Ransomware e a responsabilidade do administrador

03.11.2021 4 minutos de leitura

Autores

Luís Flaks

Assuntos

CVM | Societário e M&A | Proteção de Dados e Cybersecurity | ANPD | Segurança Cibernética | Ransomware | Luís Loria Flaks

De forma cada vez mais frequente temos visto notícias sobre ataques cibernéticos intitulados **ransomware**, aqueles seguidos de alguma forma de extorsão. Tais ataques vêm causando enormes transtornos a empresas (e respectivos clientes, fornecedores e demais parceiros comerciais), dos mais diversos setores, especialmente varejo, educação e saúde.

Por ter se tornado algo previsível, discutir o dever de diligência dos administradores nesse momento é tema da maior importância. É que esse dever abrange tanto as medidas preventivas ao ataque quanto aquelas a serem tomadas posteriormente ao mesmo.

Ao ter ciência do ataque, o diretor de Relações com Investidores deve informar sobre o início de um blackout period.

As medidas preventivas são todas aquelas tomadas com o objetivo de mitigar o risco do ataque ou, pelo menos, os seus efeitos. São vários os exemplos:

atualizações constantes do software de proteção, políticas de segurança, treinamento dos colaboradores etc.

Todavia, caso o ataque tenha sucesso, outras medidas serão necessárias de forma a mitigar os seus efeitos e proteger e recuperar as informações da companhia que tenham eventualmente sido comprometidas.

É verdade que muitas vezes surgirão dúvidas sobre a tomada de determinada decisão, especialmente em momentos de crise como esse. Afinal, os recursos de uma companhia nunca são ilimitados.

Assim, para decidir que caminho seguir, é essencial que a tomada de decisão seja precedida de alguns ritos necessários. É que a lei exige que o administrador de uma companhia tenha o mesmo cuidado e diligência que todo homem ativo e honesto teria se estivesse administrando os seus próprios negócios. Dessa forma, desde que tenha tal cuidado, o administrador não poderá ser legalmente responsabilizado se a decisão no futuro se mostrar equivocada.

Para tanto, deve-se ter sempre em mente o princípio, de origem norteamericana, adotado inclusive pela Comissão de Valores Mobiliários (CVM) em seus julgados, chamado “business judgement rule”. Segundo essa regra, para se evitar a responsabilização, uma decisão deve ser: informada (baseada, por exemplo, em informações ou memorandos preparados internamente ou por consultorias especializadas); refletida (tomada após análise das possíveis alternativas e consequências); e desinteressada (decidida sem qualquer benefício ao administrador).

No entanto, ser diligente não basta. Precisa o administrador, ainda, cumprir com seus deveres de lealdade à companhia. E, no caso de companhias abertas, dentre tais deveres, encontra-se expressamente a vedação de utilização de informação relevante, ainda não divulgada, pelo administrador e por todo e qualquer outro insider (pessoas que tenham acesso a informações relevantes relativas à companhia), com a finalidade de auferir vantagem para si ou para outrem no mercado de valores mobiliários. Tal conduta pode, inclusive, vir a ter implicações criminais (reclusão e multa de até três vezes o montante da vantagem ilícita obtida), conforme tipificado no artigo 27-D da Lei nº 6.385/76, cuja redação foi endurecida pela Lei nº 13.506/17.

O problema é que, quando da ciência de um ataque de ransomware pela administração, na maioria das vezes, não se sabe ainda as causas ou, especialmente, como aquele ataque afetou ou afetará a companhia. Ou seja, não se sabe a extensão e materialidade dos efeitos para avaliar se a companhia deve ou não divulgar um fato relevante. Por outro lado, no início do ataque, muitas vezes, nem todos os membros da administração ou do conselho fiscal têm plena ciência dos fatos e de seus possíveis efeitos.

Contudo, a recém-editada Resolução CVM nº 44, de 23 de agosto, estabeleceu algumas presunções para fins da caracterização do mencionado ilícito. Dentre elas, presume-se que a pessoa que negociou valores mobiliários dispondo de informação relevante ainda não divulgada fez uso de tal informação na referida negociação; e que os acionistas controladores, diretos ou indiretos, diretores, membros do conselho de administração e do conselho fiscal, e a própria companhia, em relação aos negócios com valores mobiliários de própria emissão, têm acesso a toda informação relevante ainda não divulgada.

Dessa forma, imediatamente ao ter ciência do ataque, aconselha-se, como medida preventiva, que o diretor de Relações com Investidores informe aos demais administradores e insiders sobre o início de um blackout period, ou seja, um período no qual estará vedada a negociação de valores mobiliários de emissão da respectiva companhia pelas pessoas que eventualmente possam ter acesso às informações sobre o ataque.

Vale lembrar, entretanto, que nem sempre o ataque implicará na divulgação de fato relevante. O Ofício Circular CVM/SEP nº 1/2021 permite, inclusive, a critério da administração da companhia, que as informações relacionadas a riscos cibernéticos sejam divulgadas por meio de comunicado ao mercado.

A obrigatoriedade de divulgação de fato relevante apenas se dará caso se verifique que o ataque de ransomware ou suas consequências podem influir de modo ponderável na cotação dos valores mobiliários de emissão da companhia; na decisão dos investidores de comprar, vender ou manter aqueles valores mobiliários; ou na decisão dos investidores de exercer quaisquer direitos atrelados a tais valores mobiliários.

Assim, o blackout period deve apenas deixar de vigorar quando se confirmar que o ataque cibernético não foi significativo, ou, caso contrário, quando da divulgação do respectivo fato relevante, momento em que o mercado terá as mesmas informações que a companhia.

*Este artigo foi escrito por nosso sócio Luís Loria Flaks, da área de Societário e M&A. A publicação foi veiculada pelo Valor Econômico em 29/10/2021. Clique aqui e confira o artigo na íntegra.

Leia também:

- E-book | Ransomware: como enfrentar ataques cibernéticos
- E-book | Sanções Administrativas da LGPD: O que você precisa saber

› PROFISSIONAIS

Profissionais que aliam visão jurídica e visão de mercado

Luís Flaks