

Seguro cobre a responsabilidades referente à proteção, gestão e manuseio de dados além de consequências das perdas de informações

Notícias de grandes vazamentos de dados inundaram veículos de comunicação mundo a fora ao longo dos primeiros meses de 2014. A exposição intensa dessa atividade de hackers e avanço das tecnologias nas empresas colocou “segurança da informação” como um dos temas mais quentes do próximo ano.

Executivos apontam o tema como uma de suas maiores preocupações para o futuro. Alinhado a isso, começam a ganhar popularidade modelos para proteger empresas que vão além dos antivírus, firewalls, proteção de rede, sistemas de acesso, tokens. Há pouco mais de um ano, seguradoras intensificaram ofertas que cobrem incidentes cibernéticos.

O seguro destinado a cobrir prejuízos oriundos de crimes eletrônicos foi regulamentado pela Superintendência de Seguros Privados (Susep) ainda em 2007. Há pouco mais de um ano ganhou força no portfólio de seguradoras ao redor do mundo, inclusive no Brasil. Uma das companhias que oferece esse tipo de serviços por aqui é a Vis Corretora, que lançou a modalidade (batizada de *cyber risk*) em meados de 2013.

A companhia percebe a procura por esses serviços subir nos últimos meses. O aumento no interesse possivelmente relaciona-se com episódios recentes, como o do Morgan Chase, Target e USPS. “Acreditamos que cada vez mais haverá um aumento quanto a preocupação de segurança nos meios eletrônicos, já que o crescimento do e-commerce e a informatização de diversos setores aumenta a exposição a esse risco”, informa.

A corretora espalhou algumas propostas. No entanto, ainda não converteu nenhum negócio. A percepção é que “poucas empresas conhecem o produto”, o que reverte processos mais longos de fechamento de eventuais contratos.

O seguro cobre a responsabilidade das empresas referente à proteção, gestão e manuseio de dados pessoais e corporativos bem como as consequências das perdas de informações ocorridas por meio de violações de segurança. Estão assegurados, nesses pacotes, por exemplo, responsabilidade por segurança e privacidade de dados, interrupção de rede, gestão de eventos e extorsão cibernética.

Para ser assegurada, a empresa precisa possuir política ou procedimentos de proteção de dados, antivírus, firewall e outras ferramentas que a seguradora entender serem necessárias após análise do questionário sobre o risco enviado pela contratante.

Cenário

Um estudo feito por uma seguradora global mostrou que o risco cibernético apareceu entre os 10 maiores riscos nas empresas em 2014. Além disso, a Bain&Company revela que os ataques diários de hackers em empresas aumentaram 30% no último ano chegando a 247,4 mil por dia.

Uma seguradora levantou que em 2011 foram aproximadamente 5,5 mil ataques de hackers na América Latina - figurando como o quarto maior crime econômico em 2011 -, 75% das organizações já foram atacadas nos últimos 12 meses e em média há uma queda de 5% nas ações de empresas que relatam falha de segurança.

Fonte: [COMPUTERWORLD](#), em 12.11.2014.