

Análise foi realizada a partir de entrevistas com mais de 2.600 executivos

A Aon acaba de lançar o Relatório de Risco Cibernético - Hoje e Amanhã. A análise aborda os oito principais riscos avaliados dentro de pequenas, médias e grandes companhias em diferentes estágios de transformação digital. A produção do estudo envolveu entrevistas com 2.600 gerentes de risco de 33 indústrias, em 60 países.

A fragilidade em lidar com as ameaças surge de fora para dentro da companhia, a partir das mudanças nas regras de comércio, ciberataques e a escassez de profissionais qualificados. Dos profissionais entrevistados, apenas 24% conseguem quantificar os 10 maiores riscos e só 10% informaram que possuem processos formais para identificá-los. "O estudo mostra, pela primeira vez desde que iniciamos, que o nível de preparação das empresas à resposta-risco é o mais baixo. É um sinal de alerta.", comenta Eduardo Takahashi, Vice-Presidente Executivo para soluções comerciais de riscos da Aon Brasil.

Por vezes precipitada, a incessante busca pela inovação em setores distintos baseia-se apenas na implantação, deixando brechas na estrutura devido aos riscos que o novo feito acarreta para a empresa. A Aon elege, no relatório, oito pilares de maior risco da segurança cibernética nas empresas, sendo eles: Tecnologia, Cadeia de Suprimento, IoT, Operações Comerciais, Funcionários, Fusões e Aquisições, Regulamentação e D&O "Directors and Officers".

O estudo alerta para novas artimanhas das comunidades hackers. Por outro lado, indica que a maneira com que as empresas se relacionam entre elas pode tornar a prevenção mais eficaz. "O relatório tem o objetivo de preparar o mercado para que não seja surpreendido no que é projetado em segurança corporativa. Para isso, entendemos que a comunicação entre as companhias é substancial para minimizar os riscos.", explica Marco Mendes, Especialista em Risco Cibernético da Aon.

No Brasil, outro fator que acentua a possibilidade de grandes riscos é a instabilidade econômica. Além disso, a economia chinesa impacta o mercado brasileiro, que depende de exportações de commodities para o país asiático. De maneira global, as transações comerciais seguem abaladas com a possibilidade de saída do Reino Unido da União Europeia (Brexit), as maiores taxas de juros nos Estados Unidos e a desaceleração econômica na Europa e Ásia.

Principais riscos**Tecnologia**

Com a transformação digital das companhias, há o incremento dos riscos cibernéticos, novos e imprevistos. O futuro é digital e há que se preparar para essa nova forma de fazer negócios.

Cadeia de fornecimento

Muitas vezes a companhia pensa em seus próprios riscos cibernéticos, mas esquece a cadeia de fornecimento. Cada vez mais complexas e globais, elas podem ser um elo fraco na segurança da informação.

IoT

Seguramente os dispositivos conectados trarão inúmeros benefícios, mas riscos iminentes. O tipo de ataque que antes ocorria "somente" em devices como computador, tablet e smartphones agora pode acontecer na sua geladeira, por exemplo.

Operações comerciais

Sistemas de controle operacional, como cadeia de logística e suprimentos, também apresentam possibilidades de risco. Hoje cada vez mais esses procedimentos estão sendo automatizados e um ataque pode causar paralisação total ou parcial da empresa.

Funcionários

Seja por falta de conhecimento, na maioria dos casos, ou até mesmo por ações má intencionadas, os funcionários acabam sendo um dos elos mais fracos e, portanto, uma das principais causas de violações de segurança.

Fusões e aquisições

Num momento de fusão e aquisição a empresa que está adquirindo a outra acaba por herdar suas vulnerabilidades, questão que muitas vezes não é levada em consideração. E ela pode, inclusive, baixar o valor de mercado dessas aquisições.

Regulamentação

Cada vez sendo mais e mais adotada em todos os países do mundo, a regulamentação de segurança cibernética e proteção de dados se tornou geral. Ela é uma grande aliada das empresas, porém traz questões como sobreposições de leis em companhias globais, que precisam seguir diferentes regulamentações, além de, em alguns casos, ser fomentada pela burocracia em vez das melhores práticas.

D&O "Directors and Officers"

Diretores, gerentes e alto escalão em geral são cada dia mais implicados em casos de violações de dados e a responsabilidade em supervisionar a segurança cibernética se tornou uma de suas atribuições.

Fonte: Assessoria de imprensa Aon, em 25.10.2019.