Sua empresa está preparada para a tripla ameaça?

Fraudes, violações de compliance e ataques cibernéticos nas Américas

Por **Emerson Melo**, sócio-líder da prática de Forensic & Litigation da KPMG no Brasil.

A pesquisa **Uma ameaça tripla nas Américas – KPMG 2022 Fraud Outlook** aponta que as fraudes, as não conformidades e os ataques cibernéticos na região prejudicaram os lucros das empresas e suscitaram maior preocupação com o futuro. O acesso mais aberto aos sistemas, forçado pelo trabalho remoto, também dificulta a prevenção, o monitoramento e o controle.

Nesse cenário, o que as organizações podem fazer? Quais são os desafios a enfrentar, incluindo o aumento da pressão regulatória local e internacional no que concerne aos critérios ESG?

De acordo com a pesquisa, 83% das empresas localizadas nas Américas sofreram pelo menos um ataque cibernético nos últimos 12 meses, 71% foram vítimas de fraudes e mais da metade pagou multas por questões regulatórias ou sofreu um prejuízo econômico em função de riscos de descumprimento não mitigados. A combinação das fraudes e não conformidades custa às empresas,

em média, 1% dos seus lucros líquidos. Um percentual de 58% indicou ter sofrido uma perda econômica direta como resultado de um ataque cibernético.

A análise traz outras conclusões relevantes: na América Latina, as fraudes internas (cometidas por profissionais) são mais frequentes do que na América do Norte, onde as fraudes externas prevalecem (realizadas por clientes, fornecedores e demais terceiros); os fraudadores atacam principalmente os alvos robustos, para mostrar que as perdas por fraudes e descumprimentos nas grandes empresas são maiores do que nas menores; 77% dos entrevistados consideram que o risco de segurança cibernética aumentará nos próximos 12 meses.

Além da tensão gerada por essa conjuntura, os fatores externos provocam desafios adicionais, tais como:

- Altos níveis de corrupção nos países da região, conforme apontado pelo Índice de Percepção da Corrupção 2021 (IPC) divulgado pela Transparência Internacional (TI). Segundo Delia Ferreira Rubio, presidente da TI, "os países latino-americanos estão completamente travados no combate à corrupção".[1]

- Aumento da aplicação da Lei Anticorrupção dos EUA (FCPA) que pode afetar os países latino-americanos. Anunciada em junho de 2021 pelo presidente Biden[2] e reforçada em dezembro do mesmo ano, ao definir o marco estratégico de combate à corrupção[3], do qual surgem: (1) a importância do combate à lavagem de dinheiro como meio de redução da corrupção; (2) maior responsabilidade individual pelas condutas corruptas; (3) a necessidade de focar o lado da demanda do suborno; e (4) um compromisso com a cooperação internacional.[4] Paralelamente a isso, o anúncio do Departamento de Justiça dos EUA[5], indicando que analisará as ações indevidas passadas das empresas com maior profundidade, exigirá informações detalhadas das pessoas ligadas aos fatos sob análise e permitirá um uso mais amplo do monitorship.[6]

- Expectativa acerca dos requisitos adicionais da SEC relacionados ao fornecimento de informações de gerenciamento de risco de segurança cibernética. Nesse sentido, a SEC indicou como áreas de relevância, aquelas que tendem a reforçar a "higiene cibernética" das empresas registradas (práticas para manter a segurança dos dispositivos, das redes e das informações) e melhorar o prazo e o conteúdo das notificações sobre ataques cibernéticos ocorridos e suas informações para clientes, investidores e a própria SEC[7].

- Requisitos multidimensionais vinculados a aspectos de ESG, que estabelecem critérios de sustentabilidade para empresas em áreas tão distintas como a gestão da segurança cibernética como condição para obter financiamentos ou emitir títulos negociáveis, gestão de risco de terceiros, realização de investigações de violações regulatórias (por exemplo, no setor de Energia), due diligence ambiental ou a necessidade de ter uma linha direta para questões antiéticas.

Esses elementos criam uma tempestade perfeita para empresas que enfrentam altos níveis de fraudes, violações de compliance e ataques cibernéticos, além de demandas crescentes, tendo que decidir o que priorizar com recursos muitas vezes limitados ou escassos.

Será impossível para as organizações responderem adequadamente a esses desafios se elas

Emerson Melo

não fizerem uma avaliação bidimensional. Em primeiro lugar, dos riscos mais sensíveis que ameaçam o negócio (de fraude, compliance e segurança cibernética), mensurados no que tange à sua probabilidade de ocorrência e impacto, e considerando seu nível de risco inerente, efetividade dos controles associados e nível de risco residual. E, dessa forma, ter um mapa de calor dos riscos críticos para o negócio, para as três categorias.

Em segundo lugar, avaliar os recursos que a organização dispõe para enfrentar esses riscos, em termos de pessoal – incluindo a existência de um responsável pela gestão das ameaças e o posicionamento desta função na empresa – sistemas, normas, procedimentos, protocolos, estilo de liderança da alta administração, comunicação e treinamento, entre outros. E assim definir sua suficiência e efetividade potencial, identificando oportunidades de melhoria.

Em seguida, é preciso identificar quais conjuntos de informações existentes nos bancos de dados/sistemas da empresa estão vinculados ao comportamento dos riscos definidos como sensíveis e, sendo assim, estabelecer quais padrões indicariam irregularidades potenciais.

Posteriormente, é essencial estabelecer rotinas de monitoramento e detecção precoce que alertem sobre possíveis desvios no seu comportamento, bem como contar com protocolos de resposta efetivos. Tudo isso de maneira que, em situações de alerta, a empresa saiba responder e tenha os dados necessários para investigar o que poderia ter ocorrido ou o que está acontecendo e, assim, informar, caso necessário, a justiça, os órgãos reguladores, investidores e/ou outros terceiros sobre o que, como e desde quando aconteceu, quem está envolvido e o impacto financeiro.

As informações que podem ser necessárias incluem: dados de arquivos-mestre e transacionais, e-mails que estão nos servidores da empresa, computadores, celulares ou outros dispositivos atribuídos pela organização às pessoas sob análise, e logs de diferentes sistemas que deverão ser mantidos por longos períodos, de forma que permitam reconstruir o que ocorreu, por exemplo, no caso de um ataque cibernético.

Essas informações devem ser obtidas e processadas mediante a aplicação de procedimentos de tecnologia forense, com o objetivo de preservar a cadeia de custódia, permitindo poder utilizá-la como uma prova válida. Por isso, recomenda-se a intervenção de especialistas, o uso de ferramentas forenses que garantam a integridade dos dados adquiridos e a participação de um tabelião no processo, o qual atesta que as informações não foram alteradas.

Portanto, será importante que, como parte do Código de Conduta da empresa, que idealmente deve ser assinado todo ano pelos funcionários após treinamento sobre ele, seja incluída a declaração de que os recursos de informática são de propriedade da entidade e, portanto, podem ser monitorados.

Além disso, contar com funcionalidades ativas que permitam preservar as informações armazenadas eletronicamente, evitando que elas sejam perdidas. Isso é fundamental em processos judiciais ou de investigações internas.

Na América Latina, apenas 20% dos entrevistados indicaram que suas empresas cumprem as melhores práticas para mitigar os riscos de segurança cibernética: 11% em termos de controles de fraudes; e 9% em termos de compliance. Entretanto, esses riscos estão aumentando. A sua empresa está preparada para enfrentá-los? ■

1 https://www.transparency.org/es/press/2021-corruption-perceptions-index-americas-regional
2 Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest | The White House
3 https://www.whitehouse.gov/wp-content/uploads/2021/12/United-States-Strategy-on-Countering-Corruption.pdf
4 https://www.corporatecomplianceinsights.com/biden-administration-attack-corruption/
5 https://www.corporatecomplianceinsights.com/doj-enforcement-2022-monaco-memo-anti-corruption/
6 Amplamente definido tanto pelo DOJ quanto pela SEC como "um terceiro independente que avalia e monitora o cumprimento por uma empresa dos requisitos de compliance de um acordo com o que foi projetado para reduzir o risco de conduta imprópria da empresa". US Dep't of Justice [DOJ] and US.
7 SEC.gov | Cybersecurity and Securities Laws