Por Juliana Casiradzi

Diretora de Responsabilidade Financeira e Profissional (FINPRO) e Cyber da consultoria de riscos e corretora Marsh Brasil

Em julho de 2024 uma falha crítica na atualização do software Falcon Sensor, ferramenta de segurança cibernética da CrowdStrike, gerou uma interrupção global em sistemas Windows. O apagão afetou diretamente grandes organizações que operam infraestruturas críticas, como companhias aéreas, bancos e hospitais.

A Delta Air Lines, por exemplo, teve que cancelar mais de 7 mil voos, com perdas estimadas em aproximadamente US$ 500 milhões. Apesar de a falha não ter sido causada por um ataque hacker, cibercriminosos aproveitaram o caos para disseminar malwares via e-mails de phishing.

O incidente gerou prejuízos financeiros, operacionais e reputacionais na ordem de bilhões de dólares, evidenciando a vulnerabilidade das empresas frente às ameaças que se multiplicam rapidamente com o avanço da conectividade digital.

Um estudo da Marsh McLennan, em parceria com a Zurich, estimou que o custo global com cibersegurança deve aumentar para quase US$24 trilhões até 2027, em comparação com US$8,5 trilhões em 2022 — e isso não inclui o custo de eventos não maliciosos.

Embora incidentes cibernéticos como o CrowdStrike pareçam imprevisíveis e incontroláveis, é possível adotar diversas medidas proativas para minimizar seus riscos e impactos. A possível falta de mecanismos internos robustos para contingência e a confiança excessiva em fornecedores externos amplificaram as consequências. Além disso, a falta de redundância e de processos rápidos de recuperação de desastres prolongou a paralisação além do necessário.

Para construir resiliência, as empresas precisam ir além das tecnologias avançadas de proteção, buscando uma abordagem mais abrangente que combine inovação no setor de seguros, colaboração intersetorial, testes de falhas, planejamento de recuperação e investimento contínuo em medidas de cibersegurança.

O mercado está crescendo, mas os riscos também

O mercado de seguros cibernéticos está em rápida expansão, com prêmios brutos projetados para saltar de US$14 bilhões em 2023 para US$29 bilhões até 2027. Por outro lado, os ataques estão se tornando cada vez mais sofisticados e sistêmicos, explorando inteligência artificial generativa para atingir infraestruturas críticas, cadeias de suprimentos e governos — o que supera a capacidade dos seguros e das abordagens tradicionais de gerenciamento de riscos.

Em 2023, apenas 1% das perdas econômicas causadas por ataques cibernéticos estavam seguradas. Apesar do aumento na procura por transferência de riscos, esse crescimento ainda é desequilibrado: há uma preocupação significativa com o número de pequenas e médias empresas sem seguro ou com cobertura insuficiente.

Recentemente, a indústria de seguros passou a incentivar a adoção das melhores práticas de segurança cibernética, como o uso de autenticação multifator, soluções de gerenciamento de identidade e acesso e backups imutáveis. Essas medidas têm demonstrado eficácia na prevenção e recuperação de ataques de ransomware e outras formas de ciberataques, reduzindo o pool de riscos seguráveis.

No entanto, a principal dificuldade do mercado de seguros cibernéticos ainda é quantificar e precificar os riscos de forma eficaz, devido à incerteza sobre a frequência e a gravidade dos ataques, além da rápida evolução tecnológica. Essa lacuna de proteção é um desafio social que urgentemente necessita de ação coletiva, envolvendo também o setor público.

Parcerias para reduzir lacunas de proteção

Embora muitos riscos cibernéticos catastróficos sejam seguráveis, eventos de grande escala podem exceder a capacidade financeira dos mercados tradicionais. Nesses casos, parcerias com o setor público serão fundamentais para sustentar o mercado e mitigar impactos econômicos.

O objetivo é compartilhar informações críticas entre os setores. Por exemplo, iniciativas como o CIDAWG, nos EUA, permitem analisar quais controles de segurança funcionam melhor contra ciberataques. Além disso, o compartilhamento de informações, como inteligência sobre ameaças, vulnerabilidades e padrões de ataques, facilita a adoção de estratégias mais informadas e robustas para enfrentamento.

Legislações como o “Digital Operational Resilience Act”, da União Europeia, visam garantir que setores essenciais, como o financeiro, adotem processos rigorosos de gestão de riscos tecnológicos, com foco especial em proteger pequenas e médias empresas.

Todo esse ciclo virtuoso coloca o mercado segurador em uma posição favorável para proteger as empresas contra os riscos cibernéticos mais críticos, cumprindo assim seu maior propósito: fomentar sociedades inovadoras, resilientes e adaptáveis, ao mesmo tempo em que protege a segurança econômica e nacional.

(13.03.2025)