appgate

iSMG
INFORMATION SECURITY
MEDIA GROUP

Faces of Fraud 2023

A Evolução da Fraude Online em 2023 e as Melhores Práticas para Fechar as Lacunas

Author: ISMG

Sumário

Sobre esta pesquisa

Esta pesquisa foi conduzida pelo Information Security Media Group e Appgate no segundo trimestre de 2023. No total, mais de 150 instituições financeiras participaram deste estudo, principalmente dos Estados Unidos e Canadá.

Introdução 3

Alguns Números 4

Resumo Executivo 5

A Lacuna de Percepção 6

Conciencia vs. Voluntad 7

Resultados Faces of Fraud 2023 8

Conclusões 18

Análise da Pesquisa 20

Sobre Appgate:

A Appgate é a empresa de acesso seguro. Reforçamos a forma como as pessoas trabalham e se conectam, fornecendo soluções desenvolvidas especificamente com base nos princípios de segurança Zero Trust. Essa abordagem de segurança definida pelas pessoas permite conexões rápidas, simples e seguras de qualquer dispositivo e local para cargas de trabalho em qualquer infraestrutura de TI em ambientes na nuvem, locais e híbridos. A Appgate ajuda empresas e agências governamentais em todo o mundo a começar de onde estão, acelerar sua jornada rumo ao Zero Trust e planejar seu futuro. Mais informações podem ser acessadas em Appgate.com.

Introdução

Bem-vindos ao nosso relatório que resume a pesquisa 'Faces of Fraud survey 2023'. Agradecemos muito aos nossos colaboradores da indústria que responderam às nossas perguntas com franqueza, o que nos permitiu oferecer uma visão das fraudes que mais preocupam os serviços financeiros em 2023. Também podemos observar como a indústria como um todo está sendo afetada e permitimos que você veja como seus colegas estão priorizando maneiras de se proteger.

Isso inclui identificar em quais áreas as instituições financeiras de hoje estão focando seus investimentos em tecnologias de prevenção de fraudes para o próximo ano.

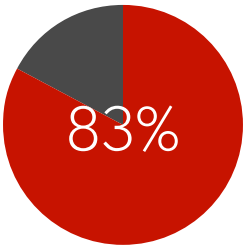
Quando se trata de ameaças, cada nova tecnologia dá origem a novas fraudes à medida que os atacantes evoluem e inovam, mas nossas defesas cibernéticas também estão evoluindo. Então, o que devemos estar observando no próximo ano e como devemos responder?

Os dados compartilhados neste relatório ajudarão a informar sua estratégia de prevenção de fraudes para o próximo ano, não apenas em relação às ameaças que você enfrenta e à tecnologia que implementa para evitá-las, mas também para estabelecer um ponto de referência sobre o que é realista em termos de conquistas.

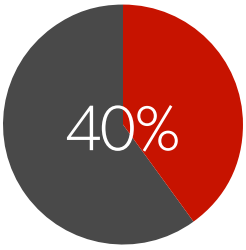
Atenciosamente,,

TONY MORBIN
Editor Ejecutivo, EU
Information Security Media Group
Tmorbin@ismg.io

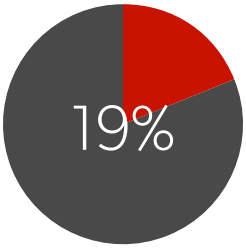
Alguns Números



83% dos entrevistados afirmam que os esquemas de fraude atuais estão evoluindo muito rapidamente para que possam acompanhar.



Apenas 40% das organizações têm a visibilidade necessária para identificar o impacto de um ataque de phishing.



Apenas 19% das organizações têm a capacidade de identificar o fraude em tempo real.

Resumo Executivo

A fraude é um problema contínuo, e os atacantes veem cada avanço na tecnologia como uma oportunidade para explorar a crescente complexidade, as superfícies de ameaça em expansão e possíveis novas brechas em nossas defesas.

Um exemplo? Assim que a inteligência artificial generativa se tornou amplamente utilizada, os fraudadores começaram a explorá-la para identificar vulnerabilidades, acelerar novos ataques e criar iscas mais convincentes, incluindo deepfakes. Eles também a utilizaram como uma palavra-chave atraente. Os atores de ameaças continuam explorando as complexidades criadas por infraestruturas de TI dispersas, digitalização, migração para a nuvem, a mudança para forças de trabalho remotas e híbridas, e o uso de dispositivos pessoais (BYOD).

A preocupação com o impacto das mudanças rápidas é refletida nos resultados da pesquisa 'Faces of Fraud' deste ano, onde os entrevistados do setor financeiro afirmam que a principal vulnerabilidade é que os esquemas de fraude atuais estão evoluindo muito rapidamente para que possam acompanhar. Embora a taxa de mudança tenha sido um problema anual nesta série 'Faces of Fraud', o número de entrevistados que o veem como sua principal preocupação quase dobrou, passando de 43% em 2019 para 83% este ano.

Uma vulnerabilidade evidente que permite tais fraudes é a falta de visibilidade que as organizações têm para identificar o impacto de um ataque de phishing, com 55% relatando ter visibilidade limitada e 5% admitindo que não têm nenhuma. Menos de metade, apenas 40%, afirma ter a visibilidade detalhada necessária para identificar o impacto de um ataque de phishing, sugerindo que esta área continua sendo um alvo de melhoria.

A Lacuna de Percepção

Na pesquisa deste ano, as percepções contraditórias são muito reveladoras ao comparar as respostas dos entrevistados a diferentes perguntas. Por exemplo, ao avaliar a capacidade da sua organização financeira para identificar e mitigar a fraude, 60% dos entrevistados dizem que é superior ou acima da média; 37% dizem que é médio; e 3% a classificam como abaixo da média.

No entanto, embora 97% dos entrevistados afirmem ter uma capacidade média ou superior para detectar e mitigar a fraude, apenas 19% dizem que podem identificar um ataque de fraude em tempo real. Ainda menos, 11%, afirmam que podem mitigar em tempo real. Vinte por cento das organizações que levam mais de uma semana para identificar a fraude não têm a capacidade de fazê-lo ou não sabem se a têm. Vinte e nove por cento das organizações que levam mais de uma semana para mitigar a fraude também dizem que não têm a capacidade de fazê-lo ou não sabem se a têm. É particularmente preocupante que os tempos de mitigação tenham aumentado em comparação com pesquisas anteriores desta série; a porcentagem daqueles que podem fazê-lo em tempo real diminuiu 3% desde 2020. Mesmo levando em consideração qualquer margem de erro estatístico, está claro que a situação não está melhorando.

Portanto, não é surpreendente que haja uma lacuna de percepção entre o quão sólida é a postura de segurança de uma organização contra o fraude em comparação com o que a organização acredita que é. A lacuna tem sido notavelmente consistente ao longo da série de pesquisas, com alta confiança nas capacidades. No Faces of Fraud survey 2021, quase três quartos dos entrevistados disseram que estavam confiantes ou muito confiantes de que a alta administração compreendia o investimento necessário para combater e mitigar as crescentes ameaças de fraude. E quase três quartos dos entrevistados na pesquisa de 2020 disseram que estavam confiantes ou muito confiantes de que os executivos de nível C 'entendiam' as medidas de investimento contra o fraude. No entanto, em ambos os casos, quase metade das instituições entrevistadas afirmou ter visibilidade limitada ou nenhuma para identificar o impacto de tal ataque.

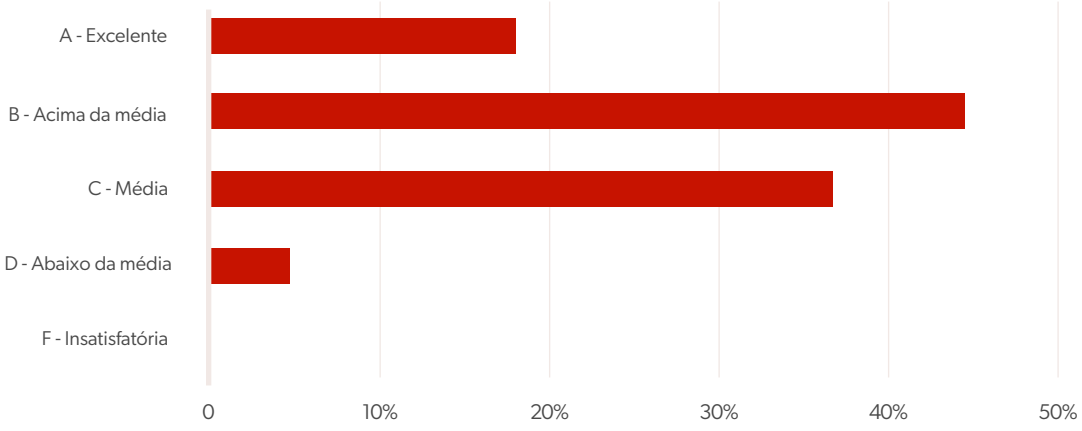
Conciencia vs. Disposición

Outra desconexão é que, embora 57% dos entrevistados afirmem que os sistemas de detecção e monitoramento de inteligência de fraude têm o impacto mais significativo na prevenção de perdas por fraude, apenas 43% dos entrevistados afirmam planejar investir em sistemas de detecção e monitoramento de inteligência de fraude nos próximos 18 meses. A inferência é que a consciência sobre os benefícios das modernas ferramentas de prevenção de fraude supera a disposição ou capacidade de se comprometer com gastos nessas mesmas ferramentas.

Também pode ser que as organizações financeiras estejam adotando uma abordagem muito segmentada em relação às ferramentas de prevenção de fraudes, já que 80% dos entrevistados afirmam que seus controles não se comunicam entre si em diferentes partes da organização. Além disso, persiste uma complacência na crença de que as organizações já estão fazendo o suficiente para prevenir o fraude, apesar da evidência sugerir o contrário.

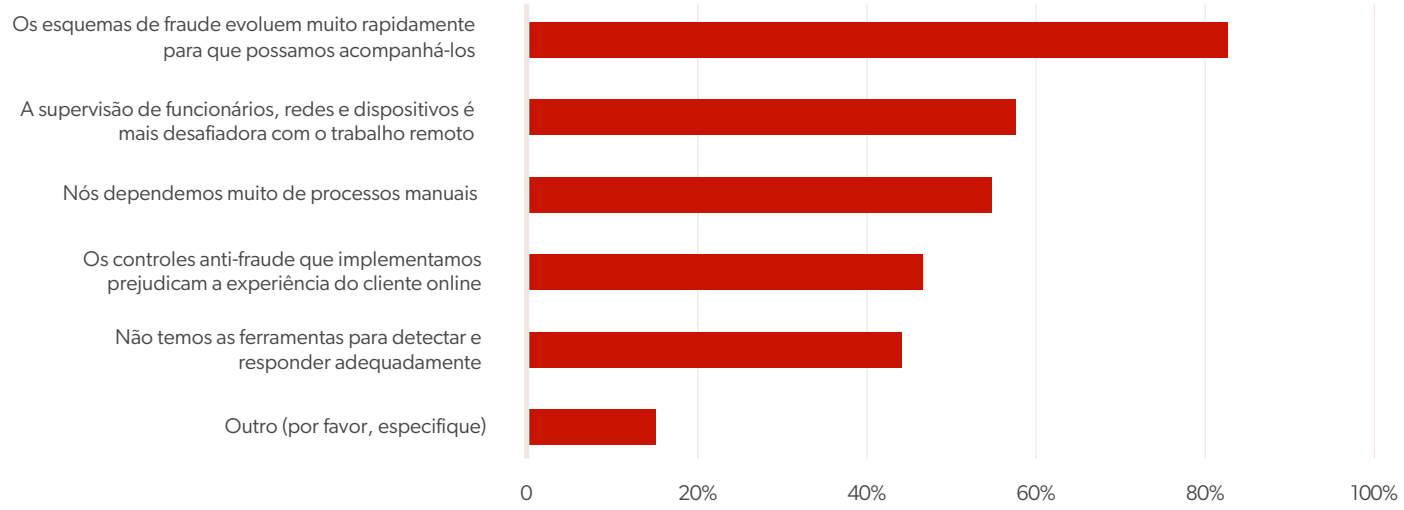
Resultados del Faces of Fraud Survey 2023

¿Que nota você daria para a capacidade de sua organização de identificar e mitigar fraudes?



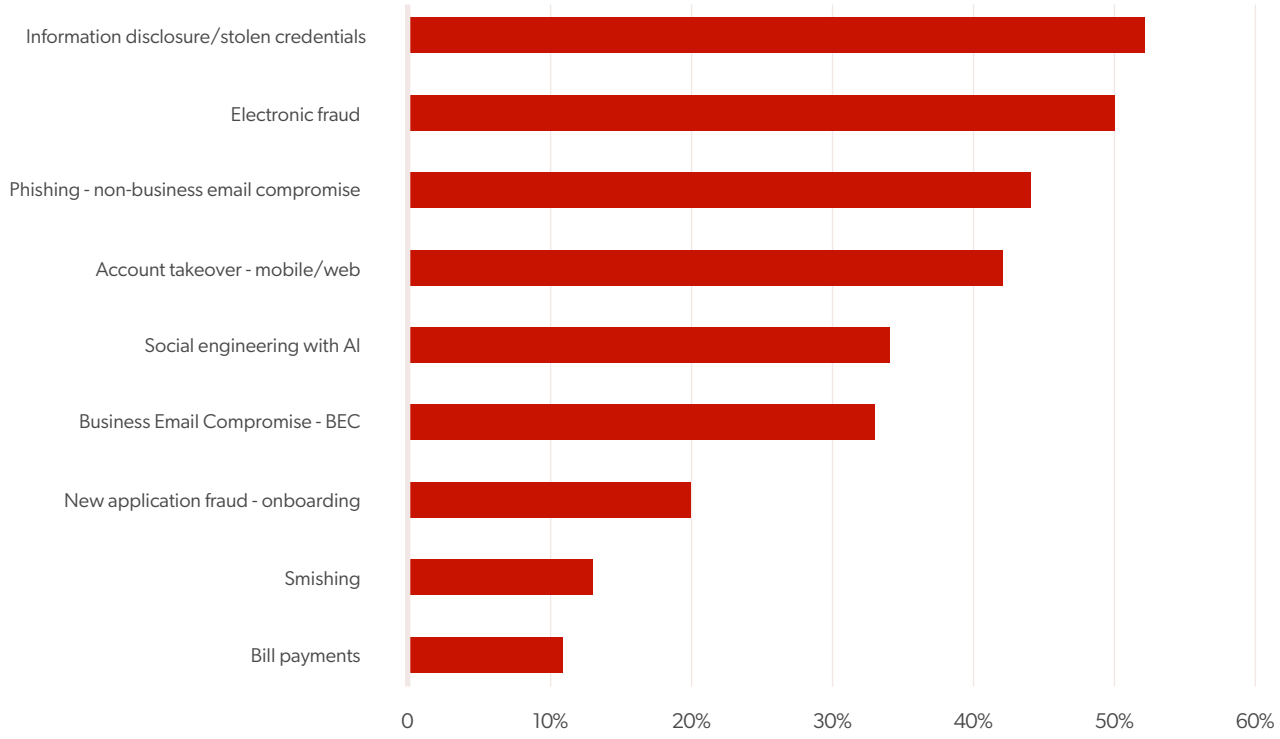
Não é surpreendente que a maioria dos entrevistados, 60%, acredite que sua capacidade de identificar e mitigar a fraude seja excelente ou acima da média, enquanto 37% considera que é média e apenas 3% acredita que está abaixo da média.

¿Quais são, na sua opinião, as três principais vulnerabilidades em suas defesas contra fraudes?



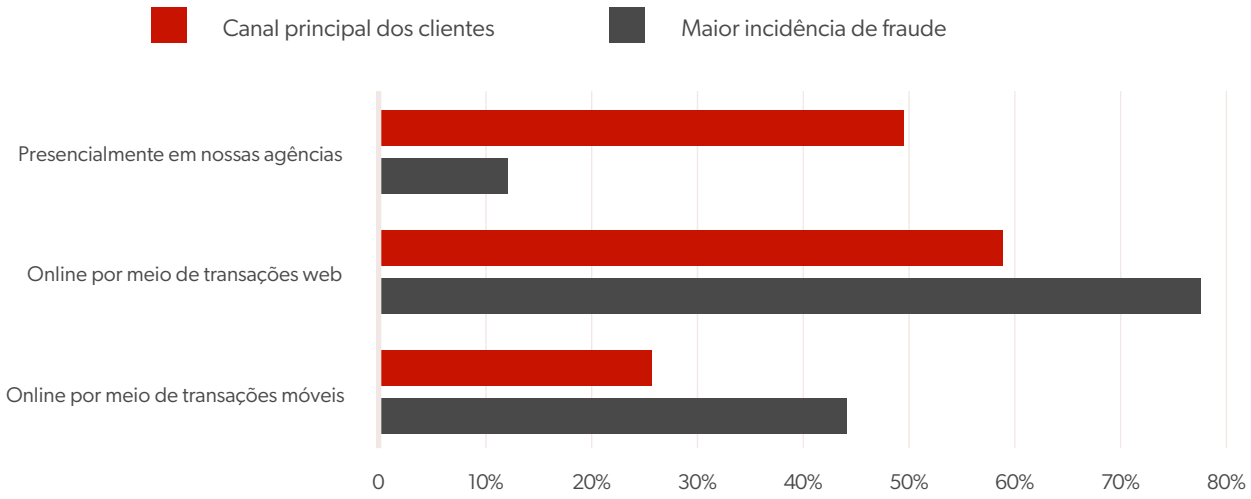
A principal vulnerabilidade para os entrevistados é que os esquemas de fraude atuais estão evoluindo muito rapidamente para que possam acompanhar, com 83%. Em segundo lugar, com 57%, está o problema relacionado com a supervisão de funcionários, redes e dispositivos tornando-se mais desafiador com as equipes de trabalho remotas. E 55% dos entrevistados afirmam estar preocupados com uma dependência excessiva de processos manuais.

Por favor, selecione os três esquemas de fraude mais preocupantes para a sua instituição no próximo ano



O esquema de fraude mais preocupante para as instituições durante o restante de 2023 e 2024 é a divulgação de informações/credenciais roubadas, com 52%, seguido de perto pelo fraude eletrônico com 50%. O phishing (sem comprometimento de e-mail corporativo) fica em terceiro lugar, com 44%, seguido pelo controle de contas (móveis/web) com 42%.

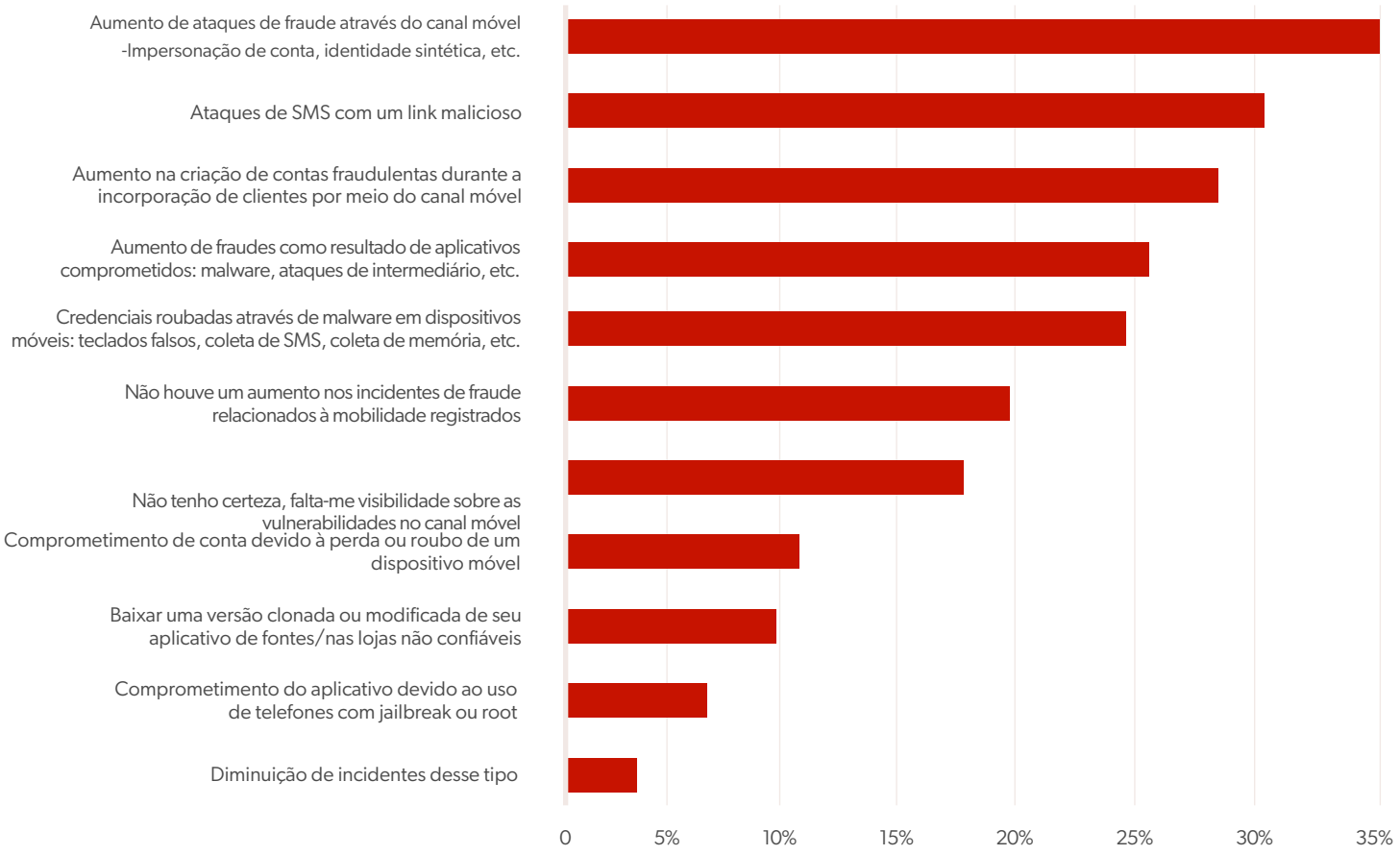
Hoje em dia, qual é o canal principal que seus clientes usam para realizar negócios com sua instituição? Qual canal tem a maior incidência de fraudes?



Os entrevistados relatam que o canal principal utilizado pelos clientes para fazer negócios com a organização são as transações online, com 44%. Eles também afirmam que este canal tem a maior incidência de fraudes, com 58%, superando amplamente o uso. Parece que os gerentes de risco, quer saibam ou não, estão aceitando o potencial de níveis mais altos de atividades fraudulentas em troca de um aumento no volume de negócios por meio dos canais online.

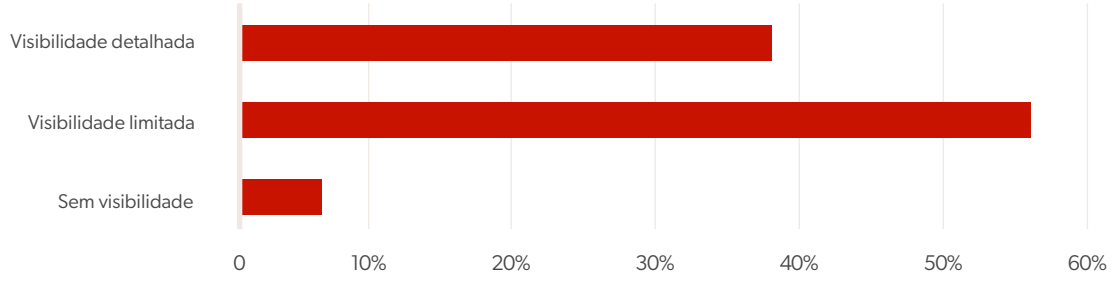
Em contraste, os entrevistados dizem que os negócios presenciais nas agências representam 37% do uso, mas apenas 9% das fraudes. As transações móveis ocupam o terceiro lugar em termos de uso, com 19%, mas o segundo lugar em fraudes, com 33%.

No último ano, você experimentou algum dos seguintes incidentes de fraude especificamente relacionados ao canal móvel?



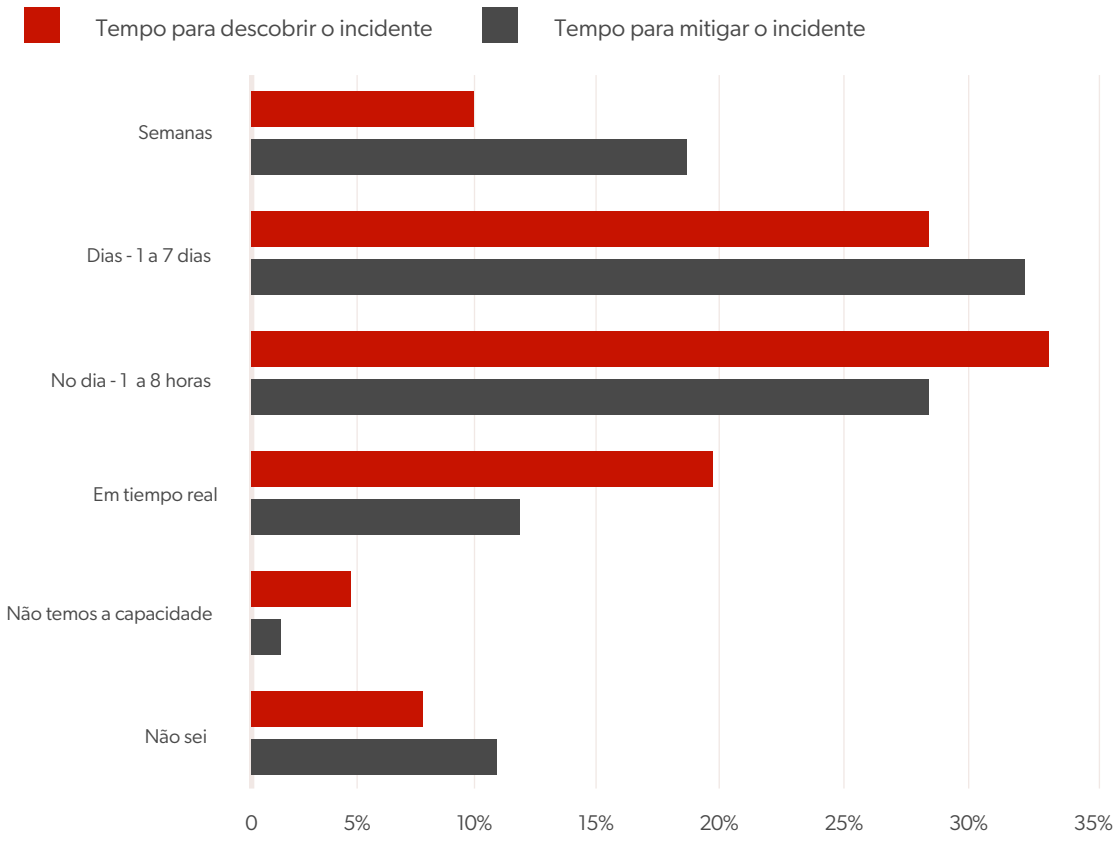
Ainda que não tenha havido um método de ataque específico destacado, 35% dos entrevistados relatam um aumento nos incidentes de fraude através do canal móvel (suplantação de identidade de conta, identidade sintética, etc.), 30% dizem que os ataques de SMS com um link malicioso estão em alta, e 28% relatam um aumento na criação de contas fraudulentas (incorporação de clientes) através do canal móvel

¿Quanto à visibilidade da sua organização para identificar o impacto de um ataque de phishing?



A maioria das organizações, 62%, afirma ter visibilidade limitada ou nenhuma quando se trata de identificar o impacto de um ataque de phishing, e apenas 38% afirma ter visibilidade detalhada. Os resultados sugerem que esta área ainda é uma oportunidade de melhoria.

Em média, quanto tempo sua organização estima levar para descobrir/mitigar um incidente de fraude depois que ocorre?

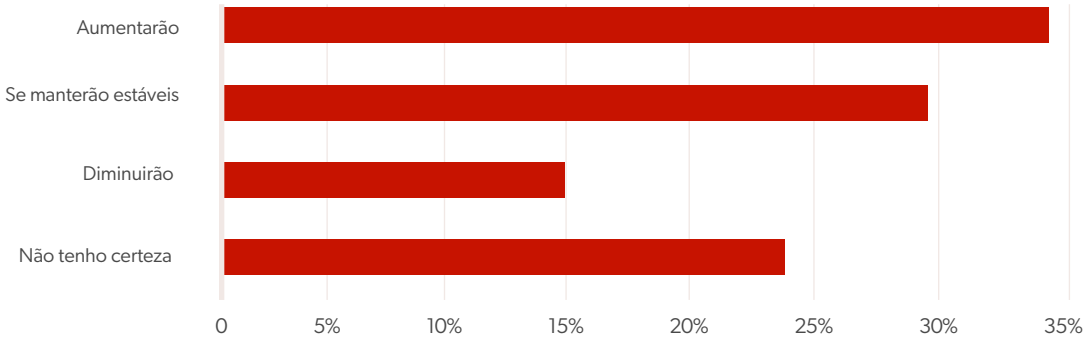


Dezenove por cento dos entrevistados afirmam que conseguem descobrir um incidente de fraude em tempo real. Isso representa um aumento de 7% desde 2019 e uma diminuição de 3% desde 2020. Onze por cento dos entrevistados afirmam que conseguem mitigar a fraude em tempo real.

Quase metade dos entrevistados diz que leva mais de um dia para identificar a fraude. Embora as porcentagens de intra-dia e de 1 a 7 dias tenham diminuído, os números de 'mais de uma semana' aumentaram desde 2019 e 2020. Além disso, ao avaliar os tempos de mitigação dos anos anteriores em geral, os tempos de mitigação aumentaram, o que significa que as instituições estão levando mais tempo.

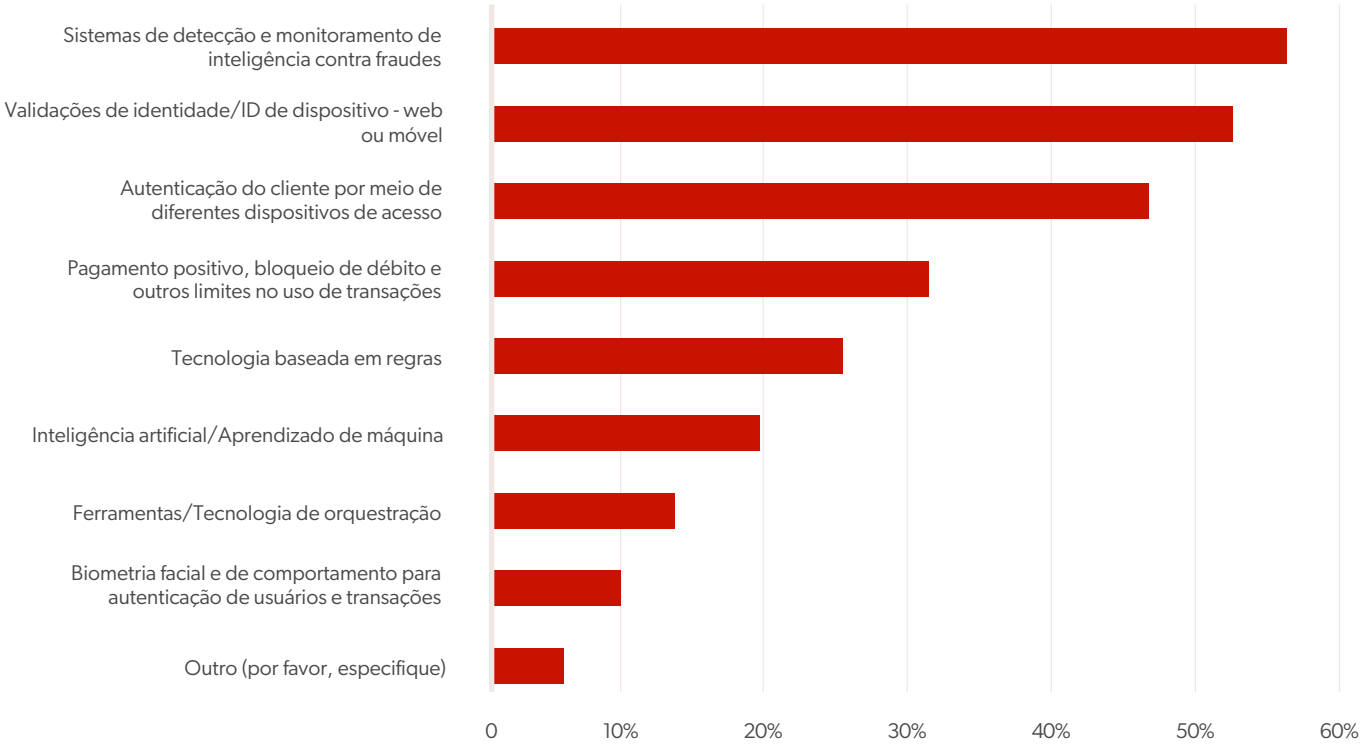
No entanto, 97% dos entrevistados afirmam que sua capacidade de detectar e mitigar a fraude é média ou superior. Portanto, existe uma desconexão entre suas percepções e a realidade.

Considerando os últimos 12 meses em relação às perdas por fraude e sua postura atual contra o fraude, como você prevê que serão suas perdas financeiras por fraude nos próximos 12 meses?



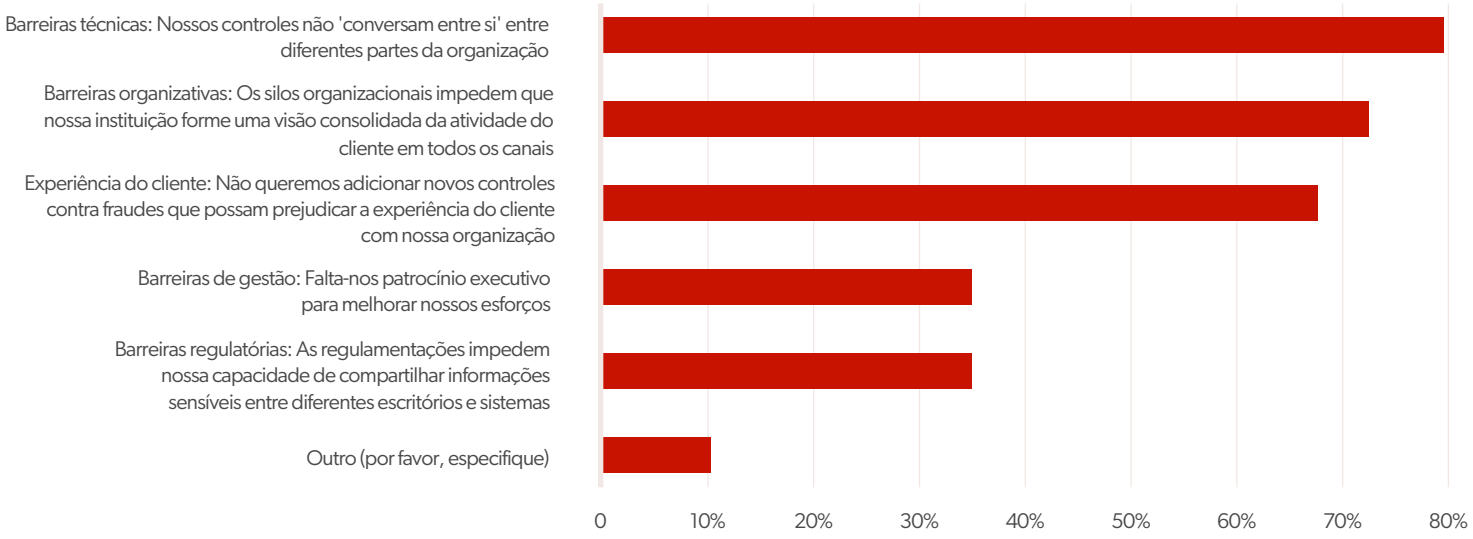
Trinta e quatro por cento dos entrevistados esperam que as perdas financeiras por fraude aumentem nos próximos 12 meses, enquanto 29% esperam que se mantenham estáveis e apenas 14% preveem uma diminuição.

¿Quais tecnologias tiveram o impacto mais significativo na prevenção de perdas por fraude?



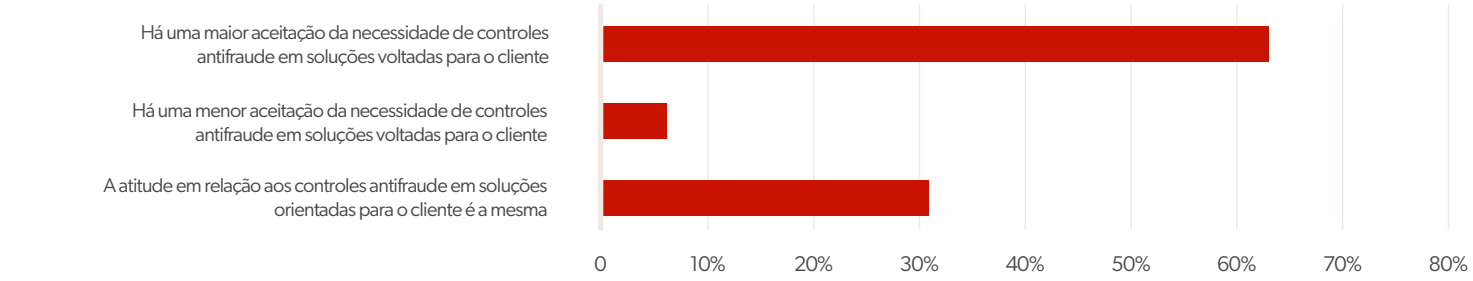
Os sistemas de detecção e monitoramento de inteligência de fraude lideram a lista das tecnologias que têm o impacto mais significativo na prevenção de perdas por fraude, com 57%. A validação de identidade/ID de dispositivo (web ou móvel) fica em segundo lugar com 53%, e a autenticação do cliente por meio de diferentes dispositivos de acesso fica em terceiro lugar com 47%

Por favor, selecione as três principais barreiras da sua organização para melhorar a prevenção de fraudes



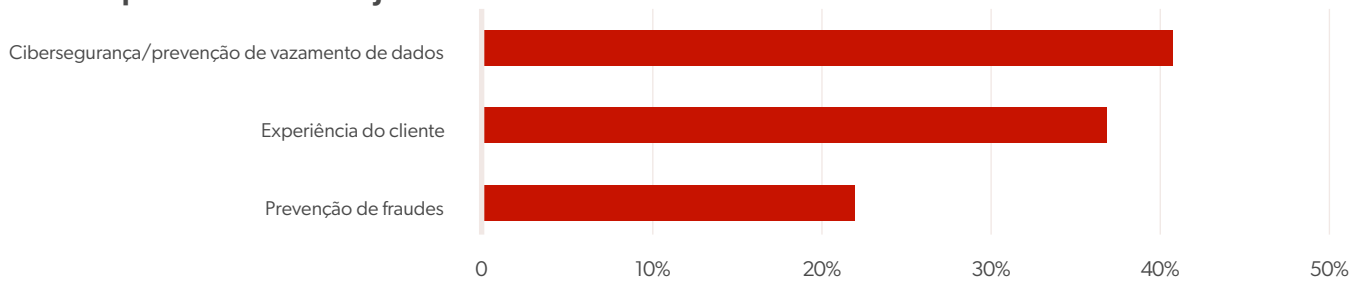
A principal barreira para melhorar a prevenção de fraudes são as barreiras técnicas, de acordo com 80% dos entrevistados. Em seguida, vêm as barreiras organizacionais, com 73%, e a experiência do cliente,com 68%.

Na sua instituição, como a atitude em relação aos controles antifraude mudou em comparação com a experiência do cliente?



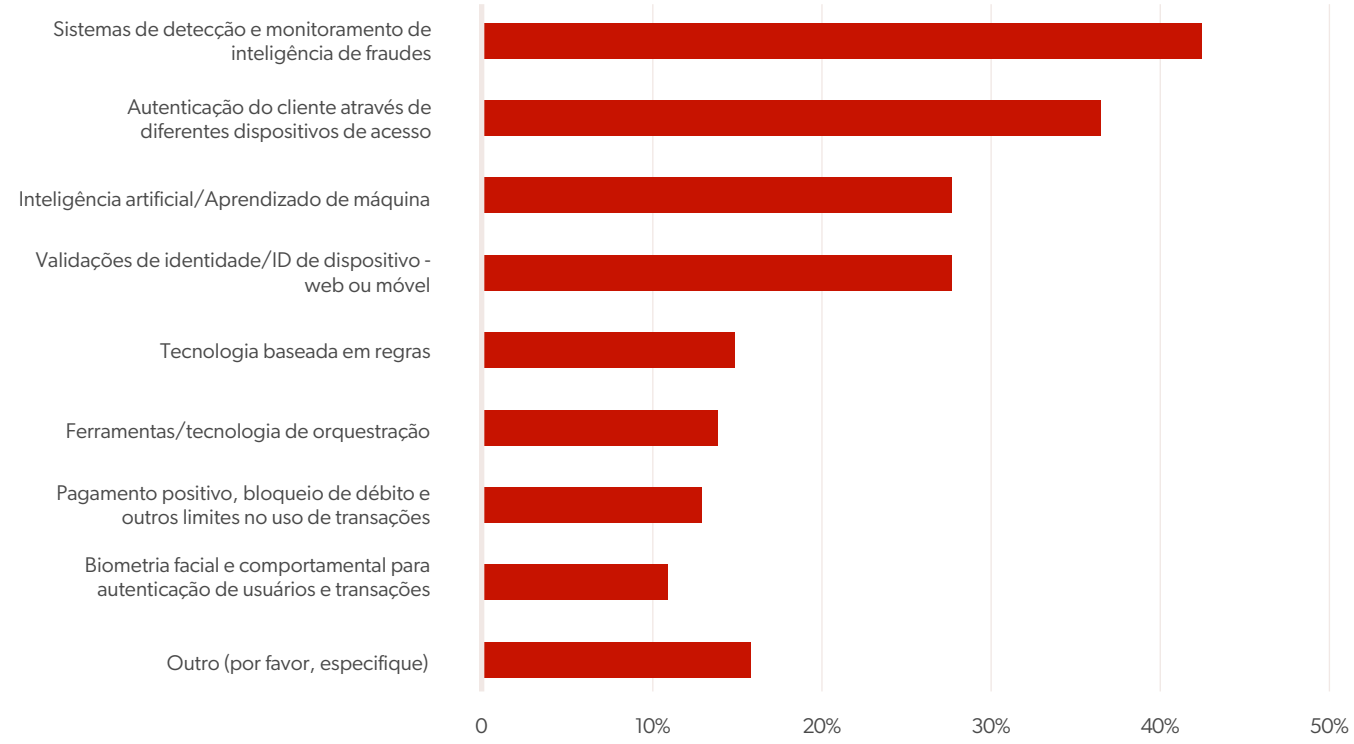
A maioria dos entrevistados, 63%, afirma que há uma maior aceitação da necessidade de controles contra fraudes em soluções voltadas para o cliente, em comparação com 31% que dizem que a atitude permanece a mesma e apenas 6% que afirmam que há uma menor aceitação.

Na sua opinião, qual destes tem a maior prioridade para a sua instituição em soluções orientadas para o cliente hoje?



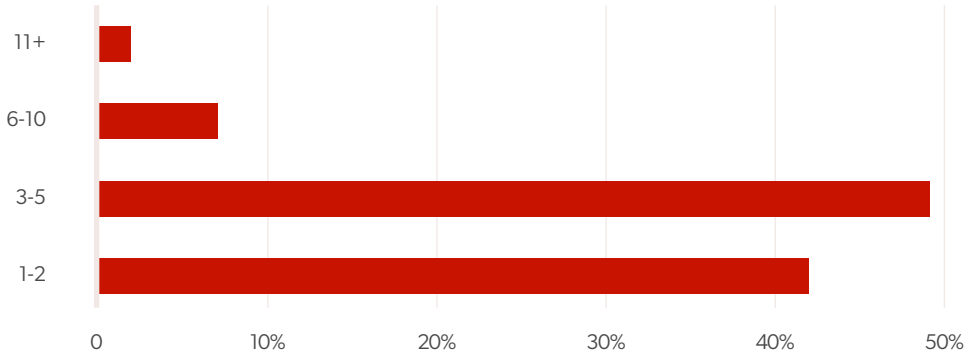
Quando perguntado sobre qual é a maior prioridade para sua instituição em soluções orientadas para o cliente atualmente, 41% dos entrevistados responderam cibersegurança/prevenção de violações de dados. A experiência do cliente ficou em segundo lugar com 37%, seguida pela prevenção de fraudes com 22%.

Em quais das seguintes tecnologias você planeja investir nos próximos 18 meses?



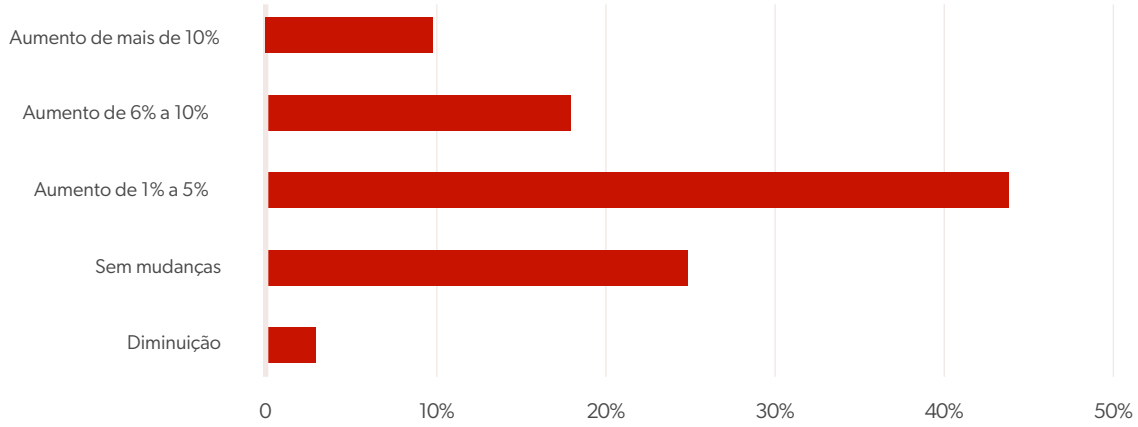
Quarenta e três por cento dos entrevistados dizem que planejam investir em sistemas de detecção e monitoramento de inteligência de fraude nos próximos 18 meses. Em seguida, vem a autenticação do cliente através de diferentes dispositivos de acesso com 37%, seguido pelas validações de identidade/ID de dispositivo (web ou móvel) e inteligência artificial/aprendizado de máquina, ambos com 28%.

Quantos fornecedores diferentes você compra para atender às suas necessidades de prevenção de fraudes?



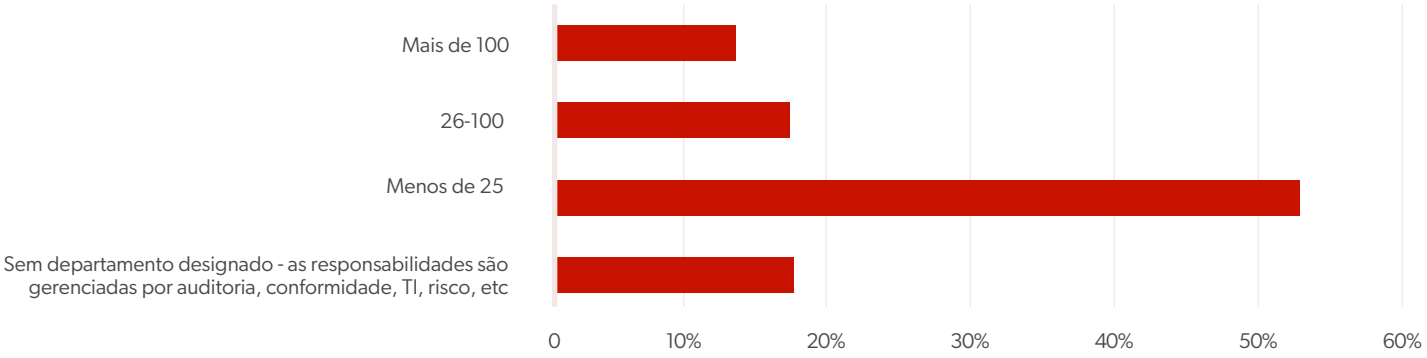
Quarenta e nove por cento dos entrevistados dizem que usam de três a cinco fornecedores, e 42% dizem que usam um ou dois. Apenas 9% dizem que usam seis ou mais.

Como você espera que seu orçamento dedicado à prevenção de fraudes mude no próximo ano?



Quarenta e quatro por cento dos entrevistados dizem que seu orçamento dedicado à prevenção de fraudes aumentará de 1% a 5% no próximo ano. Vinte e cinco por cento prevêem que não haverá mudanças, 18% esperam um aumento de 6% a 10%, e 10% esperam um aumento de mais de 10%. Apenas 3% esperam uma diminuição.

¿Qual é o tamanho do departamento de sua organização designado para prevenção e detecção de fraudes?



A maioria dos entrevistados, 53%, afirma que seu departamento designado para prevenção e detecção de fraudes consiste em menos de 25 pessoas. Dezessete por cento dizem que não têm um departamento designado, 17% relatam ter de 26 a 100 pessoas e apenas 13% dizem que têm mais de 100 pessoas.

Conclusões

Visibilidade

A maior preocupação que emerge dos dados é que apenas 19% dos entrevistados consegue identificar em tempo real o impacto de uma fraude de phishing, e os tempos de resposta estão aumentando. Isso significa que as empresas estão se tornando mais lentas em sua capacidade de identificar que foram afetadas pela fraude. A mitigação em tempo real é ainda menor, com apenas 11%.

Um fator contribuinte significativo é que 56% dos entrevistados dizem ter visibilidade limitada quando se trata de identificar o impacto de um ataque de phishing, e 6% admitem que não têm visibilidade.

Ferramentas e silos

Os entrevistados reconhecem os benefícios que podem ser obtidos com a implementação de sistemas de detecção e monitoramento de inteligência de fraude, que lideram a lista de tecnologias com o impacto mais significativo na prevenção de perdas por fraude, com 57%. No entanto, apenas 43% dos entrevistados têm planos de investir em sistemas de detecção e monitoramento de inteligência de fraude nos próximos 18 meses.

Outro problema é que a implementação de ferramentas parece estar ocorrendo de forma fragmentada, já que 80% afirmam que seus controles não se comunicam entre si, sendo essa a principal barreira para melhorar a prevenção de fraudes. É necessário um enfoque abrangente.

As organizações precisam superar suas barreiras técnicas e organizacionais. Isso tem sido uma tendência constante no relatório desde 2020. Os silos estão impedindo que as instituições adotem uma abordagem de várias camadas. Sem isso, torna-se muito difícil acompanhar a velocidade com que o cenário de fraudes evolui.

A preocupação com processos manuais, que implica a necessidade de automação, continua crescendo, mas isso pode ser visto como um desenvolvimento positivo que provavelmente impulsionará a automação no futuro.

Uma abordagem holística

Necesitamos adoptar un enfoque integral para combater a fraude. Não Precisamso adotar uma abordagem holística para combater fraudes. Não podemos analisar partes ou componentes de forma isolada. As organizações devem ser incentivadas a aproveitar os sensores que têm em cada uma das partes: usuário, dispositivo, transação/evento, para criar uma avaliação única e contínua da sessão.

Embora haja um intervalo de tempo esperado entre a conscientização da solução e sua implementação, a lacuna entre a percepção de desempenho e a evidência de desempenho é uma característica persistente desta série de pesquisas. Parece haver falta de consciência/comparação de desempenho com seus pares e alguma dose de complacência.

Esperamos que os leitores desta pesquisa reconheçam como as expectativas de prevenção de fraudes de alto desempenho continuam aumentando e, se perceberem que estão ficando para trás nas melhores práticas, se levantarão para o desafio, focando na identificação em tempo real do impacto do phishing e adotando uma abordagem holística para implementar tecnologias de prevenção de fraudes.

Análise da pesquisa

Discussão da Pesquisa Faces of Fraud da Appgate com Mike Lopez, Vicepresidente Sênior da Appgate

MIKE LOPEZ
Vice-Presidente Sênior, Appgate

Percepção vs.Realidade

TONY MORBIN: O que chamou sua atenção nos resultados da pesquisa e como isso se compara ao que você geralmente encontra no mercado?

MIKE LOPEZ: Uma das coisas que me chamou a atenção nos resultados da pesquisa foi a resposta em relação aos prazos para identificar e mitigar fraudes. Apenas 19% dos entrevistados afirmou que pode identificar fraudes em tempo real. Isso não apenas se destaca estatisticamente para mim, mas a esmagadora maioria dos entrevistados afirmou acreditar que sua capacidade de identificar e mitigar fraudes é, em sua maioria, média ou superior. Essa é uma tendência que temos visto consistentemente desde que começamos a colaborar com o ISMG por mais de cinco anos. Há uma desconexão entre a percepção da eficácia da postura antifraude da organização e a real capacidade de identificar e mitigar fraudes.

O Maior Desafio

MORBIN: Como se alinham as respostas dos entrevistados sobre quais são as maiores vulnerabilidades em suas defesas contra fraudes com o que você está observando?

LOPEZ: Desde 2019, o maior desafio que os entrevistados veem é a rapidez com que a fraude evolui e a velocidade com que os atacantes modificam seus ataques para acompanhar as tecnologias emergentes implementadas pelas instituições financeiras. Este ano, 83% dos entrevistados disseram que essa é sua maior vulnerabilidade. Isso representa um aumento em relação aos 55% em 2020, e é algo em que as instituições financeiras devem se concentrar.

Existem várias razões pelas quais isso é um problema, e isso está incorporado nas respostas. Uma delas é o fato de ainda haver uma abundância de processos manuais em operação nas instituições financeiras. A segunda parte, que é o maior contribuinte para isso, é a falta de orquestração não apenas entre as tecnologias implementadas pelas instituições financeiras e os entrevistados, mas também entre as unidades de negócio em si.

> *“Ainda estão sendo criados silos significativos entre esses componentes que estão forçando a execução de processos manuais, e isso está permitindo que os fraudadores e adversários fiquem um passo à frente das próprias instituições.”*

Ainda estão sendo criados silos significativos entre esses componentes, o que está forçando a execução de processos manuais e permitindo que fraudadores e adversários permaneçam um passo à frente das próprias instituições.

Uma Abordagem Holística

MORBIN: Quando se trata dos ataques que preocupavam os entrevistados, você concorda com as suas prioridades?

LOPEZ: A maior ameaça no momento, na perspectiva dos entrevistados, é definitivamente o canal online. No entanto, parte do problema é que a questão dos silos de dados está impedindo as instituições de tomarem decisões adequadas de forma eficaz. Eles constantemente destacam o equilíbrio entre os controles de mitigação anti-fraude e a experiência do cliente. Nesse processo, eles se concentram nesses silos, o que cria programas ineficazes que afetam diretamente a experiência do usuário. Deveriam adotar uma abordagem holística.

Melhor Orquestração

MORBIN: Fiquei surpreso com a falta de visibilidade informada para identificar o impacto de um ataque de phishing. Os entrevistados foram particularmente deficientes nesse aspecto?

LOPEZ: Geralmente, seja em cooperativas de crédito menores ou em instituições financeiras maiores, existe uma divisão entre quem é responsável por fraudes e quem é responsável pela cibersegurança. Geralmente, os controles contra phishing caem sob a responsabilidade da equipe de cibersegurança. Essas informações não estão sendo compartilhadas com a equipe de prevenção de fraudes para que eles possam correlacionar suas perdas devido a fraudes. Isso é problemático.

Automatização e Inteligência Artificial

MORBIN: Os entrevistados relataram sobre as tecnologias que acreditam ter o maior impacto na prevenção de perdas por fraude. Eles estão corretos?

LOPEZ: No final das contas, a tecnologia é o caminho a seguir. Você deve continuar investindo em automação e ser capaz de incorporar a maior quantidade possível de pontos de dados. A orquestração deve ser considerada. Não se pode olhar fatores individuais ou sensores de forma isolada. É necessário ter uma abordagem holística. Se você pretende se manter à frente dos adversários, não pode depender de pontos únicos para a detecção. É preciso analisar os padrões de usuário, os padrões de dispositivo e os padrões de transações de forma conjunta para avançar de maneira eficaz em direção a um programa que seja eficiente. Você deve investir em automação, inteligência artificial e biometria comportamental. Isso, sem dúvida, ajudará a solidificar sua posição.

> *Se você deseja manter uma vantagem sobre os adversários, não pode depender de pontos únicos para a detecção. É necessário analisar os padrões do usuário, os padrões do dispositivo e os padrões das transações de forma conjunta para avançar eficazmente em direção a um programa que seja efetivo.*

Pontuação de Risco Coletivo

MORBIN: Você viu essas necessidades refletidas nas tecnologias que as empresas relataram planejar investir nos próximos 18 meses?

LOPEZ: Estão acertando em tudo no que deveriam investir. Estão considerando sistemas de detecção e monitoramento, que representaram 43% das respostas. Também estão considerando a autenticação do cliente e a validação da identidade, seja no lado do usuário ou no lado do dispositivo, o que equivale a 37%. O restante do percentual é direcionado para inteligência artificial/aprendizado de máquina, então estão focando corretamente em todos esses aspectos. O ponto-chave é como podem fazer com que cada um desses componentes se comunique entre si. Precisam obter uma pontuação de risco coletivo que incorpore o risco do dispositivo, o risco do usuário, a identidade do usuário e a inteligência artificial ou aprendizado de máquina em torno da transação ou das próprias sessões, a fim de ter uma única pontuação de risco em vez de analisar cada um desses componentes de forma isolada.

Sobre o ISMG

Information Security Media Group (ISMG) é a maior organização de mídia do mundo dedicada exclusivamente à segurança da informação e gestão de riscos. Cada uma de nossas 36 propriedades de mídia oferece educação, pesquisa e notícias especificamente projetadas para setores verticais-chave, incluindo bancos, saúde e setor público; geografias que vão desde a América do Norte até o sudeste asiático; e tópicos como prevenção de violações de dados, avaliação de riscos cibernéticos e fraude. Nossa série anual de cúpulas globais conecta profissionais de segurança sênior com líderes da indústria para encontrar soluções práticas para os desafios urgentes de cibersegurança.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® · CU Just for Credit Unions INFO SECURITY® · GOV INFO SECURITY® · HEALTHCARE INFO SECURITY®

infoRisk TODAY · CAREERS INFO SECURITY® · Data Breach Prevention. Response. Notification. TODAY · CyberEd.io

CIO.inc · DeviceSecurity.io · PaymentSecurity.io · FraudToday.io

CYBER THEORY · CyberEdBoard · Xtra mile LIFECYCLE MARKETING · GREYHEAD

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io