SHOULD YOU PAY A RANSOMWARE RANSOM?

PREPARING FOR A RANSOMWARE ATTACK

www.dig8ital.com

dig8ital

Contents

Ransomware hacks are increasingly in the headlines, and it appears that the problem is only getting worse. In fact, 71% of German cyber professionals said that remote working has made cyber attacks worse (source), and 83% of Spanish respondents said attacks are growing more sophisticated (source).

So, if your company comes under threat, you're going to be faced with a big question: Should you pay the ransom, or not pay? In this guide we will explore this question, discuss the ramifications of either paying or fighting back, talk about the legality of paying, and offer a few tips to help you out.

1

Should you pay a ransomware ransom?

To pay or not to pay - it really is the big question. Every minute of downtime could cost your business a small fortune, and at first it's likely going to seem that paying is quicker than not paying. So, let's really drill into the discussion - should you pay, or not pay?

It will seem simplest to pay. But, while quick, it may actually be the worst thing you could do. You see, the thing is, paying a ransom demand quickly and efficiently could show that your organization is willing and able to pay up. This may encourage attackers to target you again in future - you've set yourself up as 'easy money'.

Our advice would be to never pay. Even though it will hurt, even though it will cause stress and anxiety, even though it may take longer, it's highly advisable that you don't pay. You negotiate.

"Even though it will hurt, it's advisable that you don't pay. You negotiate."

Hire a professional negotiator or work with a police negotiator if this is available to you in your area. Don't just look for an IT or business negotiator - you want someone with professional hostage negotiating experience, or equivalent skills. Because in this case, you're the hostage. You cannot accept the first ransom. Chances are, you can negotiate it down.

1

WON'T NEGOTIATING MAKE THEM ANGRY?

If your company puts its foot down and negotiates, it makes it harder for criminals to extort your business. Even if you end up paying out at the end of the experience, you made it take longer and added frustration to the process - not just for you, for them. One thing to keep in mind is that attackers tend to target more than one business at a time. In some cases it may be hundreds at a time. If yours is the one that makes it difficult, why would they bother with you in future when there are many other options? You've just, likely, reduced the chance they'll come for you again.

That said, depending on your situation you may struggle to push the ransom demand down - especially if the attacker has encrypted a vital system, or you don't have any good backups. That puts you on the back foot, and gives them leverage. But you can still negotiate, make it more difficult, try to add that element of frustration (with professional help from a negotiator), to make yourself a less appetizing target in future. It may help you tomorrow, if not today.

CASE STUDY

JBS Foods

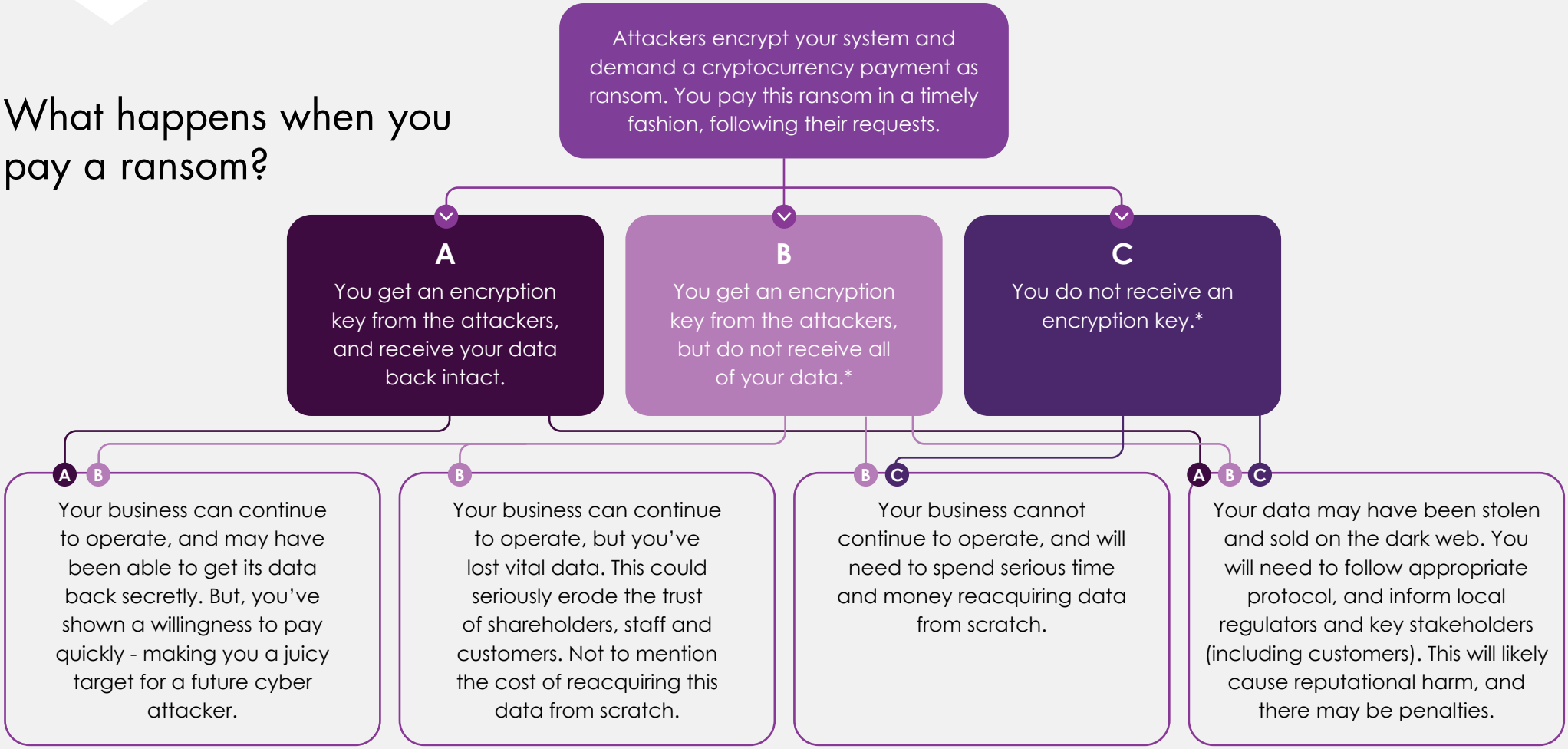
JBS is one of the world's major meat producers, leading the market in sectors like poultry, beef and lamb, with subsidiaries all over the world. You can imagine, then, the damage caused when REvil, a prolific Russia-linked ransomware group, struck JBS via what was believed to have been stolen credentials (the attack vector isn't known, but stolen JBS login credentials were leaked on the dark web). REvil supposedly stole over 5 terabytes worth of data, shutting down JBS operations temporarily in the US, Canada and Australia.

Initially, the group demanded a ransom payment of US$22.5 million (€20.7 million), but the company didn't just pay up. While operations were shut down, the company negotiated. Hard. They brought the ransom down to just $11 million, which they then paid to resume operations within a few days.

Had JBS just paid, it would have cost twice the amount and made them a future target. But, negotiating cut the price in half, got them up and running within a few days of paying, and showed attackers that they wouldn't just bow down.

2

What happens when you pay a ransom?



Note how even if you pay and get all of your data back, it's still possible that your company will face serious reputational harm and/or punitive measures from legal authorities. Paying is rarely as simple as it sounds.

*96% of companies claimed in 2021 that they got their data back after a 'significant' attack, leaving 4% who did not. However, only 65% of encrypted data was restored on average, meaning companies are losing potentially just over a third of their data. (Source: Sophos The State of Ransomware 2021).

3

Is paying a ransom legal?

WHEN PAYING IS ILLEGAL*	WHEN PAYING IS LEGAL
When the cyber attacker group is a designated terrorist organization.	Most other ransomware situations.
When the cyber attacker group is located within a sanctioned jurisdiction.	That said, paying a ransom, as discussed above, is always discouraged.
When the cyber attacker as an individual is themselves sanctioned.	Paying only encourages cyber attackers to continue their attacks.
When you are a company (i.e. insurer) helping another company make a payment to a terrorist or sanctioned group/individual.	

* Based on advice from both the United States Department of Treasury and Council of the European Union.

Why is it *not* illegal?

You can probably imagine how much the legality of paying has been debated in both IT and legal circles, and increasingly so as the problem has gotten worse. If paying ransoms is so dangerous, why are companies allowed to do it at all?

Here's how the issue stands at the moment (although check back with us in a year or two and the landscape will likely have changed - it's evolving quickly): If paying ransomware demands is made illegal, it's probable that criminals would shift their focus to companies which cannot afford any downtime while they get their data back through other mechanisms.

That means organizations such as hospitals, utilities, nuclear facilities, perhaps banks as well, would all become bigger targets than they already are. And trust us when we say they are already big targets. Making it illegal wouldn't make ransoms stop, because these facilities will always be vulnerable.

Because of this threat, it's unlikely at the time of writing this guide that paying ransoms will be made fully illegal in the near future.

4

Preparing for a ransomware attack

An attack on your company is inevitable - or at least, that's the best mindset to have. While we'd like to say that attacks can be 100% mitigated even with the biggest budget in the world, we'd be lying. Anyone who offers complete protection is, quite honestly, offering a product which does not exist.

But what you can do is prepare as much as you can, reduce the risk, and show attackers that your company isn't worth the bother. Rather than focus on 100% security, focus on preparing the best possible security that you can achieve.

THIS CHECKLIST OF 10 THINGS TO DO TO PREPARE SHOULD HELP YOU GET STARTED

1. Always use up-to-date antivirus and beware of emails, websites and files that you don't recognise.
2. Keep your company's computers (and any software/apps) patched with the latest security updates.
3. Create a whitelist of apps your company knows are safe and block the rest. Create a process for staff to request new apps in case you miss any.
4. Restrict use of personally owned devices.
5. Maintain close observation and control of system user access, especially for admin accounts.
6. Teach staff about cyber issues and common threats, to build cyber awareness.
7. Plan and test data backups of your system, and ensure that system restoration actually works.
8. Secure and isolate backups of important data so they cannot be attacked via the main IT system.
9. Develop and implement an incident recovery plan to ensure that the right people know what to do, in what order of priorities, in the event of a breach.
10. Maintain and update a list of emergency contacts for ransomware attacks, including internal teams and external agencies, like law enforcement, regulatory bodies and negotiators.

For more detail and more tips, check out our article:
10 QUICK WINS FOR PROTECTING AGAINST RANSOMWARE

Need help? We're here for you

At dig8ital, we're here and ready to assist. We have a wide range of expertise to help you plan, implement and maintain a raft of cyber security, privacy management, risk management and incident response measures to ensure your company is as prepared as it can be for a potential ransomware threat.

To learn more about how we can help your unique business, contact us for a free consultation.

W: dig8ital.com
E: contact@dig8ital.com

dig8ital