

***Na avaliação da Marsh, enquanto um incêndio em um armazém gera prejuízos de R\$ 40 milhões, com ataques cibernéticos as empresas perdem R\$ 33 milhões, em 48 horas***

Por Marta Schuh, diretora de Cyber Risk da consultoria de risco e corretora Marsh Brasil

Nos últimos 3 anos, os incidentes cibernéticos se tornaram mais presentes nos headlines da imprensa (nas manchetes). Isso é uma preocupação global de lideranças empresariais e políticas, conforme mostra o Global Risk Report 2022. O documento produzido pela Marsh McLennan, em parceria com o Fórum Econômico Mundial, detalha que as falhas de segurança cibernética estão entre as maiores ameaças para o mundo no curto e médio prazo.

À medida que as empresas se recuperam da pandemia, elas estão aprimorando o foco na resiliência organizacional e nas credenciais ESG. Com as ameaças cibernéticas crescendo mais rápido do que nossa capacidade de erradicá-las, está claro que nem a resiliência nem a governança são possíveis sem planos de gerenciamento de risco cibernético sofisticados e confiáveis.

Até então, líderes de negócios, conselheiros e gestores de risco não estavam totalmente certos da necessidade ou apresentavam um olhar cauteloso e rejeitavam a ideia de que este é um risco que traz impactos financeiros significativos. Agora, as apólices de seguro cyber e investimentos na área de segurança começam a ser vistos como prioridades.

Em 2020, quando o mundo foi abalado por uma pandemia global e as rotinas de trabalho, estruturas operacionais e a vida em geral como a conhecíamos sofreu uma reviravolta completa, equipes de TI em todo o mundo foram empurradas para as funções de a missão crítica de garantir (i) disponibilidade de sistemas e (ii) segurança de ambientes num modelo de trabalho remoto. A pandemia coincidiu com relatos de aumentos sem precedentes nos crimes cibernéticos. Em 2021, hackers cometeram ataques ainda maiores. Incidentes como o da Colonial Pipeline, por exemplo, impactaram a distribuição de combustível na costa leste americana.

Para comprar os impactos dos ataques cibernéticos, recentemente avaliamos os prejuízos de uma empresa que sofreu um incêndio com os prejuízos de uma empresa vítima de ataques de hackers. A empresa do ramo alimentício teve um prejuízo de R\$ 40 milhões decorrente de um incêndio em seu armazém contendo estoques.

Já a companhia que teve o seu sistema invadido por hackers, ficou paralisada por 48 horas e acumulou perdas de R\$ 33 milhões -- entre custos de consultorias para incidente de respostas, custos operacionais adicionais e perda de receita, amparados atualmente por apólice de seguro cyber. Como se vê, tais incidentes evidenciaram prejuízos em valores compatíveis a perdas aos riscos patrimoniais como danos da natureza, explosões/incêndios.

Esses prejuízos mudaram a forma como as organizações enquadram as ameaças e lidam com os riscos cibernéticos, considerando o custo real de um evento cibernético em seus negócios. Quando os incidentes assumem proporções maiores que os impactos apenas em TI, as consequências podem ser catastróficas.

Diferente de incidentes tradicionais patrimoniais, os quais raramente afetam mais de um local de operação, os incidentes cyber tem potencial simultâneo, podendo paralisar a totalidade da empresa em diversos locais e áreas de operação e gerando prejuízos rapidamente. De acordo com nossas análises, o tempo médio de inatividade de empresas vítimas de ransomware aumentou 53% no último ano, tendo como período médio 23 dias para restabelecer todos os sistemas, bancos de dados e operação ao normal.

Com um risco em constante evolução e as empresas cada vez mais dependentes da tecnologia, líderes organizacionais precisam estar à altura das ameaças. Para isso, é preciso elevar o nível de cyber segurança em toda a organização e considera-la não apenas como uma ferramenta, mas um

## Legismap Roncarati

Hackers geram prejuízos financeiros para as empresas semelhantes às perdas que elas têm com incêndios e catástrofes naturais

---

ponto estratégico do negócio.

**Fonte:** Conteúdo, em 14.06.2022