Ransomware payments: an insurance perspective

Insights - 20/05/2021

Last week, a Russian gang known as Wizard Spider attacked the Irish Health Service Executive (HSE) systems, deploying ransomware and demanding a ransom that is reported to be in the region of $20 million. Stephen Donnelly, Minister for Health, has made it very clear that the HSE will not be paying.

Implications of paying a ransom

If the costs of the ransom are lower than the costs that your business will incur in restoring files and systems, it is worth considering. You should, however, be aware of the implications of paying a ransom. Paying criminals will facilitate more criminality and lead to more sophisticated ransomware attacks.

There is also the risk that paying the ransom will not resolve matters. According to a report by Kaspersky, a cyber security solutions provider, over half of ransomware victims pay the ransom, but only a quarter see their full data returned. Only 29% of victims contacted for the survey were able to restore all their encrypted or blocked files following an attack.

The HSE is in a different position than other businesses. The adverse PR of a governmental organisation paying a ransom is a lot worse than any other organisation paying a ransom. A government organisation is held to a higher level of moral standards than a business. If it was paid, is this tacit acceptance that it is in order? Further, it may (is very likely to) make other government agencies a target for future attacks.

The main asset of many companies is now its data. If someone denies your company access to this data, it can be paralysed. If you called the HSE on Monday inquiring about an appointment you had in a hospital and you didn't know what doctor your appointment was with and what time it was at, the HSE had no way of directing you to the right place. Now the HSE are saying that their payroll may be affected.

Who is being targeted?

Schools, professionals and SMEs have been significant targets over the past number of years for cyber-attacks. Generally, you need a large budget in order to insulate risk. Sophisticated companies usually have viable backups and incidence response plans. They shut off old systems and migrate to new systems and there is no need to engage with threat actors. However, no one is immune to a cyber-attack. The more sophisticated cyber security becomes, the more sophisticated cyber-attacks become.

Threat actors will explore all means possible to monetise the cyber-attack. Threat actors are exfiltrating data with the aim to either hold it to ransom or sell data on the dark web. Reports suggest that some of the HSE data is being sold on the dark web.

You will need experts to deal with a cyber attack. It isn't as simple as in paying the ransom, the threat actors leave you alone and your files are restored. Experts will be able to advise you on the positives and negatives of paying the ransom and whether they believe it is right for your business. You will need to consider the alternatives and strategies.

Ransom payment

If you and your team have performed your costs benefit analysis and the decision has been made to pay the ransom, how do you do this? Reports suggest that the HSE ransom was to be paid in Bitcoin as most ransomware payments are. Most companies will not have access to Bitcoin. Cyber professional teams will know how best to deal with the payment process if the decision is to pay the ransom.

Payment of the ransom could be linked to other strategies such as injunctions or Gardaí investigations.

Cyber insurance policy

There is considerable information available online about how to plan and implement policies that will protect you from cyber attacks. Software and technology reviews should be carried out. All organisations should review their policies and procedures and ensure they are prepared. Consider the documentation and personal data you hold, assess what is critical and assess your back-up procedures.

None of this prevents a cyber attack but rather puts you in a better position if and when one occurs. Most organisations are never going to have the IT budget to facilitate large scale system upgrade overhaul.

How do you insulate the risk?: Cyber insurance.

A good cyber insurance policy should cover you for comprehensive support during the critical 48-72-hour period of a cyber-attack. It will likely include the following:

- Security and Privacy Liability
- Multimedia and Intellectual property liability
- Technology Services
- Business Interruption and recovery
- Legal fees
- Privacy regulatory defence and penalties
- Reputational Damage
- Forensic investigation and data restoration

All policies are different so you will need to liaise with your broker with respect to what you need. Cyber policies are not and should not be add-ons to your other policies. The days of cyber cover being an afterthought are and should be behind us.

Conclusion

Depending on the circumstances, the temptation will of course be there to pay a threat actor. If you have a good cyber insurance policy in place, your insurer should engage a comprehensive crisis management team that will deal with the cyber attack in a professional manner and potentially avoid any need to pay a threat actor. Your insurer should deal with the cyber attack with haste and instruct the right people at the right time.

If you don't have a good cyber insurance policy in place you may need to instruct a team of experts yourself. Although this may be costly, it will more than likely save you money in the long run by avoiding GDPR fines and by regaining control of your data which is vital to your business. These experts, in addition to everything else, should be able to advise you of the positives and negatives of paying a ransom and if the decision is ultimately made to pay it, how to make the payment.

Ogier provides advice with respect to cyber matters including pre-event management, cyber incident response and post event matters. If you have any queries, please get in touch with our Technology and Web3 team.

About Ogier

Ogier is a professional services firm with the knowledge and expertise to handle the most demanding and complex transactions and provide expert, efficient and cost-effective services to all our clients. We regularly win awards for the quality of our client service, our work and our people.

Disclaimer

This client briefing has been prepared for clients and professional associates of Ogier. The information and expressions of opinion which it contains are not intended to be a comprehensive study or to provide legal advice and should not be treated as a substitute for specific advice concerning individual situations.

Regulatory information can be found under Legal Notice

Meet the Author

Ultán Anderson

Associate

Ireland

E: ultan.anderson@ogier.com

T: +353 1 232 0287

Key Contacts

Stephen O'Connor

Partner

Ireland

E: stephen.oconnor@ogier.com

T: +353 1 232 1074

Related Services

Insurance Disputes

Crypto Disputes

Related Sectors

Technology and Web3