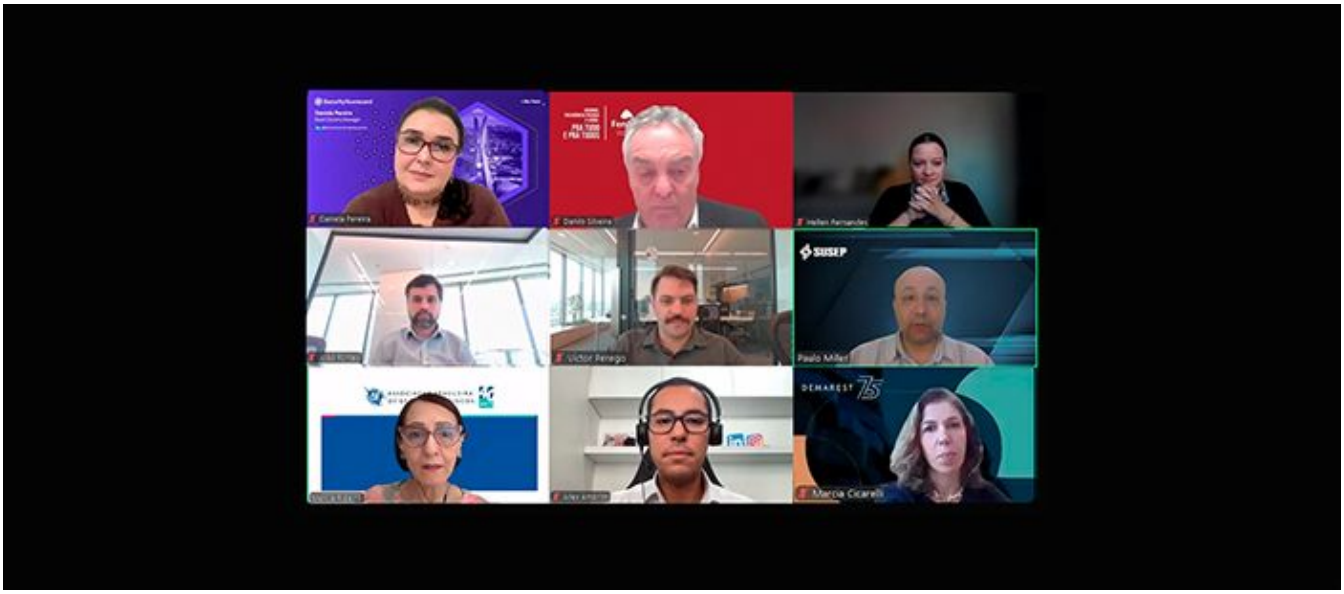

Em 2025, os prejuízos com crimes cibernéticos devem chegar a 12 trilhões de dólares em todo o mundo, de acordo com estudo informado pelo presidente do Instituto Brasileiro de Segurança, Proteção e Privacidade de Dados (IBRASPD), Allex Amorim, durante o webinar “Seguro Cibernético: Tipos de Riscos e Soluções de Seguros!”, realizado pela CNseg e pela FenSeg nesta terça-feira, dia 16 de outubro.

No Brasil, de acordo com a diretora de Vendas da consultoria Security Scorecard, Daniela Pereira, houve um aumento de 67% no número de ataques no segundo trimestre de 2024. Ainda assim, segundo ela, nosso país vai muito bem em termos de segurança cibernética, na comparação com os demais países da América Latina e Caribe. Entretanto, afirmou, isso não é motivo para nos “descuidarmos”, até porque, em 2023, fomos o 3º país com o maior número de ataques de ransomware, um dos crimes cibernéticos mais comuns, caracterizado pela instalação de um malware que sequestra dados ou dispositivos de uma vítima, bloqueando-os até que um resgate seja pago.

Os crimes cibernéticos, lembrou a sócia de Seguros e Resseguros da Demarest Advogados, Marcia Cicarelli, ameaçam a continuidade dos negócios das empresas, podendo gerar muitos prejuízos financeiros e reputacionais, além de litígios e sanções regulatórias.

As sanções regulatórias, explicou, são em função da **Lei 13.709/2018**, conhecida como Lei Geral de Proteção de Dados, ou simplesmente LGPD, que definiu que a **Autoridade Nacional de Proteção de Dados** (ANPD) tem função fiscalizatória e de aplicação de multas para as empresas que falharem na segurança dos dados pessoais que manipulam.

Mas a ANPD também tem uma função pedagógica, de fortalecimento de boas práticas, até mesmo para que os riscos cibernéticos não se tornem algo não segurável, como explicou o superintendente de Financial Lines da AIG Seguros Brasil e coordenador da subcomissão de Linhas Financeiras da FenSeg, João Fontes. Atualmente, explicou ele, há 10 seguradoras atuando ativamente em seguros de riscos cibernéticos no Brasil, tendo movimentado, até hoje quase R$ 700 milhões em prêmios.

Concordando com João Fontes, o assessor do Diretor de Regulação Prudencial e Estudos Econômicos da SUSEP, Paulo Miller, afirmou que “as melhores práticas ajudam as empresas a estarem em situação que possam ser seguráveis”. Melhores práticas, estas, que o setor segurador, além de fornecer proteção financeira, tem o papel de propagar. Ele informou que a Superintendência de Seguros Privados tem tratado com muita atenção o tema da segurança

cibernética em um grupo de trabalho interno com o objetivo de avaliar a situação e discutir propostas de melhorias na sua regulação e supervisão.

O gerente de Subscrição de Cyber da AIG Seguros Brasil e membro da subcomissão de Linhas Financeiras da FenSeg, Victor Perego, e a gerente Executiva de Subscrição Financial Lines e Cyber da Zurich Brasil, Hellen Fernandes, explicaram que os seguros contra riscos cibernéticos possuem três principais tipos de cobertura:

- **Respostas a incidentes:** envolve o reembolso dos custos que a empresa tem para se recuperar dos ataques, envolvendo uma investigação e a recuperação do ambiente tecnológico. Toda apólice tem um serviço de assistência 24/7, com um exército de pessoas bem treinadas e capacitadas para lidar com essas crises. Se o incidente se torna público, a apólice ainda oferece um trabalho de assessoria de imprensa.
- **Responsabilidade civil:** todas as empresas têm responsabilidades legais e regulatórias e quando ocorre o vazamento de dados de uma pessoa ou grupo de pessoas, a empresa pode vir a ser processada e a cobertura é acionada para o pagamento dos custos de defesa, estendendo-se até uma eventual indenização, acordo e/ou assinatura de termo de compromisso e multa pela LGPD, Ministério Público ou Procon.
- **Prejuízos ao segurado**: boa parte dos sinistros pagos decorrem dos lucros cessantes, como os relacionados ao sequestro de dados. Nesses casos, as seguradoras também disponibilizam especialistas, até mesmo para identificar se a extorsão é real e negociar o pagamento do resgate, podendo até vir a reembolsar a empresa pelo valor pago no resgate dos dados. A cobertura ainda ajuda o segurado a arcar com as despesas operacionais para que ele possa voltar a operar.

Já ao final do webinar, seu moderador, o diretor-Executivo da FenSeg, Danilo Silveira, alertou para a necessidade de desenvolvermos conceitos de análise de riscos muito mais amplos para lidar com o tema dos riscos cibernéticos. “Estamos diante de um novo paradigma que pode envolver cifras exorbitantes”, concluiu.

Fonte: CNseg, em 17.10.2024