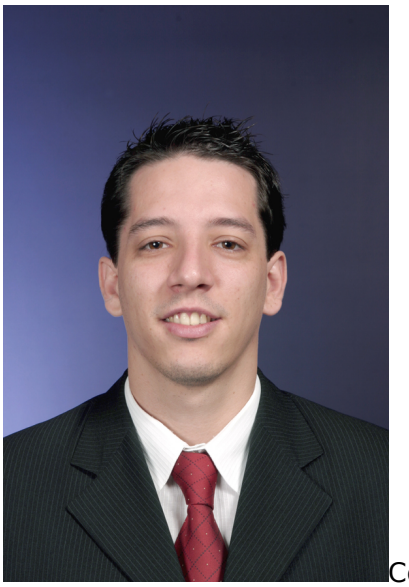
Por Leandro Marco Antonio (*)

 Com a crescente ameaça de ataques virtuais a organizações de todos os setores, o aumento do número de crimes cibernéticos tem sido um tema de destaque no cenário de riscos corporativos recentemente. Não há dúvida de que isso se tornou a questão mais urgente dos conselhos empresariais, mas com os hackers preocupados em acessar de forma furtiva as informações bancárias, dados de cartão de crédito dos clientes e cometer inúmeros outros ataques, são as empresas de varejo e instituições financeiras que lidam diretamente com o público que estão na linha de frente.

Contudo, mesmo com o trabalho incansável destas empresas em aumentar a robustez de seus meios de defesa cibernética e as exigências em termos de acesso aos sistemas sofrerem aprimoramentos, os criminosos cibernéticos têm começado a procurar outros meios de ataque e também ambientes tecnológicos que não são historicamente um foco de ataques massivos. E, assim como algumas das maiores marcas mundiais, a indústria de bens de consumo é um alvo muito atraente.

Isso posto, o setor é o alvo principal de criminosos motivados não somente pelo desejo de apoderar-se dos dados financeiros dos indivíduos. A indústria de bens de consumo ainda sofre ameaças como espionagem industrial e ataques organizados por um estado independente. Vale citar que a espionagem industrial pode ter diversas motivações. Uma delas é roubar a propriedade intelectual de outra empresa em relação à fórmula ou ao mix de produção para um determinado produto. A outra pode estar vinculada à atividade de fusões e aquisições – tentar descobrir qual empreendimento o concorrente está interessado em comprar ou acessar as informações financeiras alheias para ajudar a decidir se uma oferta de compra agressiva deve ser feita ou não. O propósito básico é obter uma vantagem em relação às organizações concorrentes. Geralmente, esse tipo de espionagem pode ser motivado politicamente ou patrocinado – os estados independentes tentam impulsionar sua própria produtividade econômica por meio do acesso a tais informações.

As organizações também precisam estar alertas a ataques direcionados aos seus funcionários, por meio de mensagens de email ou ligações telefônicas. Estes ataques conhecidos por agregar características que aproximam o hacker da vítima, por exemplo, através de mensagens com conteúdo atraente para o seu trabalho, e solicitando normalmente alguma ação por parte do colaborador.

Contudo, a ameaça não vem somente de fora: muitas vezes, é justamente o ambiente interno da

empresa que fornece o acesso às informações confidenciais que podem causar danos. Os detentores de informações confidenciais sensíveis podem ser subornados a fornecê-las. Em tempos nos quais os profissionais se movimentam cada vez mais no mercado de trabalho, existe o risco de retirar e transferir recursos sem autorização do proprietário – fazer o download de toda uma base de dados de informações para levar com eles quando forem para outra empresa ou encontrarem um comprador interessado.

Entender o valor dos ativos de informação corporativos e como o roubo, a interrupção e a destruição destes afetariam a concretização dos objetivos comerciais permite que os conselhos avaliem os benefícios empresariais decorrentes de uma gestão de riscos cibernéticos feita de forma eficaz. Esse processo de descoberta também ajuda a ilustrar como a tomada de decisão desse grupo pode aumentar ou reduzir a exposição ao risco da empresa de forma geral. Assim que os conselheiros tiverem um entendimento mais claro da forma e da escala do risco cibernético, e o que ele representa para a organização, serão mais capazes de estabelecer adequadamente o nível de apetite por risco corporativo, bem como de investir de forma mais eficiente na gestão do risco cibernético, em conformidade com os outros riscos empresariais.

A pior coisa que uma empresa pode fazer em relação à ameaça de crime cibernético é negligenciá-la. Acreditamos que as empresas que aceitam os ataques cibernéticos como uma parte inevitável do atual cenário empresarial, e que desenvolvem formas de proteção e respostas proativas, estão mais bem posicionadas para proteger o futuro de seus negócios.

(*) **Leandro Marco Antonio** é sócio de Cyber Security da KPMG.

Fonte: Viveiros, em 04.08.2015.