Ransomware and management liability

03.11.2021 4 min read

Authors

Luís Flaks

Topics

CVM | Corporate and M&A | Data Privacy and Cybersecurity | ANPD | Cybersecurity | Ransomware | Luís Loria Flaks

Reports of cyberattacks known as ransomware, which is a type of malware used to practice extortion, have become increasingly common. Ransomware attacks have caused enormous difficulties for companies (and their customers, suppliers and other business partners) in a wide range of sectors, especially retail, education, and health.

Because ransomware attacks have now become foreseeable, management's duty of diligence with respect to those attacks has also become a topic of importance, because the duty of diligence covers both measures to prevent attacks and measures taken after an attack has been made.

Preventive measures are all measures taken to reduce the risk of an attack or the severity of its effects. Some examples are constant updates of the company's security software, cybersecurity policies and cybersecurity training for personnel.

Nonetheless, if an attack is successful, other measures will have to be taken to mitigate its effects and to protect and recover information that may have been compromised.

Doubts naturally arise when making decisions in a crisis, particularly given that no company's resources, financial or otherwise, are unlimited. Thus, in deciding which course of action to take, certain conditions must be observed, not least because the law requires that the members of management of a company exercise the same care and diligence that any active and honest person would exercise in managing their own affairs. As long as members of management adhere to this standard of care, they cannot be held legally liable if their decision later turns out to have been mistaken.

The "business judgment rule", a principle originating in United States law and adopted by Brazil's securities and exchange commission, the CVM (Comissão de Valores Mobiliários) can be used to guide management decision-making in ransomware situations. According to the rule, in order to avoid liability, a decision must be informed (based on information or memorandums prepared internally or by outside consultants); considered (taken after analyzing alternatives and possible consequences; and disinterested (the decision must not result in benefit to the decision-maker).

Diligence, however, is not enough. Members of management must also fulfill their duties of loyalty to the company. In the case of publicly-traded companies, those duties include the express prohibition against use of undisclosed material information by members of management or any other insider (i.e. persons who have access to material information related to the company) in order to obtain an advantage on the securities market for themselves or other persons. Such conduct can have criminal implications (imprisonment and a fine of up to three times the amount of the illicit advantage obtained) under article 27-D of Law 6.385/1976, which was amended by Law 13.506/2017 to broaden the scope of who can be charged

with insider trading.

The problem is that when management becomes aware of a ransomware attack, they usually do not know its causes or, in particular, how the attack has affected or will affect the company. In other words, the extent and seriousness of the attack's effects are still unknown, making it difficult to determine whether the company should or should not release a statement of material fact. Moreover, at the beginning of an attack the company's management often do not have a complete understanding of the all the facts and their possible effects.

Nonetheless, some new assumptions were established by CVM Resolution 44, issued on August 23rd of this year, as to whether insider trading has occurred. Among them are the assumption that a person who trades in securities while in possession of undisclosed material information used that information in trading; and that, with respect to transactions in a company's securities, the company's direct and indirect controlling shareholders, officers, members of the board of directors, members of the fiscal council and the company itself have access to all material undisclosed information.

Accordingly, upon learning of a ransomware attack, the company's Investor Relations officer should, as a preventive measure, inform the other members of management and insiders that a blackout period has commenced – in other words, a period during which persons who may have access to inform about the attack are prohibited from trading in the company's securities.

It's important to keep in mind, too, that not all attacks must be disclosed by statement of material fact. In fact, Circular CVM/SEP 01/2021 issued by the CVM's Public Companies Supervision Branch allows information related to cybernetic risks to be disclosed, at management's discretion, by means of a communication to the market rather than by statement of material fact.

Release of a statement of material fact will only be necessary if the ransomware attack or its consequences can have a measurable influence on the quoted price of securities issued by the company, on investors' decisions to invest or not in the company, or on investors' decisions to exercise any of the rights attached to securities issued by the company.

Thus, the blackout period should last only until it is confirmed that the cyberattack was not significant or, if the attack is material, until a statement of material fact is released, at which time the market will have the same information as the company's insiders.

› PROFESSIONALS

Professionals who combine legal insight and market perspective

Luís Flaks