Ransomware: What is an organisation's obligation to prevent fraud?

Cybersecurity has taken centre stage in South African commerce, and it's no surprise, given the prevalence of ransomware attacks on businesses in Africa.

By Karl Blom & Laone Setshedi 6 Nov 2023

Image source: Jakub Jirsak – 123RF.com

South African law sets out specific obligations to address these risks if they arise.

The obligation to secure your data

The Protection of Personal Information Act (PoPIA) imposes specific obligations on businesses to maintain the integrity a confidentiality of the information that they process. This includes taking technical and organisational measures to prevent unlawful access to information in their possession or under their control.

These steps include:

- identifying internal and external risks to their information;
- implementing appropriate safeguards to address these risks (and continually updating these safeguards as new risks arise); and
- implementing generally accepted information security practices as well as security practices that are specific to thei industry.

As bad actors continue to update their techniques (and ransomware becomes more advanced), businesses are similarly required to update their safeguards to address these new risks. These practices may differ depending on whether a business is, for example, part of the telecommunications, insurance, or financial services industry.

The legal status of ransomware attacks

When a business is the victim of a ransomware attack, the attackers typically:

- gain access to the systems of the business;
- extract data from the business;
- upload malicious code to the business's servers, which encrypts the business's data and prevents the business from accessing the data; and
- issue a ransom note to the business, requiring the payment of a fee (typically in Bitcoin) to enable the business to recover its encrypted data.

A typical ransomware attack would likely constitute cyber extortion and cyber fraud, and would be considered an 'aggrava offence' if the ransomware targets a 'restricted system' (which includes the systems of financial institutions). The South African courts have, however, yet to convict a cybercriminal under the Cybercrimes Act, 2013 for committing a ransomwa attack.

Obligations after a ransomware attack

A victim of a ransomware attack is placed in a very difficult position:

- on the one hand, businesses are mandated by PoPIA to diligently protect data subjects, preventing any inadvertent disclosure of their sensitive information; and
- on the other hand, the attackers wield a potent threat, vowing to either publish or irrevocably erase the data unless th ransom is paid.

Businesses will typically be required to make several notifications arising from a ransomware attack, including notification to:

- data subjects (whose information was unlawfully accessed);
- the South African Information Regulator;
- the South African Police Service (SAPS) which might be needed under the Cybercrimes Act, depending on the business's sector or their insurance policies;
- any third parties on whose behalf the business processes personal information; and/or
- its insurers.

If a business wishes to pay the ransom (or negotiate with the attackers), it must ensure that it does not inadvertently contravene any applicable laws when doing so. This includes:

- the Cybercrimes Act which makes it illegal to aid, abet, induce, incite, instigate, instruct, command, or procure anotl person to commit an offence such as cyber extortion; and
- the Prevention and Combatting of Corrupt Activities Act (Precca) requires a person with knowledge of the commissic of the offences of theft, fraud, or extortion to report the matter to the SAPS when the offence involves an amount of R100,000 or more.

  Following notification to the SAPS, it is important to note that the SAPS may (in terms of the Cybercrimes Act) requi a business to preserve all information which may assist SAPS in their investigation of the ransomware attack, and potentially to provide police officials and investigators with reasonable technical and other support that they may nee to conduct their investigation.

  Other things to consider:

  When responding to a ransomware attack, it is often prudent to brief (through your attorneys if required) a number c experts, who may include:

  - forensic investigators (to determine how the incident occurred and prevent future incidents); and
  - public relations experts (to assist the business in managing any damage to the business's reputation).

  It is also important to ensure that, where a business holds insurance for losses arising from ransomware attacks, the is strict compliance with the terms of the insurance policy (which may regulate, for example, whether a business car make payment of a ransom).

  The prevalence of ransomware attacks and other forms of cybercrime is an ongoing concern that businesses must contend with. Taking reasonable proactive measures against these attacks and obtaining proactive legal advice is vit to ensure that these incidents do not become an existential threat to your business.

ABOUT THE AUTHOR

Karl Blom, Partner & Laone Setshedi, Candidate Attorney from Webber Wentzel