

Contratações de seguros para proteção contra ataques cibernéticos podem chegar a US\$ 20 bilhões até 2025, diz consultoria Marsh & McLennan

Os prejuízos decorrentes de ataques cibernéticos crescem ano a ano. Estima-se que o custo do cibercrime para a economia global é de US\$ 445 bilhões anuais, sendo que nos próximos três anos — 2017, incluído — deve atingir US\$ 2,1 trilhões, de acordo com o estudo [Cyber Handbook](#) da consultoria Marsh & McLennan Companies (MMC). A cifra, se confirmada, será quase quatro vezes maior que as perdas que as companhias tiveram em 2015. Mesmo assim, poucas se preocupam em se proteger contra ataques cibernéticos.

De acordo com dados da MMC, as contratações de seguros para proteção contra ataques cibernéticos já somam cerca de US\$ 2 bilhões e podem chegar a US\$ 20 bilhões até 2025. Os EUA continuam a ser o maior mercado de seguros cibernéticos, onde quase 20% de todas as organizações têm seguros para riscos cibernéticos.

Com a ascensão dos ataques de hackers aos sistemas das empresas, alguns setores da economia ficaram mais expostos aos ciberataques. Com base na carteira de risco cibernético da MMC, as indústrias de manufatura e de comunicação, mídia e tecnologia lideram a contratação desse seguro, com 63% e 41% das apólices, respectivamente (veja lista abaixo).

Segundo o estudo, em 2015, 90% das grandes corporações do Reino Unido relataram violações, destacando a urgência de abordar os riscos de ciberataques. E, embora algumas empresas tenham tomado certas medidas para garantir a segurança e a capacidade de recuperação de falhas, muito ainda precisa ser feito. A MMC destaca que as ameaças cibernéticas e o terrorismo são cada vez mais riscos que se sobrepõem uns aos outros. “A maior parte da informação sobre segurança cibernética é mantida pelo setor privado, enquanto o terrorismo é tratado pelo setor público”, diz o relatório. Em razão disso, a consultoria diz que, claramente, deve haver maior parceria entre os dois para preparar a infraestrutura crítica para esses riscos entrelaçados.

Além disso, ressalta o estudo, os países agora estão enfrentando uma dura realidade nova de ameaças contra ativos físicos — incluindo redes elétricas, barragens, redes de telecomunicações, sistemas de transporte e instalações nucleares civis. “Onipresentes, as conexões com a internet têm aumentado a vulnerabilidade de sistemas industriais que controlam esses ativos físicos”, diz o documento.

União de esforços

Como a maioria das infraestruturas críticas em muitos países pertence e é operada pelo setor privado, é vital a intervenção de governos e da indústria para confrontar este risco. Os governos reconhecem a ameaça econômica representada pelo cibercrime e muitos estão tomando uma série de medidas, que incluem a adoção de melhores práticas e tecnologias de combate às ameaças. Mais de 30 países, incluindo Alemanha, Itália, França, Reino Unido, EUA, Japão e Canadá, têm montado estratégias de segurança cibernética.

Em fevereiro de 2014, o presidente chinês Xi Jinping anunciou um novo órgão nacional para coordenar os esforços de cibersegurança; e em abril de 2015, Cingapura lançou uma agência de segurança cibernética para supervisionar políticas e realizar a sensibilização das empresas e pessoas. O centro do Reino Unido para a proteção da infraestrutura nacional fornece boas práticas, orientação técnica e facilita a troca de informações entre os setores, incluindo o setor de energia e fabricantes de equipamentos de segurança para a infraestrutura nacional. A estratégia de segurança cibernética da França, coordenada pela Agência Nacional de Segurança de Sistemas de Informação, da mesma forma, promove a cooperação entre os setores público e privado.

Mas a MMC observa que as empresas, principalmente as que atuam em um mesmo setor da indústria, também devem compartilhar informações. Assim como a polícia e autoridades legais têm um papel fundamental na luta contra ameaças cibernética. Daí a necessidade de uma abordagem conjunta entre órgãos legais, indústrias e governos.

Representatividade nas contratações do seguro cibernético por indústria:

1. Manufatura: 63%
2. Comunicação, Mídia e Tecnologia: 41%
3. Educação: 37%
4. Atacado/Varejo: 30%
5. Instituições financeiras: 28%
6. Power& Utilities: 28%
7. Indústrias: 27%
8. Hospitality and Gaming: 15%
9. Serviços: 13%
10. Healthcare: 6%

Fonte: MMC Cyber Handbook 2016/[Computerworld](#), em 01.02.2017.