

So You've Been Hit by a Ransomware Attack? Now What?

Jami Vibbert, et al.





Arnold & Porter

June 16, 2021

So You've Been Hit by a Ransomware Attack. Now What?

Advisory

By Kenneth L. Chernof, Ronald D. Lee, Jami Vibbert, Alex Altman

With ransomware attacks on the rise, potential targets in sectors including **retail**, **food**, **healthcare** and life sciences, **critical infrastructure**, financial services, and **government** must face the increasing likelihood that nefarious global actors will take their most critical systems hostage.

Am I the Victim of Ransomware?

Not every hacking event counts as “ransomware.” At its most fundamental, ransomware is malicious software deployed by bad actors to encrypt or otherwise make the victim’s data unavailable until a ransom is paid. The specific nature of these attacks is evolving, however. In the past, hackers would simply encrypt a target’s systems and then hand over the decryption keys (most of the time) once the ransom had been paid. Increasingly, however, hackers are now also stealing data that has been encrypted and threatening to release that data publicly or to sell it on the dark web. Any malware is bad malware, but ransomware comes with a specific set of consequences and obligations. If you have been hit with ransomware, you will want to take certain steps.

What Can I Do Once My Systems Are Held for Ransom?

As ransomware methods evolve, so will the resulting business and legal consequences. Although a megabyte of prevention is worth a terabyte of cure, there are steps you can—and should—take if hackers hold your systems for ransom to minimize the consequences and mitigate future risk. These measures are listed in a roughly chronological order, but many may take place simultaneously or in a different order depending on the nature of the attack.

Follow the Plan (If You Have One)

If you find that your systems have been locked up, the very first measure you should take is to consult your incident response plan (IRP), if you have one. Ideally, your IRP should address the measures below. If you do not have an IRP, you will want to implement one once the dust has settled and you have learned lessons from the ransomware attack. Or better yet, if you do not have one, you’ll want to develop and test an IRP before you become victim to a ransomware attack (that means now!).

Coordinate Your Resources and Consult Counsel

Identifying and coordinating key internal and external resources is key to an effective response. Of course, IT and information security will be heavily involved, along with one or more external forensic consultants and information security advisers. But human resources (if employee data is impacted), public relations/communications (to craft a public and internal response strategy), and finance may also have roles to play. Importantly, involving in-house and/or retained counsel early in the process is a best practice. As explained below, you may have legal obligations to notify third parties within a very narrow

timeframe and counsel should be able to shepherd this process. Moreover, having counsel direct the investigation and response can help maintain the privileged nature of certain communications and ensure the best response for mitigation of future risk (whether in the form of litigation or a regulatory investigation).

Stop the Attack!

Make sure the hacker is not still in your house! One of the most critical things to do is to make sure that the attack is over, any vulnerabilities have been remediated, and that you have made sure that the ransomware cannot spread to other, as-yet-unaffected systems. For example, you may be able to patch a system vulnerability that allowed the malware to penetrate your systems.

At the same time, begin to understand what data and systems (may) have been affected and how to stop further harm as it relates to that data or those systems. It is common for organizations to wall off certain systems to prevent the spread of ransomware, and different types of data come with different business and legal risk. You may be in the fortunate position that the data and systems subject to ransom are not particularly sensitive and data may be restored using backups. Even backups, though, are becoming less of a cure all as many ransomware attacks now exfiltrate (instead of just encrypt) systems. Even while systems are locked up, you may be able to remediate some of the risks. For example, you may be able to patch a system vulnerability that allowed the malware to penetrate your systems. If the malware entered your system through a phishing scheme, you may also be able to update your email filters and provide expedited training to prevent other incoming attacks.

Investigate

The heart of the ransomware response will be an ongoing investigation as to the causes, attack vectors, and impacts of the attack. This can, and often should, involve the retention of an external forensic investigator (and for less serious attacks, internal forensics team). In either event, it is a best practice to have the forensic team work at the direction of legal counsel to preserve privilege, to the extent possible.

Remediate

For remediation not done at the initial stages to ensure the attacker cannot continue to infiltrate your systems, any other gaps identified as part of the investigation should be addressed. This could include additional process controls, auditing, training, or third party diligence.

To Pay or Not to Pay

The **\$11 million** (or more) question is whether you should pay the ransom at all. It may be tempting to simply comply with the hacker's demands in the hopes you can get back to business (studies show that **more than 50% of ransomware targets end up paying**, with less than 25% getting their data back), but this is not always wise, or even legal. **The FBI generally advises companies not to pay ransoms but acknowledges that payments may be justified in some circumstances.** The US Department of the Treasury's Office of Foreign Assets Control (OFAC) has stated that **some ransomware payments may constitute violations of economic sanctions laws.** Even if you are inclined to pay, you will have to consider whether the systems will actually be decrypted, whether the attacker could still leak your data, and whether the attendant legal and remediation costs make the payment of ransom financially impractical.

Contact Law Enforcement

In many instances, you will want to notify law enforcement (e.g., **FBI, Secret Service** or state bureaus of investigation) of the ransomware attack before responding to a ransom demand. Instead of struggling alone, you may be able to lean on law enforcement experience to better understand what your options are with respect to particular threat actors and how to prevent future incidents. In some cases, particularly if there is reason to believe that a foreign government or other national security matters are involved, you will want to notify additional government agencies.

Understand Your Sector

Organizations in certain highly regulated sectors may have specific obligations in the event of ransomware and other cybersecurity incidents. If you have not already done so (or if your IRP doesn't contemplate it), counsel should determine what sector-specific actions must be taken, including early involvement of regulators or law enforcement.

Notify Third Parties (When Necessary)

Depending on the data and systems involved (which you should understand based on your assessment and investigation), you may have to notify a number of third parties. Under certain breach notification laws, like the GDPR and some state statutes, you may have a very narrow timeframe to notify the relevant regulator and individuals. This patchwork can be complex to navigate as these laws vary greatly depending on the type of data at issue as well as whether the data was "acquired" or merely "accessed." You may also have contractual obligations to notify customers or vendors. In addition, you may need to set up websites and call numbers, notify consumer reporting agencies, engage with the card brands, and purchase identity theft protection services, all depending on the nature of the attack and the relevant breach notification statutes. As if that wasn't enough, if you are a public company, you may also have SEC reporting obligations.

Prepare for Government Investigations and Litigation

If you are in a regulated industry such as healthcare, finance or critical infrastructure, you are likely to face some sort of government investigation. Even consumer products and services and most apps could face FTC or state AG investigations, which are common. Litigation resulting from ransomware is also becoming increasingly common. Where consumer data is involved, private rights of action under the California Consumer Privacy Act, state consumer protection laws, and a growing body of state privacy laws may lead to class action litigation. You may also face claims from business customers whose operations are disrupted in breach of an agreement and inquiries, investigations, or contract actions from government customers. Again, early involvement of legal counsel will be critical in assessing legal exposure and preserving privilege and work product protections in preparation for investigations and litigation, as well as keeping in mind risk reduction in these scenarios.

Call Your Insurer

Although not ubiquitous, more and more companies are obtaining cyber insurance to mitigate against hacking losses, including in ransomware attacks. As a matter of simple compliance, you may have notification obligations to your insurers. Moreover, your insurer's experience may be leveraged to help you navigate the process. Additionally, understanding your right to reimbursement or indemnification early in the process can help you choose the best course of action. In some instances, the policy may limit your choice of outside counsel, forensic consultants, and other service providers.

Adapt and Evolve

Even the most sophisticated organizations will learn a number of lessons from a ransomware attack. These lessons should be memorialized and drive change within the organization. Establishing or updating IRPs is the most obvious action you can take to mitigate future ransomware risk. You may also want to audit the security programs of any vendors who may have been compromised. You can also revise information security processes or even undertake significant IT infrastructure projects to reduce the likelihood of future attacks.

© Arnold & Porter Kaye Scholer LLP 2021 All Rights Reserved. This Advisory is intended to be a general summary of the law and does not constitute legal advice. You should consult with counsel to determine applicable legal requirements in a specific fact situation.