A Aon plc (NYSE: AON), empresa líder mundial em serviços profissionais, revela em seu Relatório Global de Riscos Cibernéticos 2025 que eventos cibernéticos com potencial de impacto reputacional podem resultar em uma queda média de 27% no valor de mercado para os acionistas.

As conclusões se baseiam em uma pesquisa da Aon realizada em 2023, que já indicava que incidentes cibernéticos significativos provocavam uma redução média de 9% no valor para os acionistas ao longo do ano seguinte. O relatório deste ano aprofunda essa análise, examinando mais de 1.400 eventos cibernéticos globais para identificar quais tipos de ataques têm maior probabilidade de evoluir para riscos reputacionais e quais podem causar maiores danos quando isso ocorre.

“O risco cibernético deixou de ser um problema exclusivamente tecnológico; hoje, é um desafio que envolve toda a organização”, afirma Marco Mendes, Cyber Product Leader para o Brasil na Aon. “Nossa pesquisa mais recente reforça a importância da mitigação proativa de riscos. Empresas que investem em preparação e resiliência estão muito mais bem posicionadas para evitar as consequências reputacionais e financeiras de um incidente cibernético, sendo o tempo de paralisação dos negócios o principal fator de impacto na reputação da empresa.”

Marco destaca ainda que “as empresas da América Latina avançaram no combate aos ataques cibernéticos, o que resultou em uma leve melhora na pontuação geral de risco da região. Nesse sentido, empresas locais estão mais preparadas para contratar seguros cibernéticos, graças às ações de capacitação interna (incluindo a alta liderança), que promovem maturidade digital, maior conscientização e contam com um mercado mais receptivo”.

Principais descobertas do relatório:

- Dos 1.414 eventos cibernéticos analisados, 56 evoluíram para incidentes com impacto reputacional, definidos como aqueles que geram significativa atenção da mídia e resultam em queda mensurável no preço das ações.
- Empresas afetadas por esse tipo de evento registraram uma redução média de 27% no valor de mercado para os acionistas.
- Ataques com malware e ransomware foram os mais propensos a gerar danos à reputação, representando 60% dos incidentes com impacto reputacional, embora sejam responsáveis por apenas 45% do total de eventos cibernéticos.
- Foram identificados cinco fatores-chave para a recuperação de valor: preparação, liderança, ação rápida, comunicação e transformação, considerados alavancas críticas para mitigar os efeitos reputacionais.

Sobre a América Latina, o relatório destaca:

- Em 2024, a América Latina e o Caribe foram as regiões com o crescimento mais acelerado em incidentes cibernéticos reportados, com taxa média anual de 25% na última década, segundo o Banco Mundial.
- Os países mais atacados em 2024 foram: Brasil (47% dos ataques), México (23%) e Colômbia (8%), com base em dados do setor privado.
- A leve melhora nas pontuações de risco entre clientes da Aon evidencia um esforço contínuo na região. A pontuação média de risco das empresas latino-americanas em 2024 foi de 2,59 (em uma escala de 0 a 4), indicando um estágio entre “preparação básica” e “gestão estruturada”, ligeiramente abaixo da média global de 2,71.
- A falta de investimentos em cibersegurança e a predominância de pequenas e médias empresas (99,5% do mercado) tornam a América Latina um alvo ideal para grupos especializados em ransomware, conforme apontado pela OCDE (Organização para a Cooperação e Desenvolvimento Econômico).

O relatório também enfatiza o desafio crescente da gestão de riscos não seguráveis. Embora o

seguro cibernético possa transferir parte da exposição financeira, o risco reputacional permanece, em grande parte, não transferível, o que torna a gestão proativa de riscos e a resposta a crises ainda mais essenciais.

O **Relatório Global de Riscos Cibernéticos 2025 da Aon** é baseado em dados exclusivos obtidos por meio da **Aon's Cyber Quotient Evaluation (CyQu)**, uma plataforma eletrônica proprietária que agiliza o processo de subscrição de seguros cibernéticos. Essa ferramenta oferece às organizações informações acionáveis sobre suas exposições cibernéticas e sua segurabilidade, contribuindo para resultados de subscrição mais eficazes e estratégias mais robustas de gestão de riscos.

Fonte: Aon/FSB, em 23.06.2025.