Resolução do BACEN equipara risco cibernético a risco operacional

Por Marta Schuh (*)

Este ano, o risco cibernético aparece no ranking do **Relatório de Riscos Globais 2020** como uma das principais ameaças aos negócios. Não por menos, neste relatório produzido pelo World Economic Forum em parceria com a Marsh & McLennan, a Zurich e as universidades de Oxford, Singapura e Pensilvânia, o ataque cibernético está entre os riscos que mais aumentará neste ano. Por isso, a ameaça de ataques de hackers aos sistemas das empresas é uma preocupação global.

Todos os países modernizaram os seus arcabouços regulatórios criando mecanismos legais para punir crimes cibernéticos. Também foram criadas regras para as organizações públicas e privadas que têm em suas bases um robusto volume de dados e informações dos cidadãos e consumidores. Foi aí, que seguindo o que ocorreu na União Europeia em 2018, com a entrada em vigor do GDPR (General Data Protection Regulation), o Brasil criou a Lei Geral de Proteção de Dados (LGPD) - em vigor a partir de agosto deste ano.

Neste contexto de proteger os dados dos consumidores, surge também agora a Resolução do Banco Central (BACEN). A **Circular BACEN nº 3.979 de 30.01.2020** , dispõe sobre a constituição e a atualização da base de dados de risco operacional e a remessa ao Banco Central do Brasil de informações relativas a eventos de risco operacional. Em linhas gerais, a resolução equipara o risco cibernético ao risco operacional.

A Circular nº 3.979 consolida os esforços do Banco Central de garantir que o sistema financeiro nacional se mantenha sólido e estável e proteja os consumidores. Em 2018, o BACEN já havia criado a Resolução 4.658, com o objetivo de mitigar os riscos cibernéticos e proteger as instituições financeiras. Uma preocupação pertinente. De acordo com a pesquisa da Febraban (Federação Brasileira de Bancos), as transações financeiras via aplicativos em dispositivos móveis, representou 35% do total de transações realizadas em 2017, 8% a mais que no ano de 2016.

O aumento contínuo de ataques cibernéticos, como ransomware, violações de dados e ataques de negação de serviço distribuídos são altamente direcionados a instituições financeiras. Embora raramente catastróficos, esses eventos criam custos diretos e indiretos para os bancos e essa realidade impõe às instituições financeiras a necessidade de mitigação

de riscos, seja fazendo a transferência dos mesmos para apólice de seguros ou implantando robustos programas de gerenciamento de risco.

O seguro cibernético deve ser visto como um mecanismo de mitigação de prejuízos em potencial e de resposta a incidentes que constituem as novas normas regulatórias, uma vez que o seguro não apenas indeniza os custos relacionados a incidentes, mas também possui o amparo de um time de gestão de crises.

(*) **Marta Schuh** é Líder de Cyber da **Marsh Brasil**.

21.02.2020