

RANSOMWARE: THE RISKS ARE ALL TOO REAL

Posted on June 21, 2017

Categories: [Insights](#), [Publications](#)

The Risk – Cyber attacks are considered one of the most serious risks your organisation faces and ransomware is a currently favoured variation (as evidenced by the recent “WannaCry” cyber attack). It involves accessing your system, encrypting all or an important portion of your data and then offering to give you the encryption key for the payment of a modest amount, usually in the form of a cryptocurrency such as bitcoin.

In addition to the risk of not receiving the key once the payment is made, your organisation faces the risk of others similarly exploring your system’s vulnerabilities. Your officers and board should be concerned that a ransom attack may be like the canary in the coal mine; an early warning of dangers that might lie ahead. If a later more serious cyber attack takes place, what kind of exposure might the officers and the board face if they just paid the ransom and did nothing more?

So far the authorities have not required that intrusions and ransoms be reported or held that payments of ransom constitute money laundering. If that changes, ransom attacks will take on a whole different level of risk.