Ransomware: The Consequences of doing a deal with the devil

Authors: Malcolm Dowden, David Clarke Edited by: Penny Heyes

Cyber attacks and ransomware seem to be on the increase.

The anecdotal evidence is that this is the case, despite the fact that some organizations around the world are actually declaring that there are fewer attacks at the moment and that ransoms are lower. Not in our experience.

In this article, we are going to discuss the types of attack and ransom payments. Should you or shouldn't you pay? We will also discuss some of the regulations and the fines that may be applicable if you do pay, about what you should and shouldn't do, and actually the consequences of any activity; it's not as simple as just paying the ransom.

We need to consider the effects of various types of ransomware attack. We need to look at the time periods over which those attacks are prepared and then launched and we should assess the responses that an organization can make in order to protect their position. Unfortunately, if you are hit with a ransomware attack and you are unprepared, there is likely to be very little by way of good news.

We cannot emphasise enough the importance of preparation.

What is Ransomware?
Ransomware is, in effect, a malware that puts a layer of encryption on data within a system or a network. It locks that data denying access to programs and systems unless, and until, a ransom is paid.
Although classic ransomware is concerned with locking access to data unless a payment is made, we have also seen examples of data stolen as part of the attack, which is then sold on the dark web.

The European Data Protection Board have highlighted particularly sophisticated attacks where that data exfiltration can be concealed by editing the log files that record activity in and out the system. So ransomware is not just about locking data; it can have much broader consequences.

Timing
Recent experience demonstrated that there is often a period of weeks or even months between the initial introduction of the malware and the actual launching of the attack. In that period, the attackers are probing systems for vulnerabilities. They are looking to launch lateral attacks. They are looking for access to accounts that do not have privileged access control and also to administrative functions. These attacks can be lurking and ready to go for quite a period before they become apparent.

Can we detect any kind of attack before it actually happens? Yes – many companies have DLP (data loss prevention) measures in place, and DLP has been included in the new ISO 27001 standard. Effectively, this is a way of looking at logs and detecting whether unusual things are happening. The government guidance suggests that you check if you have protective measures in your network that prevent lateral movement of data, because if an attacker can find one server, they can find the rest.

DLP was, at one time a “ nice to have” but now it is seen as best practice and is included in the top five recommendations from the Biden administration and NIST. We will look at more preparatory measures later in this article.

Timing

Timing of the attack is key; attackers have quite a sophisticated understanding of their targets, and ransom demands might well be timed to coincide, for example, with merger and acquisition processes or with quarterly valuation reporting deadlines or with other financial or regulatory obligations. This means that the leverage, the pressure on the attacked organisation is greatly enhanced.

Paying the Ransom

Ransoms are in the millions of dollars and obviously, the average cost, according to some reports of a cyber incident is around US $ 4.5 million / £ 4 million. This, of course, does not just cover the ransom but all the other associated costs around that. Ransom demands are normally made in cryptocurrencies, very often in Bitcoin. Why? Because tracing the recipients of those payments is very difficult.

This question of paying a ransom came to the attention of the National Cyber Security Centre (NCSC) and the UK regulator, Information Commissioner's Office (ICO), and together those two bodies issued a joint letter in July of 2022 to the Law Society. The reason that it was addressed to the Law Society was to remind lawyers that they really shouldn't be advising clients that paying the ransom is a safe and sensible thing to do.

The National Cyber Security Centre's position was that paying ransoms essentially encourages the “hackers”, encourages the attackers and is not to be encouraged from a regulatory perspective. The ICO emphasized that paying a ransom is not a mitigating step that will be positively recognized.

As we explained, the ransom demand tends to be made in cryptocurrencies. Over the last 18 months or so, the size of a typical ransom demand has changed with the fluctuation in the values of cryptocurrencies and often racks up quite heavily. The ransom is intended to be deemed “worth it” from the perspective of the malicious actor, but it is very often calibrated with a rationale. The ransom needs to be of a size that encourages the perception in the boardroom that it is “cheaper and easier to pay” than to carry on suffering. For example, a ransom at the level of a daily loss of revenue or of a fine incurred under regulatory sanctions for missing reporting deadlines. Thus the payment is often calibrated to make it feel as though it is worth paying.

Of course, when you are under tremendous stress as a senior executive and your business is threatened, the immediate inclination is to pay in order to get everything back on track. The critical question here is, if we are in a position where an organization has been hit with a ransomware attack and isn't able to deal with the consequences of the attack, would it just be quicker and easier to pay the ransom?

Regulations

But following the very stern advice from the NCSC and the ICO, plus the legal situation, that may not be advisable.

Paying the ransom is not in itself unlawful, nor a direct contravention of the law in itself. But if an organization pays it runs risks relating to a number of offences under other regulations.

Laws relating to sanctions are particularly significant given the significant number of state sponsored ransomware attacks. There are laws that apply to the financing of terrorism, money laundering and proceeds of crime. In addition, where there are state backed attacks, paying ransom to somebody who is an official of another regime could constitute an offence under the Bribery Act.

Using 3rd party Negotiators

In some instances organizations have been resorting to trusted, verified third parties who hold stocks of cryptocurrencies for this purpose rather than running the risk of obtaining cryptocurrencies from unregulated exchanges.

If an attacked organisation uses a 3rd party organization to pay using “clean funds”, then these don't become the proceeds of crime until they are in the hands of the criminals. So this can be managed.

Also, if paying with clean funds, this reduces the risk of being involved in situation that would be regarded as money laundering. The difficulty though with the anti-money laundering element is that one needs to consider from where the Bitcoin is coming from, or where is the cryptocurrency sourced.

It's easier to undertake due diligence on those from whom you are buying the cryptocurrency if it's a regulated exchange, but broadly if you have sources of Bitcoin that are not easily subject to due diligence, then you are running the risk of obtaining tainted cryptocurrency. Remember, any ransom agreement is not necessarily going to follow the normal rules of negotiation.

Thus, working through a third party negotiation organization may be advisable.

The criminal offences mentioned earlier can very often be avoided if an organisation undertakes robust due diligence regarding where the attack appears to have come from, who or which groups are likely to be involved. Due diligence at that level can help to insulate from criminal liability.

The Economic Transparency Act made a change last year in relation to civil monetary penalties and that created a residual and immovable risk which is that if your due diligence gives you **no reason** to suggest that:

- the person to whom you're paying the ransom is on a sanctioned list, nor
- is an organization associated with a sanctioned person, nor
- they might be terrorist or terrorist financing activities, nor
- there is money laundering going on,
- nor that you're bribing a foreign official,

you may well be in the clear as far as those criminal offences are concerned.

However, if it is subsequently proven that you've paid money to a sanctioned person or organization, whatever your due diligence, you could still end up with a monetary penalty. This is limited to £1 million or half of the value of the ransom paid to the criminal organizations.

Again, working through experienced third party negotiating organizations may very well be advisable. These organizations often have the links with law enforcement bodies and the experience in particular attacks to be able to recognize, with a reasonable degree of confidence, if an attack is likely to have come from a known source whose actions and approach are known and understood. There have been instances of law enforcement bodies recognizing the method of attack and being able to predict if the decryption keys are likely to be supplied, or not. In those circumstances, there may be pragmatic reasons to pay the ransom. In other words, the due diligence carried out by those third party organizations can help in relation to avoiding criminal offences.

Having said that, there is always an element of guesswork because there are always anonymous attacks. Identification the attacker of the group or the individuals that are involved will always be guesswork. Attackers don't necessarily need to be terribly sophisticated in order to use a method of attack that might in some circumstances look like the activities of a recognized group. But their conduct may be radically different from previous experience.

Victim and Villain

When a ransomware attack has occurred, the organisation can be simultaneously the victim of this attack and the villain in terms of data protection and privacy.

Data Breach implications

If there are data breach issues as a consequence of the attack, despite having paid the ransom, and even if the organisation obtains the decryption keys to regain access to data, that will not in itself reduce the severity of any enforcement action by the regulator.

No organization can know what has happened to that data whilst it has been out of its control. Once the data is out in the wild, it is virtually certain that a significant data reach has occurred and the organisation must act as if this is the case.

If an attack locks down data, making it unavailable, this will very likely be determined to be an “availability breach” in relation to personal data. From a GDPR perspective, if there is exfiltration of data where the data is removed from the organisation’s control, put onto the dark web, then there is a “confidentiality breach” under GDPR.

And even if the organisation gets the decryption key, the data may be corrupted in the process of decryption. In that instance, this is defined as an “integrity breach” under GDPR.

Fines and Costs

Given such scenarios, data subjects have the ability to bring a claim for compensation under Article 82 of GDPR, so in addition to the ransom payment, there are costs associated with data subject access requests and all of the work that's involved, taking personnel away from their day-to-day jobs, adding extra costs, plus the potential loss of business whilst the company is non operational.

Any of those breaches mentioned above are likely to be classed as “tier two”, which means under EU GDPR 20 million euros, 4% of global annual turnover (whichever is higher) and under UK GDPR £17.5 million or 4% if higher. Those fines are a significant concern.

Cyber Insurance

Are ransom payments included under a cybersecurity insurance policy? The answer is: sometimes.

Cyber insurance policies do very often include provision for making payments. But as with any claim on an insurance policy, liaison with the insurers is absolutely critical, and very often that comes down to identifying, as far as possible, the recipient of the payment. Take advice, liaise with law enforcement bodies, not just to get clearance or immunity from the legal consequences, but at least to get an indication that it is reasonable to make the payment.

There are also some new regulations in the EU and the UK relating to **testing for** organizations to ensure that they are prepared for any cyber attack or in fact protected against those. Earlier this month, the United States National Cybersecurity Strategy was published, which places a much more significant responsibility for cybersecurity on all organizations. To quote from this paper, the US governments wants to build a more defensible, resilient digital ecosystem. With current initiatives like the US and UK governments getting together to sanction recognized criminals, and making concerted efforts to coordinate responses against these attacks, the emphasis is definitely on mitigation and prevention.

Some of the new regulations are now requiring companies to test their cyber resilience on a regular basis and this is becoming an insurance requirement as well. We are seeing greater weight being placed behind resilience measures, not just in terms of insurance, but in terms of direct regulatory intervention when it comes to organizations that, that have a role in delivery of critical services, communications, infrastructure et al. It is important to recognize that there are different sectoral regulations and obligations depending on an organisation's place in, for example, critical infrastructure.

Response, Recovery and Rebuild

After any cyber incident there will be a major rebuild of your infrastructure with additional security otherwise it will only get exploited again and again. And this needs to happen really fast to ensure continuity of operation.

In our experience, it can take a minimum of 3-4 weeks to be operational again, and this is because often organisation find that their backups (if they have them) were not up to date, were not properly patched, passwords and IDs had not been updated or the back-ups were compromised themselves, it may not have been tested and just took too long. This has a knock on effect and becomes a false magnifier. The rebuild or the restore can take a long time.

How do you make sure that your backup hasn't been compromised at the same time? The European Data Protection Board's (EDPB) guidance is to make sure that backups are kept physically, logistically separated from the main system so that there is a distinction between the live system which has been compromised and the backup that will be triggered is the fail safe arrangement. But again it is essential to recognize the risk that the backup could be as compromised as the main systems and so some take advanced measures to create a kind of safety cordon in relation to this backups is necessary.

One key thing we advise clients is to have a fully prepared incident team, with the right participants all set up and practiced, both internal and / or external. The quicker the response, the better the outcome.

"Do we save our company or do we save our customers?" You may not have resource to do both at the same time.

All organisations need an escalation process – work out who you are going to call. A ransomware attack might well be capable of taking down all of your systems, including your internal telephony, for example. So having alternative backup methods of convening your emergency response team is pretty critical.

It can be really hard in the initial stages of an attack to work out what is happening and how far it is affecting your organization's systems and networks. In some instances, you may have to accept that you will be going to commit GDPR breaches (such as a data availability breach) by closing down systems, especially if it is not clear whether the attack is spreading and at what pace.

Therefore it is important to have a series of decision points, i.e "go/ no go" communication plans in place as a matter of corporate preparation.

Communication
You need to understand what to communicate, when to communicate, how to communicate and to whom.

- Does your business continuity plan if your internal communication is compromised?
- Is the data breach notifiable? To whom? When?
- Do you notify the media? Regulator?

Preparation
The European Data Protection Board's guidance is clear: if you have strongly encrypted data at rest, then if you do suffer a ransomware attack, then there is far less incentive on the attackers to exfiltrate that data because they would be exfiltrating encrypted data.   It is less packageable, less marketable on the dark web, less capable of being used in in subsequent attacks or crimes. So encryption is key.

There are some pessimistic concerns that we will see some examples of encrypted data being exfiltrated as encryption technology is getting more sophisticated and undergoing change as quantum computing evolves. This does mean that data which is strongly encrypted today may well be not strongly encrypted in the future. So we do need to think about the risk down the line.

Encryption is also dependent on access control so having MFA (multi factor authorisation) is a bare minimum, or 502 which uses a token that is put into devices to allow access to that specific device.

Training of staff, as ever, is also critical. Training in order to prepare people is key to mitigate any potential risk, but also to learn, react and know what to do, where, how to escalate, how to communicate what decisions to make.

A huge number of cybersecurity incidents actually involve human behaviour; traveling home on the train with the password and username on a post-it note, opening a phishing email, forwarding the phishing email that introduces malware onto a remote workstation, a laptop.   This addresses the questions about remote working. The initial security measures taken to deal with the malware on the network could come to nothing if the next time a remote workstation logs in, the malware can be reintroduced.

All organisations need preparatory and resilience measures that reflect how people are working, where devices are at the moment, when they're being logged into the system and where the security layers are.

Summary

Any organization is at risk, every organization is at risk because increasingly we see ransomware as a service rolling out and the predictability of targeting has diminished.

In terms of geopolitical situations, we also see the use of things that are not just ransomware, but wiper aware attacks. The objective of which is not to extract or ransom, but to essentially cause disruption, chaos. And some of those wipe away systems are now finding their way through as service toolkits on the dark web.

A large percentage of organisation suffering ransomware attacks were vulnerable because of their supply chain, and the actual source came from their supply chain. So due diligence of the third party supply chain and its security protocols is essential.

We might well see a attacks being launched just for the fun of it. So in those circumstances, resilience, preparation, physically and logically separated backups are absolutely key.