Cyber-attacks and ransom demands - to pay or not to pay

Cyber-attacks are constantly rising. Cyber risks have accelerated by as much as 500% ever since the first lockdown was imposed in India in March 2020. We witnessed several large cyber claims in India in 2020 and 2021, and we were involved in one of the first multi-crore business interruption claims being paid under a cyber policy in India. Some other claims regularly being paid under a cyber policy include cost of forensics investigation, legal counsel expenses, and ransom payments. Even the business interruption claim referred to above originated as a ransom demand, which the insured refused to meet. While the cost of forensics investigation was paid, coupled with crores of rupees, as business interruption loss, there is no assurance of the threat of another ransom demand being eliminated.

The most debated part of a cyber claim is usually ransom demand and payment. While most cyber policies cover ransom payment, there is always an overarching principle of insurability that covers the insurance universe. From an Indian context, there is no legislative guidance on whether payment of ransom is legal; whether the legislature intends to encourage such payments; whether there are sanctions or incentives around such payments. As a jurisdiction, India is still developing its cyber insurance space and in that, ransom and related claims have some catching up to do. In some countries, the industry is reluctant to pay a ransom, since they have observed that despite payment, the insured's systems do not get unlocked completely or that there is a delay in sharing of decryption keys/code, resulting in further losses. Having said that, payment of ransom is still being chosen as the lesser evil in cases where the consequences of not paying ransom and loss of data are far more critical and financially burdensome, as compared to the ransom amount involved.

In this article, we have tried to analyse these issues across a few jurisdictions with a view to create a comparison on how similar issues are being treated across the globe. We reached out to insurance brokers and consultants across a few jurisdictions for insights on some questions aimed at throwing light on the intricacies involved around ransom payment pursuant to a cyber-attack[1].

[1]Special thanks to John G Duncan, JMD Ross Insurance Brokers Pty Ltd, Diego Sainz, Verspieren, Kim-André Vives, Suedvers, Gautam Mahey, Pacific Prime, Simon Meech, BMS Group and Abbas Jaorawala, A M Jaorawala & Co. for their valuable insights.

Ransom payment - legal permission or prohibition

Ransom payment is not a new concept. Kidnapping, abduction, and similar offences have been in existence since time immemorial. Even from an insurance standpoint, kidnap and ransom policies have been operational for quite some time now. Yet, the question of whether ransom payment itself is legal remains a grey area. When an organisation agrees to meet ransom demands resulting from a cyber-attack, they also fear the risk of a subsequent attack.

Most jurisdictions do not have a legal prohibition on ransom payment. For instance, in the United States of America[2], no federal statutes expressly criminalise making ransom or ransomware payments. However, federal laws heavily restrict transactions with certain parties and could implicitly make ransomware payments to such parties a crime, for example, where a ransom payment is made knowingly to an entity either designated as a foreign terrorist organisation or subject to sanctions by the Department of the Treasury. There are also reports that legislatures in at least four states are considering bills that would prohibit state or local government from making ransomware payments or from using public money to do so. Similarly, there are reports about a proposed bill in New York to authorise civil penalties of up to $10,000 for governmental, business, or health care entities that make a ransomware payment. In the United Kingdom, while payment of ransom is not illegal, it is not encouraged either. If payment is being made to a terrorist, penalties may be levied. In fact, recently there was a case against a shipping company that paid ransom to pirates. The court held that since the pirates were not terrorists under UK law, the payment was not illegal. In cases where a cyber-attack results in data breach, applicable provisions of GDPR trigger.

In Australia, it is a moot point as the law is vexed on the subject. While on one hand, payment of a ransom could be a crime as you are vicariously complicit in the crime by paying a ransom, on the other hand, there is no caselaw in relation to this at present. In France, the law is silent about the payment of ransom, and there has not been much news of any company being sanctioned because of payment of ransom. The position is similar in Germany as well as Singapore. There is no legal prohibition under civil or criminal law on ransom payment, and it is a grey area, and the law might be silent on this. In Singapore, an interesting perspective came to light - organisations may be penalised if they are hit with a ransomware attack, on the basis that the organisation did not take sufficient steps to mitigate a cyber-attack or safeguard data. The onus is on the organisations to take stronger measures to prevent such attacks.

The position in India is also similar i.e. the law does not prohibit payment of ransom pursuant to a cyber-attack and practically we are hearing of organisations paying ransom to relieve the operational and financial pressure that follow a cyber-attack.

Ransom payments - are they tax-deductible?

Another question that comes to mind in such cases is whether ransom paid is tax-deductible? Some practitioners are of the opinion that this is not tax-deductible. The view is based on the rationale that for an expense to be tax deductible, it must be wholly and exclusively incurred in the production of income, and in the case of a cyber-attack resulting in a ransom demand, the expense is not incurred for income production, but rather loss mitigation. In the United States of America, online articles suggest that the payment of ransomware can be a 'normal and necessary' expense of the business and result in deduction from taxable income as a loss of theft under Internal Revenue Code Sections 162(a) and 165(a). The Internal Revenue Service's definition of theft appears broad enough to include a cyber-attack. However, if the cryptocurrency ransom payment is an unlawful bribe, or illegal kickback, it is not tax-deductible under Section 162(c). As a result, a taxpayer should differentiate illegal payments from ransomware cryptocurrency payments. Even in the UK, the position on whether ransom payments are tax deductible remains grey.

In the Indian context, while there does not appear to be a judicial precedent in the cyber-attack context, there has been an Indian High Court judgment wherein ransom paid for the release of a kidnapped director was held to be deductible as the company's business expense. One could argue that in the case of cyber-attacks resulting in ransom payments, the same principle ought to be followed.

[2]R46932 (congress.gov)

Impact of insurers refusing to cover ransom payments in their policy.

In India, most insurers do provide cover for ransom payments in their cyber policies. Globally, a similar trend was expected. However, as per a news report published in May 2021[3], one of Europe's top five insurers has indicated that it will stop reimbursing people in France who pay up after being targeted by cybercriminals with ransomware. The insurer has said that it will stop writing cyber insurance policies that cover customers for extortion payments to ransomware attackers. It is being stated that the decision is in response to concerns aired by French justice and cybersecurity officials during a senate roundtable in Paris in the previous month about the global epidemic of ransomware, in which France is the second worst-hit country in the world after the United States of America.

In our discussions with respect to potential impact of this decision on cyber-attacks with insurance brokers from different jurisdictions, we learnt that most insurance consultants believe that this is not likely to reduce the number or intensity of attacks. The primary reason is that cyber criminals do not focus on the ability of the victim's entity to seek reimbursement through insurance. Their primary factor is the vulnerability of the systems and the ability to pay. The more likely impact of this decision will be seen on the number of ransom demands that get reimbursed, and not so much on the number of demands being made. This again circles back to the point that even insured entities at times prefer paying ransom to facing consequences of non-payment like data leak, business disruption, or third-party liabilities.

From a marketing standpoint, to exclude ransom from the coverage reduces the need, usability, and requirement of the cyber policy very significantly. Ransomware is one of the primary elements which clients look for when deciding to purchase a cyber policy. Coupled with that, the insured expects better coverage, lower premium, and more economical deductibles.

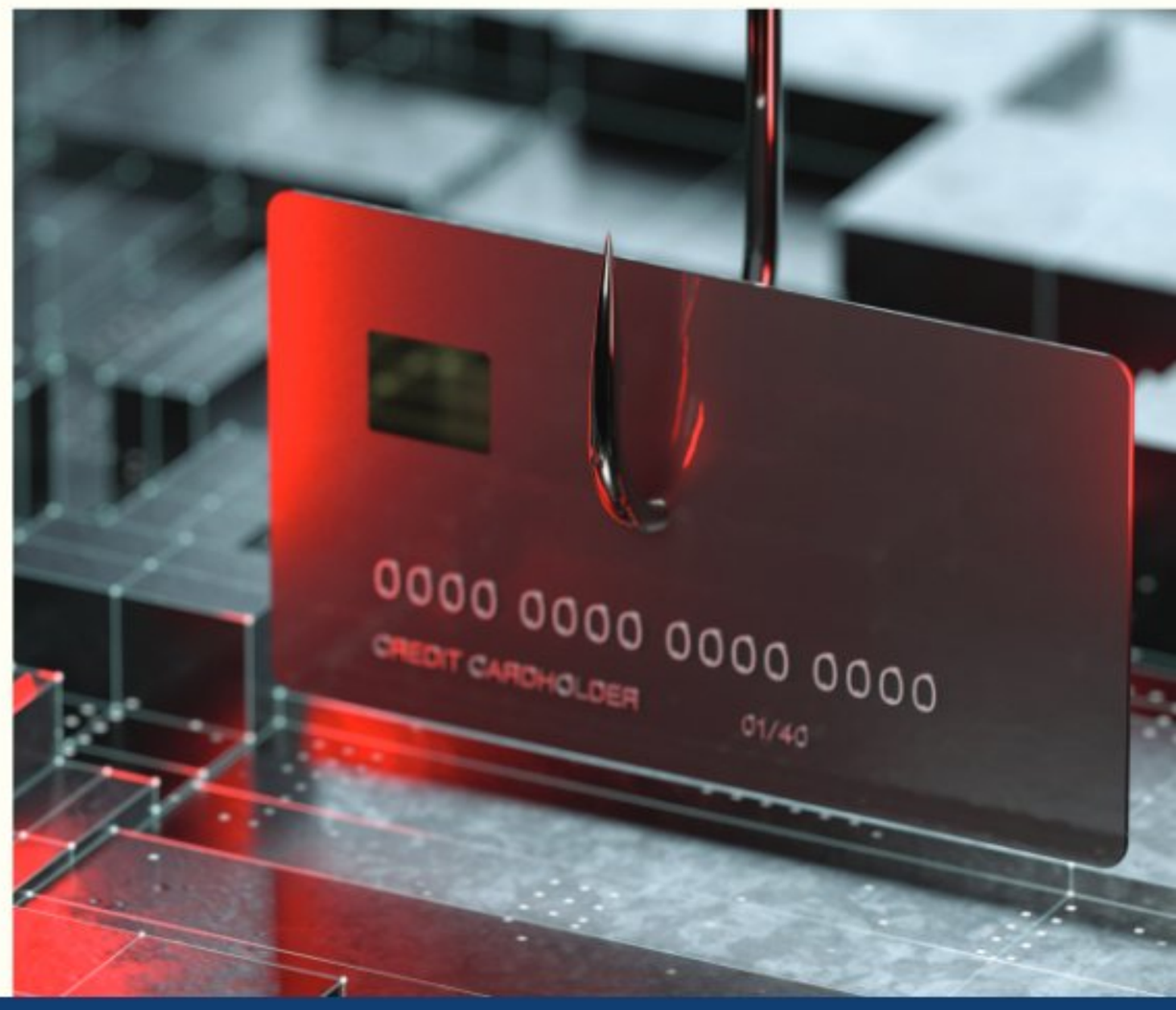
How can organisations design ransomware response policies to be better prepared for cyber-attacks?

The primary approach to mitigate cyber-attacks is to be proactive and not reactive. The CISO, CFO, and CIOs ought to focus on front line defence with mirror-imaged systems, air-gapped server backups, active 24/7/365 virus ware from two suppliers, multi-factor authentication, absence of local admin rights except for IT department, etc. Organisations need to see ransom demands like any other risk in their risk profiling. Companies need to work on a global ransomware response strategy, including a formalised response plan to ransomware, access control for security measures, better detection and response tools and qualified teams, and, of course, being covered by an adequate cyber insurance policy. CISOs, DPOs, and risk managers are the best suited to be owners of this policy within organisations.

To be better prepared for such events, organisations need to ensure they have a proper Business Continuity Plan (BCP), which every employee can act on immediately, in case of a suspected attack. While such BCP might seem like an obvious way of preparation to many, the fact is that not many organisations have this in place. We have first-hand experience of organisations where employees do not know how to react in case of such attacks; legal/compliance teams do not know whom to contact (such as law enforcement department or crisis response teams) during such situations. At times, from the moment an employee suspects a cyber attack till the moment it is proven or discovered, a lot of time is lost, which increases the risk of deeper penetration by the threat actors. Cyber insurance should be well integrated within the BCP, so that the policy can be immediately used once an incident strikes an organisation. The more prepared and rehearsed the plan, the better the likelihood of an effective outcome.

Last but not the least, it is also critical to engage with an experienced insurance broker or consultant who can handhold the insured in case of a cyber-attack and make the entire process seamless. When deciding whether to pay a ransom, technical experience on matters including the means to pay it, involvement of currencies, and regulatory sanctions involved, are some of the key aspects that need handling, which an experienced broker or consultant is best equipped to take care of. While the need to prepare for cyber threats continues to increase, it is better late than never.

For more information on cyber insurance, policy structuring, and incident breach response and coverages, please reach out to our liability department.



[3]Cybercrime: Insurance giant Axa to stop covering ransomware payments in France | Euronews

PRUDENT
THE FUTURE OF INSURANCE

www.prudentbrokers.com

FOR MORE QUERIES, PLEASE REACH OUT TO:

Tanuj Gulani
tanuj.gulani@prudentbrokers.com

Neha Anand
neha.anand@prudentbrokers.com

Jyoti Krishnan
jyoti.krishnan@prudentbrokers.com

PRUDENT INSURANCE BROKERS PVT. LTD.
101 Tower B, Peninsula Business Park, Lower Parel, Mumbai 400 013
+91 22 3306 6000

PRUDENT INSURANCE BROKERS PVT. LTD.
Registered Office at 101, Tower B, Peninsula Business Park, G.K. Marg, Lower Parel, Mumbai 400 013 Maharashtra
Tel: +91 22 3306 6000.

Certificate of Registration No. 291 (Validity: 18th February 2020 to 17th February 2023)
CIN No.: U70100MH1982PTC027681

Insurance is a subject matter of solicitation