RISK DOCTOR PARTNERSHIP BRIEFING

GERENCIANDO RISCOS DE CRIMES CIBERNÉTICOS

© Maio 2014, Ben Rendle

ben.rendle@btinternet.com

O crime cibernético é uma ameaça de crescimento vertiginoso para economia global. Mas ele não é bem definido, e muitas vezes é confundido com cyber-guerra ou cyber-terrorismo. Profissionais de risco precisam entender o crime cibernético e as suas ligações com a gestão de riscos, para fornecerem assistência valiosa na luta contra esta ameaça significativa para as empresas e a sociedade.

Alguns profissionais de risco pensam que o crime cibernético é relevante apenas para o pessoal técnico e que deveria ser combatido pelos departamentos de TI. Mas o crime cibernético representa um risco significativo para as organizações, pois afeta a sua capacidade de alcançar objetivos estratégicos e operacionais. Infelizmente, muitas empresas não sabem como é o crime cibernético, qual a probabilidade de serem afetadas, qual a extensão que o impacto poderia causar, ou qual a melhor forma de gerenciá-lo.

O crime cibernético pode afetar uma organização de muitas maneiras diferentes, incluindo:

- roubo on-line ou fraude
- roubo de identidade
- extorsão
- roubo de dados de clientes
- roubo de propriedade intelectual
- espionagem industrial

A exposição ao crime cibernético está relacionada com o nível de atividades online realizadas por uma organização, incluindo o âmbito da sua presença on-line, a quantidade de ativos e informações valiosas que são armazenados on-line, a robustez da segurança on-line, bem como o grau de consciência de risco na cultura organizacional.

Para gerenciar o risco de crimes cibernéticos, é preciso primeiro identificar o nível de nossas atividades on-line, e determinar quais ativos e atividades podem ser afetados por crimes cibernéticos. Em seguida, podemos começar a identificar, avaliar e gerenciar nossos riscos de crimes cibernéticos. Os passos seguintes serão úteis:

- **Entender claramente e definir os objetivos organizacionais para as atividades on-line**. Reconhecer os diferentes e específicos ambientes on-line das nossas partes interessadas, e avaliar seus apetites por risco online.
- **Endereçar fatores culturais e técnicos**. Estes incluem barreiras culturais, dificuldades de comunicação e os efeitos das ideias preconcebidas sobre as percepções de risco do crime cibernético.
- **Reconhecer ameaças internas e externas de criminosos cibernéticos**. Ameaças internas podem surgir a partir de erros de funcionários, perda acidental de dados, ou vazamentos maliciosos de dados corporativos sensíveis. As ameaças externas podem vir de hackers, grupos de pressão, concorrentes ou até mesmo governos estrangeiros hostis, bem como vírus, worms, cavalos de Tróia, etc.
- **Estabelecer propriedade, responsabilidade e incentivos para enfrentar os riscos do crime cibernético**. Toda alta gerência deve ser responsável pela gestão dos riscos dos crimes cibernéticos em sua área de responsabilidade, e devemos desafiar as partes interessadas que o vêem como "o problema não é nosso".
- **Gerenciar os riscos de crimes cibernéticos dentro de uma estrutura de Gestão de Riscos Corporativa (ERM)**. Riscos de crimes cibernéticos podem afetar a empresa amplamente em áreas como a reputação, a continuidade dos negócios e refletir para as subsidiárias e fornecedores, por isso deve ser gerenciado de forma coerente como parte de nossa resposta global ao risco.
- **Desenvolver uma perspectiva global sobre os impactos de risco de crimes cibernéticos**. Muitas organizações dependem de economias estrangeiras para o comércio, exportação e geração de riquezas, e isso expõe a criminalidade cibernética no exterior que não pode ser ignorada.

Como profissionais de risco, precisamos incluir o crime cibernético em nosso pensamento e prática, para que possamos oferecer conselhos práticos direcionados às nossas organizações com o objetivo de reduzir as ameaças e proteger o nosso negócio.

Traduzido voluntariamente por Marconi Fábio Vieira, PMP – marconi@infochoice.com.br