NOSSO TRABALHO. NOSSOS CASOS.

Uma coleção de insights e histórias de especialistas líderes no setor de gerenciamento de riscos abrangendo áreas-chave de risco organizacional.

LOWERS & ASSOCIATES
International Risk Mitigation Partners

PREFÁCIO

Toda corporação começa com um propósito. Por mais de 30 anos, a nossa tem assegurado que os clientes não tenham que comprometer sua segurança para entregar o deles. Nossa abordagem colaborativa tem ajudado empresas em todo o mundo a construir uma sensação de bem-estar que protege seu pessoal, marca e valores.

Neste momento, os empresários estão procurando estratégias úteis que forneçam um caminho a seguir. Nesta coleção de casos, compartilhamos dicas de segurança, insights exclusivos do setor e contas em primeira pessoa que ajudaram a refinar nosso propósito e que acreditamos que possam ser aplicados a qualquer indústria.

Esta coleção de histórias e insights abrange algumas das áreas mais comuns de gerenciamento de riscos que abrangemos. A verdade é que histórias do nosso trabalho poderiam encher muitos volumes. Por enquanto, espero que você encontre valor no que compartilhamos aqui e que isso lhe dê um vislumbre das maneiras que podemos ajudar sua organização a mitigar riscos e protege-la contra perdas.

Atenciosamente,

Mark Lowers

Mark Lowers
Presidente e CEO da Lowers & Associates

ÍNDICE

CONTRIBUIDORES

BRAD MOODY, CFI, CFE

Vice Presidente Executivo

JON D. GROUSSMAN, J.D.

VP Executivo –Divisão Consultoria

TOM DOLAN

Gerente de Sinistros e Pesquisas

DANIEL COOTES

Gerente de Operações e Atendimento ao Cliente

KRISTOPHER KEEFAUVER

Diretor para Clientes CIT e Segurança

CHRIS SOSNOSKI

Diretor de TI e SI

JOE LABROZZI

Diretor de Segurança

NEIL WATSON

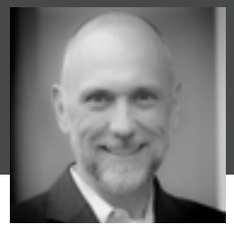
Diretor de Operações Globais

KEITH GRAY, CFE, CAMS

VP, Relações Institucionais

SEGREGAÇÃO DE FUNÇÕES

CONTRIBUIDOR CHAVE



BRAD MOODY, CFI, CFE
Vice Presidente Executivo

A FRAUDE ELETRÔNICA COMEÇA E TERMINA COM PESSOAS

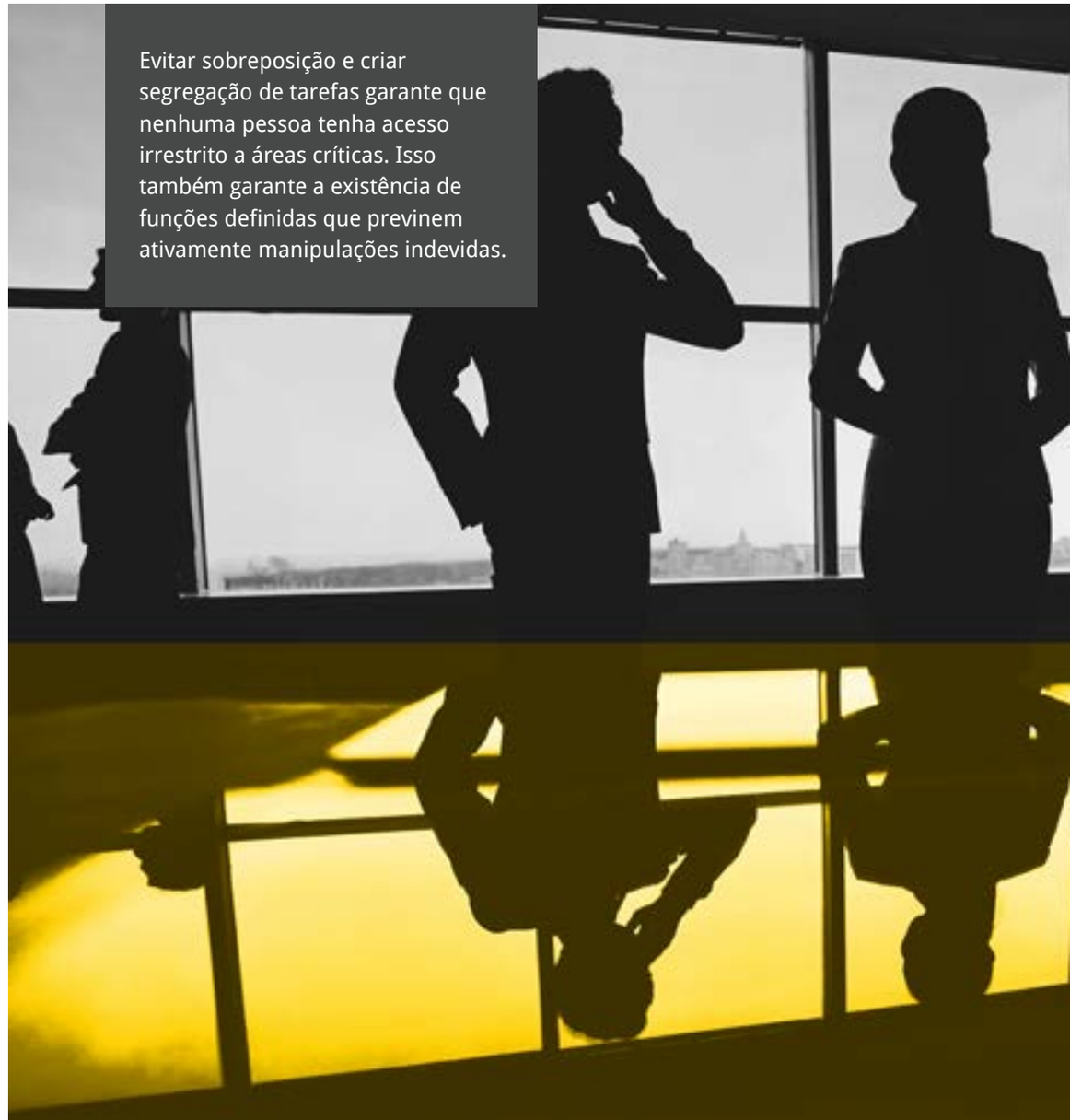
É difícil imaginar que, em qualquer dia, mais de 3 trilhões de dólares se movam via transferência eletrônica. As instituições financeiras fazem com que essas transações B2B aconteçam perfeitamente em escala global, e muitas vezes tomamos como certa as instruções muito simples necessárias (e aceitas) entre empresas que tornam possível transações únicas de milhões de dólares. Como as organizações realizam essas transações quase exclusivamente online, a Internet das Coisas (IOT) tem uma oportunidade inerente ao redirecionamento malicioso quando os funcionários da empresa se tornam complacentes com instruções de transferência eletrônica rotineiras.

As organizações responsáveis seguem práticas robustas, documentadas e aceitas em um ambiente que envolve processos. A cultura de qualquer organização de alta confiabilidade permite a intervenção dos funcionários e controles sistemáticos para evitar tentativas de fraude. Pode parecer que esses processos sejam tediosos e repetitivos, no entanto, no final das contas, ações humanas permitem que a fraude exista.

Desde 2016, estima-se que mais de US$ 26 bilhões em perdas por fraudes vieram de transferências de fundos bancárias como resultado apenas de acordos comerciais feitos por e-mail. Com o recente evento de pandemia COVID-19, os fraudadores têm uma nova capacidade de explorar corporações, especialmente em áreas altamente impactadas. É importante que as organizações mantenham uma cultura de processo e tenham planos de contingência em vigor para permitir que as transferências continuem sendo efetuadas de forma perfeita.

LEIA O ARTIGO COMPLETO →

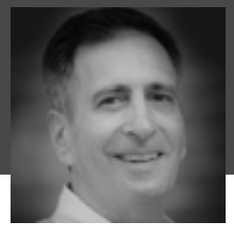
DICA DO ESPECIALISTA



Evitar sobreposição e criar segregação de tarefas garante que nenhuma pessoa tenha acesso irrestrito a áreas críticas. Isso também garante a existência de funções definidas que previnem ativamente manipulações indevidas.

CONTROLE DE ACCESSO

CONTRIBUIDOR CHAVE



JON D. GROUSSMAN, J.D.
VP Executivo – Divisão Consultoria

IGNORÂNCIA É FELICIDADE —ATÉ QUE A REALIDADE CHEGUE

À medida que as restrições do COVID-19 são lentamente aliviadas e as empresas em todo o mundo contemplam a reabertura, cada proprietário deve estar usando seu tempo agora para examinar como está a reabertura no “novo normal”. Para fornecer algumas orientações para aqueles que reavaliam suas medidas de segurança ou que estão especificamente focados na reabertura, apresentamos 10 ações que QUALQUER empresa pode tomar para minimizar riscos e eliminar o potencial de perda a qualquer momento.

1. Reavalie a alocação de recursos de segurança com base na necessidade e risco operacionais.

Se você tem um portfólio de negócios com várias localidades, deve-se considerar o ambiente de negócios específico, a natureza das ameaças, a existência de quaisquer circunstâncias incomuns e a capacidade das autoridades locais em responder.

2. Limite o número de pontos de entrada / saída para funcionários e visitantes.

Controle firmemente entrada e saída para otimizar a seguridade. Examine a viabilidade operacional antes da implementação.

3. Considere a área de recepção.

Se os seguranças forem funcionários da empresa, qual será o papel que eles desempenharão agora na recepção para auxiliar na aplicação de novas práticas?

4. Medidas e mecanismos de controle de acesso dependentes por impressão digital ou código de autorização exigem a implementação de novos protocolos de segurança.

Isso inclui software de gestão de visitantes e o uso de tablets para o processo de registro.

5. Coberturas por CFTV projetadas para manuseio de dinheiro ou identificação de roubos devem expandir os pontos focais além de apenas o enquadramento facial.

Dado o uso de máscaras faciais cada vez mais frequente para o futuro previsível, as câmeras devem cobrir a visualização de todo o corpo, incluindo sapatos (criminosos normalmente não largam seus sapatos após cometerem um roubo).

DICA DO ESPECIALISTA

Neste momento, o controle de acesso para funcionários e visitantes deve estar entre as prioridades. Ao limitar os pontos de entrada e saída, as empresas podem manter melhor as medidas de segurança implementadas durante a pandemia atual.

Antes da reabertura, as empresas devem considerar as implicações legais e de segurança dessas medidas; seja uma porta para uma pequena loja de bairro ou acesso a impressões digitais a um sofisticado edifício comercial, os detalhes importam.

LEIA TODAS AS 10 DICAS →

EMPLOYEE SCREENING

CONTRIBUIDOR CHAVE

TOM DOLAN
Gerente de Sinistros e Pesquisas

DUE DILIGENCE: SEU DIA DE SORTE?

A fraude está em toda parte, mas apenas uma pequena porção de due diligences básicas pode ajudar uma empresa a evitá-la ou a outros riscos desnecessários. Desde um penhorista de cidade pequena que perdeu seu negócio após contratar um amigo cujo passado criminoso só foi revelado após um roubo de seis dígitos, até uma corporação multinacional que perdeu milhões em pagamentos fraudulentos para um fornecedor de suprimentos obscuro vivendo muito além de seus meios, há inúmeras histórias demonstrando o alto preço pago por empresas que confiaram antes de verificar.

O que é due diligence?
A due diligence é um processo específico, mas flexível, realizado por especialistas qualificados em identificar e obter informações diversas para formar um quadro completo. No exemplo acima, a pesquisa teria incluído o histórico e os registros de negócios da empresa (por exemplo dos princípios, proprietários ou gestores-chave) e quaisquer afiliações reais ou percebidas, para citar alguns.

Por que as empresas precisam disso?
Novos funcionários ou novos parceiros podem moldar o futuro do seu negócio. Se é um treinador universitário, um membro do conselho ou fornecedor, toda a história importa e deve incluir:

- Investigação de personalidade
- Investimentos
- Fusões e Aquisições
- Levantamento patrimonial (para execução e recuperação de dívidas)
- Localização

O que mais eu deveria saber sobre due diligence?
É sempre importante entender com quem você está trabalhando para eliminar o potencial de fraude. Ao fazer sua due diligence, aqui estão algumas práticas recomendadas:

Acesso a registros públicos. A ficha criminal de um sujeito (ou a falta dela) é de grande importância, mas igualmente significativa pode ser o histórico de litígio ou falência. Mesmo questões aparentemente menores, como infrações de trânsito, podem ser indicativas, especialmente quando um sujeito já registrou dezenas.

História completa e abrangente. As investigações mais minuciosas podem revelar a verdade do que foi apresentada em um currículo ou MOU e o que pode ter sido deliberadamente omitido. Faça as perguntas que iluminam a resposta.

Verificação de ativos. Antes de entrar em qualquer acordo formal, compreenda e confirme uma potencial apreensão de recursos de um parceiro e revele quando as coisas não coincidam. Não subestime o poder da pressão no Triângulo de Fraude.

Revisão de mídias sociais. Apesar de sua prevalência, nem todos a usam sabiamente. Uma revisão de perfis pessoais e corporativos pode identificar alguns dos mais flagrantes “red flags”. Considere varreduras recorrentes para mitigar ou descobrir sua exposição.

LEIA O ARTIGO COMPLETO →

DICA DO ESPECIALISTA

O background check proativo pré-contratação é o primeiro passo importante para colocar as pessoas certas na equipe. Entretanto, um background checkindividual só garante a precisão no dia em que é processado. Já um background check recorrente –tanto para indivíduos quanto para potenciais parceiros de negócios –é igualmente essencial para garantir a segurança dos funcionários, clientes e do negócio em geral.

Seja um penhorista local ou uma corporação multinacional, a verificação deve sempresuperar a confiança cega no processo de due diligence.

INOVAÇÃO DE PROCESSOS

CONTRIBUIDOR CHAVE

DANIEL COOTES
Gerente de Operações e Atendimento ao Cliente

ADAPTAR & SUPERAR: O CASO DO LEVANTAMENTO VIRTUAL

Os melhores negócios estão agora fazendo duas coisas: (i) encontrar maneiras de permanecerem abertos e (ii) avaliando o futuro. O primeiro passo para conseguir isto é uma compreensão holística dos riscos do negócio. Isto é, pesquisando.

Para empresas que consideram um levantamento virtual, a equipe da Lowers & Associates compilou uma lista de insights e considerações que podem ser úteis em seu processo de aprendizagem:

- O principal benefício do levantamento virtual é que ele pode ser realizado a qualquer hora, em qualquer lugar. Sem viagens, a pesquisa virtual é uma das melhores maneiras das empresas que pensam para a frente controlarem os custos.
- Pesquisas virtuais são menos disruptivas para a organização e fornecem uma reviravolta mais rápida no relatório. Isso pode ser uma enorme vantagem para as organizações pressionadas por tempo ou com capacidade reduzida de pessoal.
- Sempre um exercício colaborativo e NUNCA o “menor dos dois males”, pesquisas virtuais podem muitas vezes fornecer insights mais profundos do que aqueles realizados pessoalmente (às vezes os donos de negócios se sentem mais à vontade com uma distância física entre si e o pesquisador).
- Os rápidos avanços tecnológicos vêm com uma curva de aprendizado. Os principais consultores de mitigação de riscos devem ser versados em um conjunto de aplicações tecnológicas para executar com sucesso uma pesquisa virtual.
- Informação é informação, certo? Nem tanto. Fazer as perguntas certas importa, saber analisar as respostas faz toda a diferença e consistência é crucial. Virtual ou não, os pesquisadores que revisam a documentação solicitada e/ou uma gravação audiovisual do levantamento devem ser capazes de entregar os mesmos resultados exatos.
- A consistência é fundamental tanto nos negócios quanto no levantamento. Os pesquisadores virtuais devem ser capazes de entregar responsabilidades a outro pesquisador se alguém adoecer ou ficar indisponível. O processo pode ser tanto uma flecha das corporações quanto seu calcanhar de Aquiles!
- O levantamento virtual deve incluir uma capacidade de executar:
  - Reuniões pré-pesquisa
  - Competência da equipe e entrevistas
  - Revisões das operações do dia-a-dia, segurança física do local, seguro, controles fiduciários, políticas & procedimentos, construção de cofres, crime e atividade ilegal (local e nacional)
  - Consulta de design de instalações
  - Reuniões de follow up

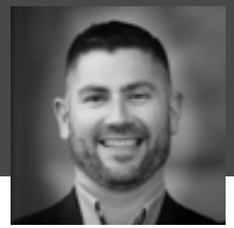
LEIA O ARTIGO COMPLETO →

DICA DO ESPECIALISTA

A inovação é o resultado do processo. Seja impulsionado por forças externas ou progressão natural, o lado positivo pode ser transformador para uma organização. Com o COVID exigindo que cada negócio se adapte, não existe uma cartilha oficial sobre a criação de um normal melhor –apenas um entendimento de que a maneira como as pessoas trabalham, compram, aprendem e interagem mudou fundamentalmente. Isso pode significar que o cozinheiro agora é agora também o caixa, o analista de dados recebe convidados à tarde, ou que o CEO embala a van às sextas-feiras. Seja qual for a inovação (ou eficiência), o processo deve incluir treinamento adequado para garantir a segurança de todos que executam uma nova responsabilidade, mesmo que seja temporariamente.

MANUSEIO DE VALORES

CONTRIBUIDOR CHAVE



KRISTOPHER KEEFAUVER
Diretor para Clientes CIT e Segurança

DINHEIRO: O REI BENEVOLENTE (DO CORAÇÃO DE CADA CRIMINOSO)

“Eu o conhecia há anos. Ele era parte da família. Como ele pode fazer isso comigo e meu negócio?

Esta é uma pergunta muito familiar depois que um funcionário antigo ou confiável é pego ou suspeito de roubar uma empresa. Então, o que acontece que faz tudo parecer tão errado?

Simplificando, o dinheiro é o grande atrativo –enquanto cada um de nós interpreta esta atração de maneira diferente, sua promessa gentil e visceral de liberdade ocasionalmente se torna irresistível demais para a natureza humana ignorar. Muitas empresas não estão cientes, ou pelo menos, não são capazes de identificar, contratar, educar e treinar consistentemente em torno deste fato. Em CIT (Cash in Transit / Transporte de Valores) e segurança, a ruptura acontece mais frequentemente em um ou mais dos “três P’s” (Política, Processo e Procedimento), mas certamente não é um fenômeno isolado. Estabelecimentos varejistas, instituições financeiras e muito mais lutam com isso.

DICA DO ESPECIALISTA

Seja uma instituição financeira, um estabelecimento de varejo ou uma empresa de CIT, a complacência pode ser uma ameaça real para futuras oportunidades quando se trata de lidar com dinheiro. Ao longo dos anos, descobrimos que baixos níveis de consciência sobre segurança frequentemente são a desculpa e desproporcionalmente minam as tentativas de construir uma cultura de complianceentre os funcionários.

Uma revisão independente dos procedimentos operacionais e de segurança pode ajudar a resolver conflitos e deficiências para criar um ambiente de trabalho mais seguro para todos.

Então, o que pode ser feito para proteger pessoas, marcas e lucros? Aqui estão algumas práticas recomendadas que podem ser aplicadas em qualquer negócio, seja ele grande ou pequeno. Revise suas políticas e processos internos e mantenha uma supervisão gerencial para garantir que os procedimentos estejam sendo cumpridos por política da empresa e que ninguém tenha privilégios de acesso a determinados ativos ou funções, incluindo:

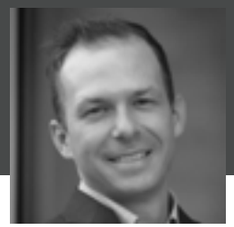
- Controle de dispositivos de acesso (chaves, cartões, combinações, códigos).
- Sistema duplo de controle/custódia de cheques e extratos. Exemplos incluem verificação da preparação de depósitos, seja por uma segunda pessoa ou virtual (FaceTime, CFTV, Zoom, etc.), coletas e depósitos bancários em pessoa (sem atividades noturnas caso apenas uma pessoa puder executar), e a confirmação do depósito ou verificação da credibilidade do malote de depósito à prova de adulteração antes da movimentação (trazendo de volta o boleto de depósito para verificação e documentação).
- Utilize tanto a verificação de antecedentes de emprego, independentemente do histórico de relacionamento ou do trabalho anterior, quanto uma verdadeira solução contínua de monitoramento de registros judiciais para obter o panorama completo.
- Exija que treinamentos específicos vinculados ao trabalho sejam documentados e confirmados através da assinatura do instrutor e dos participantes para garantir aderência, precisão e completude.
- Incorpore auditorias internas e externas aleatórias e não anunciadas, testando a política, o processo e o procedimento acima mencionados com a equipe de funcionários. Exemplos podem incluir auditorias de gavetas de dinheiro e sua documentação suporte.

Lembre-se, dinheiro pode ser rei, mas ainda é seu reino.

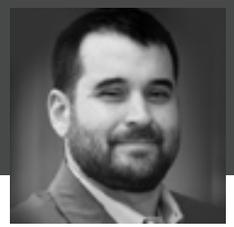
LEIA O ARTIGO COMPLETO →

CONTINUIDADE DE NEGÓCIOS

CONTRIBUIDOR CHAVE



CHRIS SOSNOSKI
Diretorde Tecnologia e Segurança da Informação



JOE LABROZZI
Diretor de Segurança

NOSSA HISTÓRIA

Quando eventos externos interrompem as operações normais, implementar um plano de continuidade de negócios torna-se prioridade máxima. Infelizmente, muitas empresas ficam paralisadas durante uma crise lutando com a implantação de seu plano, ou pior, construindo seu plano.

Quando o COVID-19 forçou a equipe da Lowers & Associates a se tornar virtual, a liderança se apoiou em um investimento antecipado em tecnologia para levar perfeitamente 550 pessoas a estarem totalmente remotas em pouco menos de 2 semanas sem nenhuma interrupção nas operações. Identificar, avaliar, orçar e testar proativamente o conjunto digital de ferramentas necessárias para realizar o projeto com anos de antecedência possibilitou nossa transição rápida, mas ter uma estratégia executável e 100% apoiada pela liderança foi a base fundamental.

RESILIÊNCIA AUTORAL DURANTE O COVID-19

Basicamente, os Planos de Continuidade de Negócios (“BCPs”) são a resposta do mundo real ao velho ditado “Esperar pelo melhor, planejar para o pior”. É um reconhecimento honesto de que ficar preso entre um lugar difícil e rochoso é melhor com um martelo, embora sem garantia de que o martelo seja grande ou pequeno o suficiente para ser útil.

No entanto, um BCP bem concebido proporciona tranquilidade, como o seguro, com a satisfação adicional que só a autoria (ou propriedade?) traz. O problema, é claro, é que todo BCP é, no final do dia, ainda apenas um plano. Como boxeador, ator, criminoso, dramaturgo e estrategista corporativo ‘Iron’ Mike Tyson uma vez disse: “Todo mundo tem um plano até levar um soco na boca“.

Para o Lowers Risk Group, como muitos outros, o COVID atingiu nosso setor, nosso negócio –nossas pessoas. Tivemos sorte, porém: nosso Plano de Continuidade de Negócios estava há cinco anos em andamento. Não importava, até que aconteceu.

Lá atrás em 2015, nosso CTO, David Lowers, o Diretor de Segurança, Joe Labrozzi e o Diretor de TI e Segurança, Chris Sosnoski, reconheceram a necessidade de nossa equipe crescente possuir capacidades remotas parciais, ou mesmo totais. O que foi inicialmente impulsionado por preocupações demográficas evoluiu com o acesso e a capacidade de novas tecnologias para suportar um trabalho totalmente seguro e remoto que reduziu o custo, aumentou a eficiência e permitiu maior flexibilidade que poderia suportar novas oportunidades de negócios dentro do Lowers Risk Group. Com essa fundação em vigor, Lowers, Sosnoski e Labrozzi foram capazes de levar a pegada global da organização de mais de 550 pessoas (espalhadas por 3 continentes) para uma realidade totalmente remota em menos de 2 semanas, sem interrupção dos negócios quando o COVID atingiu.

Eles compartilharam sua história e ofereceram essas entregas às organizações:

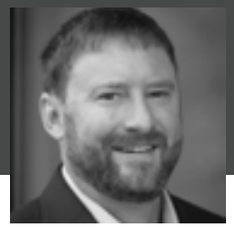
- Começamos a planejar cedo e exploramos o ambiente de risco, desenvolvemos os processos que nos proporcionariam um caminho de menor resistência à continuidade e tivemos apoio da liderança.
- Identificamos as ferramentas digitais certas e as avaliamos, orçamos e testamos estrategicamente como parte do plano; ter que fazer isso durante o COVID teria sido muito difícil.
- Estávamos todos alinhados no trabalho que precisava ser feito para alcançar a visão; que para nós era encontrar um ambiente seguro, escalável e disponível para realizar nosso trabalho de mitigação de riscos.

LEIA O ARTIGO COMPLETO →

INDENIZAÇÕES DE SEGUROS

CONTRIBUIDOR CHAVE

NEIL WATSON
Diretor Global de Operações



KEITH GRAY, CFE, CAMS
VP Relações Institucionais

INTELIGÊNCIA EMOCIONAL E O FASCÍNIO PELA FRAUDE EM SEGUROS

Uma perda segurada acontece por muitas razões. Quando um evento envolve a perda de estoque físico ou danos ao patrimônio, o prejuízo é imediato e cria uma necessidade urgente para que o empresário resolva o sinistro para que o negócio possa retomar as operações e evitar mais perdas de receitas.

Esse desejo de voltar rapidamente aos negócios como de costume é natural, mas frente a um sinistro, não é incomum durante o processo de regulação testar a determinação dos proprietários dos negócios. E enquanto a maioria dos pedidos de indenização pós-incidente são legítimas, de tempos em tempos, as emoções humanas complicarão o processo e criarão um ambiente que permita atividades fraudulentas, às vezes de maneiras inesperadas.

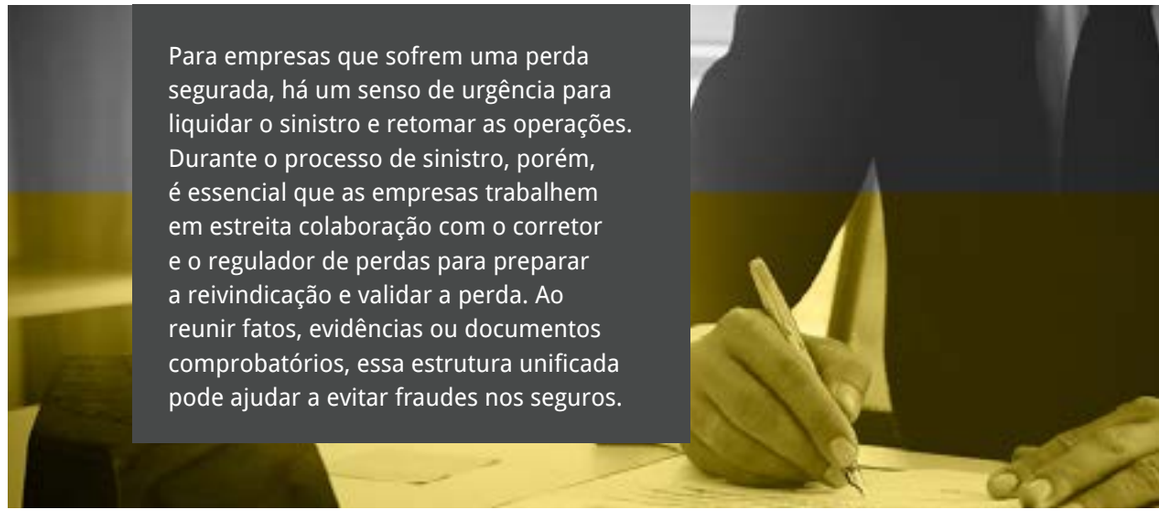
Como segurado, é importante trabalhar em estreita colaboração com seu corretor de seguros e o regulador de perdas na preparação de seu pedido de indenização e validação das perdas. Sem essa assistência profissional e supervisão, a fraude pode facilmente encontrar seu caminho durante a conversa.

Em tempos sem precedentes como estes, a possibilidade de um aumento de pedidos de indenização fraudulentas é uma preocupação real. Há um aumento, tanto nos fatores “pressão” quanto “oportunidade”, resultando em uma maior probabilidade de que potenciais infratores possam racionalizar seus pensamentos fraudulentos e agir sobre eles como resultado.

O que você pode fazer a respeito?

Idealmente, as seguradoras encomendariam uma pesquisa de pré-risco para estabelecer medidas de segurança, níveis de estoque e procedimentos operacionais padrão para satisfazer a si mesmos de que o risco atenderia às suas necessidades. Embora isso seja recomendado, nem sempre é viável devido a restrições de tempo ou custos.

DICA DO ESPECIALISTA



Para empresas que sofrem uma perda segurada, há um senso de urgência para liquidar o sinistro e retomar as operações. Durante o processo de sinistro, porém, é essencial que as empresas trabalhem em estreita colaboração com o corretor e o regulador de perdas para preparar a reivindicação e validar a perda. Ao reunir fatos, evidências ou documentos comprobatórios, essa estrutura unificada pode ajudar a evitar fraudes nos seguros.

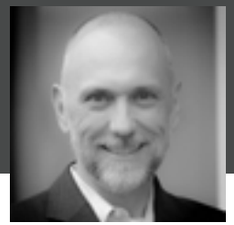
Após o evento, uma vez que um pedido de indenização foi apresentado, basear-se nas conclusões de uma investigação policial pode não ser viável devido ao tempo ou a quaisquer circunstâncias relacionadas ao evento (especialmente se for em grande escala ou um desastre natural). E mesmo que a polícia esteja fazendo uma investigação sobre o evento, pode não ser a prioridade, criando um longo período de incerteza. Por fim, as autoridades também podem ser muito hesitantes em fornecer qualquer informação que tenham conhecimento, especialmente quando se tratar de uma investigação ativa.

Para gerenciar esse processo, os empresários e as seguradoras precisam de terceiros independentes que sejam flexíveis, tenham experiência em vários setores e possam dedicar o tempo adequado necessário para trabalhar através de um sinistro (ou seja, coleta de fatos, provas e documentos necessários) para apoiar a base do pedido de indenização. Para questões verdadeiramente complexas de fraude, proprietários de empresas e seguradoras devem esperar que este terceiro tenha uma Unidade de Investigações Especiais (“SIU”) com ampla experiência em Contramedidas de Vigilância Técnica e Contrainteligência (“TSCM”) que trabalhem regularmente em atribuições internacionais.

LEIA O ARTIGO COMPLETO →

ENGENHARIA SOCIAL

CONTRIBUIDOR CHAVE



BRAD MOODY, CFI, CFE
Vice Presidente Executivo

LEÕES E CORDEIROS: UMA HISTÓRIA DE FRAUDE ATRAVÉS DA ENGENHARIA SOCIAL

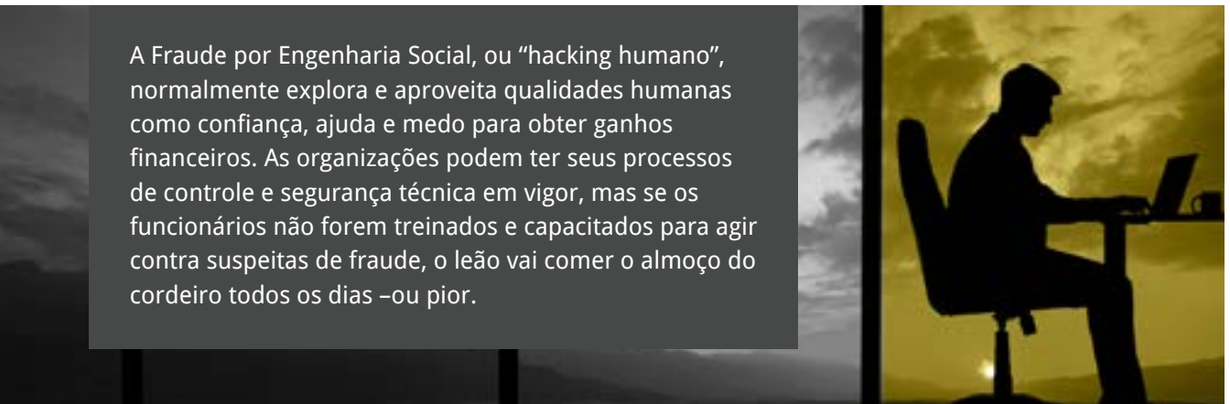
Brad Moody conta uma história de fraude de engenharia social que, se o CEO tivesse criado a cultura de uma organização de alta confiabilidade, poderia ter tido um resultado diferente.

Q: Um dos trabalhos memoráveis que você realizou envolve o CEO amante de leões. O que aconteceu nesta ocasião?

Brad Moody: Eu me dirigi ao local em nome de nosso cliente, um subscritor de seguros, para investigar um cliente deles que havia sofrido uma enorme perda que poderia ou não ter sido um evento cibernético. Nosso trabalho era descobrir isso. O que rapidamente se tornou evidente foi que o processo de transferência bancária no local foi bem documentado, realizado e controlado.

DICA DO ESPECIALISTA

A Fraude por Engenharia Social, ou “hacking humano”, normalmente explora e aproveita qualidades humanas como confiança, ajuda e medo para obter ganhos financeiros. As organizações podem ter seus processos de controle e segurança técnica em vigor, mas se os funcionários não forem treinados e capacitados para agir contra suspeitas de fraude, o leão vai comer o almoço do cordeiro todos os dias –ou pior.



No entanto, o CEO desta empresa era muito agressivo e intimidante com seus funcionários e o que parecia ser um evento cibernético foi na verdade uma fraude por engenharia social que foi possibilitada pelo comportamento do CEO.

O que aconteceu foi que este CEO mencionou nas redes sociais que eles estariam participando de uma conferência em um momento específico e engajados com o visível diálogo de “marketing” do CFO da mesma empresa (que também estava definido para participar deste evento), marcando uns aos outros neste fórum público. Eventualmente, o Controller da empresa também entrou na discussão. Para um malfeitor, isso seria uma evidência de que durante esse tempo, certos tomadores de decisão de alto nível estariam ausentes e talvez não estariam prestando total atenção aos detalhes operacionais.

O malfeitor nesta fraude realmente se aproveitou de todas essas informações e criou um domínio falso, trocando apenas duas letras do nome da empresa, com um caractere minúsculo e outro maiúsculo.

Usando o domínio falso, ele desenvolveu uma falsa cadeia de e-mails que começou com o falso CEO “enviando” ao FALSO CFO mensagem sobre o envio de uma transferência bancária. Confirmando esta transferência fraudulenta, o falso e-mail do CEO então encaminhou a série de mensagens fraudulentas para o Controller REAL, exigindo que esta transferência bancária fosse feita, no valor de mais de US$ 8 milhões.

Q: O que sua investigação revelou sobre como isso aconteceu e qual era a cobertura que eles tinham?

Brad Moody: Bem, uma das minhas recomendações acabou sendo em torno de seu processo de controle. No papel, parecia bom, mas faltavam passos. Obviamente, houve algumas coisas que deram errado neste cenário, mas clicar no botão “Responder a todos” -foi ruim. Se o Controller tivesse digitado os e-mails do CEO e do CFO, o preenchimento automático o teria ajudado. Provavelmente, ele teria notado a discrepância no tempo e teria havido pelo menos alguma hesitação, com certeza. Mas eu vi três casos similares acontecerem recentemente, então continua a funcionar para os bandidos.

Este foi um verdadeiro colapso nos controles, impulsionado pela falta de empoderamento na organização.

LEIA O ARTIGO COMPLETO →

PROCESSOS OPERACIONAIS PADRÃO

CONTRIBUIDOR CHAVE

DANIEL COOTES
Gerente de Operações e Atendimento ao Cliente

POPS E METAIS PRECIOSOS: GARIMPANDO SEU PRÓPRIO NEGÓCIO

Processos Operacionais Padrão (POPs) são exatamente o que eles dizem na lata –uma diretiva calculada e testada, usada como base para uma operação ou tarefa individual. Aqui, Daniel Cootescompartilha algumas informações sobre sua experiência avaliando uma operação de mineração na Ásia cujos POPsnão eram tão deficientes, mas vigoravam em um ambiente onde a incerteza não era um risco que a seguradora estava disposta a ignorar.

Q: Nos guie até a segurança de uma instalação, cujas ameaças incluem desde gangues locais, desastres naturais até o Estado Islâmico. Por onde você começa?

Daniel Cootes: O processo de pensamento aqui começa realmente em como responder a uma pergunta: Um ataque poderia atravessar o perímetro desta instalação, suprimir a segurança no local, chegar ao cofre, violá-lo, pegar o que quisesse e depois voltar a sair? A inteligência nos leva a acreditar que sim, esse tipo de ataque é possível, mas você também pergunta: seria provável?

DICA DO ESPECIALISTA

Quando devidamente desenvolvidos e gerenciados, os POPsajudam as organizações a evitarem riscos desnecessários. E como em qualquer função de negócio que suporte tanto a estratégia de curto quanto de longo prazo, a gestão de POPsenvolve revisões regulares. Muitas organizações se comprometem com o processo de revisão, mas ficam aquém da comunicação sobre as atualizações. Se uma empresa opera em um ambiente de alta segurança ou não, o verdadeiro benefício da aplicação de POPsatualizados é que a conformidade se torna uma parte natural da cultura da empresa, proporcionando aos funcionários mais confiança para realizarem seus trabalhos.

Q: Que recomendações você acabou fazendo e como chegou a essas conclusões?

Daniel Cootes: Dado os parâmetros e todos os diferentes ângulos que eles tinham, fiz algumas recomendações do que pensávamos ser aceitável, a operação então retornou com o que eles achavam aceitável com base em sua perspectiva operacional e cultural. Em última análise, trata-se de ser realista e o quão fácil seria para a operação implementar as atualizações. Algo assim não precisaria ser à prova de bombas nucleares, então olhamos primeiro para o portão e os muros que eles tinham, por exemplo. Tudo tinha cerca de 10 anos e numa selva, as coisas se deterioram rapidamente. Falamos em melhorar as patrulhas itinerantes. Nós também focamos em atualizar seu sistema de CFTV. A tecnologia é tão barata, que não há desculpa para não tê-la. Há outras coisas muito específicas que fizemos por eles que eu não vou abordar, mas uma boa parte disso remete aos seus procedimentos operacionais padrão e a garantia de que seu pessoal os está seguindo.

Q: POPs são incrivelmente importantes e você foi capaz de avaliar o risco desta instalação inteiramente através de um processo remoto –como você fez isso?

Daniel Cootes: Muitas perguntas. Eu gosto de começar de fora para dentro (método da "casca de cebola"). Se eu aparecesse no local, tentaria formar a imagem do que estivesse na minha frente e o que me impediria de entrar. Você apenas vai descascando o máximo de camadas da cebola e o que é necessário para chegar aos melhores itens no cofre.

Ao mesmo tempo que faço essas perguntas, tenho que tentar ser realista. Eu posso querer que eles tenham uma resposta militar, mas é preciso entender os recursos que possuem e como podem implantá-lo. Eu voltaria novamente para os POPs, que os elaborou e como –essa pessoa era credenciada para a tarefa? Há quantos anos os POPsforam elaborados e o que mudou desde então? Essas atualizações foram feitas e comunicadas?

Para mim, os POPs sãofundamentais, mantendo-os relevantes. Eles são incríveis de se ter, mas se estiverem trancados em gaveta sem ver a luz do dia por 10 anos ou até que um problema aconteça, eles não vão servir para nada, não é?

LEIA O ARTIGO COMPLETO →

FRAUDE OCUPACIONAL

CONTRIBUIDOR CHAVE

KEITH GRAY, CFE, CAMS
VP Relações Institucionais

PESSOAS & PROCESSOS –A LONG TAIL DO TRIÂNGULO DA FRAUDE

Nos negócios, o conceito da "LongTail" implica que uma organização pode encontrar benefícios financeiros significativos vendendo pequenos volumes de itens difíceis de encontrar para muitos clientes de nicho. Enquanto isso, em nosso trabalho, o Triângulo da Fraude reúne Pressão, Oportunidade e Racionalização para ajudar a explicar por que a fraude acontece.

Nesta história, Keith Gray mistura insights de uma fraude épica de oito dígitos com alguns exemplos menores para destacar como tanto as pessoas quanto o processo realmente permitem que a fraude aconteça dentro do que poderia ser descrito como o "LongTail"do Triângulo da Fraude.

Q: Em nosso trabalho, muitas vezes somos chamados para avaliar e investigar as consequências da fraude. Há algo que te surpreenda ao revisar esses casos de fraude?

Keith Gray: Eu não diria que é surpreendente, mas eu acho que é sempre muito interessante até onde as pessoas vão para cometer ou sustentar uma fraude, complexa ou não. Infelizmente, o que vemos muito é que a confiança pode levar a muitas fraudes.

Caso em questão, na época da Grande Recessão, o dono de uma grande empresa privada estava orquestrando uma grande fraude. Quando a economia estava crescendo, essa pessoa era capaz de movimentar fundos, apropriar-se indevidamente de fundos garantidos em vantagem própria através de imóveis, investimentos financeiros, veículos, várias coisas. Quando a economia estava indo bem, essa pessoa sempre podia sacar dinheiro para fazer as coisas direito, estava sempre no bolso de trás. A pessoa também era capaz de manipular os cofres e movimentar dinheiro, essencialmente como o jogo dos copos com o conteúdo dos cofres para puxar a bolinha de lã sob os olhos do banco ou qualquer um que viesse para auditar o cofre. Não houve um bom esforço coordenado para entrar e fazer a contagem completa dos cofres ou algo parecido.

Q: Por que fazer uma contagem completa de cofres seria importante?

Keith Gray: Como auditores independentes, podemos entrar e fazer uma contagem completa de cofres para entender tudo. É exatamente o tipo de coisa que nós forçamos. Uma pessoa pode entrar num banco, mas ele só irá ver seus fundos, dando oportunidade para o fraudador aplicar o jogo dos copos. Neste caso, a crise econômica ajudou na descoberta da fraude. Quando o país entrou em recessão, grande parte do valor desses investimentos desapareceu, então esse indivíduo não conseguiu compensar o que foi desviado.

Durante esse período, um dos clientes do banco se sentiu desconfortável, alertando as autoridades e trazendo a situação à tona. O resultado você sabe, US$90 milhões foram considerados desaparecidos. Passei cerca de um ano trabalhando com isso em nome de alguns clientes, apenas tentando recriar o lado do pedido de indenização.

Q: Qual a mentalidade das pessoas que cometem estas fraudes?

Keith Gray: O Triângulo de Fraude é o motivo, mas o como é a quebra de controles ou de confiança. A comunalidade é que o ladrão ou fraudador tem a oportunidade. Ganância é algo real e uma vez que eles percebem que há uma oportunidade e eles podem se safar de algo algumas vezes, eu vi um monte de fraudes que duraram de 4 a 5 anos até serem descobertas.

É incrível por quanto tempo e o montante que alguns fraudadores podem desviar quando não há supervisão independente ou Procedimentos Operacionais Padrão ("POPs").

LEIA O ARTIGO COMPLETO →

DICA DO ESPECIALISTA

Enquanto os empregadores se esforçam para contratar e reter membros honestos da equipe, roubos e fraudes por funcionários continuam sendo uma realidade. O Triângulo da Fraude explica por que ela acontece, mas a mecânica do roubo e fraude é possível por que há pessoas que exploram processos ineficazes.

Atividades como revisão e melhoria de POPs, controles internos e levantamento de antecedentes pré-emprego ajudam a limitar o risco de capital humano, mas realmente construir uma cultura que abrace a gestão de riscos corporativos significa manter todos (ou pelo menos a maioria) dos vértices do Triângulo da Fraude distantes.

EXPERIÊNCIA E TREINAMENTO

CONTRIBUIDOR CHAVE

NEIL WATSON
DiretorGlobal de Operações

VENCER OU APRENDER: AS FRAUDES QUE MOLDAM NOSSA REALIDADE

Um fraudador profissional demonstra, com o tempo, mais vitórias do que perdas, presumindo que pode ficar fora da cadeia. Por outro lado, um investigador certificado que gerencia alegações de fraude também conta mais vitórias do que perdas, fato necessário para permanecer empregado. A diferença entre fraude e investigador, ganhar e perder, aptidão e atitude é como a pessoa em questão aplica conhecimento de perda para determinar os resultados futuros que moldam sua realidade.

Em seus mais de 30 anos de trabalho, Neil viu alguns casos de fraude e nos últimos 18 meses ele identificou pelo menos seis potenciais esquemas de fraude no mercado de espécies envolvendo joias preciosas e rubis. No entanto, foi uma experiência no início de sua carreira como corretor avaliando um suposto artefato de alto valor que o deixou "cabisbaixo por descobrir a verdade" mas, em última análise, ajudou a informar sua abordagem todos os dias depois disso.

DICA DO ESPECIALISTA

Para qualquer profissional de negócios, a experiência sem treinamento é autolimitante e o treinamento sem experiência minimiza a capacidade de adaptação. Os melhores líderes do amanhã impulsionam a inovação com esse entendimento e os profissionais de segurança aplicam ativamente sua ampla gama de certificados e ganhou -conhecimento em benefício de seu cliente. Criar um ambiente seguro para qualquer organização abrange os conhecidos e desconhecidos.

Q: Sua experiência se concentra em espécies e valores. Que tipo de fraudes são mais frequentemente apresentadas a você e o que envolvem?

Neil Watson: As fraudes que chegam até nossas mesas são geralmente por valores consideráveis, centenas de milhões de dólares, às vezes até US$ 1 bilhão. É quando a primeira "red flag"se levanta. Com um pouco de pesquisa, geralmente há precedentes para possibilitar o entendimento do que é legítimo no mercado e o que precisa de um olhar mais crítico, independentemente da embalagem e detalhes que nos são mostrados.

Pode ficar um pouco mais desafiador com bens oriundos do processo de refinamento de ouro, sucata e terra, pois há muitos subprodutos que saem de uma mina de ouro que pode ter um conteúdo de ouro nele. Vimos clientes que compraram bolsas cheias de dejetos que então queriam assegurar essas bolsas, mas eles foram ativamente enganados. Um olhar atento e uma investigação prévia podem mitigar isso, mas você está tipicamente lidando com aingenuidade do comprador ou uma fraude direta sobre eles.

Q: Você está nisso há mais de 30 anos. Você já foi enganado em sua carreira?

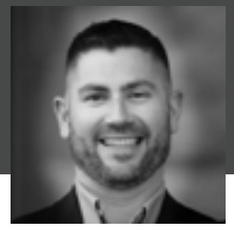
Neil Watson: Um que não esqueço foi quando eu era corretor. Era iniciante na carreira, antes da Internet, e-mail, toda a tecnologia moderna e eu tinha recebido um pacote que seria supostamente o maior Buda de ouro do mundo. Alguém queria assegurá-lo. O contato tinha tido tempo para montar uma apresentação estelar. Um lindo pacote com fotografias, anotações, certificados, tinha tudo. Obviamente, quem fez isso se esforçou muito para fazer esta estátua parecer legítima.

Como um jovem corretor, para obter esse objeto e tê-lo em minhas mãos, eu estava animado. Eu busquei obter uma cobertura para ele. Com alguns telefonemas, porém, eu estava sentindo a relutância do vigarista e tornou-se evidente para mim que isso talvez não fosse um item verdadeiro. Mas estava mantendo aesperança. Uma das razões para isso, é que na época, eu estava trabalhando para a Royal Academy, como "OneBall Total EquilibriumTank", de Jeff Coonpor 5 milhões de dólares. Isso fez com que aideia de um Buda gigante dourado, inédito, parecesse totalmente plausível. Eu tinha um bom contato em Hong Kong, um velho expatriado que estava na indústria de segurança há muito tempo e ele disse: "Não companheiro. Definitivamente não. Não é legítimo". Eu realmente confiava nele mas simplesmente não podia acreditar. Eis que, depois de um pouco mais de investigação e perguntas, poof! Aestátua, o contato, o pedido completo, desaparece na fumaça. Eu estava realmente cabisbaixo para descobrir a verdade sobre tudo.

LEIA O ARTIGO COMPLETO →

MONITORAMENTO E INVESTIGAÇÃO

CONTRIBUIDOR CHAVE



KRISTOPHER KEEFAUVER
Diretorpara Clientes, CIT e Segurança

FUGA DA PRISÃO: COMO A COLABORAÇÃO ESTÁ MUDANDO A SEGURANÇA PARA MELHOR

As empresas utilizam uma abordagem colaborativa por uma série de razões, incluindo os benefícios mais imediatos de eficiência e redução de custos. Mas benefícios adicionais do engajamento dos funcionários e da mudança cultural são duas outras razões a jusante onde a colaboração cria um impacto positivo para as organizações.

O impacto positivo da colaboração é claramente retratado neste Q & A com Kris Keefauver, como ele relata uma experiência de investigação com uma equipe de agentes de segurança que, até então, não foram capacitados nem necessariamente treinados para tomar as medidas necessárias para trabalhar através de um crime suspeito.

Q: Você representou recentemente a L&A como diretor interino de segurança de uma organização de saúde. Como isso se parecia e você pode descrever alguns dos problemas com os quais eles estavam lidando?

Kristopher L. Keefauver: Nossa tarefa foi tripla: 1) Completar uma avaliação de risco de segurança do campus; 2) Atuar como diretor interino de segurança; e 3) Estar envolvido nos esforços de remediação de qualquer um dos pontos e recomendações que fossem trazidos à tona durante a avaliação. A organização tinha uma equipe de cerca de 10 a 12 agentes de segurança e nossa equipe estava engajada em fornecer liderança e supervisão enquanto renovava o departamento de segurança. A equipe de segurança reportava-se diretamente a nós, forneceríamos direção e supervisão e depois reportaríamos diretamente ao COO da organização de saúde.

Servindo nessas capacidades, muito do que descobrimos foi que os funcionários que estavam no local não estavam necessariamente cientes das políticas, procedimentos e processos que a organização de saúde havia documentado.

DICA DO ESPECIALISTA

A teoria da Escolha Racional sugere que criminosos são menos propensos a cometer crimes se acreditarem que alguém vai vê-los ou haja um risco maior de serem pegos. Nestes casos, o Circuito Fechado de TV pode ser um impedimento significativo e eficaz contra o crime. Com a tecnologia digital mais facilmente disponível para empresas modernas, o CFTV é acessível, serve como uma forma de vigilância formal e, quando emparelhado com os processos de investigação adequados, auxilia ativamente no sistema de justiça criminal.

A organização tinha feito um grande trabalho de detalhamento de todas essas políticas e procedimentos a serem seguidos, mas em algum lugar ao longo da linha, a cadeia de comando ou a disseminação dessas informações não necessariamente chegaram à equipe de guarda.

Q: Ao ajudar a realinhar os POPs, revisitar critérios de contratação e ampliar a necessidade de treinamento, você passou muito tempo no local com sua equipe de segurança. Há algo sobre o tempo ou trabalhar juntos que se destaque?

Keefauver: O momento mais impactante para mim aconteceu no final de um turno de 12 horas. Eu estava saindo do trabalho, descendo as escadas para o estacionamento e encontrei um dos seguranças. Depois de uma conversa fiada, ele mencionou que eles achavam que alguém tinha roubado algumas camisas da loja de presentes. Perguntei qual era o plano deles, e ele disse: “Bem, eu vou sair no estacionamento para tentar encontrá-la.” Fui com ele ao estacionamento.

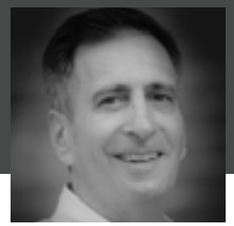
Nem preciso dizer que não a encontramos, então voltamos e conversamos com os outros agentes de segurança, perguntando o que normalmente fazem nesta situação. Foi mencionado que havia uma pessoa que sabia como trabalhar os sistemas de CFTV, mas esse indivíduo não estava lá; então, essencialmente, a equipe ia simplesmente deixá-lo ir.

Conversei com a funcionária da loja de presentes e tentei obter uma descrição da pessoa, fui ao sistema de CFTV, e consegui localizar a pessoa com base no tempo que ela estava na loja de presentes, o que ela estava vestindo e outros atributos.

LEIA O ARTIGO COMPLETO →

COMUNICAÇÃO PROATIVA

CONTRIBUIDOR CHAVE



JON D. GROUSSMAN, J.D.
VP Executivo – Divisão Consultoria

COMUNICAÇÃO PROATIVA: O ALGORITMO HUMANO PARA GERENCIAR RISCOS

Quando se trata de mitigar o risco, a capacidade preditiva da comunicação proativa é menos sobre leitura da mente e mais sobre leitura do comportamento. Ela permite que os funcionários possam usar uma estrutura para identificar e comunicar "red flags"antes que elas se transformem em má conduta e um caso judicial, ou pior, naquelas fitas de isolamento amarelas de cenas de crime.

Neste Q&A, Jon Groussman cristaliza o "antes e depois do risco" usando o exemplo de um cliente que levou um duro golpe na moral e reputação dos funcionários que, se a comunicação proativa e o monitoramento contínuo fossem opções, poderiam ter sido evitados.

Q: Este incidente em particular ocorreu em uma instalação de pesquisa e fabricação e envolveu um supervisor e um funcionário. Pode nos dizer o que aconteceu?

Jon Groussman: Eu me lembro que eu tinha chegado ao escritório um pouco mais cedo naquele dia para fazer alguma revisão. Meu telefone tocou por volta das 8h30 e era um executivo de um cliente informando que eles tiveram um incidente na noite anterior por volta das 23h. Um supervisor no turno da noite havia trazido uma arma para a fábrica, colocou a arma na cabeça de um dos funcionários e ameaçou explodir a cabeça do colega se ele falasse com o supervisor novamente. A polícia foi chamada, o supervisor foi preso por agressão agravada e posse de arma de fogo, banido da propriedade e, claro, levado sob custódia.

Infelizmente, os executivos não sabiam muito sobre o que realmente teria acontecido durante este 3º turno que, para todos os efeitos, foi um turno da noite para o dia.

DICA DO ESPECIALISTA

Organizações de todos os tamanhos podem se beneficiar da comunicação proativa. Em um ambiente seguro, ela permite ações coordenadas e ajuda a criar fluxos de trabalho coesos e eficientes. Sem comunicação proativa, o comportamento de conformidade com a segurança sofre e os riscos no local de trabalho acabam sendo permitidos, impactando negativamente a moral e a produtividade dos funcionários.

Muitas vezes, não apenas nestes ambientes, mas em outros que possuem trabalhadores em turnos ou que fiquem abertos 24 horas, a alta administração não sabe o que realmente está acontecendo durante essas horas. O que se desenvolve então é uma lacuna de comunicação. Comecei a entrevistar pessoas.

Q: Você mencionou que um padrão começou a emergir. Surgiram "red flags" que teriam sido negligenciadas?

Jon Groussman: Há quase sempre red flags; esse tipo de situação geralmente não acontece do nada. Ao falar com pessoas que trabalhavam no terceiro turno, me disseram que o agressor teve pausas mais longas do que todos os outros. Como ele era supervisor, as pessoas não questionavam porque ele também fazia o seu trabalho. O problema foi que descobrimos que ele estava saindo do local –usando a única câmera que estava bem posicionada e funcionando –para visitar uma comunidade vizinha que era muito conhecida por vender drogas. Podíamos ver seu carro ir e vir nos momentos em que seus colegas disseram que ele estaria em intervalos mais longos, e isso começou a acontecer com mais frequência nos meses anteriores ao ataque.

Com essa descoberta, fomos à polícia para ver se ele era fichado ou se já havia tido algum problema com armas antes. Acontece que ele tinha estado perante o tribunal várias vezes naquele ano anterior por comprar drogas na comunidade que mencionei, mas o cliente e instalação não possuíam um sistema para saber disso. Lembre-se, esta era uma pessoa em um papel de supervisão com acesso a ativos dentro desta planta em que uma perda ou acidente poderia ter sido muito prejudicial. Os materiais e segredos comerciais também eram muito valiosos no mercado secundário, se ele estivesse desesperado o suficiente para precisar de dinheiro para drogas ou sido coagido a roubá-los. Se esse cliente e sua planta tivessem utilizado algum tipo de monitoramento contínuo e tivessem uma política disciplinar, este incidente provavelmente nunca teria acontecido porque ele teria ido embora muito antes de acontecer.

LEIA O ARTIGO COMPLETO →

ABOUT LOWERS & ASSOCIATES

L&A PARA SEGURADORAS

Estaremos onde você precisar.

- Análise de Riscos e Avaliações
- ↓
- Estratégia
- ↓
- Mitigação de Riscos& Prevenção de Perdas
- ↓
- Recuperação de Perdas & Indenizações

VÁ EM FRENTE COM CONFIANÇA

Grandes ou pequenos, quando os problemas precisam ser resolvidos, organizações em todo o mundo confiam no nome Lowers.

A Lowers & Associates (L&A) é uma empresa de mitigação de riscos e prevenção de perdas internacionalmente reconhecida que opera orgulhosamente sob a família de empresas do Lowers Risk Group. L&A trabalha com organizações que operam em indústrias de alto risco, altamente regulamentadas e com organizações que operam com uma mentalidade de gerenciamento de riscos.

Nosso trabalho aborda uma ampla gama de questões, incluindo investigações de sinistros fraudulentos, auditorias para conformidade regulatória, políticas de segurança cibernética, suporte a litígios e segurança. Nossos especialistas têm ampla experiência em disciplinas relacionadas como gestão de riscos, contabilidade, aplicação da legislação, segurança física, tecnologia da informação e recursos humanos. Nossas diversidade de profissionais, experiência e senioridade nos permitem "zerar" as necessidades de sua organização e fornecer as soluções apropriadas para proteger pessoas, marcas e lucros.

Quando realmente importar, coloque a Lowers ao seu lado.

L&A LOWERS & ASSOCIATES
International Risk Mitigation Partners

Solicite um contato acessando lowersrisk.com