BIZCOMMUNITY

What SMEs should know before paying a cyber ransom

Increasingly, small and medium enterprises (SMEs) are becoming the target of cyberattacks, yet most are still completely unprotected. There is often a lack of preparation and awareness around the important things that small business owners need to consider before paying cybercriminals to restore their encrypted information.

Simon Colman, executive head: digital distribution at SHA.

A recent SHA Cyber Security Survey revealed that 45% of SMEs do not believe they are exposed to cyberattacks, and 50% of SMEs do not have any cyber crisis plan in place. “The reality, however, is that 30% of businesses had already fallen victim to a cyberattack in the previous 24 months, with two-thirds of victims having been threatened with litigation by clients and other stakeholders following the attack," said Simon Colman, executive head: digital distribution at SHA.

Results from this same survey also show that ransomware – malicious software that either locks a company’s systems or encrypts the important files, making them inaccessible – still poses a massive online risk for these businesses. “The SHA survey showed that one in every five successful cyber-attacks involved ransomware, with ransom demands ranging between R10,000 and R25,000 – usually in Bitcoin – for decryption.

Two options

“Disturbingly, the survey also discovered that 39% of businesses actually pay these ransoms in an attempt to regain control of their files as quickly and presumably as quietly as possible,” Colman explains. When a business experiences a ransomware attack, there are really only two options available to the business owner, either pay the ransom and hope for the encryption code or erase the hard drive and reinstall from a back-up. In larger companies, back-ups are conducted frequently and the ransom is rarely paid. In smaller businesses however, back-ups tend to be conducted on a less frequent or more erratic basis (if at all). This leaves these organisations with only one option, to pay the ransom to retrieve the valuable data.

With that said, he states that business owners should think carefully before they decide to pay the ransom demands of cybercriminals. “Firstly, it should go without saying that when dealing with criminals, there is no guarantee that paying the ransom will result in any data being released."

Whilst the Protection of Personal Information Act has not yet been fully implemented, organisations that hold personal data of customers or employees still owe a duty of care to those individuals and the right thing to do would be to inform all parties affected by the incident.

Insurance

Cyber insurers take a dim view of the payment of ransoms where the insured business has not made provisions for back-ups and for those with only basic internet security. Incidents that are sustained and are not reported to the insurer can adversely affect policy coverage. “Lastly, the survey demonstrates why it is not a wise choice to pay ransoms, as 20% of companies that paid were attacked a second time,” he adds.

Colman states that the best course of action for any business is to minimise their risks as much as possible. “As stated, around half of companies have no cyber risk management in place. Businesses need to start there by increasing cyber risk awareness among staff members, implementing proper password management policies, consulting security specialists, limiting access to sensitive information and investing in adequate safety tools.”

However, he adds that businesses also need to have a strategy in place in the event that a ransomware attack is successful. “Having a cyber-insurance policy in place is paramount. While these do not generally cover the costs of damage to physical company assets, they protect the business against legal costs in the event of litigation, loss of profits, costs related to restoring or replacing data and possible fines and penalties that could cripple one’s company. Costs pertaining to extortion and ransom attacks can also be covered with the right risk management in place”

Businesses will also need to have a clear policy on how to deal with ransom demands. “They should clearly communicate their policy regarding what senior management should do in an incident where a ransomware attack is successful, who they should communicate the incident to, and whether the company pays ransoms. With all the media attention and information available on hacking and ransomware attacks, perhaps the biggest “crime” in cyber space is not actually being prepared for an attack,” Colman concludes.