520.743.7554
info@computerdimensions.net
www.computerdimensions.net

Ransomware Attacks: To Pay Or Not To Pay?

This year has seen an escalation in the number of ransomware attacks striking organizations, with both private and public sector agencies like local government and education firmly in the firing line of ransomware. Often understaffed and under resourced, affected businesses are at the sharp end of the dilemma: to pay or not to pay? It's a quandary that has technical, ethical, legal, safety and, of course, financial dimensions. Let's explore the arguments both for and against. Our aim is to describe the implications and rationale from both angles across several different considerations.

Is Paying a Ransom to Stop a Ransomware Attack Illegal?

It may seem odd to some, but it isn't illegal to pay a ransomware demand, even though the forced encryption of someone else's data and demand for payment is itself a federal crime under at least the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act, as well as many laws passed by State legislatures. One might argue that the best way to solve the ransomware epidemic would be to make it illegal for organizations to pay. Criminals are naturally only interested in the payoff, and if that route to the payday was simply prescribed by law, it would very quickly lead both to companies exploring other options to deal with ransomware and, at least in theory, criminals moving toward some other endeavour with an easier payout. The idea of outlawing the payment of ransomware demands might seem appealing at first, until you unpack the idea to think how it would work in practice. Publicly traded companies have a legal duty to shareholders; public service companies have legally binding commitments to serve their communities. A law that threatened to fine organizations, or perhaps imprison staff, would be hugely controversial in principle and likely difficult to enforce in practice, quite aside from the ethics of criminalizing the victim of a crime whose sole intent is to coerce that victim into making a payment. Imagine a prosecutor attempting to convince a court that an employee – whose actions, say, restored a critical public service and saved the taxpayer millions of dollars after authorizing a five-figure ransomware payment – should be jailed. How would that, in principle, be different from prosecuting a parent for securing the safety of a child by paying off kidnappers? It doesn't look like an easy case to win, particularly when the employee (or organization) might cite legitimate extenuating circumstances such as preserving life or other legal obligations.

Is It Prudent To Pay a Ransomware Demand?

Even if we might have a clear idea of the legal situation and a particular take on our own ethical stance, the question of whether to pay or not to pay raises other issues. We may still feel inclined to make an unethical choice in light of other, seemingly more pressing concerns. There is a real, tangible pressure on making a choice that could save your organization or your city millions of dollars, or which might spare weeks of downtime of a critical service. A case in point: recently, three Alabama hospitals paid a ransom in order to resume operations. The hospitals' spokesperson said: "We worked with law enforcement and IT security experts to assess all options in executing the solution we felt was in the best interests of our patients and in alignment with our health system's mission. This included purchasing a decryption key from the attackers to expedite system recovery and help ensure patient safety." This "hard reality" perspective is reflected in recent changes made to the FBI's official guidance on ransomware threats. "…the FBI understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers." However, the possibility that the criminals will not hold up their side of the bargain must be factored into any decision about paying a ransomware demand. In some cases, decryption keys are not even available, and in others, the ransomware authors simply didn't respond once they were paid. We saw this to some degree with WannaCry. A further point to consider when weighing up the prudence of acquiescing to the demand for payment is how this will affect your organization beyond the present attack itself. Will paying harm your reputation or earn you plaudits? Will other – or even the same – attackers now see you as a soft target and look to strike you again? Will your financial support for the criminals' enterprise lead to further attacks against other companies, or services, that you yourself rely on? In other words, will giving in to the ransomware demand produce worse long-term effects than the immediate ones it seems to solve?

520.743.7554
info@computerdimensions.net
www.computerdimensions.net

What Happens If I Don't Pay A Ransom?

If you choose not to pay the ransom, then of course you are in the very same position the ransomware attacker first put you in by encrypting all your files in order to "twist your arm" into paying. Depending on what kind of ransomware infection you have, there is some possibility that a decryptor already exists for that strain; less likely, but not unheard of, is the possibility that an expert analysis team may discover a way to decrypt your files. A lot of ransomware is poorly written and poorly implemented, and it may be that all is not lost as it might at first seem. This can be a very valuable resource when evaluating your course of action when facing a ransomware attack. Also consider whether you have inventoried all possible backup and recovery options. Many look no further than the Maersk shipping story during the NotPetya attack to emphasize the importance of being able to rapidly restore one's entire infrastructure from backup. The most eye-opening realization for Maersk (and indeed the entire industry) was that recovery depended on a happy accident: a sole unaffected domain controller did not become infected due to a local power outage where it was residing. Without that fortunate, coincidental event, it would have taken exponentially longer to rebuild their entire infrastructure after 50,000 devices and thousands of apps were destroyed all at once. Some hail this as a success story for backups, but shareholders and operators on board the thousands of ships worldwide are quick to remind us that this incident still cost the company well over a half billion dollars in the 6 months following the incident. While backup and restoration are indeed critical, they are by no means the primary basis for a strategy to address the threat of ransomware. Finally, there is the worst case scenario, where you have no backups and no recovery software, and you will have to dig yourself out by re-building data, services and, perhaps your reputation, from the ground up. Transparency is undoubtedly your best bet in that kind of scenario. Admit to past mistakes, commit to learning those lessons, and stand tall on your ethical decision not to reward criminal behavior.

What Happens If I Pay A Ransom for Ransomware Attacks?

There is perhaps more uncertainty in paying than there is in not paying. At least when you choose not to pay a ransomware demand, what happens next is in your hands. In handing over whatever sum the ransomware attacker demands, you remain in their clutches until or unless they provide a working decryption key. Tactics like asking for 'proof of life' to decrypt a portion of the environment up front prior to payment, or to negotiate payment terms like 50% up front, and 50% only after the environment has been decrypted, can work with some groups, albeit not with others. Most ransom is still being paid in bitcoin, which is not an anonymous or untraceable currency. If you do feel forced to pay, you can work with the FBI and share wallet and payment details. Global Law Enforcement is keen to track where the money moves. And where do you go beyond that? Any sensible organization must realize the need for urgent investment in determining not only the source of that attack but all other vulnerabilities, as well as rolling out a complete cybersecurity solution that can block and rollback ransomware attacks in future. While these are all costs that need to be borne regardless of whether you pay or do not pay, the temptation to take the quick, easy way out rather than working through the entire problem risks leaving holes that may be exploited in the future. Balance the need for speed of recovery against several risks:

1. Unknown back doors the attackers leave on systems
2. Partial data recovery (note some systems will not be recovered at all)
3. Zero recovery after payment (it is rare, but in some cases the decryption key provided is 100% useless, or worse, one is never sent

Finally, note that some organizations that get hit successively by the same actors might have actually only been hit once, but encryption payloads may have been triggered in subsequent waves. Experience pays off tremendously in all of these scenarios, and 'knowing thy enemy' can make all the difference.

Pay or don't pay, make sure you notify the proper law enforcement agency: "Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to report ransomware incidents to law enforcement. Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under U.S. law, and prevent future attacks".