In the end, an organization must rely on the threat actor "business model," so no perfect proof is ever available to verify that the threat actor did not make copies of the data or save it in another location. Unlike a decryption key, which is tangible, and the efficacy of which can be validated – paying to prevent the publication of data is based solely on a promise made by a threat actor. For these reasons, the prices paid solely to prevent publication of data are often substantially less than if a decryption key is needed.

The Logistics of Ransom Payments

If, based upon the factors listed above, an organization decides that making a payment to the threat actor is necessary, there are still several procedural hurdles before payment is completed. Before tackling the procedural hurdles, organization need to identify – before an incident – the decision makers on the question of ransom payments. In many instances, the decision is made by a small group of senior leaders with subject-matter input from heads of functions, and members of the information security team. The hurdles are as follows: (i) the veracity of the decryption keys; (ii) the agreement as to the full scope of threat actor deliverables; (iii) compliance with relevant state and federal laws; (iv) obtaining funds from the insurer (when the organization is insured); and (v) transferring sufficient funds to the entity making the payment;

confirmation of all steps prior to payment to the threat actor is standard best practices.

Finalizing Negotiations with the Threat Actor

Before transferring payment to the threat actor, the negotiator first needs to determine if the decryption key works – this is the "proof of life" process. In this instance, the organization sends a handful of encrypted files containing non-sensitive information to the threat actor. The threat actor will decrypt and return the decrypted files, thereby proving that the decryption key works. Skipping this crucial step may result in payment for a decryption key that does not work or one that only works with certain files.

Based upon the organization's insurance policy, the organization may also need to prepay the money to the vendor and wait for reimbursement. All insurers will require a compelling business rationale – including certain procedural steps – in advance of payment approval and funds transfer. Additionally, it is imperative to clearly delineate the deliverables the organization will receive in exchange for payment – as this will be crucial to business rationale analysis. As referenced previously, this includes a decryption key, proof of deletion, a promise not to attack again, and in some instances an overview of how the threat actor gained access to the environment.

Compliance with Relevant Law

No federal laws have been enacted to prohibit ransom payments in connection with cyber attacks. OFAC has utilized an interpretation of two national security laws – International Emergency Powers Act and the Trading with the Enemy Act – in an attempt to restrict payments to certain restricted individuals and embargoed countries. As such, OFAC has taken the position that U.S. persons are strictly liable for any payments made to a specifically designated national. OFAC maintains this list on its Specifically Designated Nationals and Blocked Persons List ("SDN List"). Victim organizations and professional services firms providing support in a ransomware incident are expected to conduct suitable diligence to ensure any payments made is to not to member on the SDN List.

In 2020 and 2021, OFAC issued additional guidance outlining expectations for organizations prior to completing payment to a threat actor. The most recent guidance, titled "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" emphasizes the government's general position that, as a best practice, it opposes organizations making payments to threat actors but stopped short of a general prohibition. The guidance requires the victim organization to notify law enforcement (among other best practices) – typically the FBI via its Internet Crimes Complaint portal – when a ransomware incident occurs and in advance of transferring payment to a threat actor. When possible, cooperation with any ongoing FBI investigation into the threat group is encouraged.

In short, legal counsel for a victim organization will coordinate the diligence needed to ensure that payments are not in violation of OFAC guidelines. Elements of the diligence process includes aggregated data compiled during the incident response process, including the Bitcoin wallet address of the threat actor, indicators of compromise, and other evidence which may help determine the identity of the threat actor or group. Law enforcement groups and regulators utilize this data to determine if the threat actor is a sanctioned entity or has a nexus to a sanctioned entity or on the SDN List. If the threat actor turns out to be a sanctioned entity or on the SDN List, any payment made to the threat actor is a strict liability offense; the two laws, in this case, does not provide for a knowledge element on behalf of the victim organization or any professional services firm that may be assisting the victim organization. It is critical for organizations to follow advice of counsel in determining to proceed with a ransom payment.

Receiving the Key

Assuming the organization completes the steps outlined above, then it is ready to receive the decryption key and other deliverables. Before the key is deployed to the environment, it is first tested in "sandbox" – a secure, isolated environment where the key's code is observed and analyzed to ensure that it contains no malware. After the forensic firm verifies that the key is not malicious, decryption occurs in a prioritized order, allowing business-critical operations to resume as soon as possible. It is important to understand that receiving a decryption key is not a "magic button." Rather, the

decryption process usually takes days or even weeks to deploy the key across the network and decrypt the systems involved.

Conclusion

All organizations are different, and each will have a unique set of considerations to weigh in deciding to make a ransom payment. Moreover, each ransomware incident affects organizations differently – with some completely out of business and others able to restore from viable backups in a matter of hours. Before reaching a decision, consideration of each factor discussed herein, and the factors taken together will drive the organization's decision regarding payment. With a decision made, the proper execution of each step ensures compliance with relevant laws.

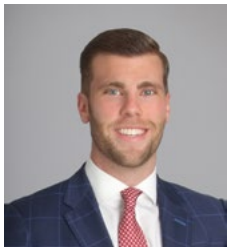
About the Authors

Theodore J. Kobus III
Partner and Chair, Digital Assets and Data Management Practice Group
New York
+1.212.271.1504 | tkobus@bakerlaw.com

Ted has been a leader, mentor and counsellor in the digital risk space for more than 20 years. He has earned authority in the areas of privacy, data security and cybersecurity, leading clients to entrust him and his attorneys with more than 15,000 data breach responses. Businesses, government and other organizations turn to Ted for sound advice on compliance, developing response strategies, breaches implicating domestic and international laws, and defense of both class action litigation and regulatory actions. Ted leads the fastest growing practice group at the firm, the Digital Assets and Data Management Practice Group, which was formed in January 2020 and focuses on the data lifecycle. Ted is also serving his third three-year term on the firm's Policy Committee.

Eric B. Gyasi
Counsel
New York
+1.212.271.1514 | egyasi@bakerlaw.com

Eric B. Gyasi provides proactive and strategic guidance to help clients address cybersecurity enterprise risk management, and he leads clients through the response to security incidents. Eric is uniquely qualified to help clients navigate the legal and business risk issues at the intersection of incident response and cybersecurity regulatory enforcement due to his legal acumen paired with his crisis communications and digital forensics background. A strategic thinker valued for his business-minded judgment, Eric advises boards of directors regarding the duty of oversight related to cybersecurity and the executive management team on compliance with complex regulatory requirements in a risk- informed manner.



Thomas I. Moran II
Associate
Cleveland
T +1.216.861.7142 | tmoran@bakerlaw.com

Tom Moran provides counsel to clients during data security incidents ranging from phishing incidents to large, high profile data security incidents. Following a data security incident, he advises clients on the legal ramifications and liabilities that may occur as a result, and assists them in fulfilling any legal obligations that may arise from the event. He also coordinates and oversees vendors that assist with the incident response process.