Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Ransomware has become an inescapable concern for every organisation. Its impact is far-reaching, causing revenue loss, brand damage and layoffs. A few years ago, organisations could simply implement offsite data back-up and recovery solutions. In the case of a ransomware attack, they could confidently rebuff the attackers’ ransom demands and restore their systems from back-ups. This was a solid strategy until ransomware purveyors evolved their methods to include double extortion, where data is first exfiltrated, then there is a threat to release the material should a ransom demand go unpaid.

A recent study of ours revealed that 55% of polled organisations had been targeted by ransomware in the past 24 months. Of these, 44% admitted to losing revenue after the attack. Two-thirds of companies experienced significant revenue loss, 5% suffered brand damage, nearly a third lost C-Level executives, 29% of companies were forced to lay off staff and 26% were either forced to close their business for a period of time or the attack put them out of business permanently. The findings also revealed that about half of companies do not have endpoint detection and response (EDR) solutions.

Ransomware attacks cannot be prevented, but we can prevent the attacks from being successful. There are steps the attackers take on the network before they drop the ransomware payload – this is where EDR/MDR solutions come into play by detecting the threat and eliminating it before any systems are encrypted.

In the UK, 83% of companies that paid a ransom to threat actors were hit a second time by a ransomware attack – slightly higher than the 80% global average. With so much on the line, many companies were inclined to pay the ransom, likely thinking they would minimise the damage and return to normal business operations as quickly as possible. In fact, 58% of the companies surveyed in the UK negotiated with the threat actors after being hit by a ransomware attack. In the US, only 29% of companies negotiated.

Unfortunately, paying a ransom doesn’t guarantee that an organisation will regain access to data and swiftly resume business operations. In the UK, nearly 43% of companies paid the ransom and received the decryption key, but found their data was corrupted. Some 5% of companies paid the ransom and didn’t regain access to any data. Globally, 46% of companies that paid a ransom found that their data was corrupted.

Whether to pay a ransom or not is one of the most important decisions a company must make after being hit by ransomware. As with any successful business model, attackers are going to seek out the highest possible return the market will bear. As companies pay larger ransoms, threat actors will seek higher payments. The fact that CNA Insurance paid a reported $40m ransom, JBS paid more than $11m and Colonial Pipeline paid $4.4m only serves as an incentive to the threat actors to demand higher ransoms.

Therefore, it is important that businesses administer a thorough ransomware risk assessment in collaboration with their legal counsel, insurance partners and law enforcement agencies. There are three key steps: follow security hygiene best practices, with timely patch management, offsite data back-ups and employee security awareness training; deploy multi-layer prevention capabilities on all enterprise endpoints across the network; and implement extended detection and remediation solutions across the environment for visibility, to end attacks before they can gain a foothold on the network.

Early detection is the key to ensuring that ransomware attacks are stopped before they can have any negative impact. Improving situational awareness will go a long way towards returning defenders to higher ground and putting threat actors on the run.