

Um novo relatório do Zurich Insurance Group, grupo segurador multilinha líder global e fornecedor de serviços de resiliência, e Marsh McLennan (NYSE: MMC), empresa líder nas áreas de risco, estratégia e pessoas, destaca a necessidade crítica de um maior envolvimento do setor público para fortalecer a resiliência social no caso de ocorrer um evento cibernético catastrófico.

O documento, intitulado “[Fechando a lacuna de proteção contra riscos cibernéticos](#)”, ressalta que é preciso criar soluções inovadoras para resolver as lacunas dos sistemas de proteção – principalmente em relação às pequenas e médias empresas – que devem receber atenção especial, pois, muitas vezes, não possuem seguro adequado para novas ameaças cibernéticas em constante evolução. Malwares em larga escala e interrupções na nuvem são alguns dos exemplos de incidentes cibernéticos que são atualmente considerados seguráveis até um certo nível de perda financeira, e eventos como falhas em infraestruturas críticas, são geralmente considerados não seguráveis.

Mario Greco, CEO do Zurich Insurance Group, ressalta que a ameaça de ataques cibernéticos representa um risco significativo para a estabilidade social e econômica. “Como seguradora, podemos oferecer algum grau de proteção, mas temos de reconhecer que eventos cibernéticos catastróficos em grande escala apresentam riscos de acumulação substanciais que não podem ser suportados apenas pelo setor privado. Por conseguinte, aumentar a resiliência cibernética é vital para fechar esta lacuna de proteção. Alcançar isto requer fortes parcerias público-privadas para desenvolver estratégias abrangentes que garantam o nosso futuro digital”.

John Doyle, CEO da Marsh McLennan, enfatiza: “A ameaça dos riscos cibernéticos requer uma ação conjunta para garantir que as organizações estejam protegidas. A indústria de seguros e o setor público devem compreender plenamente a ampla gama de riscos cibernéticos seguráveis e não seguráveis. Portanto, a colaboração é a chave para desenvolver soluções inovadoras, informar os compradores de seguros, melhorar o mercado de seguros cibernéticos e estabelecer parcerias público-privadas robustas que protejam a nossa sociedade e economia destes riscos potencialmente catastróficos”.

De acordo com o relatório, é necessário estabelecer um marco comum para reforçar o compartilhamento de dados, uma maior e mais significativa colaboração e inovação entre a indústria de seguros e o setor público, para ajudar a fechar esta lacuna de proteção, reforçar a resiliência e salvaguardar a sociedade e as economias das crescentes ameaças cibernéticas. Isso não inclui apenas ataques de ransomware e ameaças de agentes maliciosos, mas também interrupções globais de tecnologia da informação e outros incidentes cada vez mais interligados.

O marco incluiria incentivos robustos como alternativa a uma maior regulamentação, métodos para mensurar o risco cibernético catastrófico quantificável, e estratégias para gerenciar o risco cibernético não quantificável através de parcerias público-privadas. O relatório destaca que estas medidas poderiam ajudar a sustentar a economia em geral, e criar capacidade para o mercado de seguros apoiar a sociedade num contexto de graves riscos de acumulação financeira.

“A adoção de seguros cibernéticos na América Latina e no Caribe permanece extremamente baixa, e destaca o valor de colaborações como essa considerando as diferentes exposições a riscos cibernéticos, e o valor da transferência dos riscos por meio de seguros como proteção financeira”, acrescenta Holly Medforth, Líder de Prática de Cyber para Marsh Specialty na América Latina e Caribe.

Já Hellen Fernandes, gerente de Linhas Financeiras e Cyber da Zurich no Brasil, reforça que o seguro é uma ferramenta essencial para mitigar os riscos associados às ameaças cibernéticas, fornecendo suporte financeiro e operacional para ajudar na rápida recuperação das empresas, minimizando os impactos dos ataques. Porém, são a última camada de proteção contra os riscos cibernéticos.

Legismap Roncarati

Zurich e Marsh McLennan divulgam relatório defendendo ações público-privadas para fechar lacunas na proteção cibernética e aumentar a resiliência

“O custo global dos ciberataques está projetado para aumentar para quase USD 24 trilhões até 2027, em comparação com os cerca de USD 8,5 trilhões em 2022. Mesmo com estimativas de os prêmios em seguros dobrarem nesse período, passando dos atuais USD 14 bilhões para mais de USD 29 bilhões, empresas de todos os portes precisam ter em mente a importância da implementação de planos robustos de gerenciamento de risco e segurança da informação para aumentar a resiliência cibernética, para além do seguro. O mercado segurador pode ajudar nessa construção, mas são necessárias medidas mais amplas e integrativas para lidar com os riscos crescentes de exposição, que estão entre os principais riscos globais de curto prazo”, conclui.

Fonte: Zurich e Marsh McLennan/Conteúdo Comunicação, em 06.09.2024.