O inimigo invisível

Uma das mudanças de comportamento mais significativas que a pandemia da Covid-19 tem nos imputado é a aceleração vigorosa do processo de digitalização em todo o mundo. Para dar conta do trabalho em casa ou ofertar produtos e serviços de maneira virtual, pessoas e empresas se viram obrigadas a ampliar substancialmente o uso de ferramentas tecnológicas disponíveis no universo *cyber*.

Segundo a IDC Brasil (International Data Corporation Pesquisa de Mercado e Consultoria), até o fim de 2021, os investimentos em TI aumentarão 10%, principalmente em *hardware*, *software* e serviços. Na América Latina, o *software* deverá ser responsável por 18% dos investimentos, os serviços de TI por 22% e *hardware* por 60%. Já o setor de nuvem pública deverá registrar um crescimento de 46,7% entre 2019 e 2023.

O ônus deste processo, no entanto, tem nome e sobrenome, e se chama ataque cibernético. Com o volume de negócios virtuais aumentando de forma exponencial, empresas que não estão preparadas para a construção de uma blindagem cibernética podem perder cifras na casa de trilhões de dólares. Tal estimativa foi feita pela consultoria americana Gartner, no ano passado, em meio à observância da tentativa do setor privado em se proteger dos prejuízos de ataques de *hackers*, que invadiram sistemas de órgãos públicos em ações amplamente noticiadas pela imprensa mundial.

O prejuízo não é apenas financeiro. Em função da implantação da Lei Geral de Proteção de Dados (LGPD), no Brasil, e da sua equivalente europeia, a *General Data Protection Regulation (GDPR)*, empresas podem sofrer sanções legais em casos de vazamento de dados de seus clientes, causados por brechas na *cyber security*. Preocupado com este cenário, o setor privado dobrou o investimento em seguros de riscos cibernéticos entre 2019 e 2020.

De acordo com informações da Superintendência de Seguros Privados (Susep), os sinistros relacionados a ataques cibernéticos aumentaram 1.950% no Brasil em 2020. Já levantamento da Federação Nacional de Seguros Gerais (FenSeg) apontou que o valor pago a título de indenizações nesse segmento pulou de R$ 1 milhão para R$ 32 milhões no ano passado. Outro dado relevante: a arrecadação do Seguro de Riscos Cibernéticos subiu 99% em volume de prêmios, passando de R$ 21 milhões em 2019 para R$ 41 milhões em 2020.

Atenta ao crescimento dos ataques cibernéticos, a indústria de seguros está preparada para estimular a prevenção e mitigação de riscos. O portfólio de algumas seguradoras foi ampliado no período pós-pandemia, oferecendo garantias nos produtos de riscos cibernéticos como, por exemplo, suporte técnico em tempo integral por empresa especializada em gerenciamento de risco, cobertura dos gastos com a recuperação de dados, apoio jurídico e despesas com indenizações devidas a terceiros pelo vazamento de dados.

Simultaneamente, no último ano, percebemos a necessidade de um investimento cada vez maior na criação e na oferta de programas educacionais específicos para lidar com as ameaças cibernéticas. É preciso fornecer aos gestores de empresas conhecimentos estratégicos sobre o tema, para que possam entender, interpretar e reagir proativamente a este risco. A maior lacuna no mercado se deve, justamente, à falta de profissionais qualificados para a construção de uma cultura de *cyber* segurança em seus negócios ou nas empresas nas quais atuam.

A resistência que havia por parte de pessoas e empresas e, ainda, a falta de conhecimento sobre as atuais operações comerciais estão se dissipando dia após dia. A crescente exposição digital provocada pelo novo normal exige mais investimentos de ambos os polos do negócio, não apenas em aparatos tecnológicos, mas, principalmente, na capacitação e no conhecimento das pessoas sobre o tema segurança da informação.

Tarcísio Godoy é diretor-geral da Escola de Negócios e Seguros (ENS)