Relatório de pesquisa FStech e Bottomline

Fora do radar

Como as instituições financeiras podem mitigar o risco de fraude interna?

FStech Em colaboração com Bottomline

Introdução

As ameaças de fraude interna estão crescendo cada vez mais nas Instituições Financeiras (IFs). Com a pressão crescente dos custos de vida mais altos e incertezas econômicas, as soluções de trabalho remoto e híbrido estão criando mais oportunidades para atividades fraudulentas e, com um cenário digital em evolução expandindo o domínio para ataques, as ameaças internas e o risco de funcionários cometerem fraudes estão crescendo.

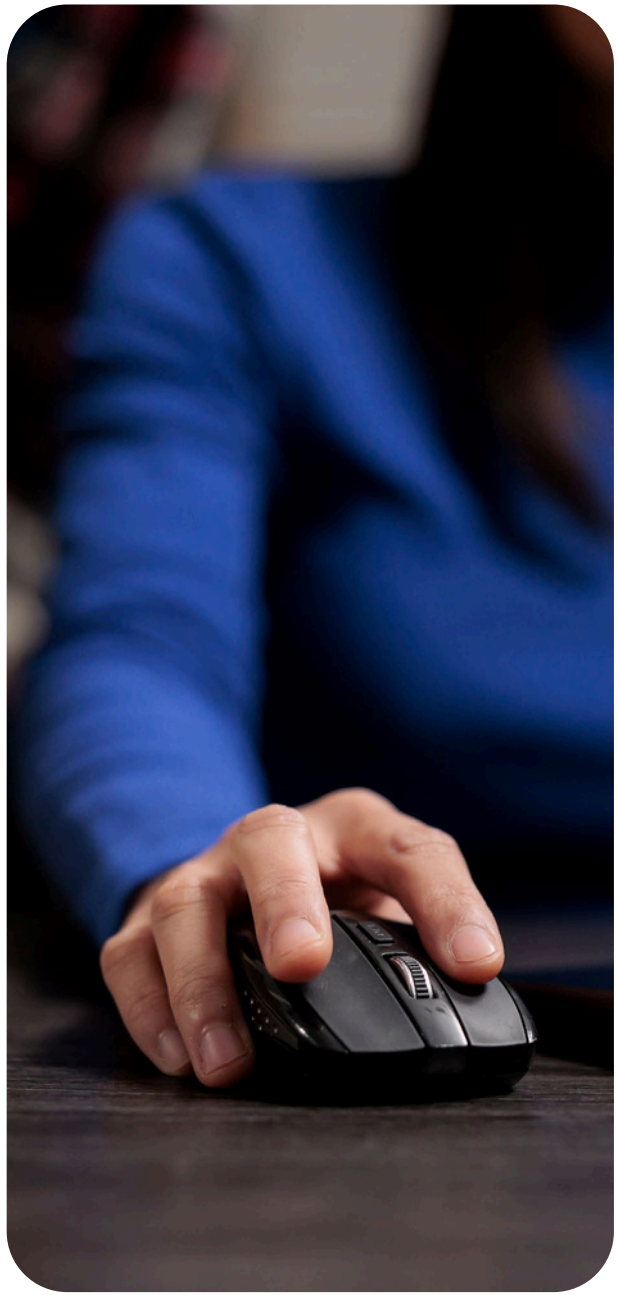
Demonstrando esse crescimento alarmante, o Insider Threat Database (ITD) anual intersetorial produzido pela associação sem fins lucrativos Cifas descobriu que o número de casos de fraude interna aumentou 14% ano a ano (YoY) em 2023, com "ação desonesta para obter benefício por roubo ou engano" identificada por 49% dos entrevistados como a ação mais comum.

Com o aumento do escrutínio regulatório em todo o mundo, incluindo exemplos como a próxima lei do Reino Unido "Falha em Prevenir Fraude", que penaliza organizações que não conseguem evitar fraudes de funcionários que beneficiam a organização, mais pressão está sendo exercida sobre as instituições financeiras para gerenciar e mitigar efetivamente as ameaças de fraude interna do que nunca. As instituições financeiras devem enfrentar essas ameaças e, ao mesmo tempo, proteger os clientes e alcançar um crescimento lucrativo.

No cenário atual, a natureza das ameaças de fraude interna se tornou mais sofisticada, levando a riscos cada vez mais complexos e sobreposições entre atividades fraudulentas internas e externas, o que exige que as empresas melhorem as maneiras de maximizar o gerenciamento de riscos e alinhar os objetivos de resiliência às metas corporativas.

Implementar medidas como integrar a tecnologia mais recente, impulsionar a comunicação entre departamentos e fornecer programas de treinamento agora é crucial para identificar ameaças internas antes que seja tarde demais. Deixar de gerenciar essas demandas pode levar a perdas financeiras, danos à reputação e interrupções operacionais, com os custos de longo prazo superando em muito o investimento inicial necessário para implementar medidas de detecção e prevenção de fraudes.

Para entender como os líderes em instituições financeiras estão lidando com a fraude interna, a Bottomline e a FStech pesquisaram os principais tomadores de decisão do setor para examinar o que está sendo feito para mitigar os riscos de fraude interna que estão enfrentando. A pesquisa mostra que as IFs estão implementando novas medidas para resolver o problema da fraude interna. No entanto, elas podem não ter acesso a sistemas unificados adequados que possam gerenciar efetivamente incidentes de ameaças internas, prever fatores de risco agravantes e ajudar a prevenir e mitigar esses riscos.



Metodologia

A FStech e a Bottomline entrevistaram 100 profissionais de serviços financeiros de diversas instituições financeiras líderes do mundo todo para explorar como as empresas estão tentando mitigar o risco de fraude interna enquanto navegam em um cenário de risco em constante mudança.

Aviso Legal: Devido ao arredondamento, as porcentagens neste relatório podem não somar exatamente 100%.

1. Quais departamentos da sua organização são responsáveis por investigar incidentes de fraude?

Os resultados demonstram uma variedade de abordagens, indicando que os profissionais de serviços financeiros dependem de vários departamentos internos para investigar incidentes de fraude. Abrangendo 50-56% dos entrevistados, os principais departamentos encarregados de investigações de fraude interna são conformidade, RH, equipes de prevenção de fraude especializada, departamentos de fraude, segurança da informação e auditoria.

Essa colaboração interdepartamental é benéfica para lidar com fraude interna, pois permite que as organizações aproveitem diversas áreas de especialização. Conformidade as equipes trazem conhecimento regulatório, o RH tem insights sobre o comportamento e as motivações dos funcionários, os departamentos de fraude são especializados em técnicas de detecção, a segurança da informação monitora as atividades digitais e a auditoria avalia a eficácia dos controles internos. Ao trabalharem juntos, esses departamentos podem detectar sinais críticos que podem passar despercebidos por qualquer equipe e responder a ameaças potenciais de forma mais holística.

No entanto, essa abordagem multifacetada também introduz desafios de coordenação, como silos de informações e propriedade pouco clara do processo de investigação. Para mitigar esses problemas, as organizações se beneficiariam da implementação de sistemas unificados de gerenciamento de casos. Eles podem reduzir silos e consolidar informações em uma única fonte segura, garantindo que os dados sejam compartilhados adequadamente em tempo hábil, ao mesmo tempo em que protegem a integridade das informações confidenciais.

A automação pode garantir ainda mais que apenas pessoal autorizado tenha acesso aos dados pertinentes, mantendo a confidencialidade e evitando vazamento de dados.

2. Quais das seguintes medidas sua organização tem atualmente em vigor para detectar e prevenir potenciais ameaças internas?

[selecione todas as opções aplicáveis]

As altas taxas de adoção dessas várias medidas demonstram que as instituições financeiras reconhecem a necessidade de uma abordagem multifacetada para lidar com ameaças internas, com cada opção sendo implantada por pelo menos 60% dos entrevistados.

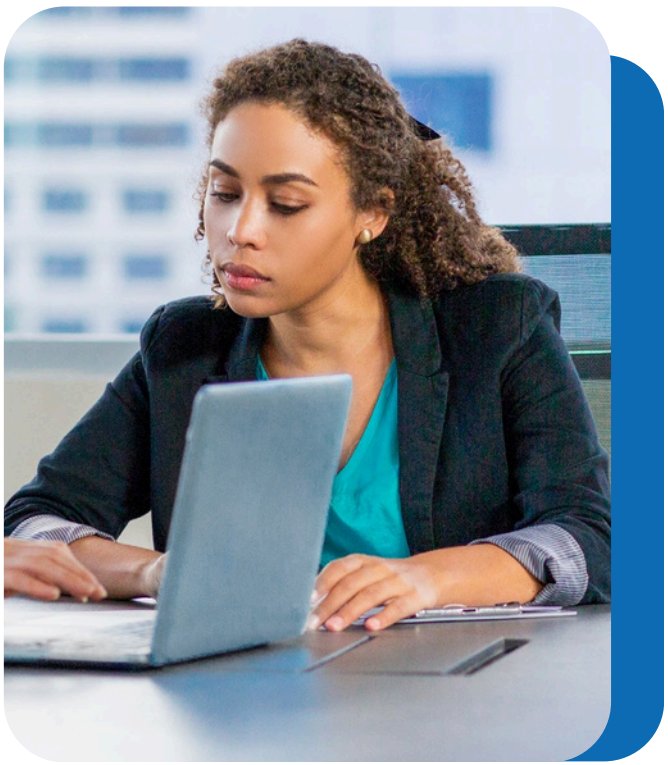
As tecnologias de monitoramento baseadas em agentes, que fornecem visibilidade em tempo real das atividades dos funcionários, são vistas como particularmente valiosas, pois podem ajudar a detectar comportamentos suspeitos ou padrões de acesso a dados que podem indicar intenção maliciosa. Da mesma forma, os recursos de análise comportamental e detecção de anomalias permitem que as organizações desenvolvam uma compreensão mais profunda do comportamento do usuário e identifiquem outliers que justificam uma investigação mais aprofundada.

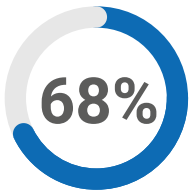
No entanto, embora todos os métodos sejam úteis, a implementação dessas medidas não é isenta de desafios. O uso de ferramentas de monitoramento baseadas em agentes por 68% dos entrevistados levanta preocupações válidas sobre a privacidade dos funcionários, pois elas têm o potencial de capturar inadvertidamente dados pessoais confidenciais. As organizações devem equilibrar cuidadosamente a necessidade de controles de segurança robustos com suas obrigações sob regulamentações de privacidade, como o GDPR.

A análise comportamental — usada por 60% dos entrevistados — por outro lado, geralmente depende muito da qualidade e disponibilidade de dados de log e auditoria, o que pode ser um problema para algumas instituições. As organizações devem garantir que tenham acesso a dados abrangentes e de alta qualidade para permitir análises precisas e detecção eficaz de anomalias.

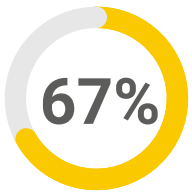
Para lidar com essas compensações, as instituições financeiras podem adotar uma abordagem multicamadas para o gerenciamento de ameaças internas. Isso deve envolver a combinação estratégica de medidas complementares, como monitoramento baseado em agentes, análise comportamental, treinamento programas e avaliações regulares de segurança. Ao implementar um programa holístico que aborda aspectos tecnológicos e centrados em humanos de ameaças internas, as organizações podem aumentar sua resiliência geral e proteger melhor contra o risco de atividades maliciosas internas.

Em cada caso, para serem maximamente eficazes, as organizações devem escolher serviços complementares para combinar holisticamente múltiplas salvaguardas.

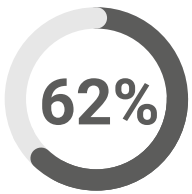




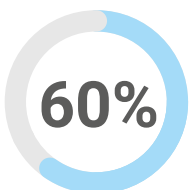
Tecnologias de monitoramento baseadas em agentes: monitoramento de ações e comunicações digitais dos funcionários dentro da organização, normalmente de seus dispositivos



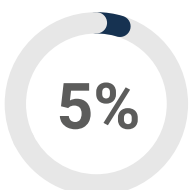
Programas de treinamento e conscientização de funcionários: fornecer programas de treinamento e conscientização para educar os funcionários sobre riscos de ameaças internas



Auditorias e avaliações regulares de segurança: realização de auditorias e avaliações periódicas de registros de acesso, configurações do sistema e privilégios do usuário para identificar lacunas de segurança

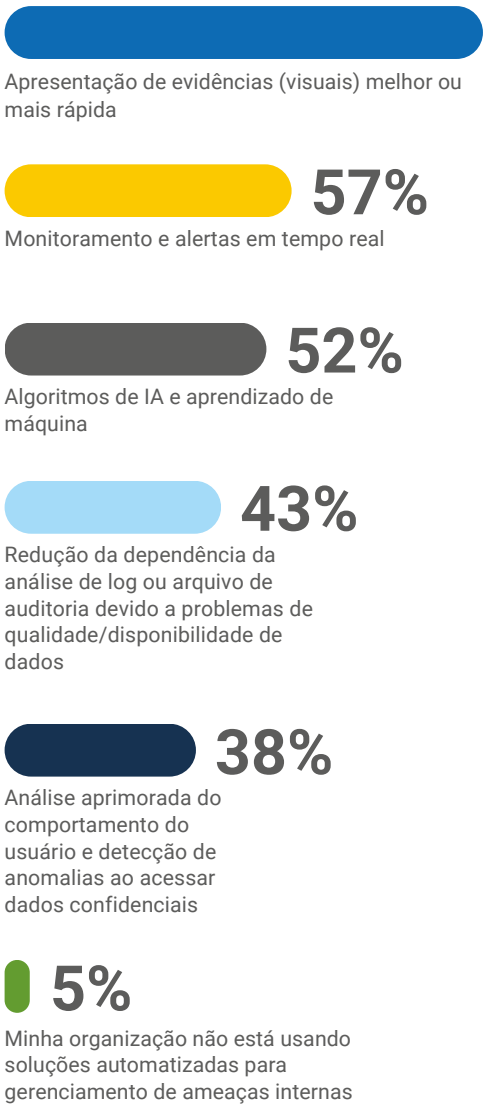


Análise de comportamento e detecção de anomalias: implementação de algoritmos de criação de perfis comportamentais para analisar padrões de comportamento dos funcionários e identificar desvios ou anomalias ao acessar dados confidenciais



Atualmente não temos nenhuma das medidas listadas em vigor

3. Qual das seguintes capacidades você acha que tornaria as soluções automatizadas atualmente usado pela sua organização para gerenciamento de ameaças internas mais eficaz? [selecione os três principais]



O relatório destaca que impressionantes 95% dos entrevistados acham que uma apresentação de evidências visuais melhor ou mais rápida melhoraria seus sistemas automatizados para gerenciamento de ameaças internas. A abordagem mais avançada combina captura de dados tela a tela com funcionalidade de gravação e reprodução, aumentando significativamente a precisão investigativa. Esse recurso permite que os investigadores criem um storyboard visual que mostra exatamente o que o funcionário estava fazendo em um aplicativo, incluindo a reprodução de todas as pesquisas e ações realizadas. Como a atividade é capturada exatamente como aconteceu, não há dados ausentes ou perspectiva alternativa para contestar os fatos.

Ao fornecer aos tomadores de decisão insights baseados em dados, a apresentação de evidências visuais pode dar suporte a ações de mitigação de riscos mais rápidas e informadas. A falta de evidências visuais claras e a dependência de modelos tradicionais podem causar dificuldades, apesar da implementação de outros sistemas, como análise comportamental e sistemas de detecção de anomalias.

O segundo recurso mais desejado, conforme indicado por 57% dos entrevistados, é o monitoramento e alertas em tempo real. Isso enfatiza a necessidade de detecção proativa de ameaças, onde as organizações podem ser imediatamente notificadas sobre anomalias ou atividades suspeitas, permitindo que elas abordem rapidamente potenciais incidentes internos antes que danos significativos ocorram.

A importância atribuída aos algoritmos de IA e aprendizado de máquina, selecionados por 52% dos entrevistados, reflete o crescente reconhecimento do papel que a análise avançada pode desempenhar no aprimoramento do gerenciamento de ameaças internas. No entanto, é importante reconhecer que a eficácia da IA e do aprendizado de máquina depende fortemente da qualidade e disponibilidade dos dados. Sem conjuntos de dados robustos, limpos e abrangentes, a confiabilidade dos modelos preditivos pode ser comprometida, levando a insights imprecisos ou tomada de decisão falha. Dados de alta qualidade são a base para a construção de modelos de IA que sejam precisos e confiáveis. Ao alavancar essas tecnologias, as organizações podem identificar padrões de forma mais eficaz, detectar outliers e descobrir indicadores sutis de intenção maliciosa que podem ser difíceis de discernir por meio de abordagens tradicionais baseadas em regras.

Em contraste, os recursos relacionados à redução da dependência da análise de log ou arquivo de auditoria devido a problemas de qualidade/disponibilidade de dados, bem como análises aprimoradas de comportamento do usuário e detecção de anomalias, foram classificados em menor prioridade. As organizações podem se sentir mais confortáveis com abordagens tradicionais, apesar de suas limitações, e podem não ver uma necessidade urgente de atualizá-las ou alterá-las, acreditando que seus sistemas atuais são adequados. No entanto, à medida que as ameaças internas se tornam mais complexas e avançadas, essas organizações podem presumir erroneamente que estão totalmente protegidas, sem saber dos riscos que ainda não entendem.

Para abordar os principais recursos desejados, nosso relatório recomenda que as instituições financeiras invistam no desenvolvimento de plataformas de análise visual robustas que possam consolidar dados de várias fontes e apresentá-los de forma clara e acionável. Essas plataformas não apenas facilitariam a análise abrangente de dados, mas também permitiriam que as instituições compilassem essas informações como evidências documentadas, o que pode ser crucial para abrir um caso contra um funcionário ou iniciar uma ação legal.

Além disso, as organizações devem implementar sistemas de monitoramento e alerta em tempo real que aproveitem análises avançadas para identificar e responder proativamente a ameaças internas. Adotar soluções baseadas em IA e aprendizado de máquina pode aumentar ainda mais a eficácia desses sistemas, melhorando a precisão e a pontualidade da detecção de ameaças.

4. Com que frequência incidentes de ameaças internas maliciosas afetam sua organização? [selecione a resposta mais apropriada]

A descoberta de que mais de 50% dos entrevistados relatam sofrer algum tipo de incidente malicioso de ameaça interna a cada ano, mesmo que em baixa frequência, ressalta a natureza persistente desse desafio para instituições financeiras. Embora seja reconfortante que a maioria das organizações raramente ou muito raramente (48%) enfrente tais incidentes, a gravidade de cada caso pode ter consequências significativas, desde perdas financeiras, devido ao tamanho potencial das transações, até danos à reputação.

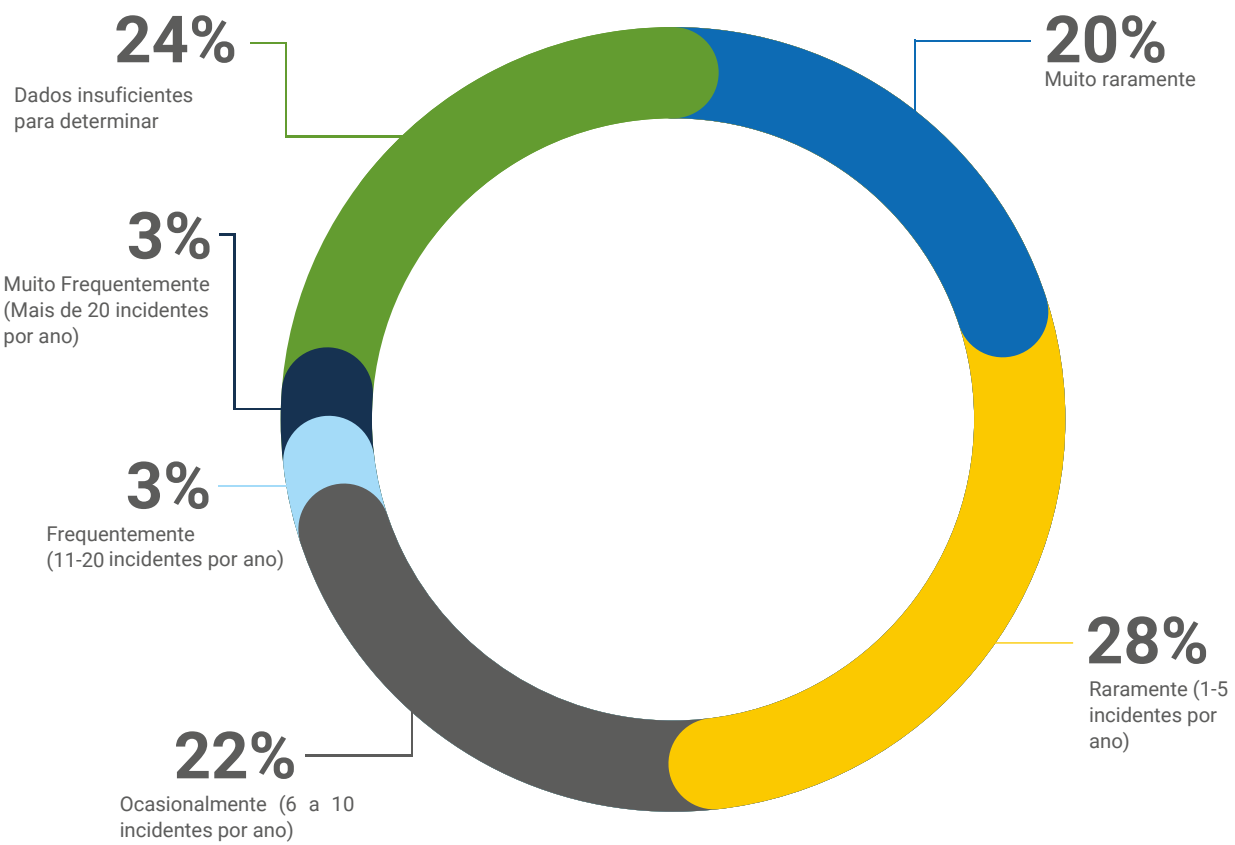
O setor de serviços bancários e financeiros é particularmente vulnerável a ameaças internas sofisticadas e prejudiciais, pois os funcionários desses setores geralmente possuem a experiência financeira para explorar fraquezas em sistemas de controle. De acordo com o último relatório da Association of Certified Fraud Examiners (ACFE), esse setor está entre os mais atingidos por fraudes internas, destacando a necessidade crítica de instituições financeiras fortalecerem suas medidas de segurança. Uma lacuna preocupante nos controles de segurança é revelada por 24% dos entrevistados alegando que não têm dados suficientes para determinar a extensão das ameaças internas em suas organizações.

Isso sugere que uma parcela significativa das instituições financeiras pode não estar ciente da verdadeira escala e impacto dos riscos internos, potencialmente deixando-as expostas a ameaças fatais nos próximos anos se não tomarem medidas para implementar capacidades abrangentes de monitoramento e relatórios.

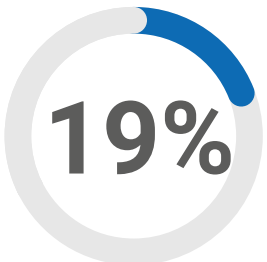
Para abordar isso, nosso relatório recomenda que as instituições financeiras invistam no desenvolvimento de soluções robustas de monitoramento e análise de segurança que forneçam uma compreensão clara e baseada em evidências do cenário de ameaças internas em suas organizações. Ao aprimorar seus processos de rastreamento e relatórios de incidentes, as instituições podem identificar melhor os padrões, quantificar a frequência e impacto de incidentes e tomar decisões informadas para fortalecer suas defesas.

Além disso, as organizações devem considerar a implementação de plataformas avançadas de análise de segurança que podem consolidar dados de várias fontes, detectar anomalias no comportamento do usuário e fornecer alertas em tempo real sobre ameaças potenciais.

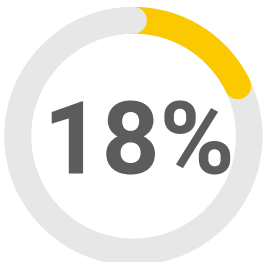
Ao obter melhor visibilidade sobre a natureza evolutiva dos riscos internos, as instituições financeiras podem abordar vulnerabilidades de forma proativa e desenvolver estratégias de mitigação mais eficazes.



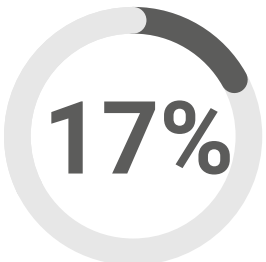
5. Qual é o tipo de ameaça interna mais predominante na sua organização?
[selecione uma resposta]



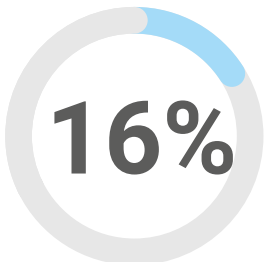
Roubo de dados: acesso não autorizado ou cópia de dados confidenciais



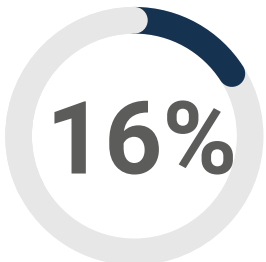
Acesso não autorizado: uso de credenciais para acessar áreas não permitidas



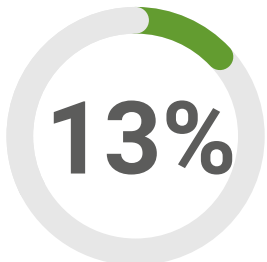
Roubo financeiro: por exemplo, peculato ou transações fraudulentas



Negligência: ações acidentais que comprometem a segurança



Violações de política: empresa infratora políticas ou procedimentos



Sabotar: interrupção intencional ou danos aos sistemas ou operações

O relatório mostra que as organizações consideram o roubo de dados como a ameaça interna mais significativa, com quase 20% dos entrevistados identificando-o como um problema importante. Isso não é surpreendente, pois o acesso não autorizado, o manuseio incorreto ou a cópia de dados confidenciais do cliente podem ser um risco sério para as empresas, levando a danos à reputação e violações regulatórias.

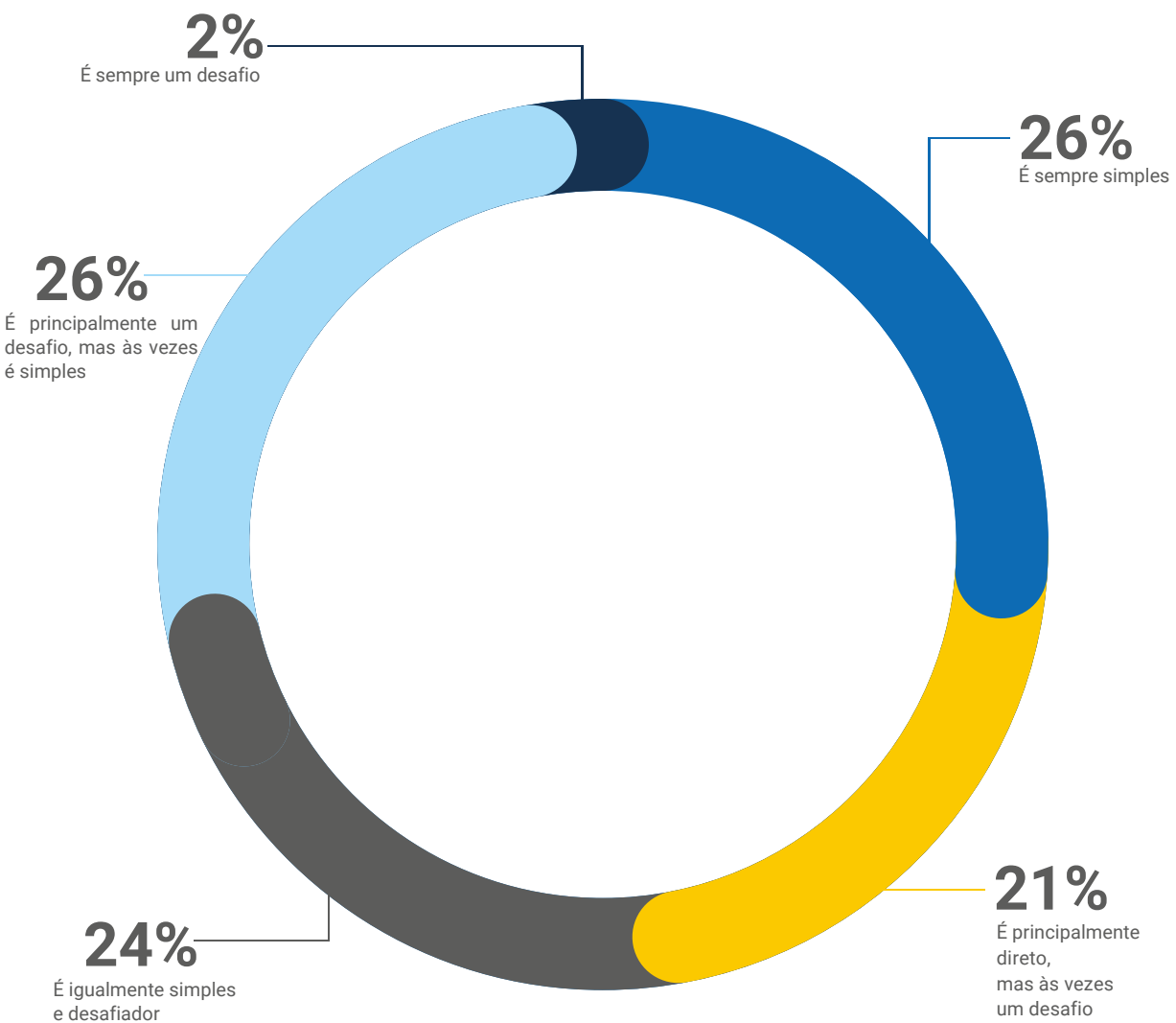
Embora o roubo financeiro, como apropriação indébita ou transações fraudulentas, seja uma preocupação para o setor, é notável que ele esteja abaixo do roubo de dados em termos de prevalência.
Isso pode indicar que as instituições financeiras historicamente colocam uma ênfase maior na proteção de seus ativos, embora o risco de ameaças internas com motivação financeira não deva ser subestimado.

Outros tipos de ameaças prevalentes, como acesso não autorizado, negligência e violações de políticas, demonstram a natureza diversa dos riscos internos enfrentados pela indústria. Essas ameaças podem não apenas permitir perdas financeiras ou de dados diretas, mas também servir como portas de entrada para ataques mais sofisticados, potencialmente explorados por agentes de ameaças externas por meio de engenharia social ou vetores como comprometimento de e-mail comercial (BEC) e fraude de pagamento push autorizado (APP).

Para lidar com esse desafio multifacetado, as instituições financeiras devem adotar uma abordagem holística para o gerenciamento de ameaças internas. Isso deve incluir uma combinação de controles de acesso robustos, análises avançadas de comportamento do usuário, programas abrangentes de treinamento de funcionários e planos claros de resposta a incidentes. Ao lidar com todo o espectro de vetores de ameaças internas, as organizações podem proteger melhor seus ativos, reputação e postura geral de segurança.

6. Quão simples é para sua organização encontrar evidências quando há suspeitas de atividades de ameaças interna?

[selecione uma resposta]



Embora 25% dos entrevistados relatem que encontrar evidências é simples, é preocupante que 71% das organizações tenham declarado que o processo envolve algum tipo de desafio. Isso sugere que muitas organizações de serviços financeiros ainda lutam com o processo de coleta, análise e apresentação de evidências de atividades internas suspeitas.

Esse é um problema recorrente que remonta ao início da pesquisa. Embora as suspeitas de fraude interna surjam com frequência, provar esses casos pode ser desafiador devido à insuficiência de evidências. Por exemplo, pesquisar e analisar registros para expor ameaças internas e compilar evidências sobre esquemas complexos de fraude geralmente carece de contexto e consome muito tempo. Essa dificuldade geralmente faz com que a fraude interna seja menos visível, subnotificada ou totalmente não notificada. Consequentemente, é erroneamente percebida como um risco menor; as organizações operam sob a suposição de que estão cientes de ameaças potenciais quando, na realidade, podem estar ignorando riscos significativos devido à falta de visibilidade dessas atividades secretas.

Para enfrentar esses desafios, as instituições financeiras devem investir no desenvolvimento de protocolos de investigação padronizados e equipar suas equipes com sistemas dedicados de gerenciamento de casos e ferramentas de análise forense baseadas em evidências. Essas capacidades podem agilizar o processo de coleta de evidências, melhorar a colaboração entre departamentos e garantir que informações críticas sejam capturadas e apresentadas de forma clara e acionável.

Além disso, as organizações devem considerar fornecer treinamento especializado para seu pessoal de conformidade, RH e segurança sobre as melhores práticas para investigações de ameaças internas. Ao desenvolver expertise interna e aprimorar as capacidades investigativas gerais da organização, as instituições financeiras podem descobrir e responder de forma mais eficaz a atividades internas suspeitas.

7. A próxima lei do Reino Unido sobre "Falha na Prevenção de Fraudes" penaliza as organizações que não conseguem prevenir fraude de funcionários beneficiando a organização.

Como você prevê que essa nova legislação (prevista para o 2º semestre de 2024 ou 1º semestre de 2025) mudará a forma como sua organização prioriza a detecção e prevenção de ameaças internas?

[selecione a resposta mais apropriada]

As respostas a esta pergunta são distribuídas uniformemente, com 29% dos entrevistados afirmando que não mudariam sua abordagem apesar da nova lei entrar em vigor. Esta é uma descoberta preocupante, pois espera-se que as organizações tenham procedimentos razoáveis de prevenção de fraudes em vigor, apesar da espera por orientação oficial, e as empresas que optarem por não priorizar a conformidade enfrentarão penalidades significativas e potenciais danos à reputação.

Uma possível explicação para essa falta de preocupação é que essas organizações podem já ter programas robustos de gerenciamento de ameaças internas em vigor e se sentirem confiantes em sua capacidade de atender aos novos requisitos regulatórios. Embora este possa ser o caso, também é possível que alguns entrevistados estejam subestimando o impacto potencial da lei e a necessidade de reavaliar sua abordagem geral para detecção e prevenção de ameaças internas.

A decisão de não priorizar a lei – conscientemente ou não – também pode ser devido a uma mudança interna de foco em direção a esquemas de treinamento de funcionários e programas de conscientização, conforme descrito nos resultados da pergunta 10.

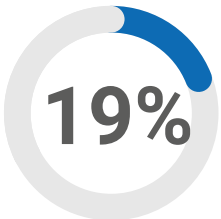
Independentemente de seu estado atual, cerca de 47% dos entrevistados estão planejando priorizar mais implementações para entender e gerenciar melhor os riscos de fraude, refletindo um compromisso robusto para abordar os riscos de fraude para melhores resultados. Isso indica que as organizações estão atualmente em busca de implementar programas, práticas e sistemas de gerenciamento de risco mais robustos.

Todas as instituições financeiras devem realizar uma revisão abrangente de suas políticas, controles e procedimentos de resposta existentes. Isso deve incluir a realização de avaliações de lacunas para identificar áreas que exigem fortalecimento, atualização de políticas internas e programas de treinamento para atender aos novos requisitos legais e implementação de soluções avançadas de monitoramento e análise para aprimorar sua capacidade de detectar e responder a atividades suspeitas.

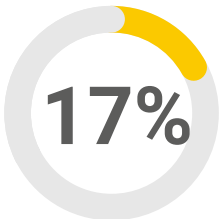
Ao abordar proativamente as implicações da lei "Failure to Prevent Fraud", as organizações podem não apenas evitar penalidades potencialmente severas, mas também fortalecer sua resiliência geral contra ameaças internas, protegendo, em última análise, seus ativos, reputação e confiança do cliente.

8. Qual é a principal preocupação da sua organização em relação à privacidade no contexto de monitoramento de informações privilegiadas?

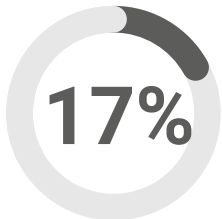
[selecione a resposta mais apropriada]



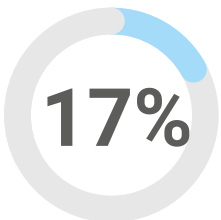
Garantir que as atividades de monitoramento sejam proporcionais e justificadas (evitando monitoramento excessivo)



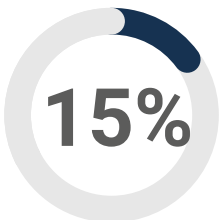
Preocupações com a privacidade dos funcionários em relação ao monitoramento de atividades que não estão relacionadas à segurança (por exemplo, histórico de navegação pessoal, e-mails, mensagens)



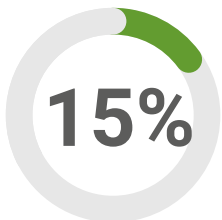
Garantir uma cultura de confiança dentro da organização



Transparência sobre as práticas de monitoramento de funcionários e o uso de dados coletados



Conformidade legal com os regulamentos de privacidade dos funcionários (por exemplo, GDPR, CCPA)



Equilibrando a privacidade dos funcionários com as necessidades de monitoramento organizacional

Os resultados da pesquisa demonstram que as instituições financeiras estão considerando ativamente as preocupações com a privacidade no contexto do monitoramento de ameaças internas, com uma pequena maioria dos entrevistados (19%) enfatizando a necessidade de garantir que as atividades de monitoramento sejam "proporcionais e justificadas" e evitar o monitoramento excessivo.

Essa ênfase na proporcionalidade reflete o equilíbrio crítico que as organizações devem atingir entre o monitoramento eficaz e o respeito à privacidade dos funcionários. Práticas de monitoramento excessivamente intrusivas ou desproporcionais podem não apenas corroem a confiança e a moral dentro da força de trabalho, mas também expõem a organização a potenciais riscos legais e de reputação.

Para enfrentar esse desafio, nosso relatório de instituições financeiras deve implementar soluções e práticas de monitoramento que priorizem a minimização de dados, como monitoramento baseado em rede e o uso de técnicas de pseudonimização. Ao coletar e processar apenas as informações essenciais necessárias para fins de segurança, as organizações podem atender aos seus objetivos de detecção e prevenção de ameaças internas, minimizando o impacto na privacidade dos funcionários.

Igualmente importante é a necessidade de transparência e comunicação clara em torno das práticas de monitoramento. As organizações devem desenvolver e articular claramente suas políticas sobre monitoramento de funcionários, explicando o propósito, o escopo e as salvaguardas em vigor para proteger informações pessoais. Ao envolver os funcionários e promover uma cultura de confiança, as instituições financeiras podem aliviar preocupações e garantir que seus esforços de gerenciamento de ameaças internas sejam percebidos como necessários e justificados.

9. Quão bem você acha que as estratégias de gerenciamento de risco da sua organização são eficazes em abordar a potencial sobreposição e interconexão entre fraudes internas e incidentes de fraude externa?

[selecione a resposta mais apropriada]

Embora a maioria dos entrevistados (65%) relate que suas estratégias de gerenciamento de risco são muito ou moderadamente eficazes para lidar com a sobreposição entre fraude interna e externa, é preocupante que 35% das organizações ainda estejam lutando com seu nível de gerenciamento de risco, sugerindo que ainda são necessárias melhorias adicionais para combater as ameaças internas de forma eficaz.

A incapacidade de gerenciar efetivamente a interconexão entre as ameaças de fraude interna e externa pode deixar as instituições financeiras vulneráveis a riscos significativos. As ameaças internas podem ser exploradas por atores externos por meio de técnicas como comprometimento de e-mail comercial ou engenharia social, enquanto ameaças externas também podem ser habilitadas ou amplificadas por insiders mal-intencionados com acesso a informações e sistemas confidenciais.

Conforme enfatizado nas respostas à pergunta 2, as instituições financeiras precisam investir em soluções de monitoramento integradas e recursos de compartilhamento de inteligência de ameaças para aprimorar sua postura geral de segurança. Elas podem capturar o comportamento do usuário em tempo real em sistemas e serviços, como monitoramento de vários aplicativos de todos os canais, um grande benefício no caso de sobreposições potenciais e interconexão entre incidentes de fraude internos e externos.

Ser capaz de capturar o comportamento do usuário em tempo real em todos os sistemas é de grande ajuda, pois fraudes externas podem ser mais visíveis para detectar, enquanto fraudes internas podem ser mais sutis e difíceis de identificar.

Além disso, as instituições financeiras devem estabelecer equipes multifuncionais e protocolos de resposta a incidentes que reúnam especialistas de áreas como conformidade, fraude, segurança cibernética e gerenciamento de risco. Ao promover a colaboração e coordenar seus esforços, essas equipes podem mitigar de forma mais eficaz os riscos complexos e interconectados apresentados por ameaças internas e externas.

33%

Muito eficazmente: nossas estratégias de gerenciamento de risco abordam a sobreposição entre fraude interna e incidentes de fraude externa

32%

Moderadamente eficaz: as estratégias de gestão de risco abordam alguns aspetos da sobreposição entre fraude interna e incidentes de fraude externa, mas há espaço para melhorias

34%

Não muito eficazmente: as estratégias de gestão de risco abordam inadequadamente a sobreposição entre fraude interna e incidentes de fraude externa, deixando potenciais vulnerabilidades na proteção de ativos e reputação

1%

De forma alguma eficaz: as estratégias de gestão de risco falham completamente em abordar a sobreposição entre fraude interna e incidentes de fraude externa, deixando ativos e reputação vulneráveis a riscos e ameaças significativas

10. Qual das seguintes opções é a principal prioridade para o gerenciamento de ameaças internas nos próximos 12 meses?

[selecione uma opção]

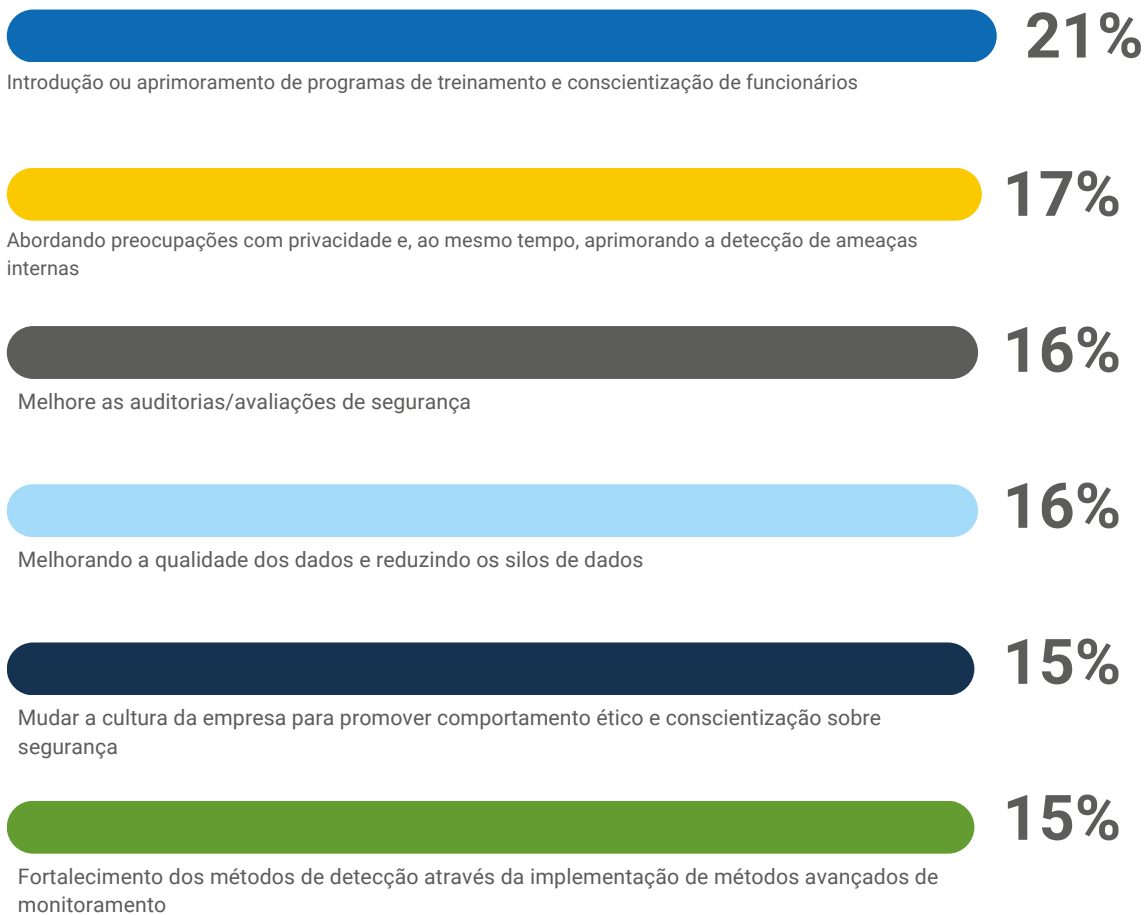
As respostas foram distribuídas uniformemente e demonstram uma variedade de visões, indicando que os profissionais de serviços financeiros têm múltiplas prioridades para melhorar ainda mais suas estratégias de ameaças de gestão.

Mais de um quinto dos entrevistados (21%) identificou a introdução ou aprimoramento de programas de treinamento e conscientização de funcionários como sua principal prioridade para o gerenciamento de ameaças internas nos próximos 12 meses. Essa ênfase no ser humano pode ensinar a equipe a detectar sinais de alerta e ser capacitada para avaliar riscos e criar uma força de trabalho mais vigilante e engajada que sirva como uma camada adicional de defesa.

Quaisquer iniciativas de treinamento de funcionários devem ser intimamente integradas a outros componentes da estratégia de gerenciamento de ameaças internas, como a implementação de tecnologias avançadas de monitoramento, o aprimoramento da qualidade e acessibilidade de dados e a promoção de comportamento ético por meio de atualizações de políticas e iniciativas de liderança.

Ao alinhar esses vários fluxos de trabalho, as instituições financeiras podem criar uma abordagem abrangente e multifacetada para lidar com o cenário de ameaças internas. Os números também indicam que as organizações estão buscando sistemas mais sofisticados que podem melhorar a qualidade dos dados e reduzir silos (16% dos entrevistados), sugerindo que uma abordagem holística que aprimore ainda mais a colaboração entre departamentos impulsionaria sua abordagem para mitigar o risco de fraude interna.

Cerca de 17% dos entrevistados relataram que abordar questões de privacidade e, ao mesmo tempo, aprimorar a detecção de ameaças internas é considerado uma prioridade, o que sugere que os entrevistados estão considerando ativamente as questões de privacidade no contexto do monitoramento de ameaças internas, considerando sistemas que podem resolver complicações legais e éticas e implementar perfeitamente as regulamentações de proteção de dados.



Conclusão

Incidentes de fraude interna são agora uma séria ameaça para instituições financeiras (IFs).

O relatório mostra que as IFs estão cientes dos perigos representados por várias ameaças de fraude interna, incluindo acesso não autorizado a áreas específicas, roubo financeiro, violações de políticas e roubo de dados.

Para fortalecer ainda mais suas defesas, muitas IFs estão gerenciando o risco interno implementando tecnologias de monitoramento, que ajudam a monitorar as ações e comunicações digitais dos funcionários dentro da organização. Consequentemente, elas estão considerando ativamente as preocupações com a privacidade, priorizando complicações legais e éticas juntamente com os regulamentos de proteção de dados.

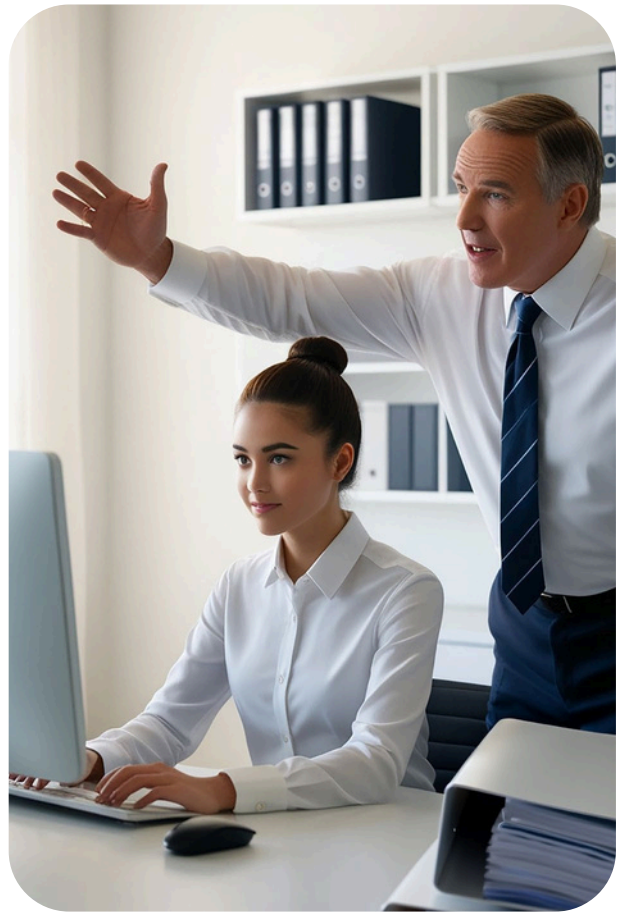
Apesar das medidas ativas para proteger contra ameaças internas, mais de 70% dos entrevistados consideram a coleta de evidências desafiadora e 35% lutam com o gerenciamento de riscos, indicando a necessidade de mais melhorias. As organizações devem implementar novas medidas e fortalecer as existentes. Embora muitas IFs se sintam confiantes em suas salvaguardas atuais, a preparação sempre pode ser aprimorada por meio de maior treinamento da equipe, colaboração com partes interessadas internas e externas e a implementação de tecnologias de monitoramento adequadas.

As organizações precisam implementar novas medidas enquanto fortalecem as anteriores. Embora muitas IFs estejam confiantes de que estão em boas mãos quando se trata de fraude interna, a preparação sempre pode ser melhorada aumentando o treinamento da equipe, ao mesmo tempo em que colabora com as partes interessadas internas e organizações externas e implementa tecnologias de monitoramento adequadas.

À luz do atual clima econômico instável em todo o Reino Unido e na Europa, juntamente com novas regulamentações iminentes que ocorrerão em breve, as IFs não devem subestimar o risco crescente de fraude interna. Abordar proativamente a fraude interna por meio de monitoramento e atualizações regulares de protocolos de segurança podem reduzir significativamente o risco de incidentes. Aproveitar tecnologias avançadas de monitoramento pode fornecer insights mais profundos sobre ameaças potenciais e aumentar a precisão da detecção de fraudes. Também é crucial que essas tecnologias apresentem evidências imediatamente, em vez de levar muito tempo para concluir a análise. Uma estratégia holística que integre soluções tecnológicas com abordagens centradas no ser humano, como treinamento de funcionários e promoção da cultura ética, é essencial para a prevenção abrangente de fraudes.

A colaboração com colegas do setor e a participação em redes de compartilhamento de inteligência de ameaças podem fornecer insights valiosos e fortalecer a postura geral de segurança. Ficar à frente das mudanças regulatórias e garantir a conformidade com novas leis, como a legislação do Reino Unido "Falha na Prevenção de Fraudes", será crucial para manter a confiança e evitar penalidades. A melhoria contínua das medidas de prevenção de fraudes, informada por avaliações e feedback regulares, ajudará as IFs a permanecerem resilientes contra ameaças em evolução.

Para estarem mais bem preparadas, as IFs devem continuar a investir nas tecnologias mais recentes e garantir que seu pessoal esteja ciente das ameaças e ramificações da fraude interna.



Sobre Bottomline

A Bottomline ajuda as empresas a transformar a maneira como pagam e recebem. Líder global em pagamentos empresariais e gestão de caixa, a Bottomline é uma plataforma abrangente e segura soluções modernizam pagamentos para empresas e instituições financeiras globalmente. Com mais de 35 anos de experiência, movimentando mais de US$ 10 trilhões em pagamentos anualmente, a Bottomline está comprometida em gerar resultados impactantes para os clientes ao reimaginar pagamentos empresariais e fornecer soluções que agreguem valor ao resultado final.

RxCorp
Soluções em TIC


11 3032 2221


rxcorp@rxcorp.com.br

rxcorp.com.br


rxcorp


rxcorpsoluçõesemtic