OLIVER WYMAN

A CRESCENTE AMEAÇA QUE VEM DE DENTRO

UMA ABORDAGEM PROATIVA E DIRECIONADA PARA GERENCIAR *INSIDER RISK*

AUTORES
Paul Mee
Rico Brandenburg
Matthew Gruber
James Cummings

MARSH GUY CARPENTER MERCER OLIVER WYMAN

MARSH & McLENNAN COMPANIES

INTRODUÇÃO

A ameaça de *insiders* representa uma parcela crescente da exposição geral ao risco cibernético de uma organização. Um número significativo de executivos é vítima de equívocos comuns no que se refere a *insider risk* e, portanto, normalmente não acredita que os próprios funcionários de sua organização representem uma ameaça considerável. Mesmo aqueles que acreditam, acham que é um desafio fazer progressos significativos, já que isso requer lidar com uma série de questões complexas jurídicas e de RH. Como resultado, muitas organizações investiram pouco nessa área.

A aplicação de tecnologia de prevenção de perda de dados, *software* de monitoramento ou ferramentas de vigilância de *compliance* não é suficiente. As organizações precisam escalar seus esforços e defesas de maneira adequada para identificar, detectar e mitigar ameaças antes que elas se materializem ou causem danos. As organizações líderes nessa área:

- Apresentam nível adequado de engajamento *"top-down"*,
- Utilizam priorização baseada em risco sobre o que monitorar e proteger e, mais importante,
- Implementaram arranjos de processos em conjunto com papéis e responsabilidades claros e testados para permitir a resposta correta quando um comportamento incomum é identificado.

Dada a crescente ameaça de *insiders*, é crucial que as organizações desenvolvam um programa eficaz para esse tipo de risco. O caminho para o sucesso é começar pequeno, com foco nas áreas de maior risco, e começar agora, porque as organizações simplesmente não podem continuar ignorando-a.

Insider

Insiders geralmente se referem a pessoas (funcionários, ex-funcionários, contratados, parceiros de negócios) que têm ou tiveram acesso autorizado aos dados, sistemas de informações ou instalações da organização. Seus atos intencionais ou mesmo não intencionais (isto é, negligência, descuido ou credenciais comprometidas) podem representar uma ameaça significativa para a organização. A ameaça de *insiders* pode assumir muitas formas diferentes, incluindo destruição e manipulação de ativos organizacionais (digitais ou físicos); espionagem; fraude; *insider trading*; e roubo de propriedade intelectual, segredos comerciais ou informações pessoais.

A AMEAÇA É REAL

Em 2018, dos 5 bilhões de registros roubados ou comprometidos, cerca de 2 bilhões foram resultado de circunstâncias internas.[1]

A ameaça de *insiders* é um dos maiores riscos de segurança que as organizações enfrentam. Normalmente, um *insider* utiliza suas credenciais (ou de outro funcionário) para obter acesso aos ativos críticos de uma determinada organização. Muitas organizações são desafiadas a detectar atos internos desonestos, frequentemente devido às limitações de controles de acesso e da capacidade de detectar atividades incomuns quando alguém já está dentro de sua rede. As funções de segurança tradicionalmente investiram muito mais no combate às ameaças externas ("proteger o perímetro") do que no combate aos riscos gerados por funcionários, contratados ou parceiros de negócios.

No entanto, as organizações estão "acordando" para o fato de que a ameaça de *insiders* pode causar danos consideráveis à sua resiliência operacional, situação financeira e reputação. Diversas indústrias, reguladores, agências governamentais e grupos sinalizaram que as organizações precisam levar a ameaça de *insiders* a sério (por exemplo, a regulação de segurança cibernética do New York State Department of Financial Services (NYDFS), National Infrastructure Advisory Council (NIAC), National Insider Threat Task Force (NITTF), Department of Energy (DoE), International Air Transport Association (IATA)).

Cerca de 75% das empresas acreditam ter controles apropriados para mitigar ameaças de *insiders* –, porém mais de 50% delas tiveram um ataque interno confirmado nos últimos 12 meses.[2]

Como os *insiders* geralmente estão familiarizados com a organização e tipicamente tem as "chaves do castelo", eles podem identificar com mais facilidade onde a organização está exposta e estão bem posicionados para explorar vulnerabilidades ou normas culturais, por exemplo, acesso baseado em confiança. A Figura 1 fornece um exemplo de como um *insider* pode se aproveitar da função de analytics em uma instituição financeira. O exemplo demonstra que um *insider* pode executar atividades que por si só podem não ser consideradas suspeitas. Mas ao se observar a série de atividades a real intenção maliciosa é revelada – e levanta-se a questão: "Por que esse padrão de comportamento não foi detectado?"

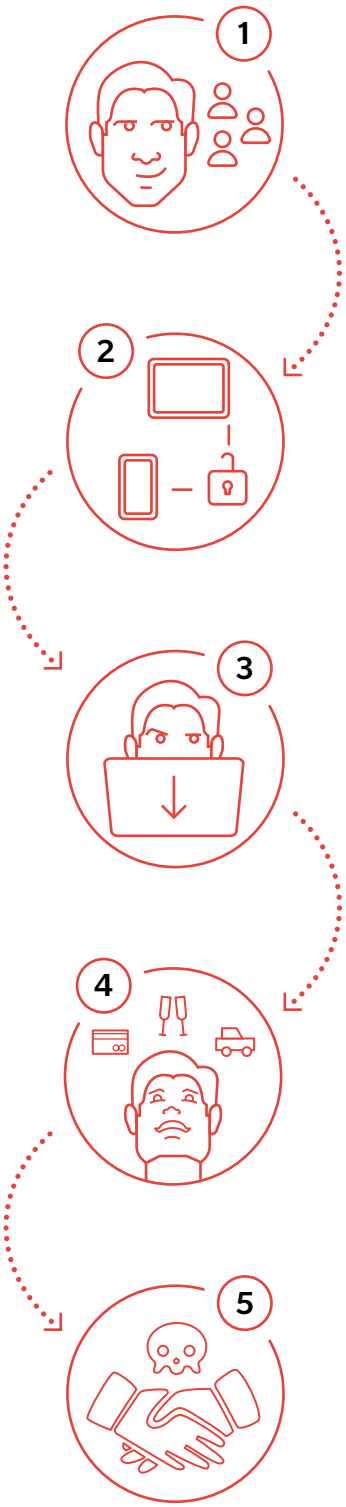
1. Segurança Baseada em Risco, Inc: Relatório "Data Breach QuickView, mid-year 2018 Data Breach Trends" ". Inclui circunstâncias maliciosas e acidentais"

2.Crowd Research Partners: 2018 Insider Threat Report

Figura 1: Mecânica de um evento causado por um *insider* (ilustrativo)

UMA SÉRIE DE ATIVIDADES SUSPEITAS

pelo talentoso Sr. Regal



- Por meio de uma transferência interna, Adam Regal se junta à equipe de análise de marketing da divisão de *"Wealth"*
- Ele está animado com o potencial de estar associado a um estilo de vida luxuoso
- Ele tem um interesse particular em clientes de alta renda (HNW)

- Adam procura os meios para obter acesso a dados de clientes (p. ex. Informação pessoalmente identificável)
- Quando ele percebe que o chefe de seu chefe está muito ocupado, Adam pede que ele aprove o acesso para algumas "novas campanhas importantes"
- Adam obtém amplo acesso privilegiado

- Adam desenvolve um conjunto de consultas para coletar dados sobre os clientes mais valiosos
- Tarde da noite, ele executa *scripts* para extrair os dados de clientes e faz o *upload* das bases (com cerca de 10 mil registros cada) em um site de compartilhamento de arquivos pouco conhecido

- O estilo de vida luxuoso apesar da renda limitada faz com que Adam tente explorar meios para monetizar os dados de clientes HNW que ele continua a acumular
- Ele aborda vários potenciais compradores, tanto de serviços financeiros quanto de outras indústrias
- Sua performance é prejudicada na medida em que ele se concentra em monetizar os dados

- Adam entra em contato com grupos criminosos pela *"Dark Web"*
- Adam compartilha os dados e recebe o pagamento combinado
- Ele recebe um pen drive para fazer mais *downloads* de dados que, sem ele saber, tem *malware* que permite o acesso remoto não detectado por pessoas de fora

Apesar do consenso crescente de que *insiders* maliciosos representam uma ameaça considerável com consequências potencialmente graves, muitas organizações permanecem negando-a. Elas são vítimas de mitos geralmente aceitos que as fazem acreditar que "isso não vai acontecer conosco" (Figura 2).

Mais de 30% das empresas consideram-se pouco ou nada vulneráveis a ameaças de *insiders*.[3]

A ameaça não é apenas difusiva, mas também é difícil de ser detectada. Frequentemente, atos maliciosos perpetrados por pessoas de dentro da empresa se misturam a comportamentos cotidianos e contornam os controles organizacionais. Embora *insiders* mal-intencionados muitas vezes demonstrem padrões pessoais comuns, muitos desses gatilhos comportamentais são dispersos/ineficientes e não resultam isoladamente em um alerta. Se vistos coletivamente esses comportamentos poderiam destacar a má intenção, mas tipicamente as organizações apenas agregam esses comportamentos após a ocorrência de um incidente, dos danos terem sido causados e do culpado ter sido identificado.

Convidamos os Conselhos e executivos a pensarem cuidadosamente sobre o perfil de risco e o ambiente de controle de suas empresas antes de se considerarem seguros. Em última análise, é necessário apenas uma pessoa com acesso às informações, sistemas ou instalações mais sensíveis e críticas da organização para realizar um ataque que pode causar danos permanentes às operações comerciais, à reputação e à situação regulatória.

Só uma pessoa é necessária para realizar um ataque que pode causar danos permanentes.

Padrões pessoais comuns

Declínios no desempenho, insatisfação com a organização, uso intenso de dispositivos pessoais no trabalho, ampla comunicação com contatos externos, atividade em horários incomuns, tentativas de obter acesso a ativos restritos (digitais ou físicos) e dificuldades financeiras foram observados em *insiders* maliciosos. As empresas também estão cada vez mais preocupadas com os trabalhadores que adotam posições políticas ou sociais mais extremas que poderiam levá-los a realizar atos maliciosos, o que pode ser evidente em suas mídias sociais e histórico de navegação na Internet.

3. Crowd Research Partners: 2018 Insider Threat Report

Figura 2: Caçadores de mitos
Equívocos comuns sobre ameaças de *insiders*

MITO	VERDADE
UMA BOA CULTURA EMPRESARIAL É SUFICIENTE PARA PROTEGER CONTRA *INSIDERS*	Uma boa cultura empresarial reduz a probabilidade de empregados insatisfeitos. Mas a motivação de *insiders* mal-intencionados pode ser impulsionada por uma variedade de fatores não relacionados à cultura da empresa, por exemplo, ganho financeiro, ideologia, desejo de reconhecimento. Mais de 50 por cento das empresas confirmam ataques internos nos últimos 12 meses.[4]
A AMEAÇA DE *INSIDERS* VEM DE FUNCIONÁRIOS TEMPORÁRIOS/ TERCEIRIZADOS	Os funcionários permanentes geralmente ficam numa empresa por mais tempo e acumulam mais acesso, de modo que representam uma ameaça maior. 56 por cento das empresas identificaram os funcionários regulares como o maior risco de segurança para as organizações.[4]
O *INSIDER RISK* É MITIGADO POR MEIO DO AMBIENTE DE CONTROLE GERAL	Os controles projetados para outros fins podem não ser tão eficazes contra *insiders* (por exemplo, exigir que as pessoas tenham credenciais válidas para entrar em um prédio ou fazer login), mas podem ser aproveitados em um programa eficiente.
ATIVIDADES MALICIOSAS INTERNAS PODEM SER IDENTIFICADAS IMEDIATAMENTE	Muitas organizações têm um monitoramento baseado em regras que detecta atividades internas básicas (por exemplo, um funcionário enviando por e-mail arquivos grandes para seu endereço pessoal). Mas poucas organizações detectam atividades internas mais sofisticadas (por exemplo, explorando o acesso que eles por direito tem, enviando informações confidenciais no corpo de um e-mail para um endereço aparentemente legítimo). Em média, as organizações levam 72 dias para conter um incidente interno, e apenas 16 por cento desses incidentes são resolvidos em menos de 30 dias.[5]
PREVENÇÃO DE PERDA DE DADOS (DLP) É UM PROGRAMA EFICAZ PARA COMBATER *INSIDER RISK*	O DLP é um componente de, mas não o mesmo que, um programa para combater *insider risk*. O DLP pode ajudar a evitar o roubo de dados por um *insider* mas fornece pouca proteção contra outros atos maliciosos (por exemplo, destruição de ativos, fraude).
A AMEAÇA DE *INSIDERS* É UM PROBLEMA APENAS PARA INDÚSTRIAS ESTRATÉGICAS	Muitos dos eventos de maior destaque aconteceram em "indústrias estratégicas" com inovação ou P&D de ponta, capacidade de defesa nacional ou dados altamente valiosos (por exemplo, registros médicos). No entanto, empresas de todos os setores[5] e todos os tipos de órgãos governamentais tiveram eventos relevantes causados por um *insider*.
A FUNÇÃO DE RECRUTAMENTO TEM UM BOM PROCESSO PARA FILTRAR FUNCIONÁRIOS POTENCIALMENTE MAL-INTENCIONADOS	As pessoas não precisam ter intenções maliciosas desde o início. Mudanças nas circunstâncias pessoais ou econômicas podem criar incentivos para atividades maliciosas ao longo do tempo.

4. Crowd Research Partners: 2018 Insider Threat Report
5. Ponemon Institute 2018 Cost of Insider Threats: Global. Inclui insiders acidentais, insiders maliciosos e ladrões de credenciais

SEU PROGRAMA DE *INSIDER RISK* PRECISA SER REDEFINIDO?

Estabelecer e operacionalizar um programa eficaz de *insider risk* não é fácil. Em comparação com atividades de defesa cibernética mais tradicionais, lidar com ameaças de *insiders* exige uma coordenação significativamente maior, afeta mais a privacidade e questões éticas relacionadas e tem mais potencial para causar danos permanentes à cultura e à reputação de uma empresa, se não for feito corretamente.

Em nossa experiência, muitas organizações acreditam que estão efetivamente enfrentando a ameaça, mas são vítimas de armadilhas comuns que prejudicam seus esforços. Se a sua organização demonstrar um ou mais sintomas relacionados a essas armadilhas (Figura 3), seu programa de *insider risk* poderá precisar de uma "reinicialização forçada".

Estudo de caso: Um programa que passou dos limites

Recentemente, a imprensa destacou o caso de uma grande empresa de serviços financeiros que usou uma empresa de mineração de dados para seu programa de *insider risk*. A coleta de dados era ilimitada e havia poucas restrições sobre como o programa de *insider risk* poderia usar essa informação. No fim, o experimento entrou em colapso quando os executivos do banco perceberam que o grau de vigilância era equivalente à espionagem invasiva, não pertencia a um ambiente corporativo e estava prejudicando a cultura da empresa. Esse caso ilustra algumas das consequências potencialmente graves de um programa de *insider risk* que deu errado, que pode incluir também maior índice de saída de funcionários, dificuldades para atrair talentos, desafios legais e danos à reputação.

Figura 3: Armadilhas comuns na abordagem eficaz da ameaça de *insiders*

ARMADILHA 1: NÃO OBTER COMPROMISSO ORGANIZACIONAL

- ☐ Executivos sêniores são céticos quanto ao perigo representado por *insiders*
- ☐ O Conselho e a diretoria não forneceram *inputs* ao programa

ARMADILHA 2: NEGLIGENCIAR O BÁSICO

- ☐ As "joias da coroa" e áreas de alto risco não foram identificadas
- ☐ Treinamento contra ameaças de *insiders* ausente ou falho
- ☐ O gerenciamento de identidade e acesso é subdesenvolvido ou variável
- ☐ Triagem/avaliação de funcionários limitada ou inexistente (geralmente nenhuma após o recrutamento inicial)

ARMADILHA 3: TER UM PROGRAMA APENAS NO NOME

- ☐ Não há manuais (*playbooks*) para responder a possíveis ameaças de *insiders*
- ☐ Articulação limitada, em silos ou fraca dos componentes do programa e de como medir o sucesso
- ☐ Processos de resposta e escalada não são detalhados e testados

ARMADILHA 4: TER INICIATIVAS, MAS NENHUM PROGRAMA HOLÍSTICO

- ☐ Os recursos e processos existentes não são efetivamente aproveitados (por exemplo, programa DLP, monitoramento de *compliance*, segurança física)
- ☐ Funções críticas (RH, Privacidade, Jurídico e Gerência) não estão consistentemente coordenadas e em comunicação com relação a *insiders risks*
- ☐ Nenhum executivo individual ou grupo com autoridade para decidir iniciar uma investigação interna

ARMADILHA 5: "MORDER MAIS DO QUE VOCÊ PODE MASTIGAR"

- ☐ O programa não é customizável e tenta monitorar toda a organização
- ☐ Não há recursos suficientes para cobrir efetivamente o escopo e processos relacionados a *insiders*

ARMADILHA 6: IGNORAR AS RAMIFICAÇÕES CULTURAIS E PREOCUPAÇÕES COM A PRIVACIDADE

- ☐ Pouca consideração sobre como o programa pode existir e se adaptar a diferentes regimes nacionais, regulatórios e societários/culturais
- ☐ Principais funções como RH, *Compliance*, Jurídico e Privacidade não envolvidas no desenho do programa
- ☐ O programa é percebido como um "Big Brother", por monitorar excessivamente o comportamento e as comunicações dos funcionários

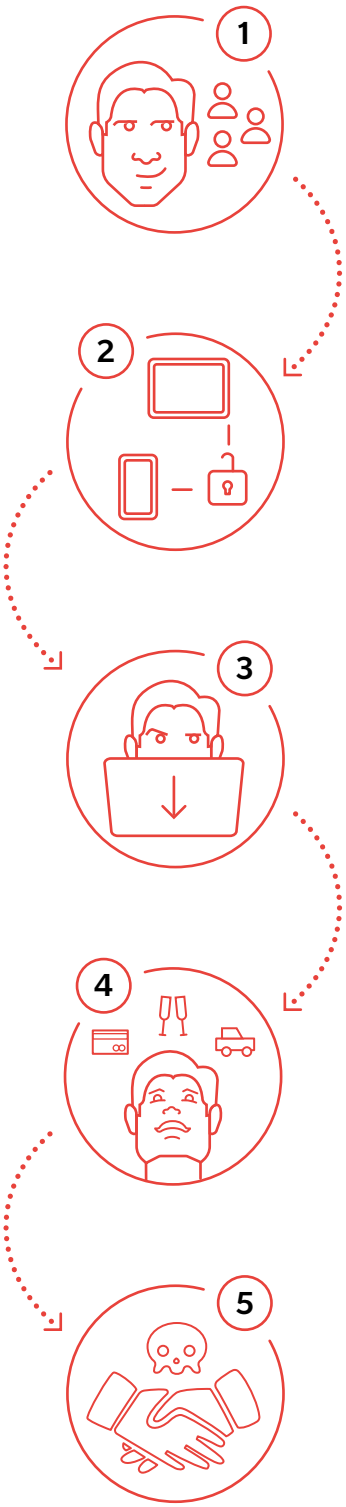
ADOTANDO UMA ABORDAGEM PRÁTICA PARA *INSIDER RISKS*

Vamos revisitar o exemplo do Sr. Regal, funcionário da divisão de *"Wealth"* de um banco, que conseguiu vender com sucesso informações confidenciais de clientes na *dark web*. A Figura 4 descreve como um programa eficaz de *insider risk* poderia ter detectado a ameaça e impedido o Sr. Regal de executar seu ataque. O conjunto de controles de detecção e proteção e recursos de monitoramento permitem que a organização identifique indivíduos que apresentam maior risco para a organização e introduza monitoramento adicional para garantir que atividades mal-intencionadas possam ser identificadas e interrompidas.

Figura 4: Mecânica de um evento causado por um *insider* – revisitado (ilustrativo)

UMA SÉRIE DE ATIVIDADES SUSPEITAS

pelo talentoso Sr. Regal



- Por meio de uma transferência interna, Adam Regal se junta à equipe de análise de marketing da divisão de *"Wealth"*
- Ele está animado com o potencial de estar associado a um estilo de vida luxuoso
- Ele tem um interesse particular em clientes de alta renda (HNW)

⚠ Verificações financeiras/de histórico realizadas em Adam devido à transferência indicam preocupação com base em seu histórico de crédito anterior e alta dívida.

- Adam procura os meios para obter acesso a dados de clientes (p. ex. Informação pessoalmente identificável)
- Quando ele percebe que o chefe de seu chefe está muito ocupado, Adam pede que ele aprove o acesso para algumas "novas campanhas importantes"
- Adam obtém amplo acesso privilegiado

⚠ Aumento de privilégios eleva a classificação de risco de Adam para "alta". Adam é colocado em uma *"watch list"* para ser monitorado mais de perto.

- Adam desenvolve um conjunto de consultas para coletar dados sobre os clientes mais valiosos
- Tarde da noite, ele executa *scripts* para extrair os dados de clientes e faz o *upload* das bases (com cerca de 10 mil registros cada) em um site de compartilhamento de arquivos pouco conhecido

⚠ Um alerta é gerado porque a análise comportamental dos membros da *"watch list"* indica que é incomum que Adam baixe dados confidenciais de clientes tarde da noite.

- O estilo de vida luxuoso apesar da renda limitada faz com que Adam tente explorar meios para monetizar os dados de clientes HNW que ele continua a acumular
- Ele aborda vários potenciais compradores, tanto de serviços financeiros quanto de outras indústrias
- Sua performance é prejudicada na medida em que ele se concentra em monetizar os dados

⚠ Um colega percebe que o Sr. Regal está agindo de maneira estranha e alerta anonimamente o RH. Seguindo os procedimentos testados, o RH informa o programa de *insider risk* para iniciar um monitoramento reforçado.

- Adam entra em contato com grupos criminosos pela *"Dark Web"*
- Adam compartilha os dados e recebe o pagamento combinado
- Ele recebe um pen drive para fazer mais *downloads* de dados que, sem ele saber, tem *malware* que permite o acesso remoto não detectado por pessoas de fora

⚠ A análise da *"Dark Web"* revela que houve uma violação de dados antes de a violação tornar-se pública

Um programa efetivo de *insider risk* é projetado para identificar possíveis ameaças e impedir a realização de atos maliciosos por *insiders*. Mas um programa é mais do que apenas um conjunto de controles. A Figura 5 descreve os cinco elementos principais para um programa eficaz:

- **Governança e organização:** Clara articulação do modelo de supervisão e operacional.
- **Compartilhamento de informações:** Um modelo eficaz multi-áreas para endereçar preocupações legais, éticas, culturais e de privacidade e entender o que é necessário para "chegar ao sim".
- **Execução e gerenciamento do programa:** Processos e controles que cobrem o ciclo de vida de ponta a ponta do gerenciamento de *insider risk* de acordo com o apetite de risco da organização.
- **Dados, tecnologia e ferramentas:** Recursos básicos que suportam o gerenciamento de *insider risk*.
- **Melhoria contínua:** Mecanismos para integrar aprendizados de eventos passados e evoluir o programa de acordo com a mudança de exposição ao risco.

Conforme destacado na Figura 5, um programa eficaz de *insider risk* não apenas reduz o risco associado a *insiders*, mas também proporciona importantes benefícios colaterais para a organização. Por exemplo, coletar dados de identificação de entrada/saída para identificar atividades suspeitas pode ajudar nos estudos de disponibilidade do local de trabalho ou na segurança durante uma emergência no prédio.

Figura 5: Framework Oliver Wyman do programa de *insider risk*[6]

6. Reflete estruturas e práticas recomendadas em toda a indústria, incluindo o NITTF Insider Threat Maturity Framework.

A maioria das organizações que apresentam algumas das armadilhas destacadas na Figura 3 precisarão redefinir de alguma forma o seu programa de *insider risk*. Isso significa reorientar os esforços da organização em casos de uso práticos que suportam o desenvolvimento de um programa de *insider risk* voltado para dados, focado em riscos e proativo. Com base em nossa experiência, identificamos práticas importantes que ajudarão a tornar um programa de *insider risk* o mais eficaz possível.

GOVERNANÇA E ORGANIZAÇÃO

Defina o "programa de *insider risk*". Defina e documente um "programa de *insider risk*" com um mandato claro e visão que inclua representantes de diferentes funções-chave da organização (por exemplo, Segurança da Informação, Segurança Física, RH, Privacidade, Jurídico, *Compliance*). Todos os envolvidos no programa devem ter papéis e responsabilidades definidos. Independentemente de a organização criar uma equipe dedicada para ameaças de *insiders* ou não, um grupo específico deve ser responsável por formular políticas relacionadas à ameaça de *insiders* e operacionalizar o programa.

Engaje a liderança sênior. Garanta que a liderança executiva ofereça supervisão e dê a direção do programa. Uma empresa global descobriu que a apresentação de um pequeno número de casos de uso ilustrativos à diretoria e ao Conselho ajudou a liderança a fornecer orientações claras sobre a tolerância para rastrear, registrar e analisar o comportamento dos seus funcionáros.

Integre os esforços existentes. Identifique outros esforços existentes relacionados e integre-os, seja colocando-os diretamente no programa de *insider risk* ou emponderando o programa de forma a fornecer requisitos a outros esforços. Por exemplo, o programa de monitoramento de *compliance* pode continuar sendo de responsabilidade da área de *Compliance*, mas deve verificar casos de uso adicionais ou encaminhar certos incidentes para o programa de *insider risk*.

COMPARTILHAMENTO DE INFORMAÇÕES

Monitore, meça e comunique o sucesso. Defina o que significa sucesso e desenvolva um conjunto de métricas para fornecer informações sobre a eficácia do programa ao longo do tempo. As organizações líderes compilam essas métricas em um *dashboard* executivo que é atualizado regularmente, com detalhes que auxiliam a liderança do programa. As métricas abrangem medidas tradicionais de sucesso, como resultados de casos de ameaças de *insiders* e mais medidas não-tradicionais, como o modo de coordenação de diferentes funções ou o conhecimento de ameaça de *insiders*.

Superar barreiras ao compartilhamento de informações. Fornecer ao programa de *insider risk* acesso às informações necessárias para identificar e investigar o comportamento suspeito geralmente envolve a superação de várias barreiras legais, éticas, culturais e de privacidade. As organizações devem definir diretrizes claras sobre as informações que podem ser coletadas/compartilhadas e manter o anonimato até que haja certeza suficiente para desmascarar o indivíduo.

EXECUÇÃO E GERENCIAMENTO DO PROGRAMA

Foque o programa. Entenda as áreas de maior risco da organização ("joias da coroa"), identifique os potenciais *insiders* (pessoas com acesso) e crie um conjunto de casos de uso para informar a prevenção e o monitoramento com base em eventos históricos e motivações prováveis dos agentes. Uma organização embarcou em um esforço corporativo para identificar os sistemas críticos que expunham a organização ao maior dano se um *insider* mal-intencionado tivesse acesso.

Não negligencie a prevenção. Concentre-se na prevenção proativa ou minimização da ameaça de *insiders*, em vez de simplesmente detectar funcionários desonestos. Algumas organizações modificam ativamente papéis através da população de alto risco para limitar o dano potencial que um funcionário poderia ocasionar. As organizações também devem aumentar a conscientização sobre ameaças de *insiders* e incentivar as pessoas a se manifestarem caso observem um comportamento incomum.

Documente rigorosamente e teste processos e *playbooks*. Documente um conjunto claro de etapas e critérios para determinar se uma investigação ou ação adicional é justificada quando uma possível ameaça ou ato mal-intencionado for detectado. As consequências potenciais de atos mal-intencionados (por exemplo, reduções na remuneração, rescisão, mudança de privilégios de acesso) devem ser documentadas e devem existir padrões para orientar a gerência sobre quando empregá-los. Os processos devem ser detalhados e testados, mesmo fora do contexto de resposta da ameaça de *insiders*. Por exemplo, a área de Segurança e o RH devem testar regularmente os processos para remover o acesso de funcionários que foram desligados (voluntariamente ou não).

DADOS, TECNOLOGIA E FERRAMENTAS

Ingerir dados relevantes. Obtenha acesso a uma ampla variedade de dados que possam esclarecer comportamentos suspeitos. Os dados podem ser internos (por exemplo, crachás, horários de login), o resultado de verificações financeiras/de histórico periódicas ou até mesmo externas (por exemplo, mídias sociais), conforme permitido por lei.

Alavancar soluções tecnológicas. Empregue uma plataforma de *analytics* para ingerir os diversos dados coletados e identificar comportamentos suspeitos com base em casos de uso definidos. A plataforma deve priorizar os alertas para investigação pelo pessoal relevante. Use um sistema de gerenciamento de casos para gerir alertas e investigações e garantir que apenas os indivíduos certos possam obter acesso a informações confidenciais relacionadas a ameaças de *insiders*.

MELHORIA CONTÍNUA

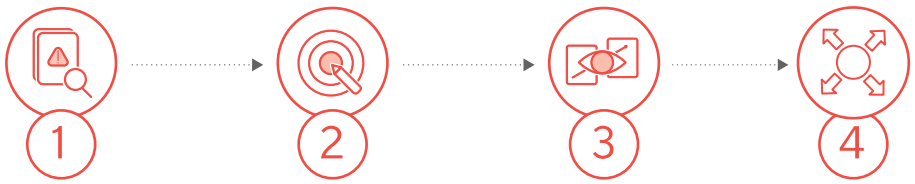
Teste a eficácia do programa. Faça com que os funcionários imitem *insiders* em um formato de *"red teaming"* para verificar se os mecanismos de detecção identificariam a ameaça. Conduza atividades de *threat hunting*, concentrando-se em ativos críticos e partindo da hipótese de que um *insider* tenha comprometido esses ativos de alguma forma. Os membros da equipe devem ser responsáveis por capturar e catalogar os aprendizados dessas atividades e sugerir aprimoramentos correspondentes ao programa.

COMECE PEQUENO E FOCADO

A implementação de um programa eficaz de *insider risk* requer um desenho adaptado à cultura, processos e riscos específicos da organização. A Figura 6 descreve a abordagem para projetar e implementar um programa de *insider risk* bem-sucedido. Ele começa com a identificação da exposição ao risco e seu impacto no negócio. Uma vez identificadas as "joias da coroa" e os *insider risks* associados, um piloto pode ser desenhado para mitigar esses riscos. É importante começar pequeno e concentrar-se em um subgrupo de funcionários de alto risco claramente definido. Mais importante ainda, o piloto precisa ajudar os *stakeholders* do programa a entender o que é necessário para "chegar ao sim" (saber quando agir com uma pessoa suspeita de ser um *insider* malicioso). Depois que os aprendizados do piloto forem comunicados aos executivos e incorporados ao desenho do programa, a organização poderá decidir como aprimorá-lo ainda mais (Figura 6).

Projetar e implementar um programa eficaz de *insider risk* é crucial para qualquer organização. Com ameaças de *insiders* cada vez mais proeminentes, as organizações não podem simplesmente ignorá-las. Acertar no programa trará benefícios claros, enquanto que atrasos podem custar caro. Adote uma abordagem proativa ao gerenciamento de *insider risk* - comece pequeno, mas comece agora.

Figura 6: Desenho e implementação bem-sucedidos de um programa de *insider risk*



Identificação e avaliação de riscos

- Classificação de "joias da coroa"
- Identificação de vetores internos de ameaça
- Desenvolvimento de cenários de risco orientados a negócios

Projeto piloto e execução

- Definição dos principais fatores de risco e desenvolvimento de uma classificação de risco dos funcionários
- Identificação de um subgrupo de funcionários de alto risco como "população piloto"
- Criação de uma governança interfuncional eficaz e eficiente para impulsionar o engajamento
- Design de casos de uso em torno da "população-alvo"
- Desenvolvimento de monitoramento e relatórios

Refinamento e expansão de casos de uso

- Refinamento de casos de uso e classificação de risco dos funcionários com base nos resultados do piloto
- Identificação de grupos adicionais de indivíduos de alto risco
- Integração de fontes de dados
- Desenvolvimento de casos de uso adicionais

Lançamento em áreas de alto risco

- Planejamento de implementação e avaliação de impacto
- Plano de comunicação
- Desenvolvimento de processos de manutenção e melhoria contínua

A Oliver Wyman é uma líder global na consultoria de gestão que combina um profundo conhecimento da indústria com expertise especializada em estratégia, operações, gestão de risco e transformação organizacional.

Para mais informações, por favor, contate o departamento de marketing pelo e-mail info-FS@oliverwyman.com ou pelo telefone de um dos seguintes locais:

AMERICAS
+1 212 541 8100

EMEA
+44 20 7333 8333

ASIA PACIFIC
+65 6510 9700

Paul Mee
Sócio nas práticas de Digital e Serviços Financeiros e líder da plataforma de Cyber
paul.mee@oliverwyman.com

Rico Brandenburg
Sócio nas práticas de Risco & Políticas Públicas e Digital
rico.brandenburg@oliverwyman.com

Matthew Gruber
Gerente de Projeto nas práticas de Risco & Políticas Públicas e Digital
matthew.gruber@oliverwyman.com

James Cummings
Senior Advisor em gestão de risco cibernético e defesas cibernéticas
James.Cummings@affiliate.oliverwyman.com

www.oliverwyman.com

OLIVER WYMAN