Os cinco maiores riscos de terceiros

As ameaças difundidas e as ações que você pode tomar para ajudar a proteger a reputação e as posições regulatória e financeira de seu negócio.

Ser criativo transforma negócios

kpmg.com.br

Introdução

O conhecimento é o maior escudo contra a volatilidade do risco oculto.

Os benefícios de uma rede de terceiros vêm com muitos riscos. Conforme o mercado global se torna mais complexo e competitivo, as relações com terceiros se tornam cruciais para reduzir custos, administrar e mitigar riscos, aperfeiçoar as experiências de clientes e aumentar o valor e a lucratividade no ecossistema em que a organização está inserida. Sem terceiros confiáveis e conceituados (isto é, fornecedores, prestadores de serviços, distribuidores e empreiteiros - além de corretores, agentes, revendedores e fabricantes), as empresas não conseguem competir com organizações mais dinâmicas em suas indústrias. No entanto, ao convidar essas entidades para sua rede, pode estar também abrindo as portas para casos indesejados ou até mesmo ocultos.

Apesar de relacionamentos eficazes com terceiros elevarem o nível de uma empresa, é cada vez mais importante proteger seu negócio contra inúmeras ameaças que essa conexão pode abrigar. Riscos regulatórios, legais e de *compliance*, segurança de informações/cyber segurança, continuidade dos negócios estratégicos, de viabilidade financeira e de reputação representam uma gama de tópicos que podem apresentar surpresas se não forem adequadamente apurados ou avaliados para administrar corretamente as respectivas ameaças à sua organização.

Estes riscos associados a relacionamentos com terceiros apresentam um perigo particularmente difícil. Com a velocidade implacável e a vigilância do cenário da mídia moderna, se houver informações prejudiciais, é muito provável que sejam descobertas e expostas. Um estudo da Oxford Metrica sugere que, depois de sofrer um "evento extremo de reputação", uma empresa tem 80% de probabilidade de perder pelo menos 20% do seu valor. Isto é ainda mais preocupante, pois toda empresa examinada neste estudo da Oxford sofreu uma perda geral de valor.

O conhecimento é seu maior escudo contra a volatilidade do risco oculto. Com tanto dano potencial em jogo, entender o que esperar e quais práticas evitar é primordial para manter a boa reputação com as partes interessadas de sua organização, bem como proteger a sua empresa. Neste material, estão os cinco principais riscos que merecem atenção prioritária para, assim, você proteger seu negócio do desconhecido.

[1] Source: Aon, "Oxford Metrica Reputation Review" (2012).

1. *Due diligence*

"80% das ações de execução do Ministério da Justiça dos EUA são resultantes de violações de terceiros."

Quando sua due diligence de terceiros é sensível, processual, minuciosa e previsível, você reduz os riscos de ações de execução prontamente.

A Iniciativa de Parceria Contra a Corrupção do Fórum Econômico Mundial divide o processo de pré-integração em três etapas essenciais nas suas orientações oficiais para uma due diligence apropriada:

[1] entender o escopo do universo de terceiros, [2] realizar avaliações de risco em entidades individuais para determinar o nível de due diligence necessário e [3] realizar procedimentos de due diligence. Além disso, o guia do Departamento de Justiça dos EUA (DOJ) e da Comissão de Valores Mobiliários dos EUA (SEC) para o FCPA estipula que as empresas devem realizar uma "due diligence baseada nos riscos" e entender "as qualificações e associações de [seus] parceiros terceirizados, incluindo [sua] reputação de negócios e relacionamento, se houver, com autoridades estrangeiras". Para cada uma dessas organizações, o tema dominante é encarar a due diligence levianamente.

As organizações que não alocam os recursos necessários nos estágios iniciais com práticas próprias de exame ficam excessivamente expostas ao acaso. Ao confiar em procedimentos superficiais, como buscas básicas na internet e verificações de bases de dados, embarca-se em uma jornada sem saber quais ameaças estão em jogo ou até mesmo onde começar a procurar.

[1] http://fcpa.stanford.edu/chart-intermediary.html
[2] http://www3.weforum.org/docs/WEF_PACI_ConductingThirdPartyDueDiligence_Guidelines_2013.pdf
[3] https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf

2. Visualização dos riscos em silos versus integração com relação ao impacto

O entendimento parcial e inadequado dos riscos leva a soluções ineficazes.

Os silos organizacionais podem cultivar um ambiente acolhedor para o crescimento de risco de terceiros. Quando uma empresa separa as funções de acompanhamento e gerenciamento das áreas de finanças e geopolítica, e com base no desempenho de gerenciamento de riscos, resulta em uma estrutura descentralizada de supervisão.

Ademais, as descentralizações administrativa e física vêm como resultado, com unidades de negócios separadas que operam em isolamento físico, criando defasagens de comunicação cruzada onde o perigo pode florescer.

Muitas empresas são seduzidas pela abordagem em silo com a ideia de que um alto grau de especialização seja benéfica e resulta em uma diversidade de habilidades de gerenciamento de riscos operacionais; isto é, quatro departamentos especializados superiores a um departamento geral. Embora uma grande variação de estilos e técnicas agreguem um elemento de versatilidade à equipe, ela não faz muita diferença no sentido de mitigação de risco.

Quando se percebe que os riscos pertencem a categorias distintas, exigindo estratégias diferentes de mitigação, a análise multifacetada é descartada, os procedimentos padrão passam a dominar e os fatores-chave são perdidos. Se, por exemplo, uma empresa descobre que um de seus fornecedores teve projeções anormalmente abaladoras, informariam ao seu departamento financeiro sobre um risco e providenciariam uma análise no mesmo nível financeiro. Por mais que isto pareça satisfatório, ao ignorar os potenciais fatores geopolíticos e de desempenho - isto é, recente violência política, descumprimento dos

principais prazos etc. -, uma organização pode criar soluções inadequadas com base em um entendimento parcial ou incorreto.

Uma estratégia eficiente e efetiva para governar e definir os riscos envolvidos em relacionamentos com terceiros só é possível quando as funções de gerenciamento são integradas para um impacto mais robusto. Quando você implementa soluções "bem redondas" que consideram múltiplas esferas de gerenciamento de riscos de terceiros e facilita a colaboração cruzada de divisões, você poderá entender melhor as questões potenciais e criar respostas abrangentes com várias nuances. E, no final, esta abordagem resulta em uma governança aperfeiçoada, respostas rápidas e decisões mais assertivas em sua organização.

3. Ausência de monitoramento de risco contínuo

A estabilidade pode gerar complacência, e esta pode levar a um relaxamento de padrões e rigor processual.

Na ausência de monitoramento de risco regular, a reação constante é o único recurso de uma empresa.

Sem monitoramento periódico, os riscos podem aparecer inesperadamente sem indício ou causa compreendida, prejudicando sua capacidade - e limitando seu prazo - para assumir o controle de situações perigosas.

Os estágios iniciais da due diligence e implantação podem muitas vezes dar um sentimento falso de segurança para uma organização, preparando o terreno para monitoramento insuficiente e alta exposição ao risco. No Guidance FCPA anteriormente mencionado, o monitoramento contínuo está relacionado como o terceiro passo na prática complacente, com sugestão de medidas que variam de due diligence periódica para solicitações de certificação de compliance. O raciocínio é bem simples: a natureza de uma relação comercial muda constantemente, e, como tal, o monitoramento também deveria ser.

Mesmo que você esteja ciente das empresas envolvidas em fraudes ou desvios de conduta, outro fator prejudicial e comum que deve ser monitorado é o de terceiros bem-intencionados que podem se envolver em atos menos óbvios de não conformidade para, assim, potencialmente tentar uma vantagem competitiva.

Esses são os tipos de fatores desconhecidos, aonde, muitas vezes, não são ou não podem ser sinalizados no estágio de implantação. Pensar que você já tem todas as informações nunca é uma maneira eficaz de conduzir um negócio, e o gerenciamento de riscos de terceiros não é diferente. O acompanhamento periódico de indicadores-chave de risco e buscas regulares por meio de bases de dados de contencioso é a melhor maneira de realizar internamente o monitoramento contínuo, embora, talvez, não mostre-se tão capaz como uma solução verdadeira de gerenciamento de riscos do fornecedor.

4. Proteções insuficientes para terceiros em sua rede

Um relatório da Forbes Insights revela que 46% das organizações sofreram danos de reputação na esteira de um incidente de violação.

Práticas efetivas e proativas de segurança de informação interna são críticas para manter os dados de uma empresa protegidos; contudo, podem se revelar inadequadas quando trata-se de gerenciamento de risco de terceiros. Em um mercado cada vez mais digital, os terceiros, muitas vezes, acessam ou se encarregam de seus dados. Isto deixa a sua empresa e os clientes vulneráveis ao risco de reputação originado da insegurança de dados da parte deles.

As estatísticas indicam que a insegurança de dados de terceiros prevalece e persiste. Um relatório da Bomgar de 2017 encontrou vários pontos perturbadores de dados:

1. 67% dos entrevistados tiveram violação de dados como resultado de acesso do fornecedor.
2. O número de fornecedores com acesso semanal à rede de uma empresa disparou em 103% de 2016 a 2017.
3. 34% das empresas operam um modelo de acesso de terceiro ativo/não ativo, fornecendo nenhum ou completo acesso.

Este último dado indica, especialmente, uma atitude negligente em relação à insegurança de dados de terceiros, demonstrando que a apuração caso a caso é menosprezada em favor de decisões gerais. O assunto vai além do relacionamento com terceiros, pois, de acordo com um levantamento conduzido pelo Ponemon Institute, 37% dos entrevistados afirmaram duvidar que receberiam a notificação de seu fornecedor terceirizado em caso de violação e; 73% duvidavam que receberiam algum aviso no caso de violação de um quarteirizado. Quanto mais longe se vai na linha do acesso direto, menos se encontra confiança e segurança. A abordagem negligente da segurança de dados é ainda mais perturbadora, pois um relatório da Forbes Insights descobriu que 46% das organizações sofreram danos à reputação na esteira de um incidente de violação.

As dezenas de recentes ocorrências notórias de invasão de dados de grandes marcas expuseram-nas aos danos de reputação derivados da insegurança de dados de terceiros.

Em um caso, os criminosos hackearam a senha de um fornecedor terceirizado e roubaram milhões de perfis de cartões de crédito e e-mails de usuários. Os pagamentos de acordos e honorários advocatícios chegaram a dezenas de milhões se não centenas de milhões de dólares. Embora essas grandes empresas tivessem, felizmente, os recursos para sobreviverem ao escândalo, qualquer violação de dados ilustra os potenciais custos, tanto financeiros quanto de reputação das lacunas presentes em segurança de dados terceirizada.

[1] Source: Bomgar, "The Secure Access Threat Report" (2017).
[2] Source: Forbes Insights, "The Reputational Impact of IT Risk" (2014).

5. Pensar no seu programa teórico o deixa seguro

Sem um sistema adequado de execução, mesmo os programas bem documentados e elaborados, podem se revelar inadequados no caso de um evento prejudicial à reputação.

As organizações passam meses pesquisando, comprando, contratando e implantando suas soluções ideais de gerenciamento de riscos de terceiros.

Entretanto, mesmo quando o sistema de avaliação de risco é robusto, sinais de alerta são tratados instantaneamente e o fluxo de trabalho de ponta a ponta é abrangente e hermético - um erro crucial pode estar esperando e, dessa forma, pegar a empresa de surpresa. Apesar de o senso comum indicar que esta organização fez todo o trabalho necessário para gerir seus riscos e antecipar futuros problemas, estão cometendo um erro crítico de gerenciamento de riscos de terceiros conhecido como "programa teórico".

Um programa teórico é qualquer estrutura processual que não presta contas da execução integral. Os procedimentos tecnicamente existem, mas somente na teoria, diminuindo a sua relevância. As empresas que simplesmente documentam ou "verificam" os procedimentos, porém não os executam totalmente, confiam demais em um programa teórico. Isto pode significar, por exemplo, que monitoram os sinais de alerta regularmente e têm redes eficazes de comunicação interna. Pode significar também que há estratégias de avaliação de risco inadequadas sobre prováveis terceiros, ou que não acompanham os processos atuais e contínuos adequadamente. Devido à natureza do gerenciamento de riscos de terceiros, todos os aspectos do programa devem estar instalados e ativos a todo momento para garantir eficácia e tranquilidade.

A maneira como o relacionamento com o fornecedor pode ser estruturado na fase inicial de due diligence, o acesso a seus dados "debaixo da superfície" e a avaliação da execução poderiam ser um desafio. Para os que aguentam firme, os resultados gerarão indubitavelmente melhores retornos no longo prazo. É fundamental implementar práticas sólidas de execução para evitar a armadilha do programa teórico, e, assim, impedir eventos prejudiciais à reputação que acompanham o mau gerenciamento de riscos de terceiros. Os fatores prejudiciais à reputação acontecem em diversos formatos e dimensões; todavia, todo programa eficaz de gerenciamento de riscos tem algo em comum: manter foco total e claro na execução integrada.

Resumo

Para proteger a sua organização contra a volatilidade e eventos destrutivos que prejudicam a reputação, os executivos e gestores deveriam aperfeiçoar seu processo de gerenciamento de riscos de terceiros e certificar-se de que sua rede de terceiros permanece como um benefício contínuo para a sua organização e não como um perigo iminente.

O gerenciamento de riscos de terceiros eficaz demanda papeis e responsabilidades claras, consistência, conectividade e execução total para governar e mitigar os fatos adequadamente. A escolha da plataforma correta pode dar a sua organização uma chance de lutar contra catástrofes imprevisíveis que possa surgir. Com a plataforma certa, sua empresa pode sair de um evento potencialmente prejudicial à reputação com uma resposta rápida a qual ajuda a mitigar sua perda e manter sua imagem na indústria. Proteger a organização requer um entendimento do custo da má prática e a necessidade de implementar uma solução confiável e eficaz que lhe fornece monitoramento e percepção dos riscos de terceiros.

Para obter mais informações sobre gerenciamento de riscos de terceiros, assim como inteligência de terceiros para ajudar a mitigar os riscos, entre em contato com a nossa equipe:

Emerson Melo
Sócio-líder da prática de Compliance
KPMG no Brasil
Tel.: (11) 3940-4526
emersonmelo@kpmg.com.br

Phelipe Linhares
Sócio de Accounting & Financial Risk
da KPMG no Brasil
Tel.: (11) 3940-6667
plinhares@kpmg.com.br

Ricardo Santana
Sócio-líder de Data & Analytics da
KPMG no Brasil
Tel.: (11) 3940-3816
santana@kpmg.com.br

#KPMGTransforma

Baixe o APP
KPMG Brasil

kpmg.com.br
/kpmgbrasil

© 2020 KPMG Consultoria Ltda., uma sociedade simples brasileira, de responsabilidade limitada, e firma-membro da rede KPMG de firmas-membro independentes e afiliadas à KPMG International Cooperative ("KPMG International"), uma entidade suíça. Todos os direitos reservados. Impresso no Brasil.

O nome KPMG e o logotipo são marcas registradas ou comerciais da KPMG International.

Todas as informações apresentadas neste documento são de natureza genérica e não têm por finalidade abordar as circunstâncias de uma pessoa ou entidade específica. Embora tenhamos nos empenhado em prestar informações precisas e atualizadas, não há garantia de sua exatidão na data em que forem recebidas nem de que tal exatidão permanecerá no futuro. Essas informações não devem servir de base para se empreenderem ações sem orientação profissional qualificada, precedida de um exame minucioso da situação em pauta.

Projeto gráfico e diagramação: Gaudí Creative Thinking