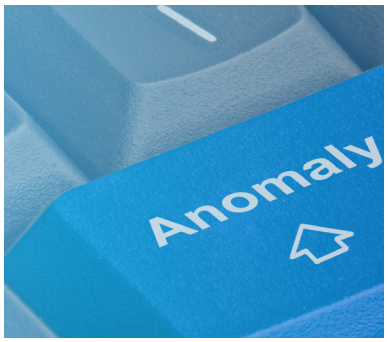
A AMEAÇA INTERNA:

Mitigando Riscos no DNA da Sua Organização

StoneTurn

Índice



Introdução

Entender e gerenciar os riscos de *insider* não é uma disciplina nova. Episódios relativos a riscos de *insider* podem ser desastrosos, e o fato de esses eventos serem causados por pessoas de dentro da própria organização raramente recebe atenção suficiente. Isso pode acontecer porque não está claro para nós o que são *insiders* e as ameaças que eles representam. Todos os anos, *insiders* causam danos prolongados e às vezes catastróficos a empresas de todos os tamanhos e setores. Contudo, deixamos de classificar vários desses atos como "atos internos". Por conta disso, perdemos a oportunidade de ter uma visão mais sistemática e holística dos riscos representados pelos *insiders*.

O QUE É UM *INSIDER*

De acordo com o Centro para a Proteção da Infraestrutura Nacional (CPNI), do Reino Unido, um *insider* é "uma pessoa que explora, ou tem a intenção de explorar, seu acesso legítimo aos ativos de uma organização para fins não autorizados". Seria qualquer pessoa que tenha acesso aos ativos de uma organização (físicos ou virtuais) e que, portanto, podem incluir funcionários, subcontratados e parceiros. O risco pode se manifestar na forma de fraude, perda de dados, roubo, sabotagem e vazamento de informações confidenciais. Esse risco pode prejudicar a reputação e os resultados financeiros de uma organização, além de impactar todos os colaboradores, tornando a mitigação do risco de *insider* uma exigência estratégica para todas as organizações. Os impactos são muitas vezes difíceis de serem definidos e mensurados. Por exemplo, enquanto é possível calcular as perdas diretas ligadas a um episódio de fraude, é mais difícil identificar os danos no longo prazo causados à confiança dos investidores, a reação do mercado, e a consequente perda em ganhos futuros. As perdas relacionadas a propriedade intelectual, em alguns casos, podem ser fatais para o negócio.

Os riscos de *insider* evoluíram e se adaptaram, tornando-se mais complicados e disseminados. Por exemplo, muitas organizações que migraram para o trabalho remoto para continuar funcionando durante os lockdowns da COVID-19 estão agora utilizando, gerenciando e armazenando ativos críticos de maneira diferente, sem pensar o suficiente em como seu pessoal está interagindo com a tecnologia e quais consequências podem surgir a partir do acesso interno irrestrito. Além disso, a mudança no cenário geopolítico, incluindo a invasão da Ucrânia e a ascensão da China, entre

POR QUE É UM PROBLEMA

Na essência de quase todos os negócios estão as pessoas. Elas, junto com as ideias coletivas e a sua criatividade, são o DNA que forma a estrutura e a proposta de valor de quase toda organização. E embora os seres humanos sejam ativos críticos e o sucesso de um negócio normalmente dependa deles, eles também estão entre os maiores e mais custosos riscos para o negócio.

Para se ter uma ideia de quão difundido e custoso é o problema do risco de *insider*, vejamos alguns números. A **Association of Certified Fraud Examiners** – ("ACFE" estima que o total de perdas globais devido a fraudes chegue a quase US$ 5,0 trilhões de dólares. A fraude ocupacional — fraude cometida por um executivo ou colaborador — é responsável por aproximadamente 40% do valor total, ou US$ 2,0 trilhões. Em seu estudo de 2021, a ACFE analisou 2.110 casos em 133 países e descobriu que cada caso teve uma perda média de quase US$ 1,8 milhão, o que se traduz em uma média de perda por fraude de 5% da receita das empresas mundialmente.

outros fatores, estão impactando o perfil de risco dos negócios.Esses avanços tecnológicos representam uma ameaça mais persistente e grave, incluindo esforços contínuos e aprimorados para explorar *insiders*. Consequentemente, embora as organizações fortaleçam suas defesas cibernéticas contra ameaças externas, devem também procurar fortalecer suas defesas de segurança pessoal, caso contrário, se tornam vulneráveis.

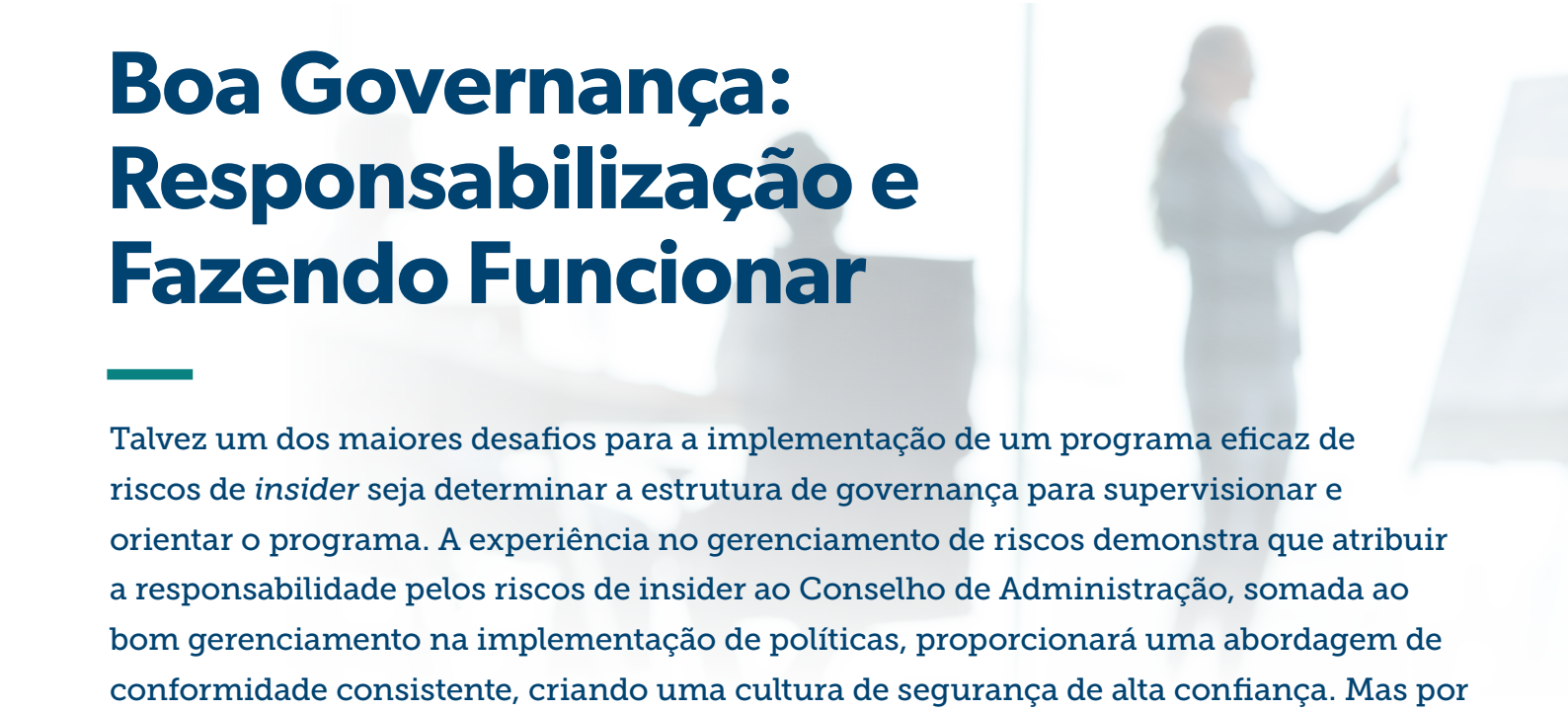
Não apresentamos este quadro para retratá-lo como sombrio e sem esperança. Pelo contrário: acreditamos que, com uma compreensão mais profunda e holística dos riscos enfrentados pelas empresas hoje, bem como com a adoção da infraestrutura certa para proteger os seus sistemas e ativos internos, as organizações podem estar mais preparadas para mitigar riscos de *insider*.

Nossos *insights* estão fundamentados em décadas de experiência e na evolução do nosso conhecimento para enfrentar os desafios do momento. À medida que o cenário muda e os riscos evoluem, continuaremos os nossos esforços para mitigar e eliminar ameaças às organizações.

Brad Wilson

Brad Wilson,
Managing Partner & CEO, StoneTurn

Boa Governança: Responsabilização e Fazendo Funcionar



Talvez um dos maiores desafios para a implementação de um programa eficaz de riscos de *insider* seja determinar a estrutura de governança para supervisionar e orientar o programa. A experiência no gerenciamento de riscos demonstra que atribuir a responsabilidade pelos riscos de insider ao Conselho de Administração, somada ao bom gerenciamento na implementação de políticas, proporcionará uma abordagem de conformidade consistente, criando uma cultura de segurança de alta confiança. Mas por onde as organizações podem começar a estabelecer esse tipo de responsabilidade?

Estruturas eficazes de governança corporativa e a conscientização de executivos C-Level sobre quais são os riscos de insider promoverão estratégias holísticas e eficazes de segurança para gerenciá-los. Essa abordagem garantirá o engajamento pessoal de todos na estratégia de gerenciamento de risco. Isso exigirá a participação de vários departamentos internos, incluindo as áreas de recursos humanos, jurídica, segurança cibernética, segurança física, compliance e de investigações. Todas essas partes interessadas devem ter uma compreensão clara e compartilhada do que é o risco de insider e aceitar trabalhar em seu gerenciamento na empresa como um todo.

Como parte de uma estratégia abrangente de segurança, uma forte governança impedirá aqueles que podem querer prejudicar a organização, criando uma estrutura organizacional aberta e transparente onde a segurança é ativamente promovida como responsabilidade de todos. Aliado a isso, deve haver recursos e suporte adequados para promover uma abordagem multidisciplinar proporcional, dinâmica e holística para gerenciar os riscos de insider. O suporte positivo e visível por parte do Conselho, além do apoio à governança, são essenciais para demonstrar às organizações o valor atribuído ao pessoal e às políticas e procedimentos de segurança relacionados a pessoas.

Uma forte liderança apoiada por uma boa governança em toda a organização irá:

- Garantir consistência e linhas claras de responsabilidade para o gerenciamento de riscos de segurança
- Incentivar uma abordagem multidisciplinar para gerenciar riscos de *insider*
- Garantir o uso proporcional e econômico de recursos
- Fornecer informações de gerenciamento essenciais para fins de planejamento de segurança e gerenciamento de pessoas
- Dar um forte exemplo que desenvolva e sustente uma cultura de segurança eficaz
- Apoiar os esforços para construir uma organização dinâmica e inclusiva, ao promover uma cultura de "speak-up" (falar ao ver algo errado)

O papel do Conselho

Na prática, observamos que apenas o apoio do Conselho não é suficiente para constituir uma governança eficaz sobre o programa de riscos de insider. É necessário que haja comprometimento individual e pessoal dos conselheiros, aliado a um alinhamento próximo de objetivos com os executivos da empresa. Pode ser benéfico, e em certos casos até essencial, designar um membro do conselho para se responsabilizar pelo programa.

O membro responsável do Conselho deve supervisionar e nomear um Grupo de Trabalho de Riscos de Insider com os principais profissionais de departamentos interessados em gerenciar tais riscos. Esse grupo deve ser liderado por um profissional sênior de um dos departamentos envolvidos.

Estabelecendo um Grupo de Trabalho de Riscos de *Insider*

Ao examinarmos os riscos de *insider* ao longo do tempo, vemos estudos de caso repletos de histórias em que uma intervenção teria ajudado a minimizar ou evitar danos, se uma ação conjunta e coletiva tivesse sido tomada anteriormente.

Reunir um grupo de profissionais pode trazer imensos benefícios. Estes profissionais podem atuar como um "amigo crítico" para qualquer programa de segurança de pessoal. Talvez mais importante, com alguns princípios acordados, eles podem trabalhar com problemas práticos e soluções quando sinais de alerta são disparados na organização. Em outras palavras, eles podem ajudar a responder à pergunta "o que faremos?" quando uma situação se apresenta.

O grupo multidisciplinar trabalhará em silos, coletando informações e discutindo as etapas práticas a fim de proteger a organização. O uso holístico de medidas e intervenções de segurança direcionadas (por ex., cibernéticas, de informações, análise de dados, de pessoal e físicas) pode ajudar a detectar comportamentos de risco relacionados ao local de trabalho e facilitar a intervenção precoce para reduzir o potencial de ataques maliciosos de colaboradores.

Além disso, espera-se que esse grupo produza relatórios periódicos para a diretoria sobre a eficácia do programa, principais estatísticas, aprendizados e melhorias feitas ao longo do tempo. Ao aprender com cada incidente e inserir as lições aprendidas no processo de avaliação de riscos, a organização poderá melhorar seu gerenciamento de riscos de colaboradores continuamente.

Os objetivos do Grupo de Trabalho de Riscos de Insider serão:

- Mitigar os riscos de pessoas que os apresentem (os riscos envolvem o comportamento contraproducente de colaboradores, seja ele um comportamento inadvertido, negligente ou malicioso, que possa prejudicar a organização)
- Desenvolver uma "orientação de resposta" avançada para um incidente interno: como reagir, como minimizar os danos e manter a confiança das partes interessadas
- Auxiliar o Conselho sobre respostas a danos à reputação externa e interna
- Prever tendências regulatórias
- Prever as expectativas de colaboradores e partes interessadas em geral
- Refletir, fortalecer e contribuir para a cultura de segurança da organização
- Avaliar a evolução do risco de *insider* para a organização

A proteção contra riscos de *insider* começa com a responsabilidade. Um Grupo de Trabalho ajudará na condução da estratégia e abordagem de uma organização, garantindo que os departamentos e setores dentro de uma organização estejam acompanhando de perto suas áreas de responsabilidade. Começar pode parecer intimidador, mas, ao adotarem esta cultura, as organizações estarão mais bem protegidas a longo prazo.

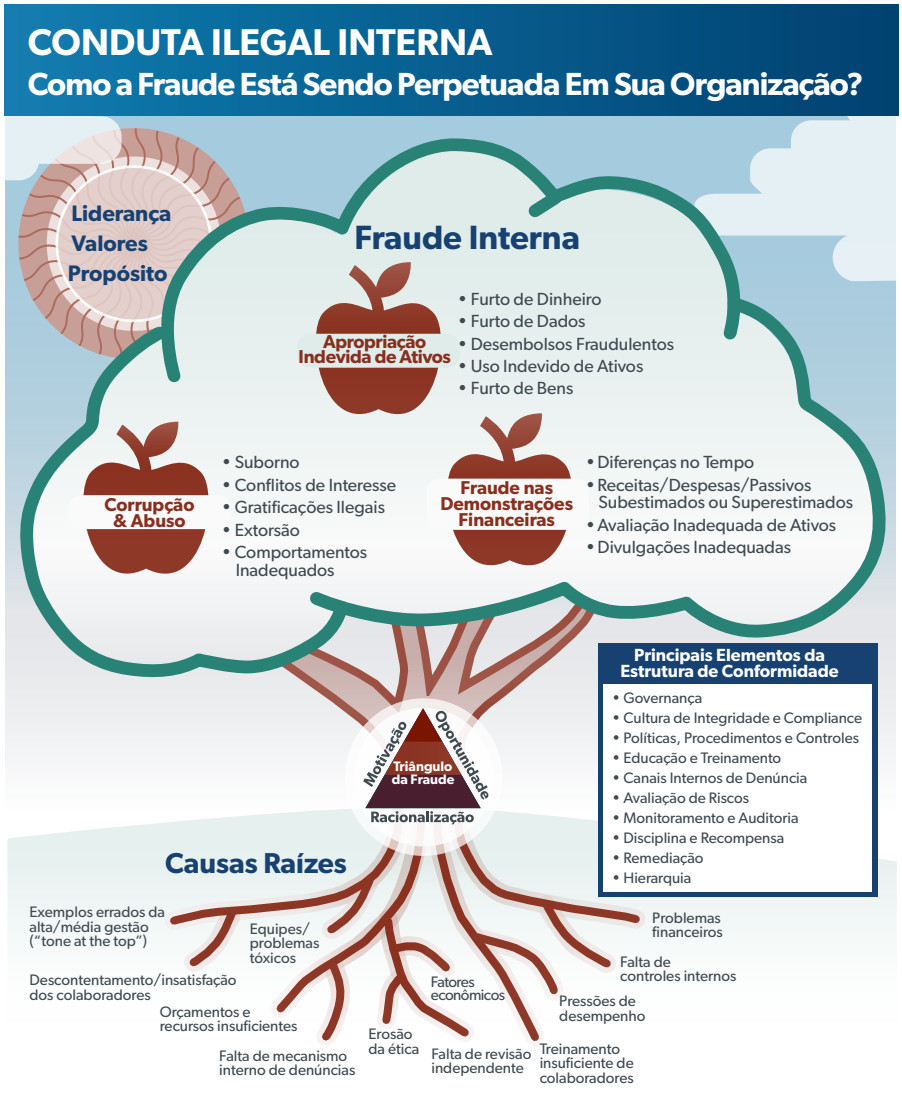
Risco de *Insider*: O Fator Humano

Quando se envolve pessoas, haverá comportamentos. Quando há comportamentos, alguns são ideais e adequados, enquanto outros quebram as regras e até mesmo ultrapassam limites éticos. As organizações devem atentar ao fator humano e estarem alertas a comportamentos antiéticos e indesejados ou que não estejam alinhados a políticas e valores das empresas.

As coisas, porém, não são tão simples quanto parecem à primeira vista. Como podemos saber se nossas decisões e comportamentos são éticos e íntegros? Embora gostemos de pensar que estamos tomando decisões com base em princípios, **pesquisas** nos mostram que não somos tão éticos quanto gostaríamos de acreditar.

Pessoas boas fazem coisas ruins

Pessoas boas podem fazer coisas ruins sem ter consciência de que estão fazendo algo errado. Embora gostemos de nos considerar justos, éticos e dentro da lei, a ciência e a experiência nos mostram que todos somos capazes de cometer atos antiéticos. Podemos aprovar os atos desonestos dos outros, por exemplo, mesmo quando acreditamos que estamos fazendo a coisa certa. Estes são chamados de "pontos cegos éticos". Em síntese, há uma lacuna entre o que pretendemos fazer e o nosso comportamento



Fonte: Sistema de classificação de fraudes da ACFE.

de fato. Reconhecemos o que devemos fazer, mas acabamos fazendo o que queremos fazer. Uma pesquisa publicada pela **Harvard Business Review** nos revela que a cegueira comportamental ou ética é uma "ladeira escorregadia" criada por vieses cognitivos. O resultado de uma decisão influencia desproporcionalmente a percepção de um observador sobre se o comportamento envolvido na decisão é ético ou não. Ou seja, se o resultado for positivo, o comportamento antiético que ocorreu para se chegar àquele resultado tende a ser relevado ou até mesmo totalmente ignorado.

Pessoas boas podem fazer coisas ruins sem ter consciência de que estão fazendo algo errado. Embora gostemos de nos considerar justos, éticos e dentro da lei, a ciência e a experiência nos mostram que todos somos capazes de cometer atos antiéticos.

Desvanecimento ético

Por que sofremos com esses colapsos éticos e processos de tomada de decisão falhos? Todos os seres humanos são pessoas inerentemente más? Existem boas razões para isso acontecer. **"Desvanecimento ético"** descreve um fenômeno em que os aspectos éticos de uma ação desaparecem de nossa visão. Uma tendência psicológica humana comum é o autoengano para racionalizar ações, tornando-se parte integrante da "ladeira escorregadia". Nossas mentes estão sujeitas à ética limitada ou limitações cognitivas que podem nos tornar inconscientes das implicações morais de nossas decisões.

Aspectos do dia a dia do trabalho, tais como metas de negócios, recompensa e reconhecimento, normas de compliance e objetivos de desempenho, podem nos impedir de perceber as implicações éticas de uma decisão, transformando nossas escolhas em uma "decisão de negócios" ao invés de uma "decisão ética", aumentando assim a probabilidade de agirmos de maneira antiética.

Por exemplo: em profissões que exigem que colaboradores registrem suas horas faturáveis em projetos, novos colaboradores podem acreditar firmemente que nunca registrariam horas que de fato não foram trabalhadas. No entanto, com o tempo, o colaborador pode se encontrar em uma situação em que esteja trabalhando menos horas do que o esperado. Para compensar a diferença, o colaborador adiciona 15 minutos a cada um dos cinco projetos em seu timesheet. São apenas 15 minutos por projeto, não é grande coisa, certo?

O que importa é o que aconteceu psicologicamente com o colaborador. Os padrões éticos agora são outros, a linha divisória entre o que é ético e antiético mudou, e a exigência de cumprir metas de horas faturáveis cegou o colaborador para qualquer identificação de quebra de limites éticos. Ocorreu um desvanecimento ético. E não para por aí. O entorpecimento ético começa a se instalar e cada vez que o colaborador registra um tempo falso, torna-se menos eticamente doloroso e o desengajamento moral vai se arraigando, de forma profunda e difícil de mudar.

Isso acaba se tornando a coisa certa a se fazer.

É o fator humano.

Colapsos éticos, a ladeira escorregadia, pontos cegos e desvanecimento ético são exemplos de riscos de *insider*. Estes não ocorrem devido a forças externas e refletem o fato de que, como seres humanos, todos nós temos uma suscetibilidade intrínseca a comportamentos indesejados e processos de tomada de decisão falhos que inevitavelmente ocorrerão, a menos que as condições em que operamos sejam controladas e monitoradas com ética em mente.

Colapsos éticos, a ladeira escorregadia, pontos cegos e desvanecimento ético são exemplos de riscos de *insider*.

As organizações devem monitorar se estão criando instituições, estruturas ou incentivos que aumentam as chances de uma ética limitada. A ética limitada descreve as formas sistêmicas e previsíveis pelas quais as pessoas tomam decisões sem perceber as implicações de seu comportamento, incluindo preconceito implícito e conflitos de interesse. Por exemplo, mesmo indivíduos que defendem a justiça e a diversidade podem discriminar com base em gênero ou raça sem estarem cientes disso. Quando as empresas permitem que esses preconceitos ou conflitos de interesse permaneçam sem controle, as consequências serão as ações sem limites éticos que inevitavelmente se seguirão e, por fim, causarão danos. É necessário trazer atenção a estes preconceitos e deslizes éticos, reforçando constantemente a cultura ética e o padrão de comportamento esperado pela organização.

Intencionais e não intencionais; Maliciosos e não maliciosos

Uma maneira de pensar sobre os diferentes tipos de *insiders* é distingui-los entre os intencionais e não intencionais e os maliciosos e não maliciosos.

Um insider não intencional e não malicioso seria alguém que inadvertidamente viola as regras. Eles não são maliciosos e não sabem que estão fazendo algo errado, mas ainda podem causar danos significativos. Muitas organizações se esforçam bastante para conscientizar os funcionários sobre os riscos cibernéticos, por exemplo, exatamente por esse motivo. Quando um funcionário clica num link malicioso num e-mail no computador corporativo ou guarda informações confidenciais sem a devida proteção, ele pode não ter uma intenção maliciosa, mas o impacto daquela ação na organização pode ser devastador. É por isso que o treinamento constante é um importante aliado na mitigação de riscos de *Insider*.

O intencional, mas não malicioso é a pessoa que conscientemente quebra as regras, mas não tem a intenção de causar danos. Isso geralmente acontece quando as pessoas ignoram deliberadamente os controles. Por exemplo, um funcionário pode optar por eliminar alguns controles da empresa em nome da eficiência e rapidez, sem considerar o risco que isso gera para o negócio.

Já o *insider* intencional e malicioso viola as regras deliberadamente e pretende causar danos. São casos como o roubo intencional de propriedade intelectual da empresa, por exemplo.

Abordagem do fator humano de riscos de *insider*

O comportamento humano não é totalmente bom ou totalmente ruim. As pessoas podem ser éticas e antiéticas, podem cometer atos hediondos ou heroicos. O fator humano pode representar tanto a fraqueza quanto a força no combate ao risco de insider. Precisamos estreitar a lacuna entre o comportamento pretendido e o real, preparar as pessoas para que saibam fazer a coisa certa e abordar os processos psicológicos que criam pontos cegos e levam a colapsos éticos.

As organizações precisam reconhecer que comportamentos baseados em valores, conduta ética e cultura constituem uma primeira linha de defesa para o risco de *insider*, sendo elementos críticos de qualquer estrutura eficaz de gerenciamento de tais riscos.

Por que somente regras não são suficientes

A implementação de regras, regulamentos, políticas e procedimentos é necessária, porém, insuficiente por si só para mitigar os riscos de insider. Controles são necessários em qualquer processo de negócios em que queremos que os grupos apliquem consistência ou quando precisamos lembrar às pessoas sobre o que priorizar, especialmente ao introduzir uma mudança.

No entanto, os controles e as políticas e procedimentos não serão suficientes por si só para evitar riscos, pois presumem que as decisões são sempre uma escolha entre um "caminho certo" e um "caminho errado". Muitas decisões envolvem escolhas entre duas opções aceitáveis e, nestes casos, a ética pode nos ajudar a escolher o caminho certo.

É preciso aplicar princípios baseados na integridade, dentro dos limites das regras e leis aceitas, a fim de elevar a tomada de decisões e expandir os horizontes de modo a incluir escolhas além de simplesmente o que é certo versus o que é errado. É por essa razão que as organizações têm códigos de conduta e ética e equipes de compliance, para ajudar as pessoas a lidar com a complexidade e a tomar as decisões certas. Isso permitirá que os colaboradores ampliem seu pensamento de tomada de decisão não apenas para o que devem fazer conforme as leis e regras, mas também para o que podem fazer, alinhados às políticas e valores da empresa. Dessa forma, podemos começar a enfrentar a lacuna entre o comportamento pretendido e o real, interrompendo os processos psicológicos que podem nos levar à "ladeira escorregadia".

Interrompa os processos psicológicos que levam a colapsos éticos:

Educando, capacitando e preparando
seus líderes e colaboradores para reconhecerem seus pontos cegos e o motivo de muitas vezes não alcançarmos nossos próprios padrões éticos – não porque somos inerentemente maus, mas porque somos seres humanos.

Identificando
quaisquer valores ou normas informais ocultos, mas poderosos, que motivem as escolhas individuais e induzam a comportamentos na organização.

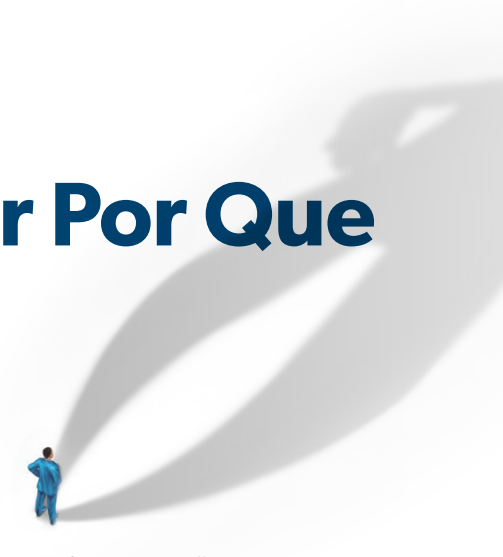
Implementando
controles e princípios baseados em integridade nos processos de tomada de decisão do dia a dia para atuarem como uma bússola ética ou moral que possa navegar por escolhas baseadas em risco e encontrar consequências não intencionais.

Próximos passos

Os colapsos éticos são uma parte inerente da condição humana e contribuem para os riscos de insider em uma organização. Isso não vai mudar. Não há um modelo ou solução de "tamanho único" para abordar a pura beleza e complexidade dos seres humanos: fundir inovação, criatividade e diversidade com pontos cegos, vieses e preconceitos. As pessoas fazem escolhas e as escolhas fazem a cultura. As organizações precisam fazer — e ajudar os outros a fazer — escolhas melhores.

As organizações precisam estar mais vigilantes em relação ao fator humano de riscos de *insider*. Promova o engajamento e capacite seu pessoal para estar mais consciente de suas vulnerabilidades humanas. Molde e projete um ecossistema cultural formado a partir de valores corporativos e delimitado por políticas, controles e procedimentos baseados em integridade. E construa uma crença compartilhada em fazer a coisa certa em toda a organização, começando do topo e conectando-a a uma norma cultural de "como fazemos as coisas por aqui".

Esforce-se para Entender Por Que *Insiders* Podem Agir Mal



Descobrir um comportamento antiético ou mal-intencionado de um colaborador pode ser complexo para uma organização. No entanto, com anos de experiência investigando fraudes e má conduta no setor privado e dentro da segurança nacional dos EUA, David Burroughs e Nathan Fisher, identificaram os fatores motivadores para *insiders* e os principais controles efetivos para mitigar ameaças. Eles compartilham suas perspectivas únicas e histórias da linha de frente nesta sessão de perguntas e respostas.

Quais são algumas das motivações mais comuns que vocês observaram em casos envolvendo riscos de *insider*?

Burroughs: As pessoas tomam decisões erradas por diferentes motivos. As circunstâncias podem alterar as perspectivas e a ética das pessoas, e o ego desempenha um papel significativo no comportamento interno. Por exemplo, um funcionário que acaba não recebendo um aumento salarial ou promoção de cargo, se sente subestimado ou seus sentimentos são feridos e decide "mostrar a eles o quão bom ou inteligente ele é".

Algumas pessoas procuram explorar processos, perguntando "Como posso derrotar o sistema?" Muitas vezes, isso pode começar como uma pequena operação teste ou talvez até um ato não intencional - como pedir um reembolso acidentalmente de algo que o funcionário não pretendia - e se a operação não for detectada, o ato provavelmente se transformará em um esquema maior assim que a pessoa perceber que ninguém está vendo.

Outros se sentem encorajados por uma sensação de que seu empregador provavelmente não os processará se houver potencial para danos reputacionais caso seus atos se tornem conhecidos publicamente. A ganância também costuma ser um fator. A menos que tomem uma decisão espontânea de se aproveitarem de uma vulnerabilidade, os *insiders* que cometem crimes geralmente precisam contemplar suas ações e pesar os ganhos potenciais contra as consequências de serem pegos. As pessoas racionalizam seus próprios comportamentos o tempo todo.

Como investigador, acredito que a empatia é um componente essencial na avaliação do comportamento ao tentar identificar sua motivação. Acho fundamental tentar entender o que eles sentiram e, se possível, por quê? A perspectiva da empatia geralmente ajuda a contextualizar as ações de um *insider*, o que, por sua vez, pode ajudar a desvendar o que aconteceu e os motivadores por trás disso.

Poderia dar exemplos de risco de *insider* que você já viu?

Burroughs: Quando se trata de ameaças internas, cada setor tem riscos e desafios únicos.

Das muitas fraudes que investiguei, algumas se destacam como relativamente comuns em vários setores. O diretor financeiro (CFO) de uma empresa global tinha controle exclusivo sobre o desembolso e conciliação de todas as finanças. Não havia controles financeiros ou supervisão, o que permitiu ao CFO aprovar empréstimos para si mesmo totalizando mais de US$ 1 milhão em um período de dois anos.

Além de seus deveres fiduciários, outro CFO também era responsável por conciliar as contas de cartão de crédito de sua empresa. O CFO não havia recebido o bônus que esperava ou aumento salarial ao qual achava que tinha direito. Ele era um exemplo típico de empregado insatisfeito e, consequentemente, sentia-se no direito de usar os recursos da empresa para despesas pessoais - uma grande festa em sua casa custando milhares de dólares, viagens, artigos de luxo, contas altíssimas em bares, massagens, adiantamentos em dinheiro, e por aí vai. Ele acabou roubando mais de US$ 325 mil. Às vezes, o *insider* é a própria pessoa a quem é confiada a responsabilidade de proteger as finanças da empresa.

Houve também uma investigação que envolveu uma contadora de um grande banco, responsável pelo pagamento de vários prestadores de serviços. Um dia, ela decidiu testar se conseguiria pagar sua conta de gás e fez o pagamento como se fosse para um fornecedor. Assim que o pagamento foi

compensado, ela fez vários outros pequenos pagamentos que também não foram sinalizados ou detectados. Assim que teve confiança de que não havia controles de auditoria para detectar esses tipos de pagamentos, ela rapidamente aumentou suas compras, e acabou comprando carros, barcos, equipamentos de mergulho e até mesmo uma casa. É um bom exemplo de que não implementar controles financeiros robustos permitirá que até mesmo funcionários juniores tenham a oportunidade de explorar o processo.

Como as organizações podem identificar ameaças internas?

Fisher: Incidentes envolvendo *insiders* podem ser difíceis de se detectar. Sem vestígios de comprovantes, como papel ou rastros digitais, é difícil encontrar os malfeitores. A tecnologia e os controles podem ajudar a fornecer algumas informações, mas muitas vezes as organizações devem procurar mudanças no comportamento de uma pessoa como as primeiras indicações. Mudanças na personalidade podem ser um indicador, podendo sinalizar que algo está acontecendo com aquele colaborador. As organizações devem observar as mudanças no comportamento, no desempenho ou na forma de interação com os colegas. Mudanças nos hábitos financeiros –gastos atípicos ou vultuosos, ou dificuldades recentes – podem indicar que algo está errado. Ser sociável de forma anormal ou de repente preferir o isolamento podem também ser sinais de alerta que justifiquem um olhar mais atento sobre as atividades de um *insider*.

Esse comportamento anormal pode se manifestar em situações como a recusa de se tirar férias ou de ser sempre o primeiro a chegar e o último a sair do escritório. O colaborador pode ter medo que suas atividades sejam descobertas se não estiver disponível para responder a perguntas sobre anomalias descobertas em sua ausência. Demonstrar um novo interesse em uma área específica dentro da empresa, fora do escopo de suas responsabilidades, também pode ser motivo de preocupação.

6 Categorias de Motivação

Por trás de um comportamento indesejado pode haver inúmeras motivações, mas a maioria dos atos tende a se enquadrar em seis categorias, a saber:

1. **Psicológica.** Isso inclui *insiders* que podem estar com raiva, estressados e/ou deprimidos. Por exemplo, insiders podem agir em retaliação por algum descontentamento, como ser ignorado na época do bônus. Sentimentos de "eu mereço isso" ou "vou mostrar que sou mais esperto do que todos vocês" podem servir para justificar ou racionalizar a má conduta de um *insider*.

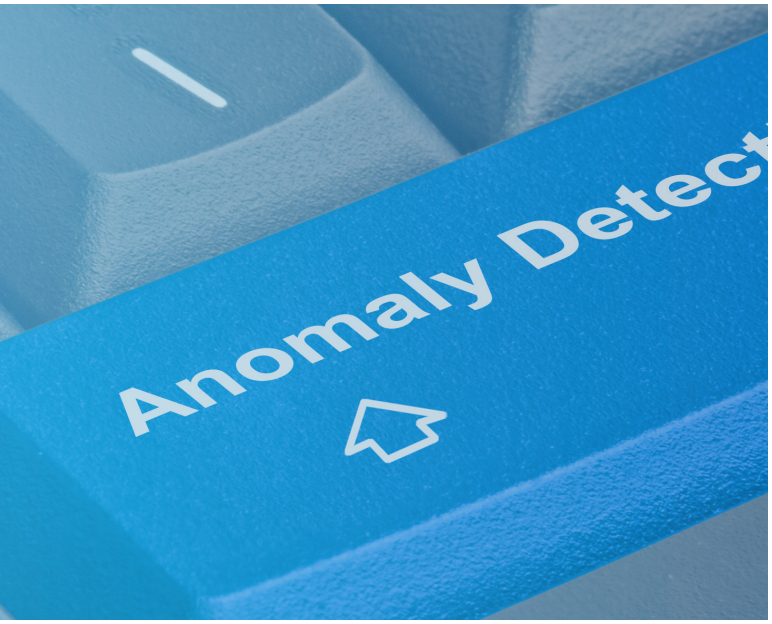
2. **Financeira.** Dívidas, doenças familiares, vícios ligados ao álcool ou substâncias químicas ou jogos de azar e viver além das próprias posses podem ser motivos para furto, peculato ou conspiração com terceiros para obter ganhos financeiros. A pura ganância também é um motivador muito forte.

3. **Relacional.** *Insiders* às vezes são abordados para se juntar a esquemas contra a organização. Esses esquemas podem vir na forma de convite de colegas ou, dependendo da sensibilidade da posição do *insider*, por meio de chantagem ou extorsão. A relação pode surgir com ameaças como "Se você não fizer isso...", seguida de outras chantagens envolvendo relatos a superiores ou familiares sobre alguma transgressão passada ou fato comprometedor.

4. **Ambiental.** Controles deficientes e/ou uma cultura deficiente em uma organização podem servir como motivação para atos maliciosos ou comportamentos ilegais. A percepção de que as chances de ser flagrado são baixas pode contribuir para a ação do *insider*.

5. **Situacional.** Colaboradores que estão isolados e têm poucas interações com colegas de trabalho e supervisores também são um risco. Com um número cada vez maior de pessoas trabalhando remotamente, a oportunidade de agir quando "ninguém está olhando" é muito mais prevalecente.

6. **Ideológica.** *Insiders* também podem encontrar motivação em ações por uma causa ou ambição. A lenda inglesa de Robin Hood, que supostamente roubava os ricos para dar aos pobres, pode ter sido fictícia, mas ideologias semelhantes podem ser bastante reais.



Como os *insiders* normalmente são pegos?

Fisher: Se os processos de controle não detectarem anomalias, a irregularidade interna poderá, às vezes, vir à tona quando outro funcionário disser que notou algo. Mas isso depende de os funcionários se sentirem à vontade para falar. Isso geralmente ocorre somente se houver uma percepção ou um histórico de que a organização tomou as medidas apropriadas no passado em outros casos de irregularidades, quando outros se manifestaram. A confidencialidade e o medo de possíveis retaliações também podem afetar a disposição de um funcionário de se manifestar. A cultura da organização desempenha um papel direto no estabelecimento de tais denúncias.

> *Observar anomalias no comportamento dos colaboradores é essencial, mas é importante considerar a totalidade dos indicadores, não apenas alguns.*

Um evento pode levar alguém na organização a verificar um fato que parecia "estranho" e então a irregularidade é descoberta, como alguém entrar no espaço físico do trabalho fora do expediente. Certa vez, tive um caso em que um agente de segurança notou que um funcionário parecia excessivamente dedicado – saía tarde da noite e chegava muito cedo pela manhã. Descobrimos que esse funcionário estava acessando informações da empresa quando ninguém estava olhando, demonstrando que essas longas horas nem sempre indicam muito trabalho ou dedicação à missão de uma empresa.

Observar anomalias no comportamento dos colaboradores é essencial, mas é importante considerar a totalidade dos indicadores, não apenas alguns. Pode haver boas explicações para comportamentos anômalos, mas é importante que as organizações entendam o que está acontecendo com seus funcionários.

Dois Principais Motivos Pelos Quais os Programas de Denúncia— ou de Comunicação Ativa — Falham

1. **MEDO:** Funcionários se preocupam com uma retaliação ou represália
2. **INAÇÃO:** Funcionários observam ou percebem que a organização não dará uma resposta a suas preocupações

Data Analytics: Ferramentas para Visualizar e Mitigar Riscos de *Insider*

O risco de insider atinge todas as áreas de uma organização, desde o Conselho até a alta administração, a diretoria jurídica e a equipe de compliance. Por isso, organizações de todos os portes precisam de informações acionáveis que sejam relevantes para cada função, sintetizadas e apresentadas de forma a permitir uma resposta a essas situações. Quando devidamente configurada para oferecer suporte a essas partes interessadas, o **data analytics,** ou análise de dados, é uma ferramenta poderosa para auxiliar na identificação e mitigação dos riscos de insider.

Um dos recursos mais úteis da análise robusta de dados é a visualização do risco. Os dados podem nos contar uma história sobre as atividades de insiders. O data analytics ajuda a mostrar essa história integrando vários conjuntos de dados e exibindo-os de uma forma que ofereça insights rápidos, como por meio de relatórios personalizados para a diretoria, Conselho, departamento jurídico, além de outras funções. Isso, juntamente a uma avaliação e análise humana, investigações e experiência, poderá ajudar a traçar uma imagem mais clara do perfil de risco de uma organização.

Há uma diferença fundamental entre as organizações aparentemente saudáveis e as não saudáveis, ou as organizações em que o risco de *insider* está se manifestando ou não. Mas, o *data analytics* pode ser uma ferramenta poderosa para ambas. Para uma organização aparentemente saudável, profissionais qualificados podem utilizar os dados para ajudar a identificar onde pode estar o maior risco. Para uma organização não saudável, os dados podem revelar onde as coisas podem ter dado errado, ajudando a encontrar a "agulha no palheiro".

Como exemplo, um número excessivo de lançamentos por um funcionário de vendas pode levantar suspeitas, como aconteceu com uma organização que descobriu que um funcionário estava saindo para jantar com o mesmo cliente várias vezes por mês, custando à empresa milhares de dólares. Se os processos manuais forem a única forma para revisar e aprovar despesas, essa atividade pode levar muito tempo para ser descoberta. Com os dados certos e os parâmetros definidos pela organização, comportamentos suspeitos podem surgir muito mais cedo e permitir que os líderes consigam olhar mais de perto antes que um problema se transforme em um assunto sério de compliance.

Poderia haver razões plausíveis para despesas frequentes de entretenimento relacionadas a um cliente. Podem representar negócios adicionais que a organização buscou obter. Mas também podem indicar uma atividade imprudente e potencialmente ilegal, capaz de causar danos significativos à reputação da empresa, como pagamentos de propina a agentes públicos ou algo pior. De qualquer forma, é melhor para a organização saber sobre isso e investigar.

Se antecipando às tendências

Uma proposta de valor para o *data analytics* é a sua capacidade de permitir que as organizações se antecipem às tendências antes que elas se tornem problemáticas. Não há substituto para saber o que está acontecendo dentro da organização em tempo real, e esse conhecimento geralmente está disponível por meio da análise correta.

Assim que uma organização tiver controle sobre as atividades atuais, ela poderá começar a passar da percepção atual para a previsão. Ou seja, a organização poderá identificar – e mitigar – futuras ameaças internas por meio de análises preditivas.

Um equívoco comum sobre análises preditivas é que exigem sistemas sofisticados de inteligência artificial e *machine learning*. Estes são de fato ferramentas úteis na análise de volumes de dados, mas as organizações podem obter insights valiosos por meio de abordagens simples baseadas em regras. Se você observar X nos dados, isso pode indicar um tipo de risco Y em um nível Z de criticidade.

Veja como seria na prática: há uma instância nos dados de despesas de viagem e entretenimento de um colaborador que enviou recibos duplicados buscando o reembolso para ambos; isso é marcado como fraude potencial com nível de risco 2 em uma escala de 1 a 5 (pode ter sido um descuido isolado). Se instâncias repetidas de tal anomalia pelo mesmo colaborador forem observadas durante um período de tempo, o nível de risco pode ser marcado como 4 ou 5, pois pode ser uma tentativa de fraude. Uma solução de *data analytics* poderia ser desenvolvida para codificar as regras IF-THEN-ELSE que analisariam dados, atribuiriam pontuações de risco e os publicariam em um painel para revisão e ação - tudo de maneira totalmente automatizada.

Colaborar para enriquecer os dados

A implementação de *data analytics* para abordar o risco de insider de maneira ideal exige um aspecto cultural. A colaboração deve ocorrer em relação a pessoas, dados e processos. Quando uma organização tem uma cultura de colaboração e conformidade, as áreas conversam entre si e aprendem umas com as outras e, essencialmente, compartilham informações.

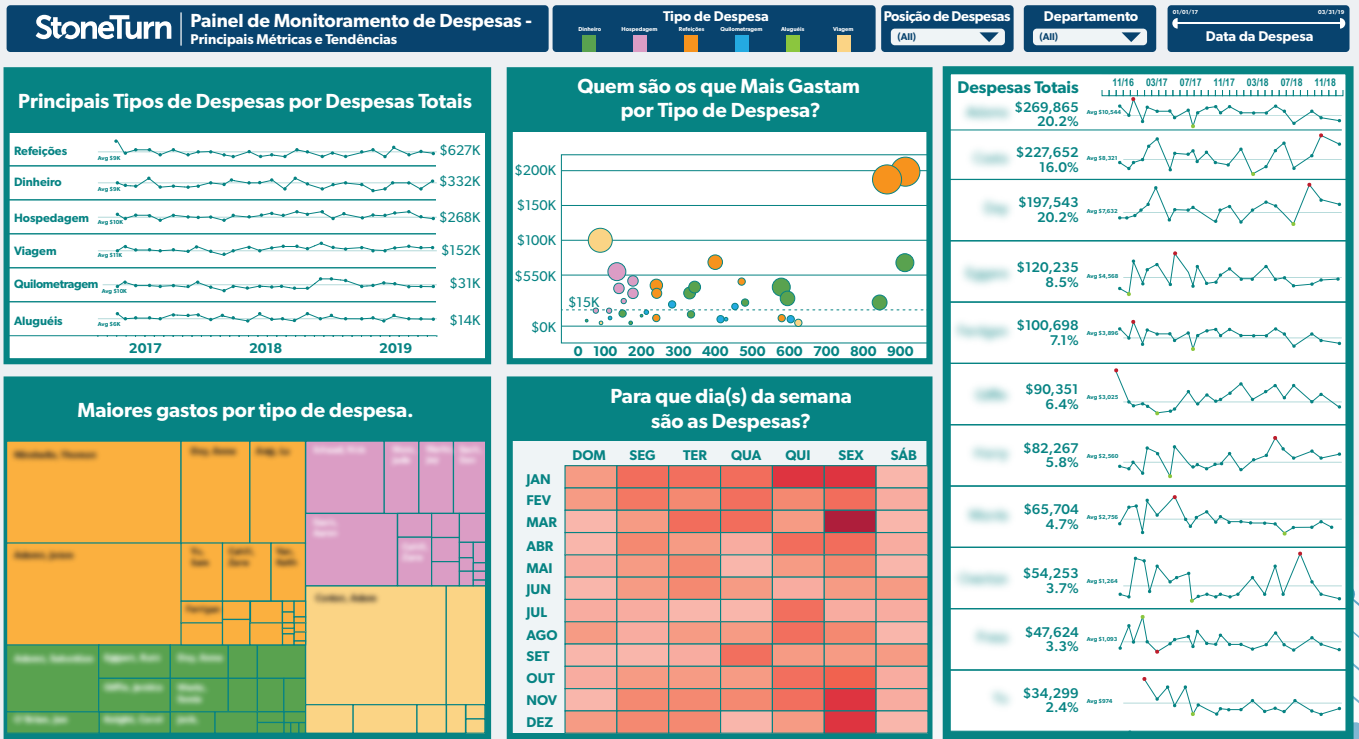
Quando uma organização tem uma cultura de colaboração e conformidade, as áreas conversam entre si e aprendem umas com as outras e, essencialmente, compartilham informações.

Por exemplo, os dados de compliance sobre treinamentos, canais de denúncia, conflitos de interesses e registro de presentes em conjunto com

Amostra de Painel: Fraude em Gastos e Reembolsos

Painel de Despesas de Funcionários

Um painel de amostra demonstrando padrões de risco em vários conjuntos de dados



dados de RH, incluindo avaliações de desempenho, estrutura organizacional, relações com funcionários, pesquisas e muito mais, podem oferecer uma visão mais profunda dos possíveis riscos de insider relacionados a má conduta no local de trabalho. Além disso, com dados do jurídico, da auditoria interna e de suprimentos, as organizações terão um conjunto de dados sobre riscos de *insider* em 360 graus.

Mas não devemos parar nas fontes de dados internas. Dados externos, como geodemografia, e benchmarks salariais, entre outros, podem aumentar ainda mais o poder e a especificidade dos insights. Uma empresa de varejo com várias localidades poderia, por exemplo, aproveitar esses dados para controlar a discriminação salarial baseada em gênero, discriminação racial no recrutamento, entre outros riscos.

Denúncia

Além dos dados coletados pelos líderes das empresas, os insights sobre comportamentos internos podem vir de outros colaboradores, incluindo denúncias. É fundamental monitorar as medidas que uma organização toma quando recebe uma denúncia. Quais dados são coletados sobre a linha direta do canal de denúncia? Qual é o índice de fundamentação das reclamações? Um **2020 study of internal whistleblowing systems** descobriu que um aumento de 10% nas reclamações de delatores estava associado a uma redução de 2% nas multas do governo e uma redução de 1% nos valores de acordos judiciais. O que uma organização faz com as reclamações internas é importante, é claro.

Aja agora

Não existe uma "solução" tecnológica para gerenciar os riscos de insider. Se devidamente reunidos, analisados e apresentados, os dados podem auxiliar na compreensão dos riscos dentro da organização. O principal aprendizado sobre o uso de *data analytics* para o gerenciamento de riscos de insider é não esperar até que surja um problema. Se houver espaço para melhorar e se tornar mais eficiente enquanto aprimora a conformidade, as organizações devem agir assim que possível.

Dicas para uma Avaliação Analítica Bem-Sucedida

- Obtenha aprovação e comunicação da alta administração desde o início
- Tenha uma equipe apropriada
- Não tente forçar uma metodologia quantitativa
- Avalie utilizar uma abordagem em três frentes: top-down, bottom-up e benchmarking do setor
- Avalie os requisitos futuros, não as necessidades atuais
- Priorize resultados e impacto
- Não se esqueça de desenvolver um roteiro para o que está por vir

Controles de Segurança Cibernética: Um Passo à Frente dos *Insiders*

Intencionalmente ou não, **82% dos incidentes cibernéticos globais** envolvem o elemento humano. Infelizmente, as organizações nem sempre avaliam o problema do risco de *insider* até que algo ocorra.

Na segurança cibernética, *insiders* humanos fazem parte da defesa do perímetro de uma organização – sendo geralmente sua vulnerabilidade mais significativa. Da engenharia social às tentativas de phishing, à negligência e erros inadvertidos, como, por exemplo, o envio de dados confidenciais para um endereço de e-mail incorreto, os *insiders* têm um papel central em muitos dos incidentes de comprometimento de redes e dados.

Novas situações alteram o equilíbrio dos riscos; nos últimos anos, vimos a rapidez com que novos cenários podem alterar os riscos do negócio. É vital que as organizações analisem as mudanças relacionadas à tecnologia e reavaliem suas vulnerabilidades e eficácia dos controles.

Quatro Tipos de Ameaças Internas no Ciberespaço

Organizações de todos os setores enfrentam ameaças variadas, conforme exploramos ao longo deste documento, mas, normalmente, quatro tipos de ameaças cibernéticas internas são predominantes:

1. **Sabotagem.** Um *insider* comete ataques destrutivos, causando danos físicos a servidores ou mídia de armazenamento e/ou destruindo dados por meio de programas maliciosos.
2. **Fraude.** Ganância ou dificuldades financeiras podem levar um *insider* a fraudar a organização para ganho pessoal. O uso indevido de recursos da empresa para pagar despesas pessoais é um exemplo.
3. **Roubo de propriedade intelectual.** Roubar segredos comerciais pode ser um ato de vingança de um funcionário descontente. Um *insider* pode roubar dados como parte de um plano para criar um concorrente ou realizar o roubo para vender- os dados para ganhos financeiros.
4. **Espionagem Corporativa.** Concorrentes e outros agentes externos podem atrair *insiders* para que forneçam dados ou produtos confidenciais para obtenção de uma vantagem competitiva.

Ciclo de Vida de uma Ameaça Interna Intencional:

Motivação

Qual é a necessidade ou objetivo que convence o *insider* a agir? Exemplos comuns incluem ganhos financeiros, ideologia, reclamações, vingança ou ter sido comprometido e coagido a agir por uma parte externa.

O Alvo

O *insider* identifica a capacidade ou poder que tem por conta de sua função e seus acessos dentro da organização

O Esquema

O *insider* desenvolve seu plano para explorar a vulnerabilidade que identificou e aproveitá-la para realizar sua a ação.

Reconhecimento

O *insider* refina seu plano identificando nele possíveis obstáculos e pontos fracos. Ele pode realizar monitoramentos, testar controles e salvaguardas, ou mesmo realizar ensaios ou simulações, fazendo melhorias com base no feedback obtido.

Ação

O *insider* executa o plano. Com base na motivação subjacente, o sucesso alcançado e seu acesso, isso deve concluir toda a extensão da atividade de ameaça do *insider*, ou o *insider* poderá continuar a aproveitar seu acesso para explorar continuamente a vulnerabilidade ou planejar ações de ameaças adicionais.

Controles a Considerar

Um elemento fundamental a ser implementado na segurança cibernética são os controles de acesso. Nem todos os colaboradores necessitam do mesmo nível de acesso às unidades de rede e aos dados de sua organização para realizar seus trabalhos. Assim, os privilégios de acesso devem estar alinhados com as responsabilidades específicas de cada colaborador. E esses controles devem ser atualizados à medida que o colaborador avança, assume responsabilidades adicionais ou muda de cargo. A regra padrão é que cada funcionário só deve ter acesso aos dados de que precisa para desempenhar sua função de trabalho, devendo todos os outros dados ser segregados.

Outro controle é o monitoramento regular de acessos

e rastreamento de logins e downloads de dados. Os sinais de atenção a serem observados incluem horas e dias atípicos para logins, logins em aplicativos atípicos, aumento na quantidade de dados baixados, downloads em locais suspeitos e tentativas de aumentar os privilégios de acesso de rede. Saber o que é "normal" para um determinado funcionário ou função facilita a identificação de comportamentos anômalos.

Os métodos comuns que funcionários utilizam para roubar dados são enviá-los por e-mail para uma conta pessoal, fazer o upload de arquivos para uma conta de nuvem pessoal ou copiar informações para um dispositivo externo. Por exemplo, um funcionário júnior de recursos humanos pode ficar chateado com a forma como um amigo no trabalho foi tratado, então ele baixa arquivos pessoais que não deveria. Em outro cenário, um funcionário de gerencial, ao se desligar para trabalhar em um

concorrente leva dados de propriedade intelectual com ele em um pendrive.

Os sistemas de prevenção de perda de dados podem rastrear os dados que saem da rede de uma organização de acordo com parâmetros personalizados. Quando as transmissões de dados ficam fora desses parâmetros ou parecem anormais, os sistemas podem alertar a equipe de segurança cibernética. A equipe de computação forense pode determinar se um usuário específico enviou ou baixou dados violando regras da empresa, sendo que algumas organizações solicitam tais verificações depois que um funcionário é desligado.

Entre os controles básicos, senhas longas e difíceis de decifrar são eficazes para impedir o acesso não autorizado. Quanto mais caracteres uma senha tiver, mais tempo levará para uma tentativa de ataque de "força bruta". Outro controle é a autenticação multifator ("MFA", na sigla em inglês). A tendência de "traga seu próprio dispositivo" (ou "bring your own device"e "BYOD" nos termos em inglês) para comunicações pessoais e de trabalho é particularmente arriscada, especialmente na era do trabalho remoto. A melhor maneira de proteger o trabalho remoto contra incidentes cibernéticos é a organização fornecer o dispositivo e configurá-lo para segurança.

Compromisso com a Cibersegurança

O mundo corporativo tem uma preocupação crescente da necessidade de segurança, devido ao número de incidentes cibernéticos que ocorrem todos os anos. No entanto, os compromissos para melhorar a segurança cibernética estão ocorrendo lentamente, pois envolvem despesas e mudanças de comportamento. Muitas organizações relutam em investir em segurança cibernética porque acreditam que a segurança não melhora os resultados ou não percebem sua necessidade imediata. Logo, muitas empresas tentam utilizar o mínimo de recursos possível, enquanto outros enxergam a segurança cibernética como uma área para possíveis cortes de orçamento.

Os riscos de *insider* não vão desaparecer, com os impactos aumentando em tempos de crise econômica e incerteza. Tornar as organizações mais seguras envolve uma cultura sustentada pelos mais altos níveis, disseminada através de treinamento contínuo e orçamento adequado para ferramentas e recursos.

Características de Ameaças Internas

Como é uma ameaça interna? Em geral, um *insider* responsável por um incidente de segurança cibernética se enquadra em uma das três categorias:

PESSOA COMPLACENTE

A complacência pode aparecer em colaboradores indiferentes, preguiçosos, sobrecarregados, superqualificados ou subqualificados em suas funções. Identificação incorreta, armazenamento equivocado de dados e controles inadequados aumentam os riscos de segurança cibernética. Conveniência e complacência geralmente andam juntas, como manter senhas em um post-it anexado à mesa ou computador do usuário.

USUÁRIO COMPROMETIDO

Um *insider* pode ser coagido ou ameaçado por estranhos a colaborar com um roubo ou violação de dados. Nessas situações, pessoas de fora podem tentar explorar a fraqueza ou vulnerabilidade do *insider*, cujo comportamento pode ser influenciado por questões pessoais ou familiares, como dívidas, doenças, jogos de azar ou vícios. Um *insider* comprometido pode se sentir impotente para resistir.

FUNCIONÁRIO MALICIOSO

Um *insider* malicioso pode tentar explorar vulnerabilidades ou roubar para se enriquecer ou prejudicar sua organização. Funcionários descontentes com acesso a dados e locais confidenciais podem causar muitos danos se não forem monitorados.

Aprimorando os Controles e a Supervisão a Longo Prazo

Vários tipos de controles podem ser eficazes na redução de riscos de *insider*. As organizações devem ter uma visão holística de seus controles e protocolos ao considerar sua suficiência. Mas, acima de tudo, os controles só serão eficazes se coordenados de forma holística. Garantir que os sinais de alerta sejam identificados e comunicados aos responsáveis pelo gerenciamento do risco é essencial para um programa eficaz. Esses controles incluem:

Manter um Inventário de Segredos Comerciais e Informações Proprietárias

As organizações devem fazer um registro de suas informações confidenciais e definir segredos comerciais e outras informações confidenciais ou críticas. Uma vez identificadas e inventariadas, as informações consideradas segredos comerciais devem ser marcados como tal e um administrador deve ser designado para garantir seu tratamento adequado.

Contratos de trabalho

Todos os colaboradores da empresa devem firmar acordos de confidencialidade nos quais concordam em não compartilhar informações confidenciais. Da mesma forma, o código de conduta da empresa e o manual do colaborador também devem abranger os requisitos de confidencialidade e as obrigações dos colaboradores de se pronunciarem em relação a incidentes de violação de confidencialidade ou outros vazamentos ou perdas de dados proprietários.

Controles Físicos

Saber se alguém está no prédio a qualquer momento pode ajudar a reduzir as oportunidades de crimes internos, além de fornecer informações vitais sobre onde está o pessoal durante crises como incêndios, desastres naturais ou incidentes violentos. Controles físicos robustos também limitam o acesso a arquivos ou áreas confidenciais, como salas de servidores. As organizações que deixam de reconhecer vulnerabilidades físicas se expõem a riscos desnecessários de acesso não autorizado a dados importantes e outros ativos, não apenas por pessoas internas, mas também por fornecedores terceirizados, como serviços de manutenção ou limpeza após o expediente.

Controles de Pessoal

Como as pessoas representam a maior vulnerabilidade a qualquer programa de segurança, as organizações devem ter procedimentos abrangentes para realizar verificações de antecedentes criminais e reavaliar seus colaboradores à medida que progridem na organização. As políticas sobre uso de drogas e substâncias químicas como parte de um código de conduta podem ajudar a lidar com anomalias de comportamento que podem levar a comportamento criminoso interno. Uma assistência a colaboradores ou linhas diretas confidenciais para que busquem ajuda para si mesmos ou para outros, ou para compartilhar preocupações ou até mesmo relatar irregularidades, também constituem ferramentas importantes que ajudam a fortalecer uma melhor infraestrutura de segurança, reforçando a cultura focada no funcionário.

Controles Cibernéticos

O gerenciamento de privilégios é uma forma fundamental de controle cibernético. Nem todo colaborador precisa ter acesso de administrador a sistemas, redes e unidades de dados. Outras formas de controles cibernéticos essenciais são a autenticação multifatorial e senhas longas e complexas, difíceis de *hackear*. Sistemas e softwares que sinalizam ou identificam possíveis acessos ou downloads não autorizados oferecem a segurança necessária para dados confidenciais. De forma criteriosa, as pessoas que avaliam os alertas nos sistemas precisam estar cientes de como a atividade interna pode se apresentar, ou elas poderão perder possíveis pistas importantes. A conscientização dos envolvidos na identificação e gerenciamento dos riscos de *insider* é vital.

> *"Um programa de risco de insider pode ser ampliado (ou reduzido) e flexibilizado dependendo do tamanho, perfil de risco e recursos disponíveis da organização. Não há duas organizações iguais. Até mesmo para as menores organizações, uma avaliação dos riscos de* insider *e a implementação dos principais controles ajudarão a mitigar os riscos sem exigir recursos significativos.*

Políticas e Procedimentos para o Tratamento de Segredos Comerciais

Políticas e procedimentos para segredos comerciais e informações confidenciais devem ser desenvolvidos para controlar o acesso, uso e medidas para proteger sua confidencialidade. As políticas devem incluir: um princípio da "necessidade de saber" para acessar segredos comerciais; restrições ao compartilhamento ou transmissão de informações de segredos comerciais; uma obrigação explícita para todos os colaboradores de manter a confidencialidade dos segredos comerciais; e processos para proteger segredos comerciais, como políticas de "mesa limpa".

Treinamentos

Após a contratação, todos devem ser treinados sobre a natureza dos segredos comerciais da empresa, bem como os métodos e suas responsabilidades para protegê-los. O treinamento deve incluir não apenas um conteúdo específico sobre segredos comerciais, mas também abranger o uso de computadores, medidas de segurança física utilizadas pela empresa e como relatar preocupações através de linha direta de compliance da empresa. Colaboradores com responsabilidades especialmente sensíveis devem receber treinamento complementar conforme necessário. Todos os treinamentos devem ser regulares e continuamente atualizados para refletir as mudanças nos negócios.

Controles Financeiros

Pesos e contrapesos (checks and balances) e o princípio de dupla checagem na aprovação de desembolsos são controles financeiros importantes. Auditorias pontuais e/ou verificações de segurança aleatórias podem aprimorar esses controles e dificultar a ação de agentes mal-intencionados.

Controles de Liderança

Casos após casos têm mostrado que o maior impacto das ameaças internas pode vir de executivos que têm acesso a dados confidenciais. Funcionários júniores e subordinados diretos tem menor propensão a questionar ou reportar o comportamento suspeito de um executivo. Uma estratégia bem-sucedida para minimizar a má conduta de executivos é a avaliação consistente e contínua, principalmente à medida que os executivos progridem em suas organizações. Os executivos devem passar pela mesma triagem periódico que outros funcionários. O feedback anônimo por meio de uma linha direta confidencial pode ser valioso para as organizações na identificação de comportamentos problemáticos, ao mesmo tempo em que minimiza o medo de retaliação por parte dos funcionários.

Controles de Saída

No desligamento de qualquer colaborador da empresa, deve haver uma lista abrangente de verificação para garantir que todos os dispositivos, credenciais e cartões de acesso tenham sido coletados e desativados. Quando os líderes ou colaboradores com acesso a dados valiosos da empresa deixam seus cargos, uma análise pode ser realizada em relação a todos os dados das redes ou sistemas da empresa acessados, bem como uma revisão de métodos manuais, como registros de utilização de impressoras. As organizações também devem considerar a realização de entrevistas de saída, tanto como uma forma de lembrar os que estão saindo de suas obrigações legais como também para coletar informações valiosas sobre o que está acontecendo dentro da organização.

Também é importante tomar cuidado com o "*Insider* Externo".

No últimos dois anos, o trabalho remoto ou híbrido em grande escala se tornou realidade para a maioria das organizações. Embora a flexibilidade seja amplamente vista como um benefício para a maioria das organizações, isso acabou apresentando um risco: controles internos deficientes, criando para um ambiente em que o risco de *insider* pode progredir. Funcionários que costumavam ser internos 100% do tempo agora estão trabalhando em casa ou em escritórios remotos. As organizações devem testar e ajustar regularmente seus controles e sistemas a fim de ajustar a necessidade de facilidade de acesso com a capacidade de proteger suas "joias da coroa".

Avaliar controles e configurar estruturas pode ser intimidador, mas as organizações podem começar fazendo um balanço do que está ao seu alcance. Abaixo apresentamos listas de verificação a serem consideradas e perguntas a serem feitas para ajudar a impulsionar seu programa agora.

Perguntas a Serem Feitas: Controles de Riscos de *Insider*

Começando

- **Você tem alguma propriedade intelectual sensível?**
- **A perda da sua propriedade intelectual** ameaçaria o futuro do seu negócio?
- **A sua empresa está ligada a novas tecnologias emergentes,** como de computação quântica, inteligência artificial, tecnologia de fusão, biofarmacêutica?
- **Você está passando ou passou recentemente** por um período de mudança significativa (como expansão, fusão, aquisição, contração)?
- **Você firmou ou poderá firmar** contratos com o governo?
- **Você já teve algum caso de *insider,*** de que tenha conhecimento, como fraude, roubo de propriedade intelectual, furto, sabotagem de instalações ou dados, ou teve algum desligamento de "funcionário insatisfeito"?
- **Você está ciente de algum ataque cibernético** contra sua empresa?

Governança e Responsabilidade

- **Quem é responsável** por riscos de insider na sua organização?
- **Você tem um programa** para receber, encaminhar e analisar questões de conduta levantadas internamente?
- **Quais** canais você utiliza para receber preocupações, além de uma linha direta de denúncias?
- **Como os líderes da sua organização** promovem uma cultura de "speak up", ou "fale algo se identificar algo estranho?
- **Que treinamento sua organização oferece** sobre seu código de conduta e para promover a sua cultura de transparência e ética?
- **Você revisa e atualiza regularmente** seu código de conduta?
- **Quais políticas, procedimentos e controles** sua organização utiliza para impulsionar a capacidade de resposta às preocupações e responsabilidades?
- **Como sua organização mede** a eficácia de seu canal de denúncias?
- **Com que frequência sua organização testa** seu canal de denúncias?

Mitigação de Riscos e Resposta a Incidentes

- **Sua organização** possui um processo de resposta a incidentes?
- **Você tem controles** para garantir que os ativos não sejam adquiridos, utilizados ou alienados para atos ou ocultação de má conduta?
- **Você avaliou** como a cultura corporativa e o ambiente de controle impactaram a ocorrência e detecção do incidente ou má conduta?
- **Você comunicou** políticas, normas e procedimentos visíveis e claros em toda a organização?
- **Suas políticas** são comunicadas de forma adequada e eficaz a terceiros estratégicos, como parceiros de joint venture, representantes, fornecedores e clientes?
- **Você avalia regularmente** como os problemas de informação e comunicação podem impactar a ocorrência e detecção da má conduta?
- **O processo previu** a adoção de medidas para remediar o dano e evitar má conduta futura? A organização tomou essas medidas?

Entre em contato conosco no Brasil

Snežana Gebauer
Partner
sgebauer@stoneturn.com

Patrícia Latorre
Partner
platorre@stoneturn.com

Ian Cook
Managing Director
icook@stoneturn.com

Carlos Flávio Lopes
Managing Director
clopes@stoneturn.com

Camila Rombaldi
Managing Director
crombaldi@stoneturn.com

Contribuiram na elaboração deste material

David Burroughs **Joshua Dennis** **Nathan Fisher** **Daron Hartvigsen**

David Holley **Sarah Keeling** **Richard Mackintosh** **Mike Roos**

Luke Tenery **Brad Wilson**

Agradecimentos especiais a Tracey Groves, Ray Manna e Emilia Drozda

Leaving no stone unturned.

A StoneTurn é uma empresa global de consultoria que auxilia empresas, seus advogados e agências governamentais em questões regulatórias, de risco e compliance, investigações e disputas comerciais. Atendemos a nossos clientes a partir de 15 escritórios distribuídos em 5 continentes.

StoneTurn.com

StoneTurn