A palestra Cyber: Aspectos de Risco e Regulação de Sinistro debateu a necessidade do cyber insurance nos dias de hoje

Da direita para a esquerda: o diretor de Cyber Security and Investigations da Kroll, Marcelo Martinez; o Financial Lines Manager da AIG Seguro, Flávio Sá, e a sócia da Área de Seguros e Resseguros, Demarest Advogados, Marcia Cicarelli

Não é exagero dizer que uma onda de ataques cibernéticos vem atingindo países do mundo inteiro. Essa guerra virtual é capaz de causar estragos financeiros e de reputação gigantescos às empresas, principalmente àquelas que trabalham com dados pessoais e financeiros de terceiros. Em contrapartida, pelo menos no Brasil, o seguro cibernético ainda caminha a passos lentos. A necessidade de conscientização das organizações sobre os riscos de exposição de informações contidas na rede foi o tema debatido na palestra Cyber: Aspectos de Risco e Regulação de Sinistro, realizada no primeiro dia do 7º Encontro de Resseguro do Rio de Janeiro.

A palestra teve mediação de Flávio Sá, Financial Lines Manager da AIG Seguros, e a participação de Marcelo Martinez (palestrante), diretor de Cyber Security and Investigations da Kroll, e Marcia Cicarelli (debatedora), sócia da Área de Seguros e Resseguros Demarest Advogados.

"Ataque cibernético é assunto debatido em todos os Conselhos de Administração de empresas. Existe um longo caminho a ser percorrido no Brasil no caso de seguros que cobrem riscos cibernéticos, mas é fato que muitas organizações já estão sofrendo prejuízos", salientou Flávio Sá.

Marcelo Martinez causou espanto no público ao apresentar casos reais de empresas que sofreram ataques cibernéticos nos últimos anos. Em alguns casos, hackers criminosos se fizeram passar por funcionários do alto escalão de grandes corporações, utilizando contas de e-mail, para enganar funcionários responsáveis por movimentações financeiras.

"Antigamente o risco de um cyber attack era irrisório, pois não havia essa quantidade de mídias que existe hoje. As empresas atualmente estão nas redes sociais, em diversos dispositivos, como tablet, celular. O aumento do volume de dados fez as empresas recorrerem à nuvem. Há muitos pontos de vulnerabilidade que podem ser alvos para os hackers", ressaltou Martinez.

O executivo apresentou também uma pesquisa feita pela Kroll, em 2017, em nível mundial, que incluiu o Brasil entre os respondentes. O levantamento esmiuçou o cenário de ameaças virtuais e teve o objetivo de saber a opinião de diretores de empresas sobre os incidentes cibernéticos. Um dado surpreendeu: 89% dos entrevistados disseram que já foram alvos de ataques cibernéticos. O número é 13% maior do registrado em 2016.

O diretor da Kroll destacou que uma das maiores ameaças está relacionada ao tempo que as empresas levam para descobrir que sofreram um ataque cibernético. "Geralmente levam semanas, podendo ser meses ou anos. Os hackers conseguem em questões de minutos extrair dados valiosos, mas as empresas só percebem que estão sendo alvos quando o estrago já está feito e as perdas são grandes".

A Deep Web também foi um dos temas destacados por Martinez. Essa zona da internet que não pode ser detectada facilmente pelos tradicionais motores de busca, garantindo privacidade e anonimato para os seus navegantes, tem uma variedade de páginas que oferecem ataques cibernéticos como serviço. É possível colocar o tipo de ataque que se planeja executar em um carrinho de compras, como se estivesse adquirindo qualquer outro produto pela internet. O processo é tão sofisticado e intuitivo que hoje, afirma Martinez, qualquer pessoa que não tenha receio de ser pego pela justiça, mas tenha tempo e dinheiro (os ataques podem ser pagos com bitcoins) pode executar ataques cibernéticos contra empresas ou cidadãos. "Não é preciso mais ser especialista para fazer isso", reforçou.

O diretor da Kroll chamou atenção também para as coberturas mais comuns oferecidas pelo seguro cibernético. Algumas delas são: despesas relacionadas com a gestão do incidente, investigação, remediação, notificação, custos legais e procedimentos em tribunais; custos relacionados à violação de propriedade intelectual, direitos autorais, calúnia e difamação; despesas relacionadas a casos de extorsão, mediando o sequestro de dados e servidores, e criptografia de arquivos realizadas pelo crime organizado; custos relacionados à inoperância ou indisponibilidade da rede de computadores, além do roubo de dados.

Recursos legais

Marcia Cicarelli falou sobre o Marco Civil da Internet (Lei 12.965\14), que como o nome próprio já diz, foi um marco para assuntos ligados a ataques cibernéticos. "Trata-se de uma lei moderna, que tem a finalidade de proteger dados de pessoas com base no direito consitutcional da privacidade. Dentro das nossas garantias, os dados pessoais estão em um nível alto de proteção. Sempre que houver uma divulgação não consentida, o responsável deve responder perante a justiça, independentemente de culpa", explicou.

Marcia falou também sobre o Projeto de Lei 5276\2016, em discussão no Congresso. Se aprovado, o Brasil terá uma legislação muito parecida com a que se tem na Europa, por meio do General Data Protection Regulation (GDPR), aprovado pelo parlamento europeu em 2016. "O GDPR foi projetado para harmonizar as leis relacionadas à privacidade de dados na Europa e reforçar o direito de proteção destes dados para os cidadãos".

Marcia citou casos de empresas no Brasil que tiveram que reparar terceiros por vazamento de dados devido a ataques cibernéticos, e não deixou de falar do Facebook, que recentemente foi acusado de usar dados de pessoas cadastradas na rede social. "Quanto maior a empresa, maior a responsabilidade de guardar com segurança dados da prórpia corporação e de terceiros", finalizou.

Fonte: CNseg, em 10.04.2018.