November 5, 2021

Why You Will Pay the Ransom (Hint: It's Not the Ransomware) and How to Avoid Paying

by Jon Neiditz

Everybody is talking at you about ransomware, but you do not need to hear most of what they are saying, because they are talking about something they have not seen hundreds of times, so they have not been following the rapid evolution of the painful decisions you must anticipate. The biggest issue almost all of them miss is that for the vast majority of companies, payment of the ransom is no longer about getting the decryption key for the ransomware at all; it is simply about protecting sensitive information from publication, so the ransomware itself amounts to little more than a hard-to-miss delivery system for a threat (on all now-encrypted files) of insurable risks less about business interruption than about publication.

1. **Ransomware and Backups**: Our clients have known since 2016 – when ransomware became capable of spreading quickly across vast networks – that the best way to avoid paying ransoms was to make sure that usable backups were very well protected against the ransomware tide rolling in. Yes, since then the ransomware has become more patient; the attackers learned to "live off the land" to try to get to the backups before deploying the ransomware, but the defenders got better both at detecting the attackers and protecting the backup data.

   In those olden days of mere ransomware – encrypting your network often with no exfiltration of your data – the decision to pay was usually a close and difficult call, even though the ransom demands were orders of magnitude lower than today's. For example: Were your backups good enough? How much time would it take to restore and rebuild with the decryption key versus without? Can we trust this threat actor if we pay?

2. **Publication, Sensitive Personal Data and Crown Jewels**: Those days are gone, thanks to "ransomware plus," which for years now has been the leading cybercriminal business model, sending routine ransom demands into the (many) millions. The "plus" part is the exfiltration and threat of publication, which is often a "breach" as a matter of law, but not – as we spend a lot of time explaining to customers, regulators and media – a breach as commonly understood; in other words, nobody is stealing your customer, consumer or employee data to sell it to identity thieves. Why should they bother with data theft and selling when they can be paid so much more and quickly by just threatening to publish?

The hard truth is that you will have to pay (not millions; see #3) unless you have done something harder than fixing your backups as in #1; you must have fixed where you process and store sensitive data. Many of you outsource the systems in which you process sensitive and notice-triggering customer, consumer and/or employee data with companies that can afford to keep up with the threat actors; if so; the publication threat problem arises if you allow sensitive personal data to be copied to shared and personal drives, and also if you keep your most important secrets or "crown jewels" on those drives. The threat actors are particularly good at finding the sensitive personal data so they can show you they took a copy. Bottom line, when they do that: You will probably pay to protect your customers.

3. **Negotiation, Payment, Hardening and Detection**: Having now seen hundreds of companies and governments face that hard truth, we can also offer you an equally-strange piece of good news: Negotiation can work wonders with ransomware plus threat actors, who may first consider themselves to be Robin Hood and you to be the Sheriff of Nottingham. Let us say you're a small community company or local government still suffering from COVID. There are so many powerful, sad stories that you should make sure to tell. Discounts of 80% or even 90% off the original ransom demands are achievable, and not needing the decryption key, you can take the time to get the lowest price. We just helped a small county get a 93% discount that it could proudly publish to show its citizens that both their tax dollars and sensitive personal data were protected.

Be prepared to negotiate – including learning all about the credibility and M.O. of the threat actor from experts and the FBI – as well as to obtain cryptocurrency and perform/obtain OFAC checks. Harden your systems and deploy sensors quickly after the attack, so if and when you explain how you protected personal information, you will not be as vulnerable. (Those who proclaim that negotiation or disclosure of ransomware only makes you more vulnerable have not figured that sequence out.) Then you can start to deal with the hard truths, for example that this probably all happened because an employee clicked on a phishing email (think multi-factor authentication and anti-phishing training), and the big hard #2 truth of data management.