por Ana Albuquerque*

A gestão dos riscos cibernéticos desempenha um papel crucial nos processos de governança corporativa, à medida que as empresas enfrentam ameaças e ataques cibernéticos em um mundo cada vez mais globalizado. A proteção de ativos, dados e a preservação da reputação da empresa são elementos essenciais de governança corporativa, e a gestão dos riscos cibernéticos está ganhando cada vez mais destaque em empresas de todos os portes e segmentos.

O vazamento de dados é uma ameaça crescente para a segurança da informação e pode causar sérios danos à privacidade, à reputação e às finanças de indivíduos e de empresas. Ele pode ocorrer de diversas maneiras, incluindo ataques cibernéticos, falhas humanas, erros de programação e falta de proteção adequada de dados.

Segundo o relatório Reported Claim Index, da WTW, os funcionários estão no topo das causas de violações cibernéticas e de vazamento de dados nas empresas. A negligência ou atos maliciosos de empregados, como a divulgação acidental ou proposital de uma lista de contatos e perda e roubo de dispositivos móveis – são responsáveis por 58% das violações cibernéticas, seguido de 23% de ransomware. Uma observação relevante é que a principal causa de violações de dados na nuvem, de acordo com pesquisas, é o erro humano, representando 55% das ocorrências. Isso frequentemente resulta de funcionários clicando em links em e-mails de phishing ou respondendo a mensagens falsas. A cultura e o engajamento dos empregados desempenham um papel crucial na probabilidade de ocorrer uma violação cibernética, bem como a falta de apoio da liderança e especialistas em TI competentes.

Essas violações podem acarretar prejuízos significativos, incluindo extorsão, recuperação de dados, interrupção da rede, responsabilidade civil, além de multas e penalidades cíveis e administrativas, especialmente em conformidade com a LGPD.

Muitas vezes, só tomamos conhecimento do vazamento de dados de uma empresa quando este atinge uma magnitude significativa e causa danos substanciais. Buscando aumentar a transparência nesse processo, no final de julho, a SEC (sigla em inglês para Comissão de Valores Mobiliários dos Estados Unidos) divulgou os novos requisitos sobre os comunicados dos incidentes e a gestão dos riscos cibernéticos para todas as empresas de capital aberto listadas em Bolsa de Valores.

Após várias sugestões do setor privado, a SEC definiu as regras que as empresas obrigadas a cumprir a partir desse. A principal dela é que todos os incidentes materiais de segurança cibernética vivenciados pelas empresas deverão ser divulgados em até quatro dias úteis.

Além disso, as empresas precisarão divulgar, anualmente, informações relevantes sobre sua gestão, estratégia e governança de riscos de segurança cibernética.

A nova regra também fez alterações no conteúdo da divulgação. As empresas agora são obrigadas a divulgar os aspectos materiais da natureza, escopo e momento do incidente, seja nas questões operacionais, em relação aos clientes investidores e ao mercado em geral.

Outro ponto é que empresas deverão descrever como seus conselhos de administração estruturam processos para supervisionar riscos de segurança cibernética e como estas informações estarão descritas nos relatórios aos investidores.

Dessa forma, a regra da Comissão de Valores Mobiliários dos Estados Unidos busca facilitar a identificação do impacto financeiro de eventuais incidentes para o mercado como um todo. Esse impacto não é pequeno, como indicado pelo Reported Claim Index, que revelou que os prejuízos globais causados por ransomwares, no ano passado, totalizaram U$ 20 bilhões, e esse valor continua em. Para o próximo ano, as estimativas apontam para prejuízos na ordem de U$ 42

bilhões, com projeções de atingir a marca de U$ 265 bilhões até 2031.

É provável que o Brasil – assim como outros países do mundo – deva seguir o modelo proposto pelos Estados Unidos e implementar regulamentações similares em poucos meses. Lembrando que, empresas brasileiras listadas nas bolsas americanas, deverão cumprir de imediato as diretrizes estabelecidas nessa regulamentação.

As empresas se deparam com desafios significativos na proteção de de seus dados sensíveis e críticos. Por isso, é primordial que elas implementem medidas de segurança cibernética abrangendo controles preventivos, detectivos e responsivos, além de conduzirem auditorias regulares para identificar vulnerabilidades.Agora, empresas e gestores não podem mais encarar o risco cibernético apenas como um problema técnico; ele deve ser considerado como uma questão de governança.

*__Ana Albuquerque__
é diretora de Linhas Financeiras na WTW

(12.12.2023)