Riscos cibernéticos e a nova realidade empresarial

MARTA HELENA SCHUH

Os riscos cibernéticos não são algo do futuro, mas uma realidade do presente, e atingem todas as empresas, sem distinção de tamanho, setor ou geografia. O impacto dos ataques relacionados à tecnologia assume diversas formas, como violações de proteção de dados, roubo de propriedade intelectual, danos à propriedade e à reputação e interrupção de negócios. Nesse ambiente, aumentaram acentuadamente os custos empresariais.

No Brasil, não se conhece a maioria dos incidentes cibernéticos porque não há obrigatoriedade de notificação a órgãos reguladores. Estima-se que menos de 10% das principais violações sejam reveladas. Uma prévia da pesquisa JLT Cyber View 2018 demonstra que 30% das empresas já foram alvo de incidentes e, de acordo com relatório IBM Ponenon 2018, o Brasil lidera a maior probabilidade de um vazamento de dados, com risco de 43% entre 15 países do estudo.

Desde de janeiro deste ano, o Ministério Público Federal tem adotado uma série de ações contra empresas cujos dados de clientes foram violados. Com a aprovação da nova Lei Geral de Proteção de Dados – LGPD, que entrará em vigor em fevereiro 2020, as medidas serão intensificadas, o que inclui a obrigatoriedade da notificação ao órgão regulador e aos indivíduos impactados em incidentes.

Na percepção da maioria de clientes, companhias que sofrem violações de dados são vistas como culpadas pelo ocorrido.

É fundamental que os gestores estejam mais envolvidos na abordagem adequada sobre segurança cibernética para evitar prejuízos – financeiros e de imagem.

UM RISCO DO PRESENTE

Os riscos cibernéticos representam um dos maiores desafios hoje para as empresas. Não só os ataques se tornaram mais frequentes como seu escopo e sofisticação estão aumentando. Diante disso, a segurança cibernética emergiu rapidamente como uma área-chave de risco corporativo. A pesquisa JLT mostra que cerca de 22% das empresas respondentes tiveram paradas operacionais diante de um incidente cibernético, resultando em 13% de perdas diretas de receita.

Essas situações devem ser consideradas seriamente pelo conselho de administração das empresas. Na percepção da maioria de clientes, companhias que sofrem violações de dados são vistas como culpadas pelo ocorrido. É fundamental que os gestores estejam mais envolvidos na abordagem adequada sobre segurança cibernética para evitar prejuízos – financeiros e de imagem.

Embora esta seja vista como uma nova era de riscos, o cybercrime não difere dos demais delitos e incidentes que as empresas sempre enfrentaram, como fraude, roubo, danos físicos, espionagem e outros. Os crimes sãos os mesmos, a forma é que mudou, devido à tecnologia. Os danos, no entanto, são tão severos quanto antes, ou até mesmo maiores.

Essa recente realidade exige das corporações uma nova cultura. Tradicionalmente, as empresas avaliavam investimentos em tecnologia como algo voltado à melhoria operacional e para provocar inovação em sua indústria, não em necessidades de segurança. Não é mais viável manter esse comportamento.

Se anteriormente esta era uma responsabilidade do diretor de TI, a pauta passou a ser do conselho, que tem o dever fiduciário de entender o tema e supervisionar ações, já que um ataque cibernético pode causar perdas até mais significativas do que se costuma ver nos ramos usualmente protegidos por uma apólice de seguros.

O aumento global de ataques fez com que as empresas considerassem uma apólice de Seguro Cyber, de cobertura ampla e bem planejada, não apenas para os riscos decorrentes de uma violação de vazamento de dados, mas também para o imediato acesso a especialistas previstos nessa documentação.

Hoje as empresas estão sujeitas ao escrutínio público imediato e a nova realidade essencialmente removeu a distinção entre membro do conselho e o executivo de TI. Além disso, com a entrada de leis de proteção de dados e normas de

segurança cibernéticas por diferentes órgãos reguladores, amplia-se o espaço não apenas para o Seguro Cyber, mas também para o Seguro de D&O. Com a prestação de contas e *compliance* das medidas figurando como um tema central nos novos regulamentos, o Cyber não é o único seguro relevante a ser considerado, e a ênfase também deve ser colocada no seguro de Responsabilidade de Diretores.

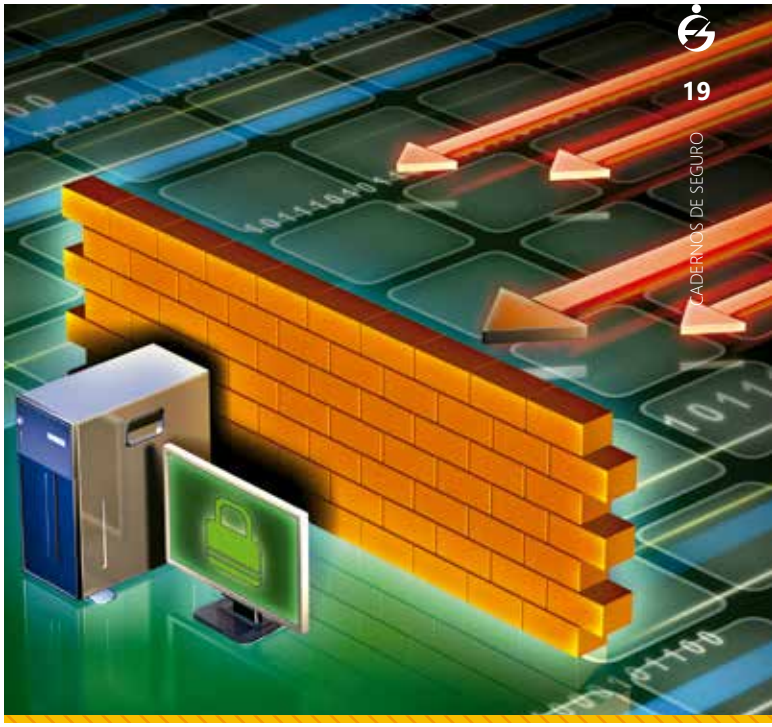
O engajamento de segurança cibernética para os membros da alta gestão das empresas não significa que devam obter graus de ciência da computação ou conferir pessoalmente o firewall, implantações de sistemas ou testes de intrusão. Conselhos de administração podem realizar a supervisão da segurança cibernética através do envolvimento ativo no acompanhamento das medidas adotadas. É crucial apoiar as iniciativas de TI não só no que se diz respeito à aquisição de ferramentas operacionais, mas também ao investimento em segurança. Nenhuma ferramenta é 100% eficaz, e se um *hacker* invadir sistemas e causar prejuízos, a empresa terá que que arcar com os custos. Ter um comitê estruturado para acompanhamento das medidas, uma auditoria anual, além do seguro, são medidas a serem consideradas para mitigar esses riscos.

MERCADO SEGURO CYBER

A KPMG estima um crescimento desse mercado de US$ 2,5 bilhões em 2015 para US$ 7,5 bilhões em 2020, alcançando US$ 20 bilhões até 2025 devido às mudanças em regulação como a que entrou em vigor na Europa em maio 2018, a GDPR.

No Brasil, o produto, que até este ano era pouco visado e enfrentava certa resistência de clientes, passou a despertar o interesse das companhias frente aos impactos financeiros a que podem estar expostas. Cerca de 13% das companhias que responderam à pesquisa JLT adquiriram uma apólice de Seguro Cibernético no Brasil nos últimos 12 meses, e 35% estão prevendo a contratação no próximo ano, com inclusão no orçamento. Estima-se que o mercado tenha R$10 milhões em valor de prêmio emitido até o presente momento. Com a aprovação da Lei Geral de Proteção de Dados no país, a procura pelo seguro e o número de cotações já aumentaram significantemente desde agosto. O mercado espera um crescimento de 200% na emissão de novas apólices.

Um dos maiores desafios enfrentados por clientes e corretores é determinar o limite e as necessidades de coberturas. As organizações têm dificuldade para identificar e avaliar o risco cibernético de maneira quantitativa, em termos que permitam que os níveis de Executivo e Diretoria entendam as consequências financeiras em suas organizações.



A estrutura de modelagem utiliza técnicas da ciência atuarial e uma medida do risco operacional para estimar as perdas agregadas por ataques cibernéticos. Isso requer uma avaliação dos dados individuais, sistemas, processos e outras peculiaridades do cliente, bem como frequência dos ataques às diferentes indústrias, além de uma ideia da distribuição das perdas causadas por esses incidentes. De toda forma, como outras apólices sem um valor de ativo – como D&O, Responsabilidade Civil, E&O –, o valor em risco é subjetivo em relação ao apetite do cliente em questão.

A constante evolução das ameaças está claramente impondo responsabilidades adicionais aos diretores e conselho administrativo das empresas. O prejuízo financeiro de uma violação de dados pode ser enorme; como tal, os diretores devem se preocupar tanto com sua obrigação fiduciária perante a empresa quanto com seus acionistas, bem como com os seus ativos pessoais, que estão em risco no caso de uma reivindicação por alegada gestão ilícita. A apólice de riscos cibernéticos é a única que pode prover tal proteção. ●

MARTA HELENA SCHUH
Especialista em riscos cibernéticos da JLT Brasil. Bacharelada em Business pela University of London, Certificada em Economics of Cybersecurity pela Delft University of Technology, Direito Digital pelo Insper, Cybersecurity for Insurance pela UCLA e em Cyber Attacks pela NYU Tandon School of Engineering.
Marta_Schuh@jltbrasil.com