Case study

Ransomware riddle

Ransomware attack results in system damage, business interruption and contractual liability

Cybercrime is becoming increasingly prevalent across the board, with managed service providers (MSPs) a prime target for hackers as a single point of failure for many businesses.

MSPs provide services to multiple clients and their vulnerability revolves around a single point of access that will enable hackers to not only access the MSP infrastructure, but also the systems of their customer base.

Sodinokibi variant causes system entire MSP infrastructure to crash

An MSP was subjected to a Sodinokibi variant ransomware attack affecting approximately 400 of their customers. The MSP was unable to access their network because the ransomware encrypted their data and deleted their backup systems so data could not be restored. The attack was possible due to a vulnerability in the MSP's RMM (remote management and monitoring) software.

The MSP alerted CFC of the attack and CFC engaged a third-party digital forensics specialist to identify the source of the breach to isolate the issue and implement new infrastructure to provide greater security.

The hackers threatened to publish sensitive data unless their demands were met, and also demanded payment in the form of Bitcoin within 48 hours in exchange for a decryption key. CFC's claims team swiftly enlisted the CFC Response team's help in dealing with hackers and they were able to negotiate the ransom payment and get the decryption key.

System damage and system business interruption

Unfortunately, due to the complex nature of the Sodinokibi variant the decryption key did not restore all their data and a third party was engaged by CFC Response to manually restore the missing data – a labour-intensive, time-consuming task for any business. The impact of data losses due to the ransomware attack proved costly. Labour costs amounted to six figures due to efforts to restore the lost data including staff overtime and third party resources.

The MSP also experienced significant downtime as their entire network was inaccessible. They were unable to provide their services to their clients and their clients were unable to operate as a result and so suffered income losses as a consequence.

The attack resulted in reputational damage for the MSP and 10% of their customer base chose not to renew their contracts with them.

The domino effect: Contractual and privacy liabilities

A digital forensics specialist was engaged to identify the nature of the data which may have been compromised.

Many of the MSP's customers processed sensitive data and faced a significant threat to their continuity and reputation because of the ransomware attack. The MSP, although not required to, decided to notify all affected customers of the ransomware attack to try and salvage their reputation as a responsible and trusted provider.

The MSP was contractually required to provide uninterrupted service to their customers and given the downtime, legal action was taken by their customers for the loss of revenue suffered by being unable to trade as usual. Initial letters requesting compensation were handled by the CFC claims team, and they negotiated settlements with their customers. Due to the number of customers affected the settlement figures were substantial.

The importance of comprehensive technology E&O and cyber insurance.

This claim highlights the harmful consequences of ransomware attacks against MSPs. Having adequate errors and omissions (E&O) and cyber coverage was crucial to the ability of the MSP continuing to trade given the heavy losses that stemmed from the attack.

A comprehensive tech E&O and cyber policy covers the costs associated with defending litigation and paying an indemnity, and also crucially provides services to help manage a dialogue with the attacker, reimbursement of a ransomware demand, digital forensic investigation costs, data reconstitution costs and reputational costs from lost business, as well as business interruption losses.

For more information about insurance for MSPs or any questions about this case study, please email tech@cfcunderwriting.com