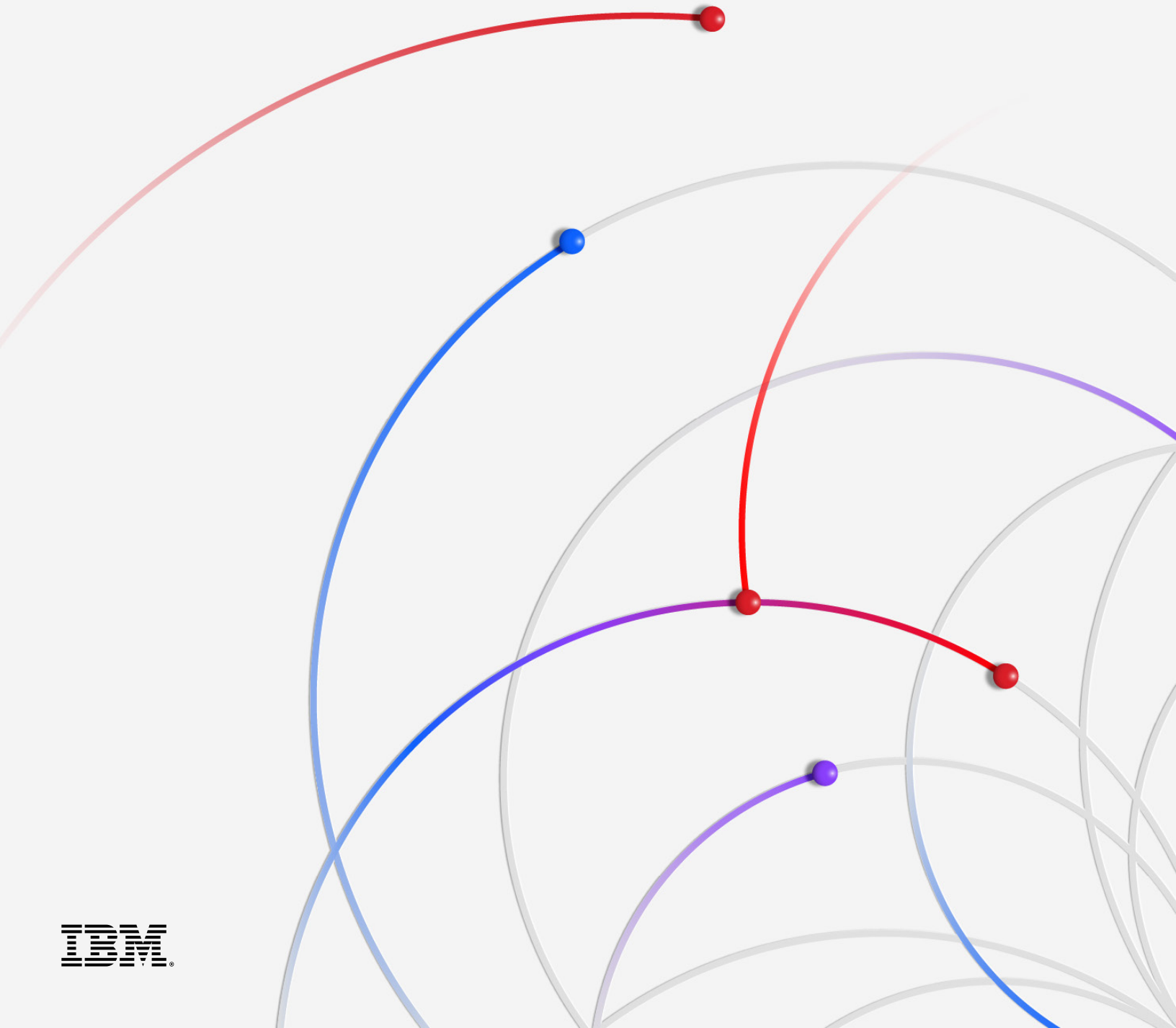
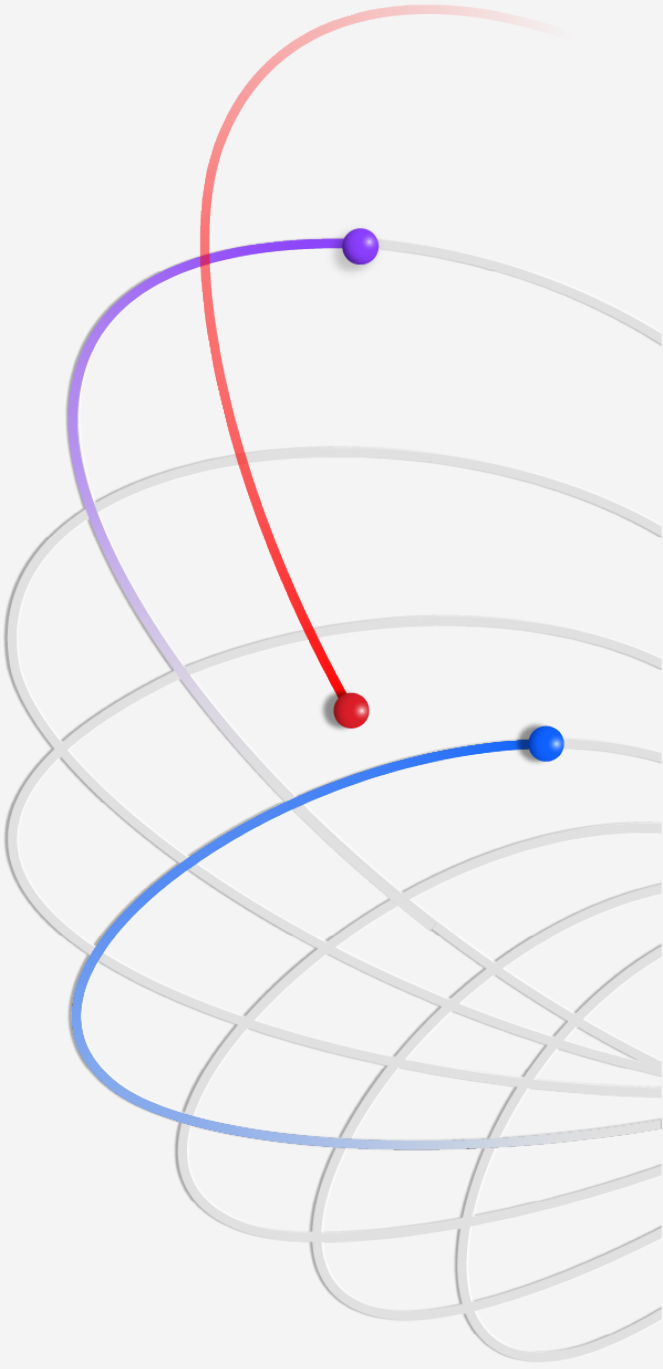
Relatório do custo das violações de dados 2024



IBM

Índice

Resumo executivo



O relatório anual do custo das violações de dados da IBM oferece aos líderes de TI gerenciamento de riscos e segurança evidências oportunas e quantificáveis para orientá-los em suas decisões estratégicas. Também os ajuda a gerenciar melhor seus perfis de risco e investimentos em segurança. O relatório deste ano — o 19º da série — reflete mudanças causadas por transformações tecnológicas, como o aumento dos dados ocultos, que são dados que residem em fontes de dados não gerenciadas, e a extensão e os custos da interrupção dos negócios causados por violações de dados.

A pesquisa do relatório — conduzida de forma independente pelo Ponemon Institute e patrocinada, analisada e publicada pela IBM — estudou 604 organizações impactadas por violações de dados entre março de 2023 e fevereiro de 2024. Os pesquisadores analisaram organizações de 17 setores, em 16 países e regiões, e violações que variaram de 2.100 a 113.000 registros comprometidos. Para obter insights diretos, os pesquisadores do Ponemon Institute entrevistaram 3.556 líderes de segurança e executivos com conhecimento direto dos incidentes de violação de dados em suas organizações.

O resultado é um relatório de referência que líderes empresariais e de segurança podem usar para fortalecer suas defesas de segurança e impulsionar a inovação, especialmente em torno da adoção de IA na segurança e segurança para suas iniciativas de IA generativa (gen AI).

Lideramos o relatório deste ano com dois desenvolvimentos principais. Primeiro, o custo médio global de uma violação de dados aumentou 10% em relação ao ano anterior, atingindo US$ 4,88 milhões, o maior salto desde a pandemia. A interrupção dos negócios e o suporte e remediação ao cliente pós-violação impulsionaram esse aumento de custo. Quando perguntados como estão lidando com esses custos, mais da metade das organizações disse que estão repassando esses custos aos clientes. Fazer com que os clientes absorvam esses custos pode ser problemático em um mercado competitivo já enfrentando pressões de preços devido à inflação.

Segundo, do lado dos defensores, os pesquisadores também descobriram que a aplicação de IA de segurança e automação está trazendo resultados, reduzindo os custos de violação em alguns casos em uma média de US$ 2,2 milhões. Soluções de IA e automação estão reduzindo o tempo necessário para identificar e conter uma violação e os danos resultantes. Em outras palavras, os defensores sem IA e automação para assisti-los podem levar mais tempo para detectar e conter uma violação, e ver os custos aumentarem em comparação com aqueles que usam essas soluções.

Como vimos em todo o setor, as equipes de cibersegurança estão consistentemente com falta de pessoal. O estudo deste ano descobriu que mais da metade das organizações violadas enfrentaram grave escassez de pessoal de segurança, uma lacuna de habilidades que aumentou em dois dígitos em relação ao ano anterior. Essa falta de pessoal de segurança treinado está crescendo à medida que o cenário de ameaças se amplia. A corrida contínua para adotar IA generativa em quase todas as funções da organização deve trazer riscos sem precedentes e colocar ainda mais pressão sobre essas equipes de cibersegurança.

Este relatório fornece insights e recomendações da pesquisa para ajudar a reduzir os potenciais danos financeiros e de reputação de uma violação de dados.

O que há de novo no relatório de 2024

A cada ano, continuamos a evoluir o relatório do custo das violações de dados para refletir novas tecnologias, táticas emergentes e eventos recentes. Pela primeira vez, a pesquisa deste ano explora:

- Se as organizações experimentaram uma interrupção operacional de longo prazo, por exemplo, a incapacidade de processar pedidos de vendas, um fechamento completo das instalações de produção, serviços de atendimento ao cliente ineficazes.
- Se a violação incluiu dados armazenados em fontes de dados não gerenciadas, também conhecidos como dados ocultos.
- Até que ponto as organizações estão usando IA e automação em cada uma das 4 áreas das operações de segurança: prevenção, detecção, investigação e resposta.
- A natureza dos ataques de extorsão, por exemplo, ataques de extorsão e ransomware ou extorsão e exfiltração de dados apenas.
- O tempo necessário para restaurar dados, sistemas ou serviços ao seu estado anterior à violação.
- Quanto tempo as organizações levaram para relatar a violação se foram obrigadas a fazê-lo.
- Se as organizações que envolveram a aplicação da lei após um ataque de ransomware pagaram o resgate.

Principais descobertas

As principais descobertas descritas aqui são baseadas na análise da IBM de dados de pesquisa compilados pelo Ponemon Institute.

US$ 4,88 milhões

Média de custo total da violação
O custo médio de uma violação de dados saltou para US$ 4,88 milhões em comparação com US$ 4,45 milhões em 2023, um aumento de 10% e o maior aumento desde a pandemia. Um aumento no custo dos negócios perdidos, incluindo downtime operacional e clientes perdidos, e o custo das respostas pós-violação, como a contratação de pessoal para help desks de atendimento ao cliente e o pagamento de multas regulatórias mais altas, impulsionou esse aumento. Juntos, esses custos totalizaram US$ 2,8 milhões, o maior valor combinado para negócios perdidos e atividades pós-violação nos últimos 6 anos.

US$ 2,2 milhões

Economia de custos com o uso extensivo de IA na prevenção
Duas em cada três organizações estudadas afirmaram que estão implementado IA de segurança e automação em seus centros de operações de segurança, um aumento de 10% em relação ao ano anterior. Quando implementadas extensivamente em fluxos de trabalho de prevenção — gestão da superfície de ataque (ASM), red-teaming e gerenciamento de postura — as organizações economizaram em média US$ 2,2 milhões nos custos de violação em comparação com aquelas que não usam IA em fluxos de trabalho de prevenção. Essa descoberta foi a maior economia de custos revelada no relatório de 2024.

26,2%

Crescimento da escassez de skills em cibersegurança
Mais da metade das organizações violadas enfrentam altos níveis de escassez de pessoal de segurança. Essa questão representa um aumento de 26,2% em relação ao ano anterior, uma situação que correspondeu a uma média de US$ 1,76 milhões a mais em custos de violação. Mesmo com uma em cada cinco organizações afirmando que usaram alguma forma de ferramentas de segurança de IA generativa — que devem ajudar a fechar a lacuna, aumentando a produtividade e a eficiência — essa lacuna de habilidades permanece um desafio.

1 em 3

Participação de violações envolvendo dados ocultos
35% das violações envolveram dados ocultos, mostrando que a proliferação de dados está dificultando o rastreamento e a proteção. O roubo de dados ocultos está correlacionado a um custo 16% maior de uma violação. Os pesquisadores descobriram que armazenar dados em diferentes ambientes provou ser uma estratégia de armazenamento comum, responsável por 40% das violações. Essas violações também levaram mais tempo para serem identificadas e contidas. Por outro lado, os dados armazenados em apenas um tipo de ambiente foram violados com menos frequência, quer esse ambiente fosse de nuvem pública (25%), no local (20%) ou nuvem privada (15%).

US$ 4,99 milhões

Custo médio de um ataque de agente malicioso interno
Comparado a outros vetores, ataques de agentes internos maliciosos resultaram nos maiores custos, com uma média de US$ 4,99 milhões. Entre outros vetores de ataque caros estavam comprometimentos de e-mail comercial, phishing, engenharia social e credenciais roubadas ou comprometidas. A IA generativa pode estar desempenhando um papel na criação de alguns desses ataques de phishing. Por exemplo, a IA generativa torna mais fácil do que nunca até mesmo para falantes não nativos de inglês produzirem mensagens de phishing gramaticalmente corretas e plausíveis.

46%

Participação de violações envolvendo dados pessoais de clientes
Quase metade de todas as violações envolveram informações pessoais identificáveis (PII) de clientes, que podem incluir números de identificação fiscal, e-mails, números de telefone e endereços residenciais. Registros de propriedade intelectual (PI) ficaram em segundo lugar (43% das violações). O custo dos registros de PI aumentou consideravelmente em relação ao ano passado, para US$ 173 por registro no estudo deste ano, em comparação com US$ 156 por registro no relatório do ano passado.

US$ 1 mi

Economia de custos quando a aplicação da lei está envolvida em ataques de ransomware
As vítimas de ransomware que envolveram a polícia acabaram reduzindo o custo da violação em uma média de quase US$ 1 milhão, e isso exclui o custo de qualquer resgate pago. O envolvimento da polícia também ajudou a reduzir o tempo necessário para identificar e conter as violações de 297 dias para 281 dias.

292

Dias para identificar e conter violações envolvendo credenciais roubadas
Violações envolvendo credenciais roubadas ou comprometidas levaram mais tempo para serem identificadas e contidas (292 dias) do que qualquer outro vetor de ataque. Ataques semelhantes que envolviam a exploração de funcionários e acesso de funcionários também demoraram muito para serem resolvidos. Por exemplo, ataques de phishing duraram em média 261 dias, enquanto ataques de engenharia social levaram em média 257 dias.

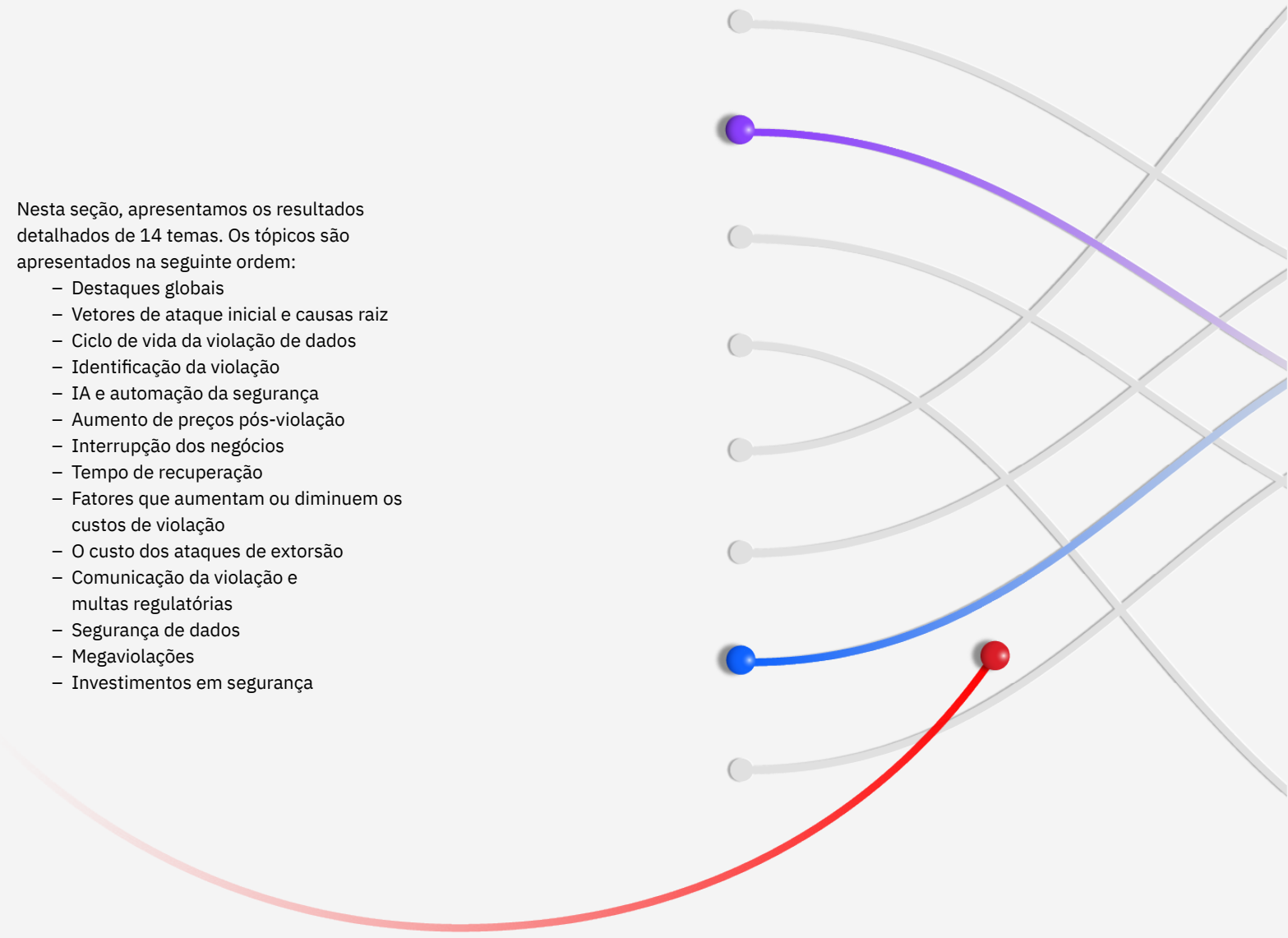
US$ 830.000

Maior aumento médio de custo entre todos os setores
O setor industrial teve o maior aumento de custo de todos os setores, com um aumento médio de US$ 830.000 por violação em relação ao ano passado. Esse aumento de custo pode refletir a necessidade de as organizações industriais se prepararem para uma resposta mais rápida, já que as organizações desse setor são altamente sensíveis ao downtime operacional. Ainda assim, o tempo para identificação e contenção de uma violação de dados nas organizações industriais estava acima da mediana do setor, com 199 dias para identificar e 73 dias para conter.

Conclusões completas

Nesta seção, apresentamos os resultados detalhados de 14 temas. Os tópicos são apresentados na seguinte ordem:

- Destaques globais
- Vetores de ataque inicial e causas raiz
- Ciclo de vida da violação de dados
- Identificação da violação
- IA e automação da segurança
- Aumento de preços pós-violação
- Interrupção dos negócios
- Tempo de recuperação
- Fatores que aumentam ou diminuem os custos de violação
- O custo dos ataques de extorsão
- Comunicação da violação e multas regulatórias
- Segurança de dados
- Megaviolações
- Investimentos em segurança



US$ 4,88 milhões

O custo médio global de uma violação de dados aumenta

Destaques globais

Globalmente, as equipes de segurança estão fazendo um trabalho muito melhor na detecção e contenção de violações, apesar da persistente escassez de skills. Mais da metade das organizações que sofreram violações estão enfrentando escassez de pessoal de segurança, e os líderes de segurança, por sua vez, estão mobilizando soluções de IA e automação para preencher a lacuna de habilidades. Apesar de seus esforços, os custos de violação estão aumentando, principalmente devido às despesas relacionadas à interrupção dos negócios e às respostas pós-violação. Na seção a seguir, analisamos essas e outras questões, em todos os setores, países e regiões, para oferecer aos líderes de segurança uma visão dos riscos existentes, para que você possa aprender com eles.

O custo médio global de uma violação de dados aumentou
O custo médio global de uma violação de dados aumentou 10% em um ano, chegando a US$ 4,88 milhões, o maior salto desde a pandemia. A interrupção dos negócios e as atividades de resposta pós-violação foram responsáveis pela maior parte desse aumento anual de custos. Veja a Figura 11.

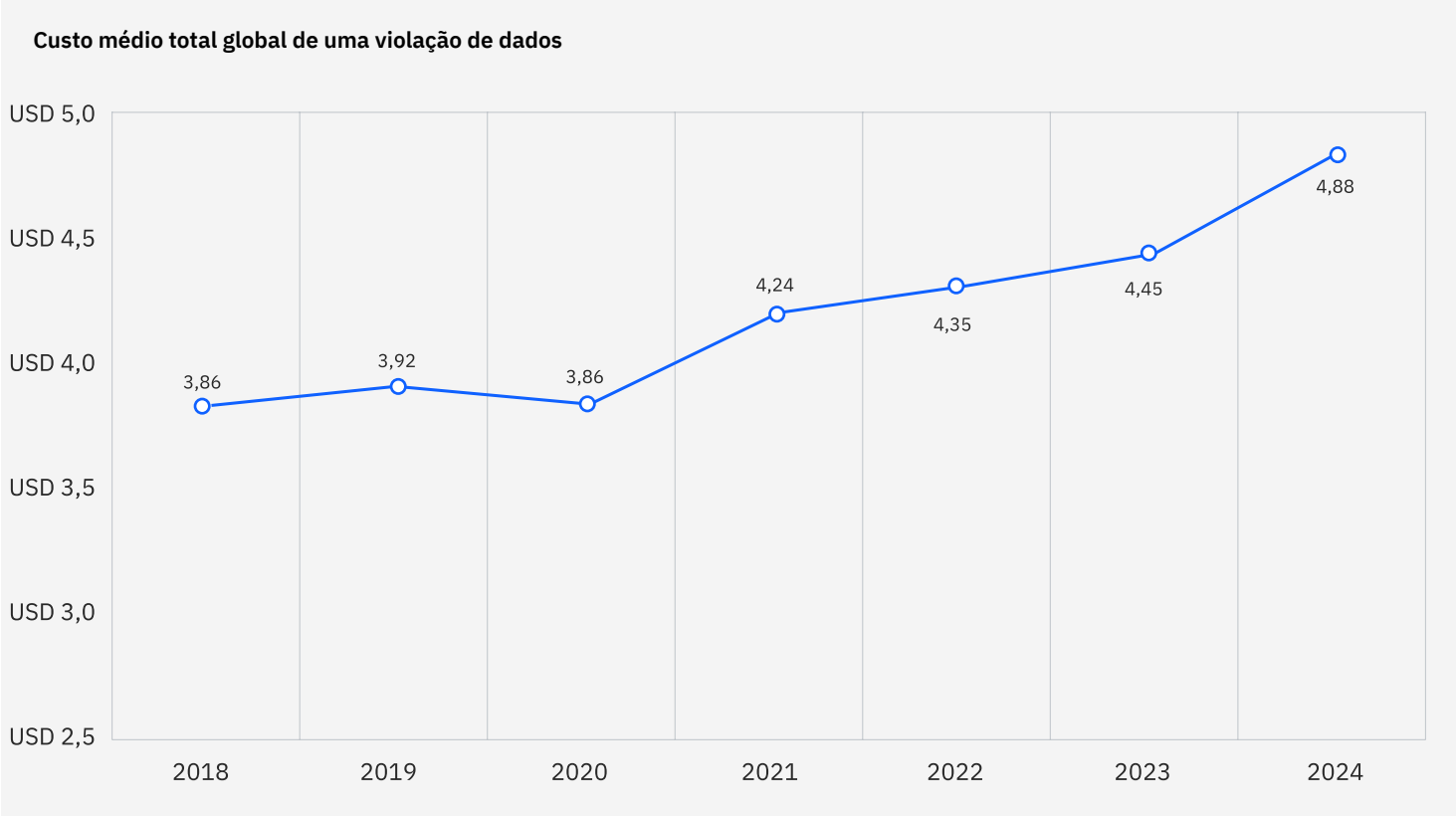


Figura 1. Medido em US$ milhões

Os Estados Unidos lideram o mundo em custo médio de violação
Pelo 14º ano, os Estados Unidos tiveram o maior custo médio de violação de dados (US$ 9,36 milhões) entre os 16 países e regiões estudados. Completando o cinco principais, estão o Oriente Médio, a Alemanha, a Itália e Benelux. O Benelux é a união econômica entre Bélgica, Holanda e Luxemburgo, e é uma nova adição deste ano. Destacadamente, o Canadá e o Japão registraram uma queda nos custos médios, enquanto a Itália e o Oriente Médio registraram aumentos significativos. Veja as Figuras 2A e 2B.

Custo de uma violação de dados por país ou região

#	País	2024	2023
1	Estados Unidos	US$ 9,36	US$ 9,48
2	Oriente Médio	US$ 8,75	US$ 8,07
3	Benelux	US$ 5,90	—
4	Alemanha	US$ 5,31	US$ 4,67
5	Itália	US$ 4,73	US$ 3,86
6	Canadá	US$ 4,66	US$ 5,13
7	Reino Unido	US$ 4,53	US$ 4,21
8	Japão	US$ 4,19	US$ 4,52
9	França	US$ 4,17	US$ 4,08
10	América Latina	US$ 4,16	US$ 3,69
11	Coreia do Sul	US$ 3,62	US$ 3,48
12	ASEAN	US$ 3,23	US$ 3,05
13	Austrália	US$ 2,78	US$ 2,70
14	África do Sul	US$ 2,78	US$ 2,79
15	Índia	US$ 2,35	US$ 2,18
16	Brasil	US$ 1,36	US$ 1,22

Figura 2A. Medido em US$ milhões

Cinco principais países e regiões de 2024 vs. 2023

#	Mudança de custos	2024	2023
1	↓	**Estados Unidos** US$ 9,36	**Estados Unidos** US$ 9,48
2	↑	**Oriente Médio** US$ 8,75	**Oriente Médio** US$ 8,07
3	↑	**Benelux** US$ 5,90	**Canadá** US$ 5,13
4	↑	**Alemanha** US$ 5,31	**Alemanha** US$ 4,67
5	↑	**Itália** US$ 4,73	**Japão** US$ 4,52

Figura 2B. Medido em US$ milhões

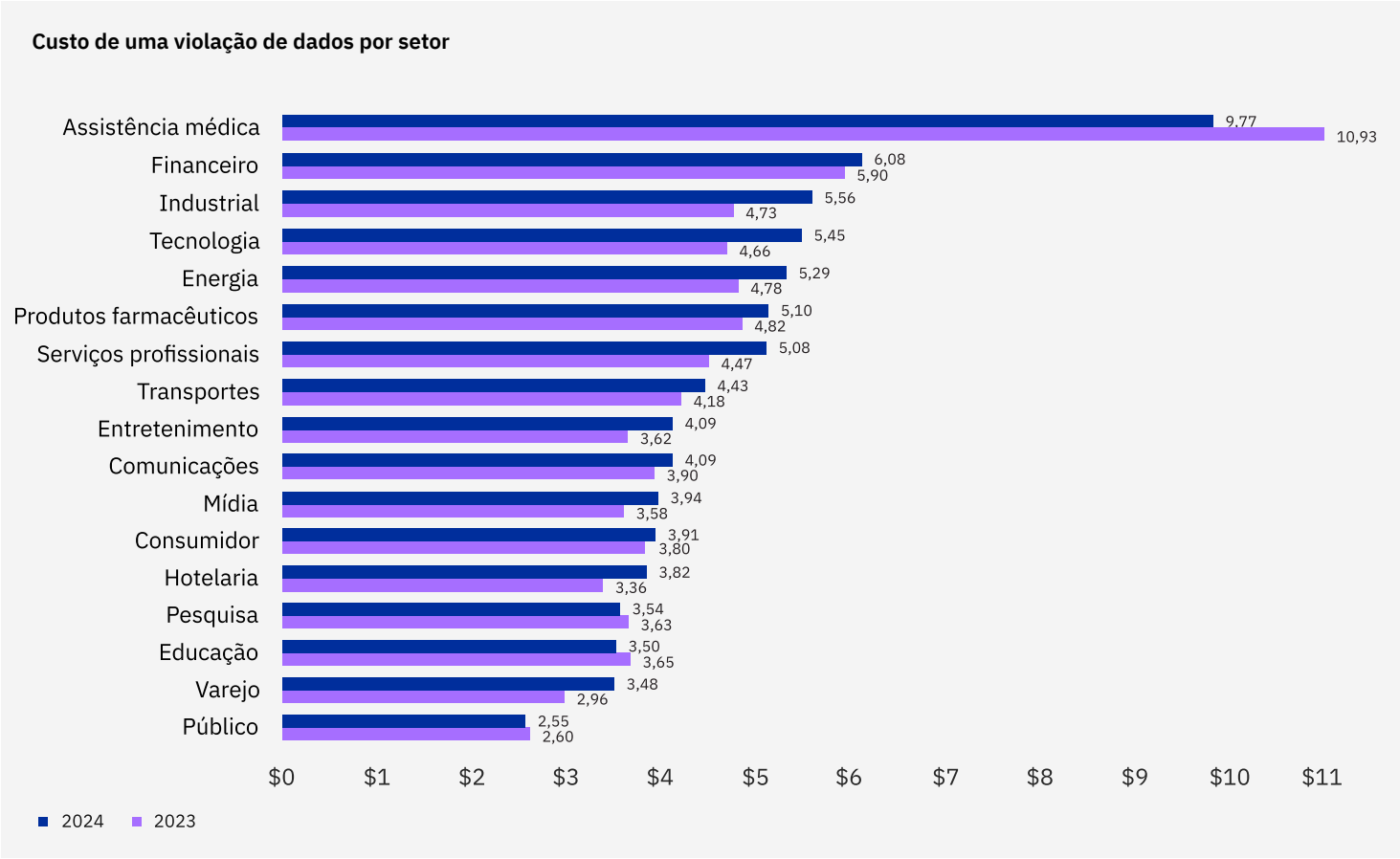


Figura 3. Medido em US$ milhões

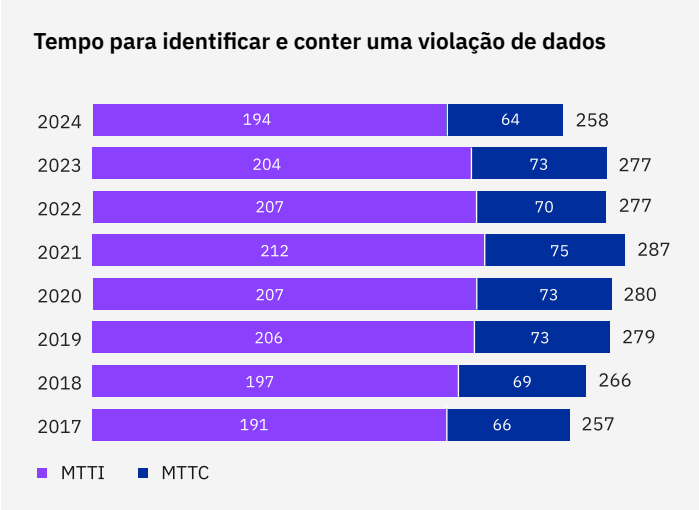


Figura 4. Medido em dias

A saúde teve novamente o maior custo entre os setores
O custo médio de violação no setor de saúde caiu 10,6%, para US$ 9,77 milhões. Mas esse fator não foi suficiente para tirá-lo dos setores mais caros em termos de violações — um lugar que ele ocupa desde 2011. A área da saúde continua sendo um alvo para os invasores, visto que o setor geralmente sofre com as tecnologias existentes e é altamente vulnerável a interrupções, o que pode colocar em risco a segurança dos pacientes. Veja a Figura 3.

O tempo médio para identificar e conter uma violação caiu
O tempo médio que os defensores levaram para identificar e conter uma violação caiu para 258 dias, atingindo uma mínima de sete anos, em comparação com os 277 dias do ano anterior. Observação: essa média global do tempo médio para identificar (MTTI) e do tempo médio para conter (MTTC) exclui o Benelux porque, por ser uma região nova no estudo, estava tendo uma influência desproporcional e distorcia os resultados muito mais do que a média. Veja a Figura 4.

Os custos de perda de negócios e os custos de resposta pós-violação dispararam

Os custos de perda de negócios e de resposta pós-violação aumentaram quase 11% em relação ao ano anterior, o que contribuiu para o aumento significativo dos custos gerais de violação. Os custos de negócios perdidos incluem a perda de receita devido ao downtime do sistema e o custo da perda de clientes e danos à reputação. Os custos pós-violação podem incluir a despesa de criação de centrais de atendimento e serviços de monitoramento de crédito para os clientes afetados, além do pagamento de multas regulatórias. Veja a Figura 5.

Custo médio de uma violação de dados em quatro componentes

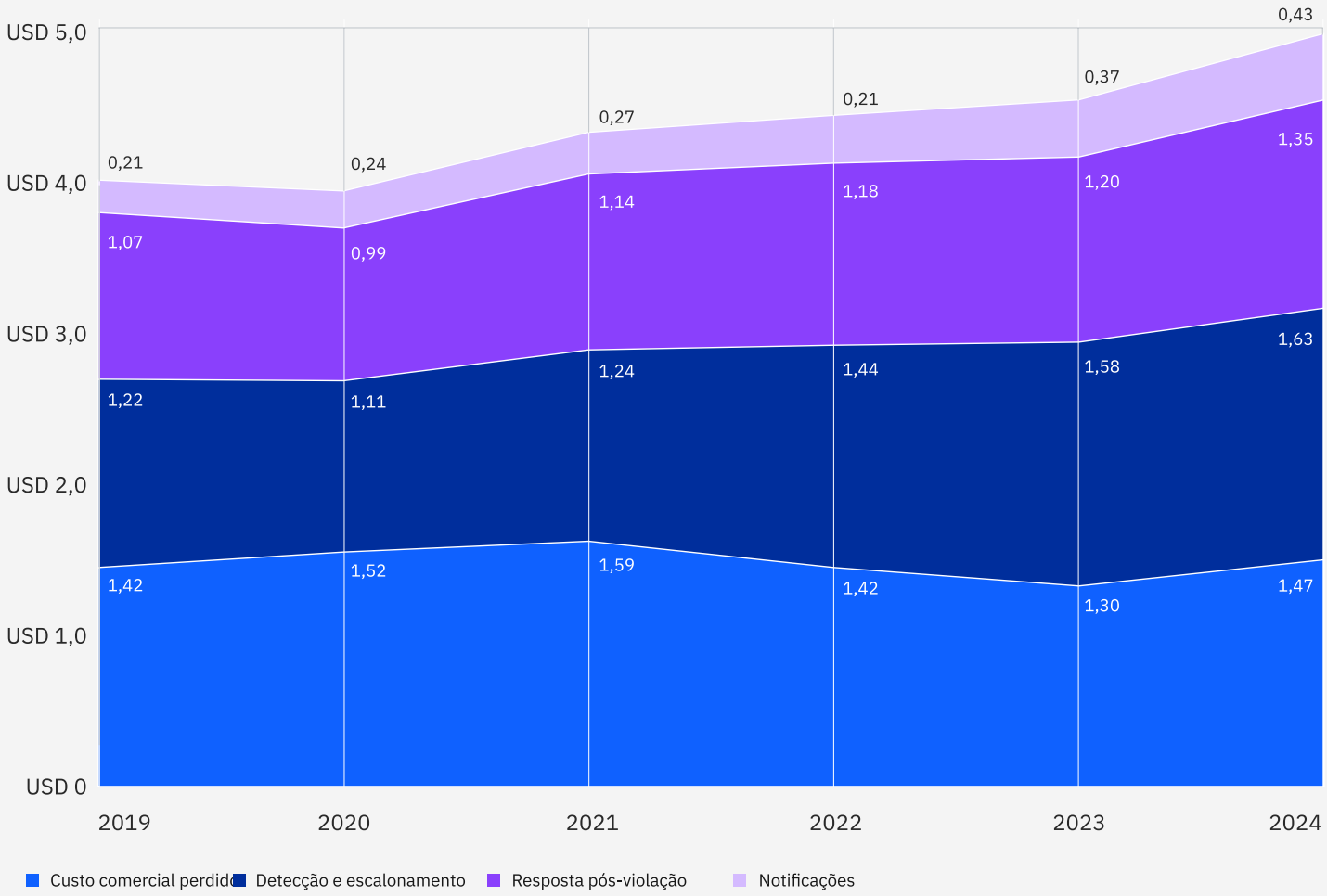


Figura 5. Medido em US$ milhões

A maioria das violações envolveu PII de clientes
O tipo mais comum de dados roubados ou comprometidos foi PII de clientes, com 46%. As PII podem incluir números de identificação fiscal, e-mails e dados residenciais, e podem ser usadas para roubo de identidade e fraude de cartão de crédito. A média global de todos os tipos de registros roubados subiu para US$ 169, sendo as PIIs de funcionários as mais caras. Veja as Figuras 6A e 6B.

Tipo de dados comprometidos por porcentagem

Figura 6A. É permitida mais de uma resposta

Custo por registro de uma violação de dados por tipo de registro comprometido

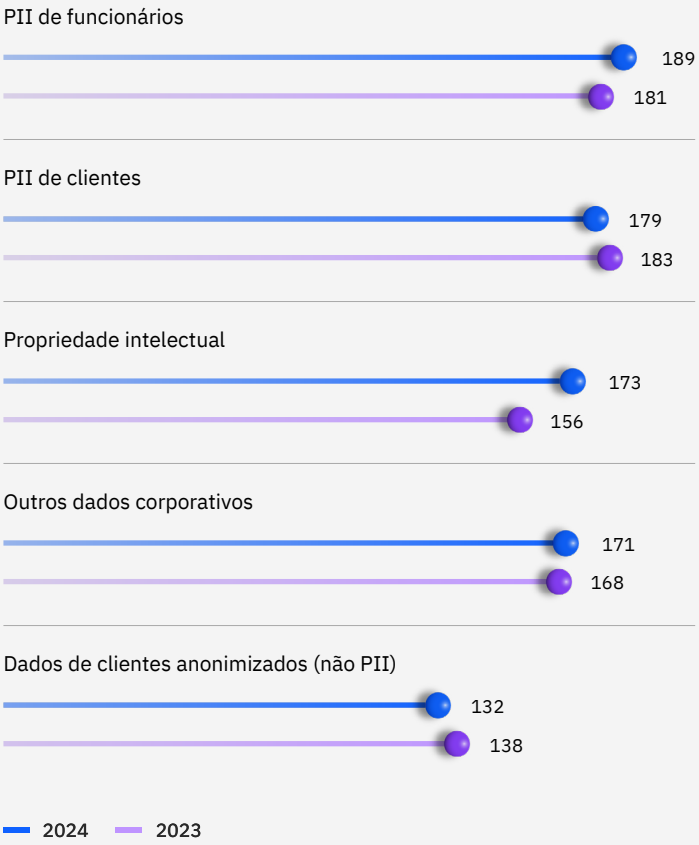


Figure 6B. Medido em US$ milhões

US$ 4.81 milhões

O custo médio de uma violação quando os invasores usaram credenciais comprometidas, o que aconteceu em 16% dos casos de violação estudados.

Vetores de ataque inicial e causas raiz

Pelo segundo ano consecutivo, phishing e credenciais roubadas ou comprometidas foram os dois vetores de ataque mais predominantes. Ambos também se classificaram entre os quatro tipos de incidentes mais caros. Além de identificar as causas raiz mais comuns das violações, o estudo comparou o custo médio de cada categoria, bem como o tempo médio para identificar e conter essas violações.

As credenciais comprometidas são os principais vetores de ataque inicial

O uso de credenciais comprometidas beneficiou os invasores em 16% das violações. Os ataques com credenciais comprometidas também podem ser caros para a organização, representando, em média, US$ 4,81 milhões por violação. O phishing ficou em um segundo lugar, com 15% dos vetores de ataque, mas no final custou mais, US$ 4,88 milhões. Os ataques de agentes internos maliciosos tiveram o maior custo, de US$ 4,99 milhões, mas representaram apenas 7% de todos os métodos de violação. Veja a Figura 7.

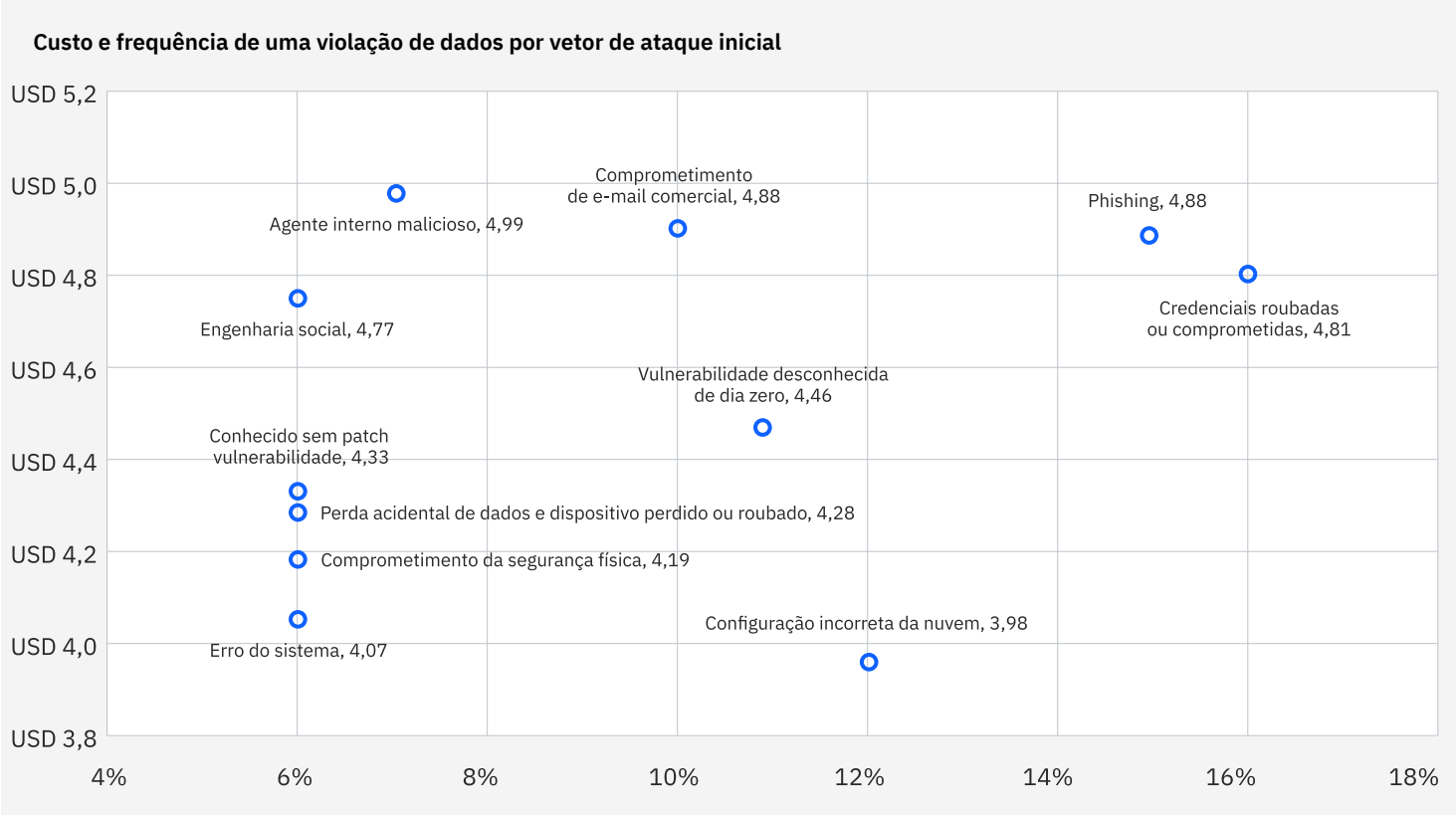


Figura 7. Medido em milhões de dólares; porcentagem de todas as violações

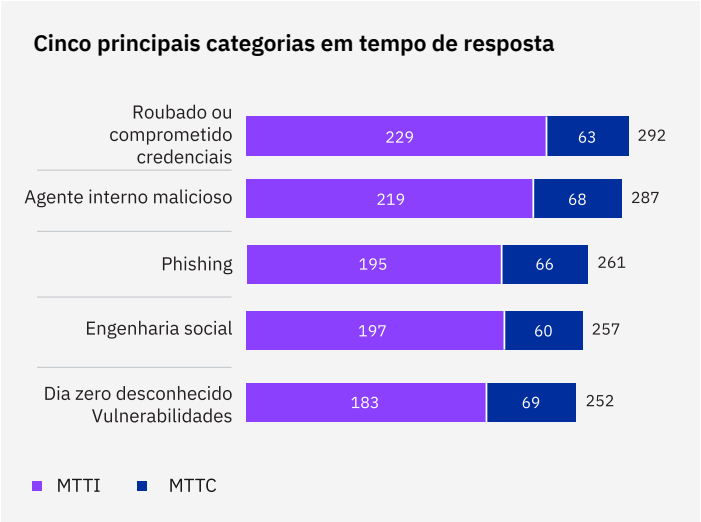


Figura 8. Medido em dias

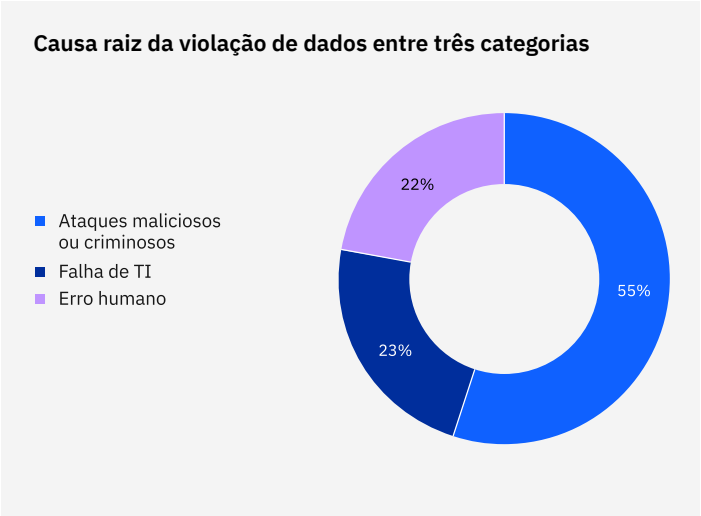


Figura 9.

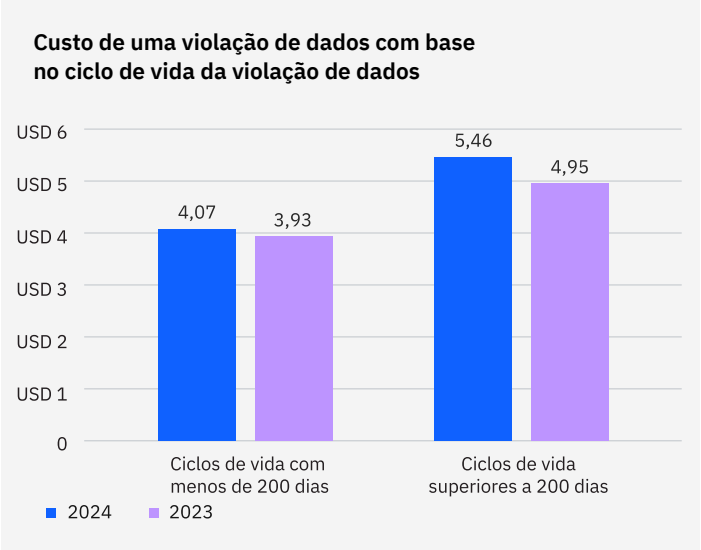


Figura 10. Medido em US$ milhões

Os ataques baseados em credenciais levaram mais tempo para serem identificados e contidos

Independentemente de as credenciais terem sido roubadas ou usadas por agentes internos maliciosos, o tempo de identificação e contenção do ataque aumentou, gerando um tempo médio combinado de 292 e 287 dias, respectivamente. Os defensores precisavam distinguir entre a atividade legítima e maliciosa do usuário na rede, o que dificultava a identificação das ameaças. Por outro lado, os ataques que usaram vulnerabilidades de dia zero foram os mais demorados para serem contidos. Veja a Figura 8.

Falhas de TI ou erro humano causaram quase a metade de todas as violações

Os ataques maliciosos (aqueles cometidos por invasores externos ou agentes criminosos internos) representaram 55% de todas as violações. Por mais preocupantes que sejam essas violações, é importante lembrar que os 23% restantes se devem a falhas de TI e 22% se devem a erros humanos. Veja a Figura 9.

Ciclo de vida da violação de dados

Em uma violação de dados, tempo significa dinheiro, e as violações com ciclos de vida mais longos foram mais caras, de acordo com nossas pesquisas de 2024 e 2023. O ciclo de vida completo de uma violação é a combinação do número médio de dias para identificar e conter uma violação. Em ambos os relatórios, comparamos os custos médios da violação de dados em que o ciclo de vida completo da violação foi inferior a 200 dias com o custo médio das violações em que os ciclos de vida completos excederam 200 dias.

Ciclos de vida mais longos das violações levaram a custos mais altos

No relatório deste ano, os pesquisadores descobriram que as violações de dados com um ciclo de vida superior a 200 dias tiveram o custo médio mais alto, de US$ 5,46 milhões, em comparação com as violações com ciclos de vida inferiores a 200 dias. Esses resultados são consistentes com os do ano anterior. Notavelmente, embora os custos dos ciclos de vida mais longos de violação de dados tenham aumentado 10,3% este ano em relação ao ano passado, os custos dos ciclos de vida mais curtos também aumentaram, mas em um valor menor, 3,6%. Veja a Figura 10.

Identificação da violação

Para conter uma violação de dados, ela primeiro precisa ser identificada. Quem a identifica e com que rapidez faz a diferença nos custos resultantes da violação de dados. Este ano, descobrimos que as equipes de segurança que trabalham com suas próprias ferramentas melhoraram seu desempenho nessa área. Em outros casos, as violações foram identificadas por terceiros benignos, como pesquisadores de segurança, autoridades policiais e consultores, ou pelos próprios invasores.

As equipes de segurança identificaram a maioria das violações
As equipes de segurança e suas ferramentas detectaram violações com muito mais frequência, em 42% das vezes, do que terceiros benignos, em 34%, e os próprios invasores, em 24%. Esse número foi uma melhoria em relação ao relatório de 2023, quando as equipes de segurança descobriram as violações em apenas um terço das vezes. A mudança mostra que as equipes de segurança conseguiram acelerar a detecção. Veja a Figura 11.

Como a violação foi identificada?

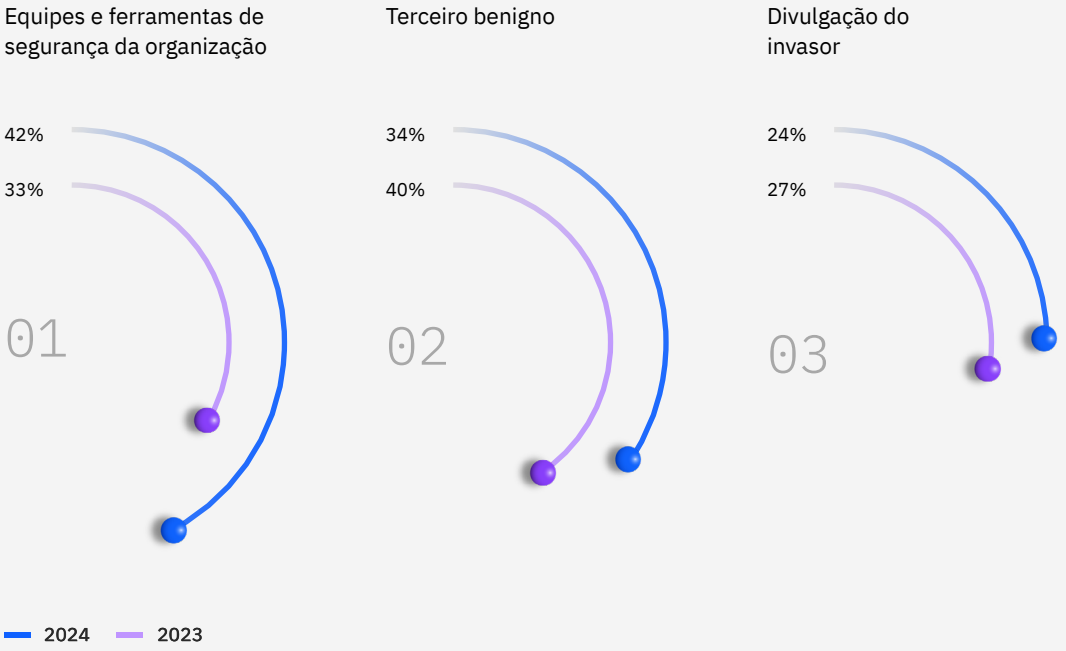


Figura 1. É permitida apenas uma resposta

US$ 5,53 milhões

O custo médio de uma violação quando a violação foi divulgada por um invasor.

As violações divulgadas pelos invasores custam mais
Quando um invasor divulga uma violação, ele provavelmente já atingiu seu objetivo e causou danos consideráveis, aumentando os custos gerais da violação. Quando uma violação foi divulgada por um invasor, o custo médio foi de US$ 5,53 milhões. Por outro lado, quando uma equipe de segurança identificou uma violação, o custo médio foi de US$ 4,55 milhões. Veja a Figura 12.

Identificação e contenção mais rápidas de violações
O relatório constatou que, independentemente de como a violação tenha sido descoberta, as organizações as identificaram e contiveram mais rapidamente, em média, em 2024 do que no ano anterior. O uso de IA e automação provavelmente contribuiu para essa aceleração, como mostra a próxima seção deste relatório. Veja a Figura 13.

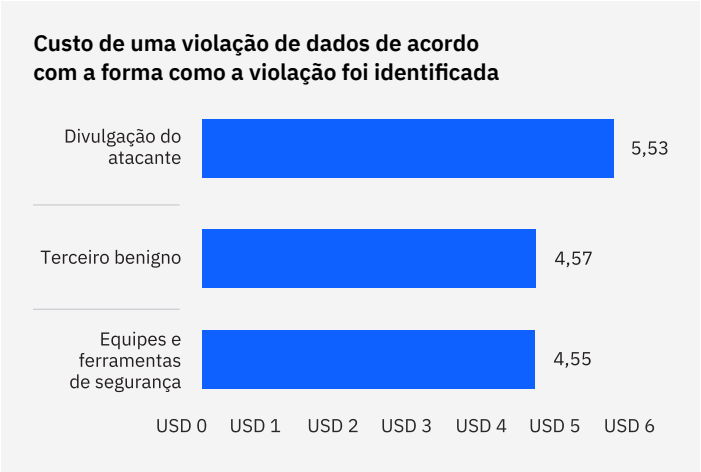


Figura 12. Medido em US$ milhões

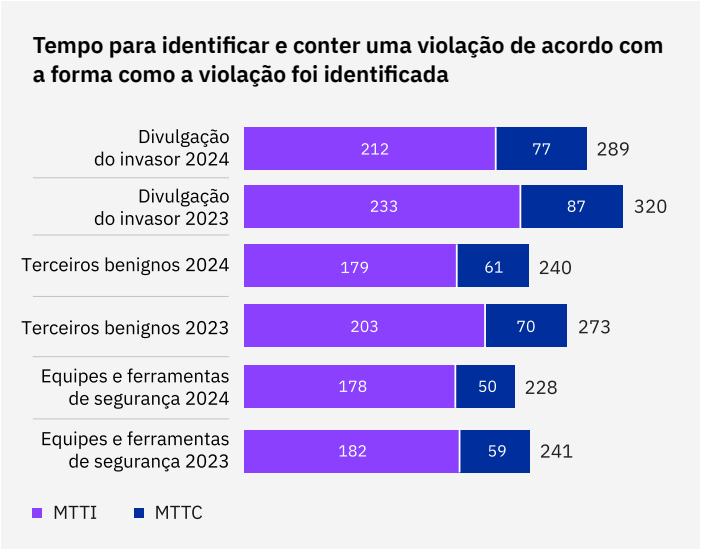


Figura 13. Medido em dias

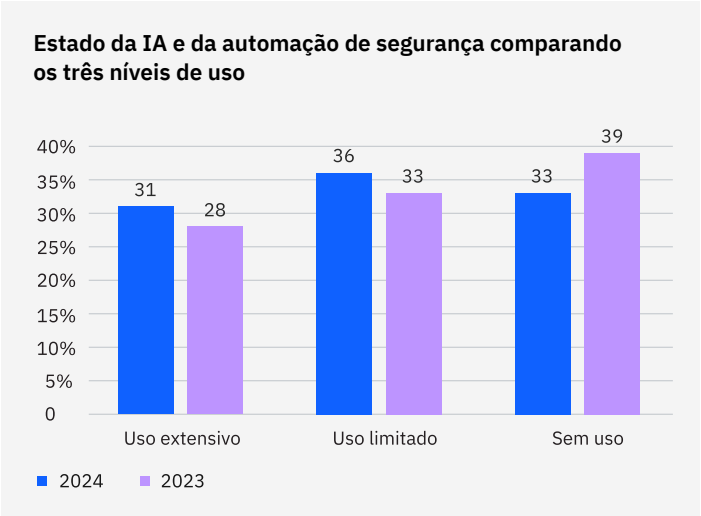


Figura 14. Porcentagem das organizações por nível de uso

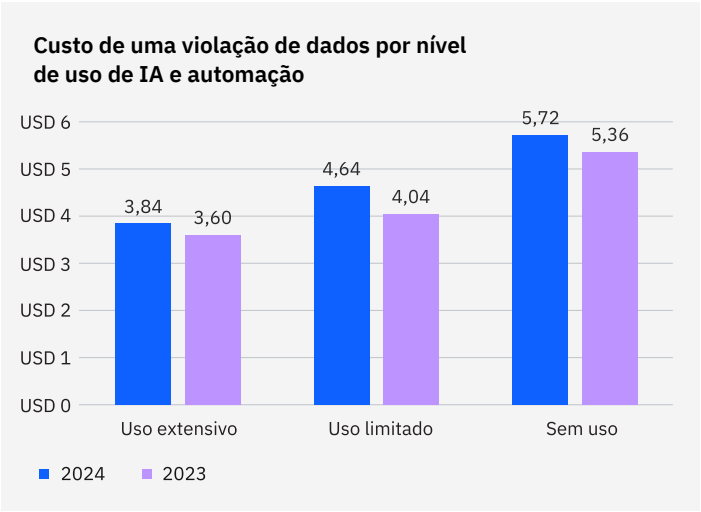


Figura 15. Medido em US$ milhões

IA e automação da segurança

A IA e a automação estão transformando o mundo da cibersegurança. Elas tornam mais fácil do que nunca para os malfeitores criar e lançar ataques em escala e fornecem aos defensores novas ferramentas para identificar rapidamente as ameaças e automatizar as respostas a essas ameaças. O relatório deste ano constatou que essas tecnologias aceleraram o trabalho de identificar e conter violações e reduzir custos.

O uso de IA e automação cresceu

O número de organizações que usaram amplamente a IA e a automação na segurança cresceu para 31% no estudo deste ano, em comparação com 28% no ano passado. Embora seja uma diferença de apenas 3 pontos percentuais, representa um aumento de 10,7% no uso. A parcela dos que usam IA e automação de forma limitada também cresceu de 33% para 36%, um aumento de 9,1%. Veja a Figura 14.

Mais IA e automação significaram menores custos de violação

Quanto mais as organizações usaram IA e automação, menores foram seus custos médios de violação. Essa correlação é impressionante e é uma das principais conclusões do relatório deste ano. As organizações que não usaram IA e automação tiveram custos médios de US$ 5,72 milhões, enquanto as que fizeram uso extensivo de IA e automação tiveram custos médios de US$ 3,84 milhões, uma economia de US$ 1,88 milhão. Veja a Figura 15.

27%

Parcela das organizações que usaram IA e automação em quatro categorias de segurança.

Mais IA equivale a identificação e contenção mais rápidas
As organizações que usam amplamente a IA e a automação na segurança identificaram e contiveram a violação de dados quase 100 dias mais rápido, em média, do que as organizações que não usaram essas tecnologias. Veja a Figura 16.

As equipes de segurança aplicaram IA e automação uniformemente em todas as funções
Entre as organizações que declararam usar amplamente a IA e a automação, cerca de 27% usaram amplamente a IA em cada uma das seguintes categorias: prevenção, detecção, investigação e resposta. Cerca de 40% usaram tecnologias de IA pelo menos um pouco. Veja a Figura 17.

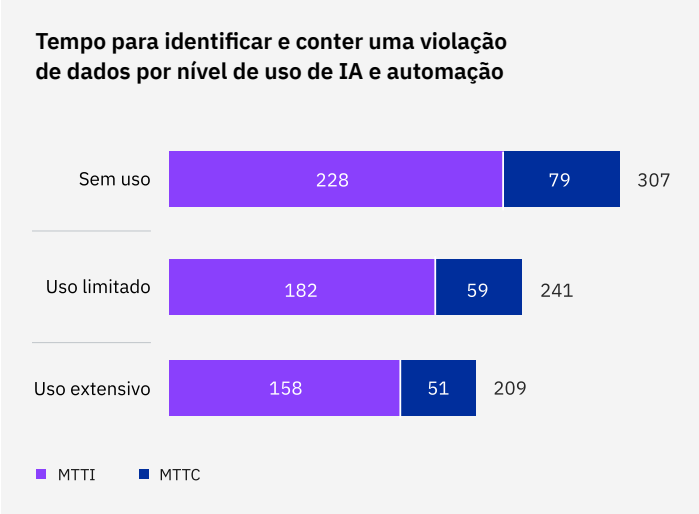


Figura 16. Medido em dias

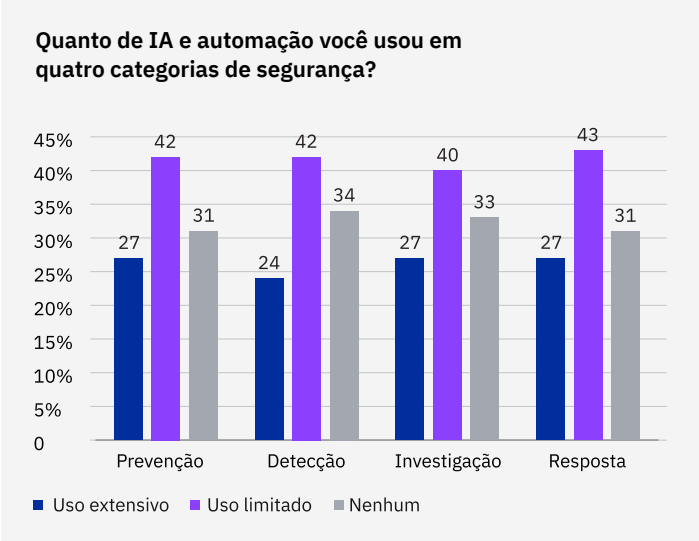


Figura 17. Dos entrevistados que relataram uso extensivo de IA e automação; consulte o gráfico 14

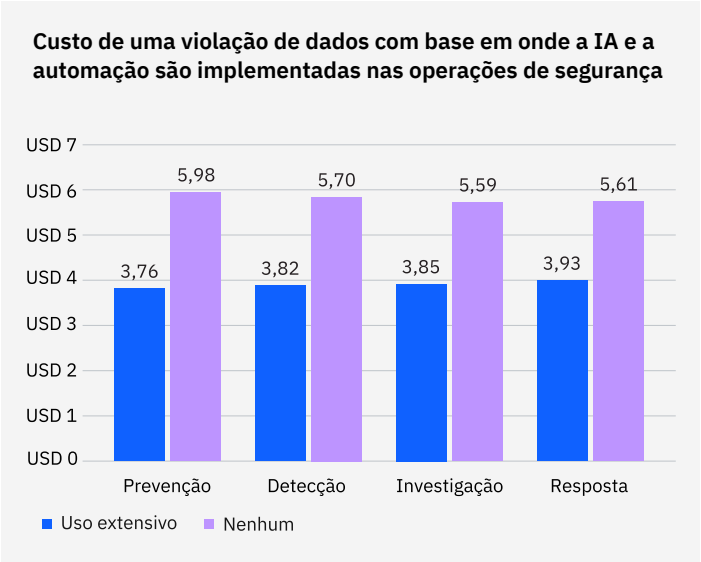


Figura 18. Das organizações que relataram o uso extensivo de IA e automação, medido em US$ milhões; consulte o gráfico 14

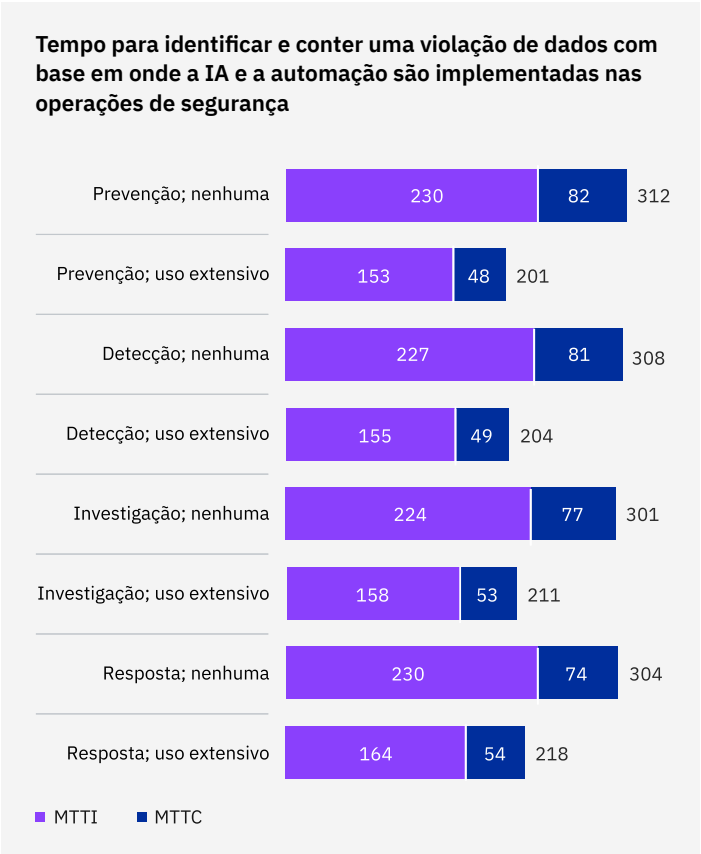


Figura 19. Das organizações que relataram o uso extensivo de IA e automação, medido em dias; consulte o gráfico 14

O uso extensivo de IA e automação reduziu os custos
Quando a IA e a automação foram usadas extensivamente em cada uma das quatro áreas de segurança, os custos médios de violação foram drasticamente reduzidos em comparação com as organizações que não usaram essas tecnologias nessas áreas. Por exemplo, quando as organizações usaram amplamente a IA e a automação para prevenção, o custo médio de violação foi de US$ 3,76 milhões. Enquanto isso, as organizações que não usaram essas ferramentas na prevenção tiveram custos de US$ 5,98 milhões, uma diferença de 45,6%. Veja a Figura 18.

A IA e a automação aceleraram o tempo para identificar e conter uma violação
Onde quer que a IA e a automação tenham sido aplicadas, elas aceleraram o trabalho de identificação e contenção de violações. O uso extensivo de IA e automação em qualquer função de segurança (prevenção, detecção, investigação ou resposta) reduziu o MTTI e o MTTC médios para as violações de dados em 33% para resposta e 43% para prevenção. Veja a Figura 19.

70%

Parcela das organizações que sofreram uma interrupção significativa ou muito significativa nos negócios devido a uma violação.

Aumento de preços pós-violação

Por sua natureza, as violações de dados são caras. Quando as organizações se veem sobrecarregadas com custos multimilionários, elas podem procurar recuperar esses custos em outro lugar. Uma opção é repassá-los aos seus próprios clientes na forma de aumentos de preços, o que é uma tendência crescente. Aumentar os preços pode ser arriscado em um mercado que já está enfrentando pressão de preços.

As organizações repassaram os custos das violações aos clientes
A maioria das organizações disse que planejava aumentar os preços dos bens e serviços após uma violação de dados, repassando os custos aos clientes. O número de organizações que planejavam fazer isso aumentou de 57% no ano passado para 63% neste ano, representando um aumento de 10,5%. Veja a Figura 20.

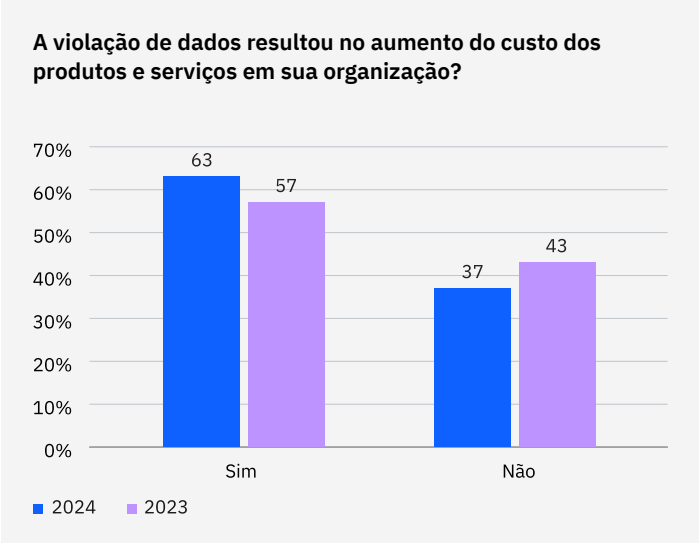


Figura 20. Parcela de todas as organizações

Interrupção dos negócios

Os negócios funcionam com base em dados. Quando os dados são violados, os negócios são interrompidos. Essas interrupções podem variar de pequenas violações, que afetam apenas alguns sistemas, a interrupções operacionais de longa duração em toda a organização. Nossa pesquisa explorou o quão pequenas ou significativas foram essas interrupções e como a gravidade de uma interrupção se correlacionou com os custos da violação de dados.

A interrupção dos negócios foi substancial
70% das organizações que participaram do estudo deste ano sofreram uma interrupção significativa ou muito significativa nos negócios em decorrência de uma violação. Apenas 1% descreveram seu nível de interrupção como baixo. Veja a Figura 21.

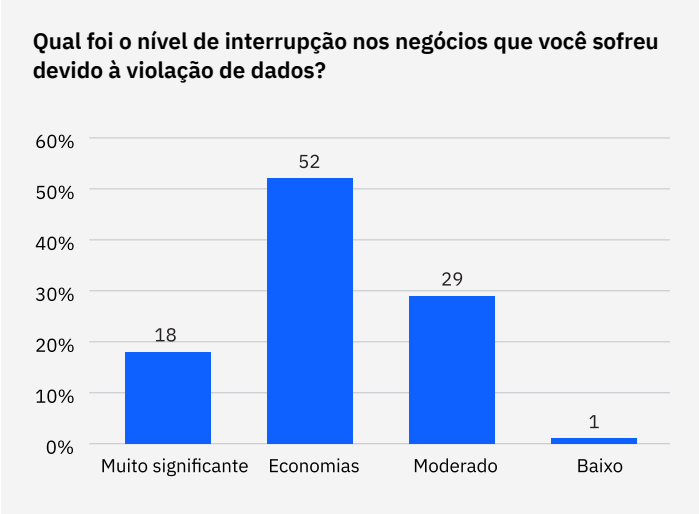


Figura 21. É permitida apenas uma resposta

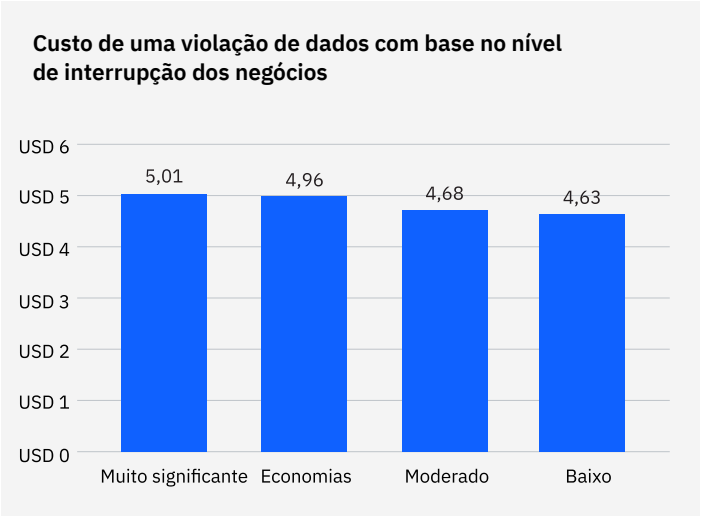


Figura 22. Medido em US$ milhões

Figura 23. Parcela de todas as organizações violadas

O custo médio de uma violação aumentou com a interrupção
Os custos médios de violações foram mais altos quando a interrupção dos negócios foi maior. Mesmo as organizações que relataram baixos níveis de interrupção incorreram em custos médios de violações de dados de US$ 4,63 milhões. Para as organizações que registraram interrupções muito significativas, os custos médios foram 7,9% mais altos, chegando a US$ 5,01 milhões.
Veja a Figura 22.

Tempo de recuperação

Mesmo depois que uma violação é contida, o trabalho de recuperação continua. Neste estudo, recuperação significa que:

- As operações de negócios voltaram ao normal nas áreas afetadas pela violação.
- As organizações cumpriram as obrigações de conformidade, como o pagamento de multas.
- A confiança dos clientes e dos funcionários foi restaurada.
- As organizações implementaram controles, tecnologias e conhecimento especializado para evitar futuras violações de dados.

Grande parte desse trabalho, como o restabelecimento da confiança do cliente, envolve fatores que vão além da tecnologia. Para a maioria das organizações, o trabalho árduo de recuperação pode levar meses.

As taxas de recuperação de violações foram baixas
Apenas 12% das organizações consultadas durante o relatório deste ano afirmaram ter se recuperado totalmente de suas violações de dados. A maioria das organizações disse que ainda estava trabalhando nelas. Veja a Figura 23.

A recuperação total levou mais de 100 dias
Entre as organizações que se recuperaram totalmente, mais de três quartos disseram que levaram mais de 100 dias. A recuperação é um processo demorado. Aproximadamente um terço das organizações que se recuperaram totalmente disseram que precisaram de mais de 150 dias para isso. Uma pequena parcela, 3%, das organizações totalmente recuperadas conseguiu se recuperar em menos de 50 dias. Veja a Figura 24.

Tempo médio de recuperação de uma violação de dados

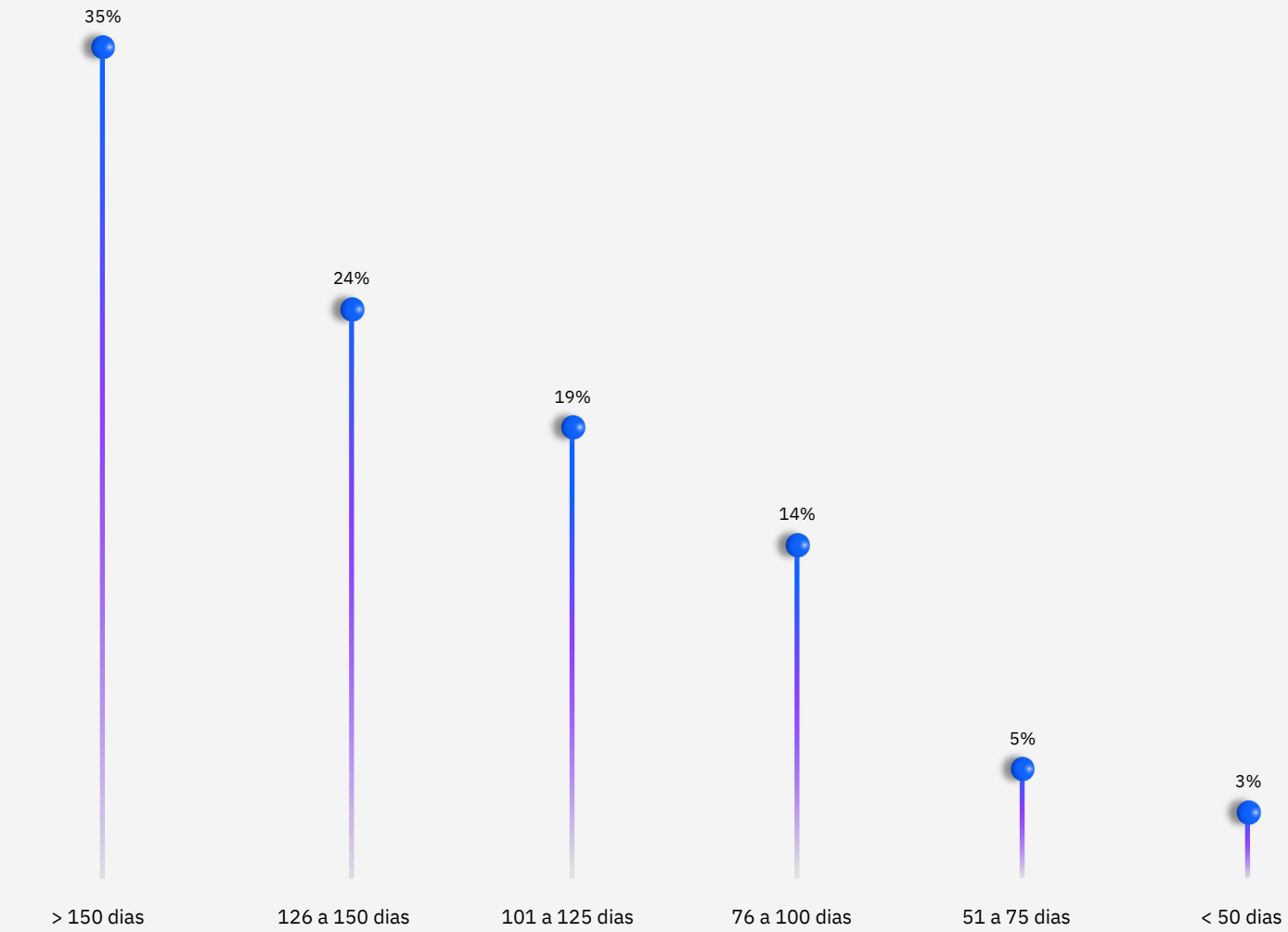


Figura 24. Das organizações que relataram ter se recuperado totalmente do incidente, medido em dias (consulte o gráfico 23)

Figura 25. Diferença de custo em relação à média de violação de US$ 4,88 milhões; medida em US$

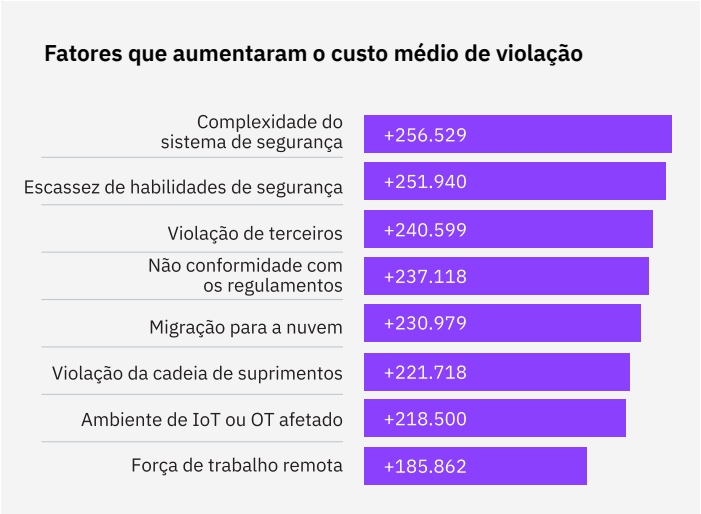


Figura 26. Diferença de custo em relação à média de violação de US$ 4,88 milhões; medida em US$

Fatores que diminuíram ou aumentaram o custo médio de violação

Ao analisar os custos, é útil saber quais tecnologias ou eventos tendem a reduzi-los ou aumentá-los. Uma constante que encontramos: a IA e a automação reduzem os custos, enquanto um alto nível de escassez de habilidades cibernéticas os aumenta. Nesta análise, examinamos 28 fatores contribuintes. Examinamos o impacto de cada um isoladamente em relação à média global. Em seguida, analisamos os três principais fatores que ampliam ou atenuam o custo médio de violação de dados.

Os principais fatores que reduziram os custos
O treinamento dos funcionários e o uso da IA e dos insights do aprendizado de máquina foram os principais fatores que reduziram os custos médios de violação de dados nessa análise. O treinamento de funcionários continua sendo um elemento essencial nas estratégias de defesa cibernética, especificamente para detectar e interromper os ataques de phishing. A IA e os insights do aprendizado de máquina vêm logo em seguida, em segundo lugar. Veja a Figura 25.

Os principais fatores que aumentaram os custos
Os três principais fatores que aumentaram os custos de violação nessa análise foram a complexidade do sistema de segurança, a escassez de habilidades de segurança e as violações de terceiros, que podem incluir violações da cadeia de suprimentos. Veja a Figura 26.

US$ 5,74 milhões

Custos médios de violação das organizações que sofreram uma escassez de alto nível de habilidades de segurança.

Níveis altos versus baixos dos principais fatores de aumento dos custos

Quando as organizações sofriam de um alto nível de escassez de habilidades de segurança, os custos médios da violação foram de US$ 5,74 milhões, em comparação com as organizações com um baixo nível de escassez de habilidades, com US$ 3,98 milhões. Disparidades semelhantes foram observadas em duas outras áreas importantes de fatores de custo. Veja a Figura 27.

Níveis altos versus baixos dos principais fatores de redução dos custos

Quando as organizações sofriam com baixos níveis de treinamento dos funcionários, os custos médios de violação foram de US$ 5,10 milhões, em comparação com as organizações com altos níveis de treinamento dos funcionários, com US$ 4,15 milhões. Disparidades semelhantes foram observadas em duas outras áreas importantes de fatores de custo. Veja a Figura 28.

Custo de uma violação de dados para organizações com um alto nível versus um baixo nível de três fatores amplificadores de custo

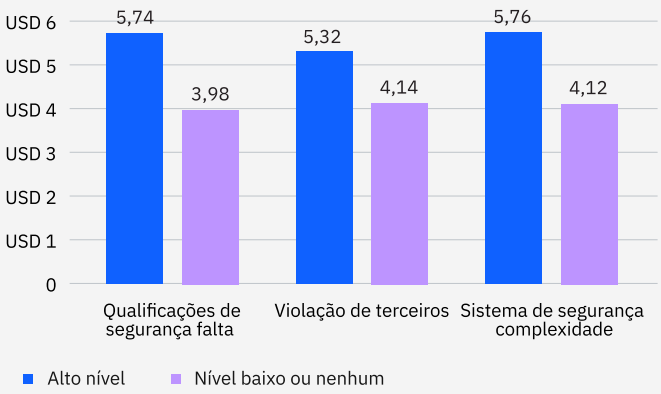


Figura 27. Medido em US$ milhões

Custo de uma violação de dados para organizações com um alto nível versus um baixo nível de três fatores atenuantes de custo

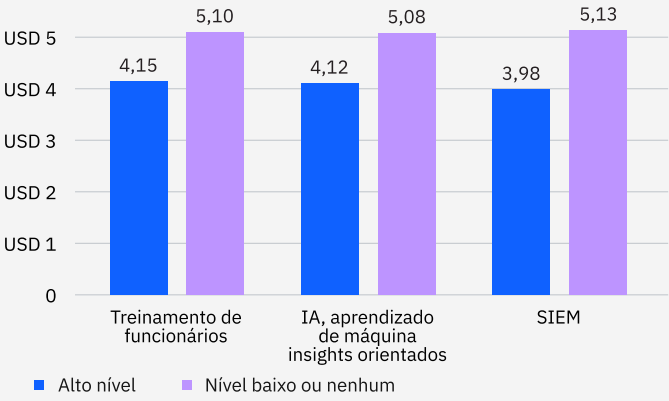


Figura 28. Medido em US$ milhões

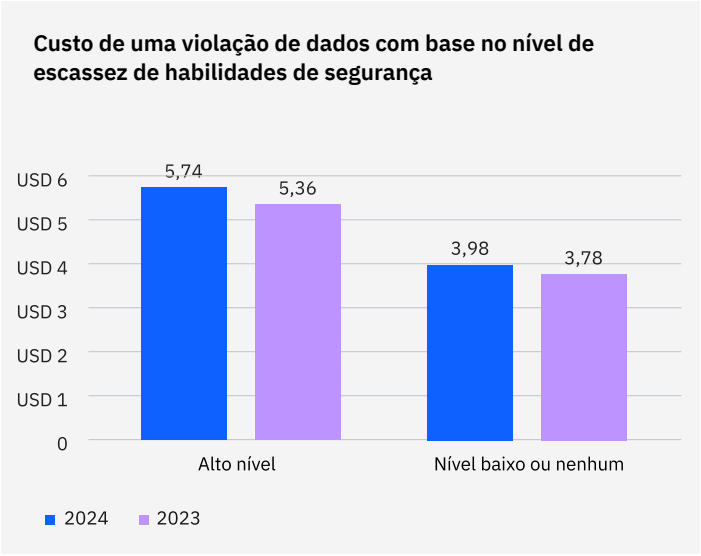


Figura 29. Medido em US$ milhões

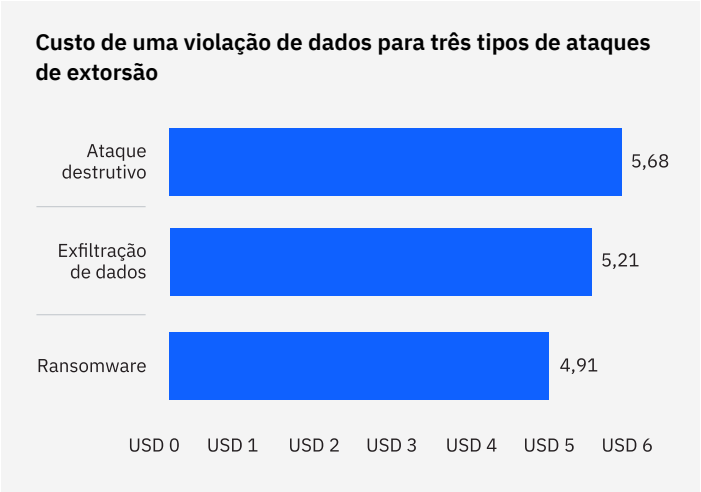


Figura 30. Medido em US$ milhões

Escassez de habilidades de segurança

O número de organizações que enfrentam uma falta crítica de funcionários da área de segurança qualificados aumentou drasticamente, para 53% em 2024, em comparação com 42% no ano passado. A pesquisa deste ano encontrou uma forte ligação entre o agravamento da escassez de habilidades e o aumento dos custos de violação de dados.

A escassez de habilidades equivale a custos de violação mais altos
Em 2024, o custo médio das violações associadas a um alto nível de escassez de habilidades saltou de US$ 5,36 milhões, no ano passado, para US$ 5,74 milhões, um aumento de 7,1%. Esse aumento foi US$ 860.000 a mais do que o custo médio global de violações. Veja a Figura 29.

O custo dos ataques de extorsão

O valor que uma organização gasta em ataques de extorsão pode variar de acordo com o tipo (ransomware, exfiltração de dados e destrutivo) e também com a forma como a organização responde. Esse fator é particularmente verdadeiro se a autoridade policial for acionada, como mostra o estudo deste ano, em que os custos caíram drasticamente quando investigadores da polícia estavam envolvidos. Todos os três tipos de ataques foram examinados, incluindo ransomware, em que os dados são criptografados e é exigido um resgate; exfiltração de dados, em que os dados são roubados e a organização às vezes é extorquida; e destrutivo, em que os invasores excluem dados e destroem sistemas para seus próprios objetivos.

O custo dos ataques destrutivos superou o de outras extorsões
Os ataques destrutivos, ou aqueles que têm a intenção de causar danos duradouros e caros, atingiram uma média de US$ 5,68 milhões e se mostraram mais caros do que os ataques de ransomware ou de exfiltração de dados. Veja a Figura 30.

63%

Parcela das vítimas de ransomware que envolveram as autoridades policiais e evitaram pagar um resgate.

Tempo para identificar e conter três tipos de ataques de extorsão
Todos os três tipos de ataques exigiram entre 284 e 294 dias para serem identificados e contidos. Veja a Figura 31.

Pagamento de resgate
Quando as organizações foram vítimas de ransomware, 52% recorreram às autoridades policiais. A maioria das que o fizeram, 63%, acabou não pagando o resgate. Veja a Figura 32.

Tempo para identificar e conter uma violação de dados com base na ocorrência de três tipos de ataques de extorsão

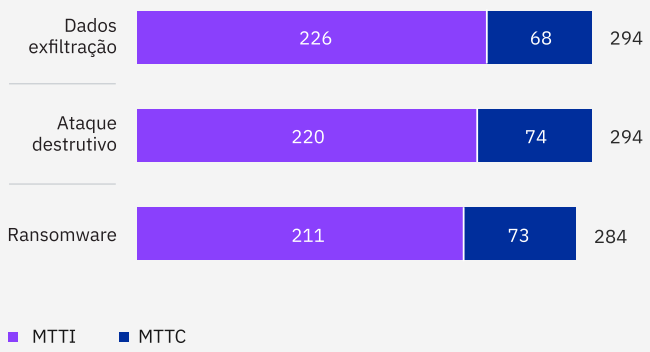


Figura 31. Medido em dias

Parcela das vítimas de ransomware que envolveram as autoridades policiais que pagaram um resgate

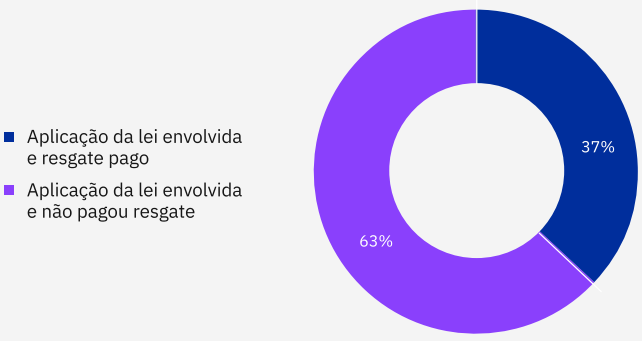


Figura 32.

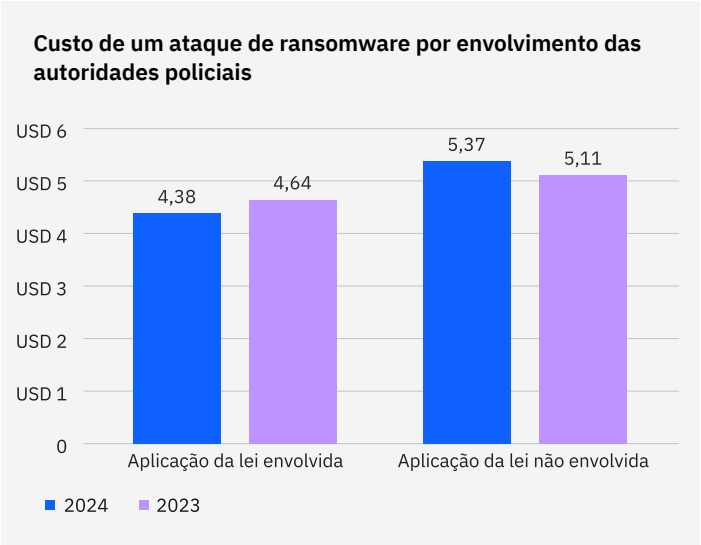


Figura 33. Medido em US$ milhões

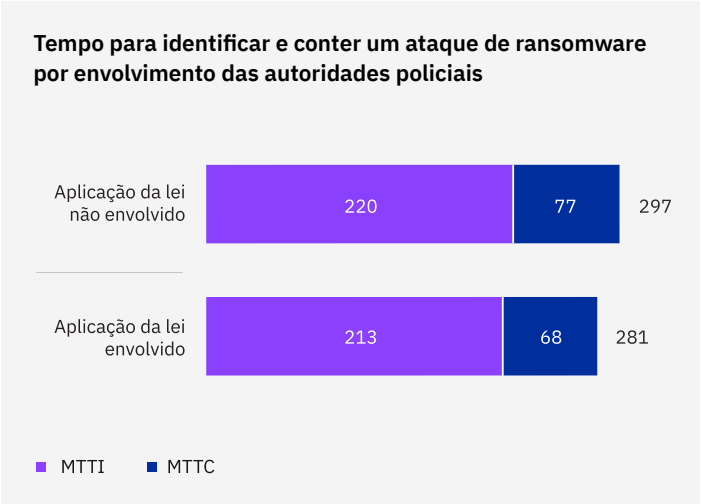


Figura 34. Medido em dias

O envolvimento das autoridades policiais reduziu os custos de violações

Os custos médios de violação variaram de US$ 4,38 milhões com o envolvimento das autoridades policiais a US$ 5,37 milhões sem o envolvimento das autoridades policiais, uma diferença de custos de mais de 20%, ou quase US$ 1 milhão. Observação: esses valores de custos não incluíram pagamentos de resgates. Veja a Figura 33. O envolvimento das autoridades policiais também acelerou o tempo necessário para identificar e conter uma violação. Veja a figura 34.

↑22,7%

Aumento na parcela de organizações que pagaram multas de mais de US$ 50.000.

Comunicação da violação e multas regulatórias

O relatório deste ano descobriu que a maioria das organizações relatou suas violações aos órgãos reguladores ou a outras agências governamentais. Cerca de um terço também pagou multas. Como resultado, a denúncia e o pagamento de multas se tornaram partes comuns das respostas pós-violação. O estudo analisou o valor das multas, bem como o tempo que as organizações levaram para divulgar a violação aos órgãos reguladores. A maioria das organizações relatou a violação em poucos dias.

Tempos médios de comunicação de violações
Mais da metade das organizações comunicou sua violação de dados em menos de 72 horas, enquanto 34% levou mais de 72 horas para comunicar. Apenas 11% não foram obrigadas a comunicar a violação. Veja a Figura 35.

O valor das multas regulatórias está aumentando
Mais organizações pagaram multas regulatórias mais altas, sendo que as que pagaram mais de US$ 50.000 aumentaram 22,7% em relação ao ano passado, e as que pagaram mais de US$ 100.000 aumentaram 19,5%. Veja a Figura 36.

Você teve que comunicar a violação devido a exigências regulatórias e, em caso afirmativo, quanto tempo levou para comunicar após a descoberta?

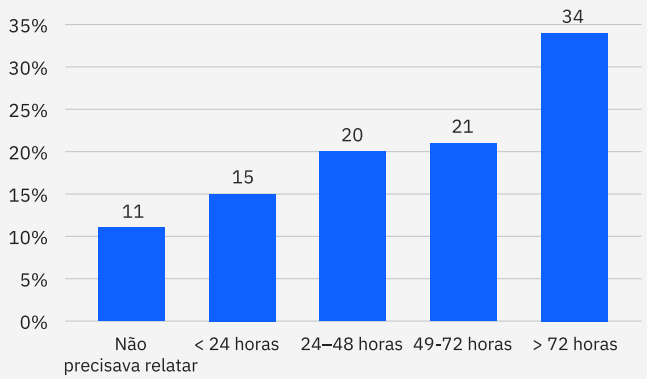


Figura 35. Parcela de todas as violações; é permitida apenas uma resposta

Distribuição do custo das multas decorrentes de uma violação de dados

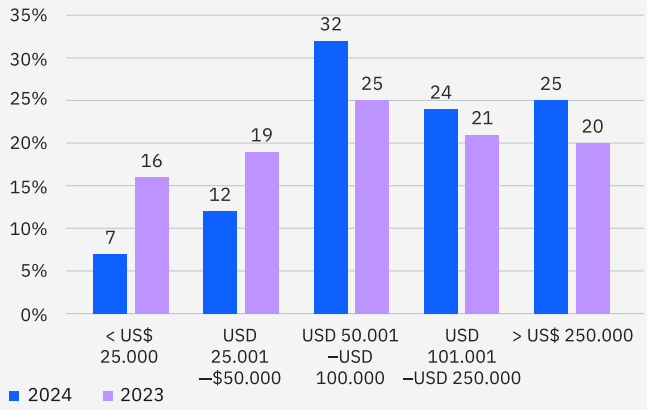


Figura 36. Entre aquelas que receberam multas, medidas em US$

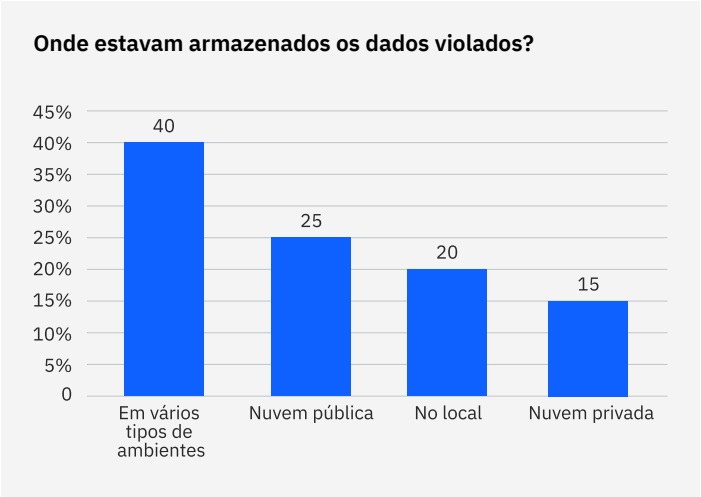


Figura 37. Parcela de todas as organizações; é permitida uma resposta

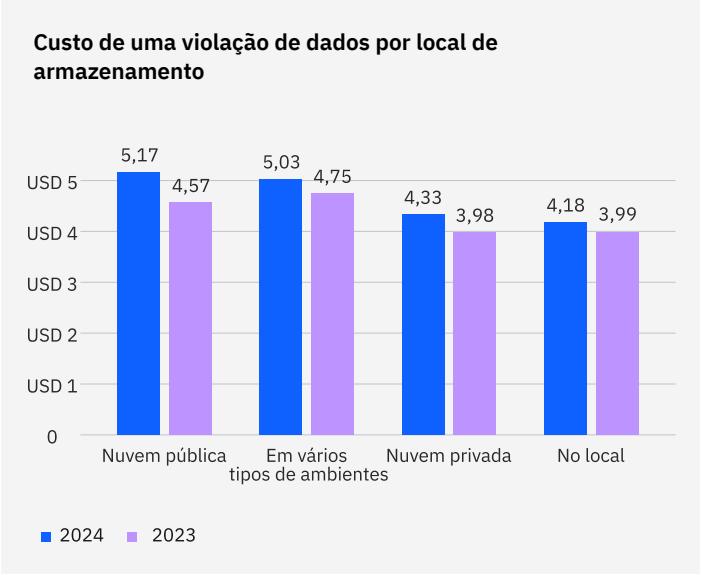


Figura 38. Medido em US$ milhões

Segurança de dados

Independentemente de onde os dados são armazenados, eles podem estar vulneráveis a uma violação. O estudo deste ano mostra que alguns lugares são mais vulneráveis e mais caros por violação do que outros. A maioria das violações envolveu dados distribuídos em vários ambientes ou em nuvens públicas. Ambas as opções de armazenamento foram associadas a ciclos de vida de violação mais longos e custos de violação mais altos.

Mesmo quando as organizações expandem e refinam suas estratégias de gerenciamento de dados, elas geralmente ignoram os dados ocultos, que são dados não gerenciados e provavelmente invisíveis para o departamento de TI. Isso pode ser resultado de funcionários que compartilham dados por meio de aplicações não autorizadas ou que os carregam em buckets de nuvem não oficiais. O relatório constatou que, quando as violações envolviam dados ocultos, elas duravam mais tempo e geravam custos maiores.

Violações na nuvem

Violações por local de dados
Cerca de 40% de todas as violações envolveram dados distribuídos em vários ambientes, como as nuvens públicas, nuvens privadas e no local. O menor número de violações no estudo envolveu o armazenamento de dados exclusivamente em uma nuvem pública, nuvem privada ou no local. Com os dados se tornando mais dinâmicos e ativos em todos os ambientes, é mais difícil descobrir, classificar, rastrear e também proteger. Veja a Figura 37.

Violações por local e custo
As violações de dados envolvendo exclusivamente nuvens públicas foram o tipo mais caro de violação de dados, custando em média US$ 5,17 milhões, um aumento de 13,1% em relação ao ano passado. As violações que envolviam vários ambientes eram mais comuns, mas um pouco mais baratas do que as violações de nuvem pública. As violações no local foram as menos dispendiosas. Veja a Figura 38.

US$ 5,27 milhões

Custo médio de uma violação de dados envolvendo dados ocultos.

Um controle centralizado significou uma remediação mais rápida
Quanto mais centralizado o controle que as organizações tinham sobre seus dados, mais rápido, em média, elas puderam identificar e conter uma violação. As violações envolvendo o armazenamento de dados exclusivamente no local levaram uma média de 224 dias para serem identificadas e contidas, 23,3% menos tempo do que os dados distribuídos entre ambientes, que levaram 283 dias. O mesmo padrão de controle local e ciclos de vida de violação mais curtos apareceu na comparação entre arquiteturas de nuvem privada e arquiteturas de nuvem pública. Veja a Figura 39.

Dados ocultos

Custos de violação dos dados ocultos
O custo médio de uma violação de dados envolvendo dados ocultos foi de US$ 5,27 milhões, 16,2% maior do que o custo médio sem dados ocultos. Veja a Figura 40.

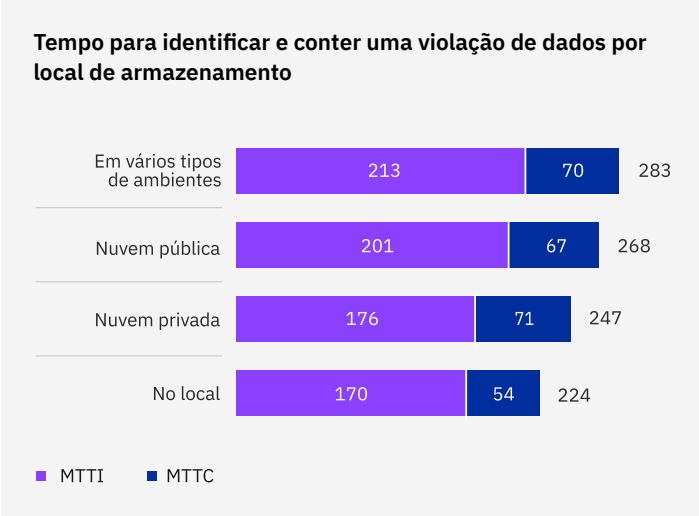


Figura 39. Medido em dias

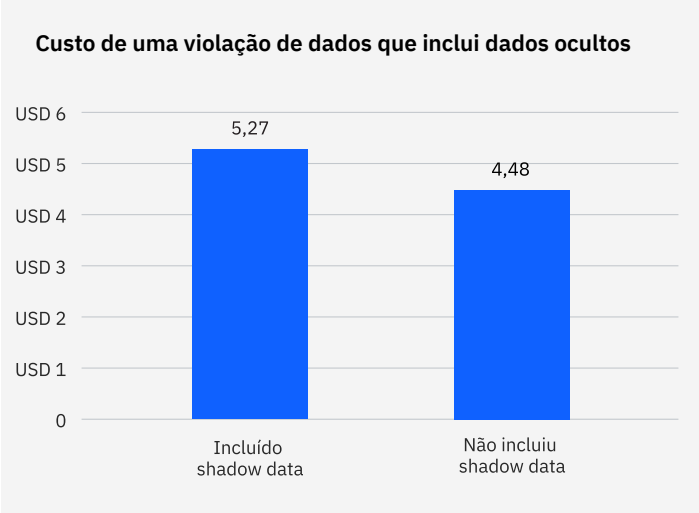


Figura 40. Medido em US$ milhões

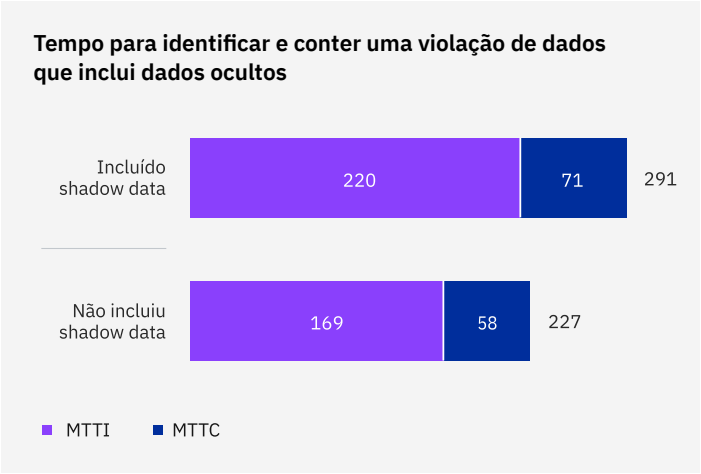


Figura 41. Medido em dias

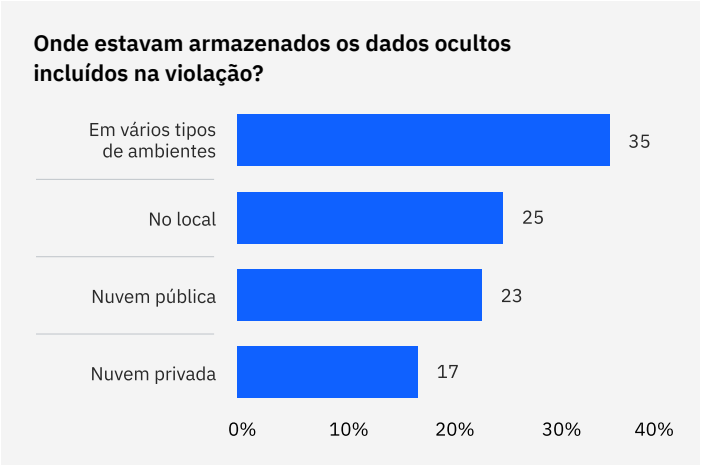
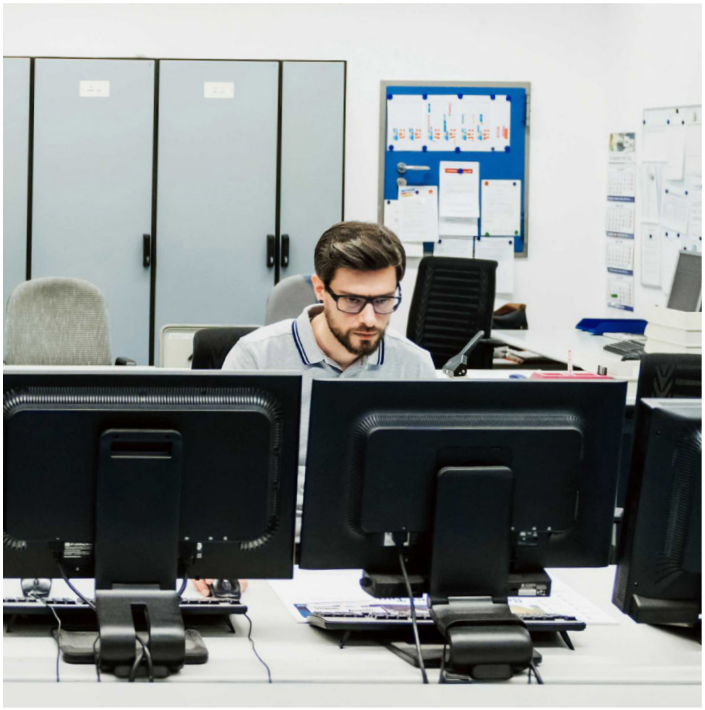


Figura 42. Porcentagem de violações envolvendo dados ocultos; é permitida uma resposta

Ciclos de vida das violações de dados ocultos
As violações que envolveram dados ocultos levaram 26,2% mais tempo, em média, para serem identificadas e 20,2% mais tempo, em média, para serem contidas do que aquelas que não envolveram dados ocultos. Esses aumentos resultaram na violação de dados com um ciclo de vida médio de 291 dias, 24,7% mais longo do que as violações de dados sem dados ocultos. Veja a Figura 41.

Dados ocultos em vários ambientes
Embora os dados ocultos tenham sido encontrados em todos os tipos de ambientes (nuvens públicas e privadas, no local e em vários ambientes), 25% das violações envolvendo dados ocultos foram exclusivamente no local. Essa descoberta significa que os dados ocultos não são estritamente um problema relacionado ao armazenamento em nuvem. Veja a Figura 42.



Megaviolações

As megaviolações, caracterizadas por mais de um milhão de registros comprometidos, são relativamente raras. Dessa forma, a pesquisa as trata separadamente da maioria das outras violações, em parte para que não distorçam a análise de violações de dados mais típicas.

Aumento dos custos das megaviolações
O custo médio de todas as categorias de tamanhos de megaviolações foi maior neste ano do que no ano passado. O salto foi mais acentuado nas maiores violações, que afetaram entre 50 milhões e 60 milhões de registros. O custo médio aumentou em 13%, e essas violações foram muitas vezes mais caras do que uma violação típica. Mesmo para a menor megaviolação (de um milhão a 10 milhões de registros), o custo médio foi quase nove vezes maior do que o custo médio global de US$ 4,88 milhões. Veja a Figura 43.

Custo de uma megaviolação por número de registros perdidos

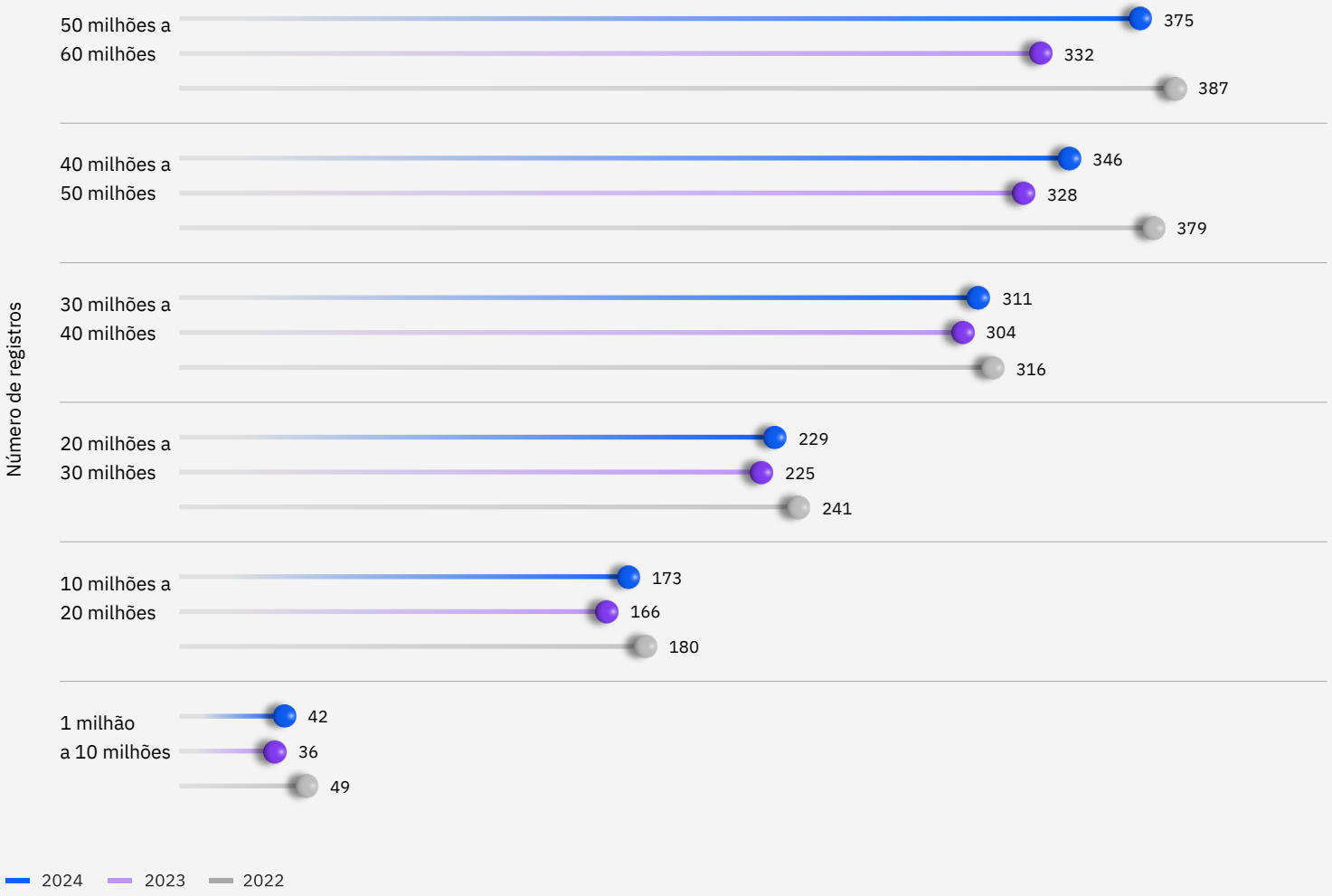


Figura 43. Medido em US$ milhões

↑23,5%

Aumento na parcela de organizações que planejam aumentar seus investimentos em segurança após uma violação.

Investimentos em segurança

Quando uma organização sofre uma violação, seus líderes de negócios e de TI geralmente aumentam seus investimentos em segurança. O estudo deste ano perguntou às organizações sobre seus planos para gastos futuros com segurança. Foi permitido que as organizações identificassem mais de uma área de investimento.

A parcela de organizações que fazem investimentos em segurança aumentou

Quase dois terços das organizações planejaram aumentar os investimentos em segurança após uma violação, um aumento de 23,5% em relação ao ano passado. Esse aumento pode refletir a percepção de que os custos de violações relacionados à perda de negócios e multas regulatórias continuam crescendo, juntamente com o potencial de danos à reputação. Veja a Figura 44.

Áreas populares de investimento em segurança

As duas áreas mais populares de investimento em segurança relatadas este ano foram planejamento e testes de IR, com 55%, e detecção de ameaças e tecnologias de resposta, com 51%. O foco das duas principais áreas de investimento foi a detecção de incidentes e ameaças suspeitas e a resposta mais rápida a eles. Muitas organizações também estavam planejando investir em segurança de dados e ferramentas de proteção, com 34%, e IAM, com 42%. Veja a Figura 45.

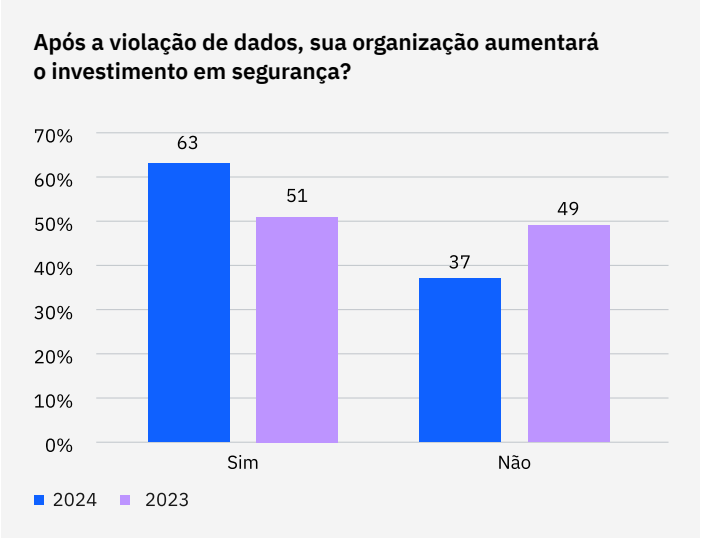
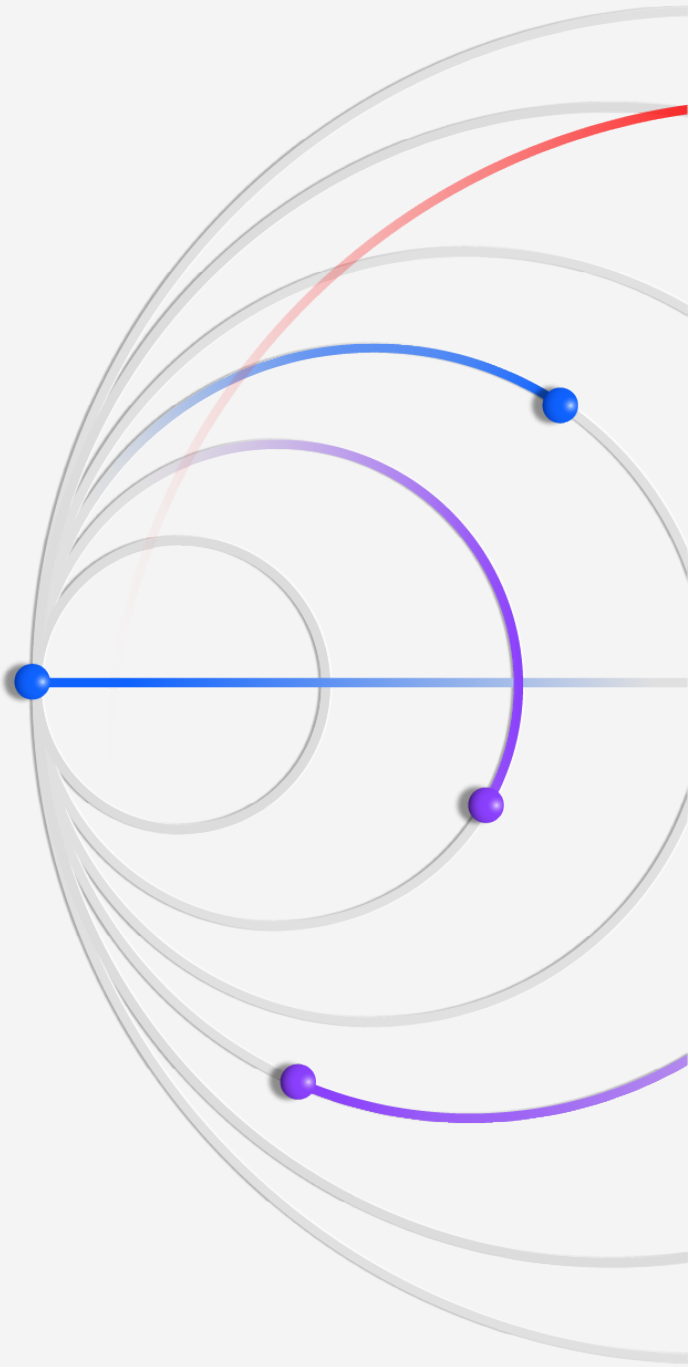


Figura 44. Porcentagem de todas as organizações

Figura 45. Parcela entre as organizações que estão aumentando o investimento em segurança; é permitida mais de uma resposta

Recomendações para ajudar a reduzir o custo da violação de dados



Nossas recomendações incluem abordagens de segurança de sucesso associadas a menores custos e menos tempo para identificar e conter violações.

Conheça seu cenário de informações

A maioria das organizações distribui dados em vários ambientes, incluindo repositórios de dados locais, nuvens privadas e nuvens públicas. No entanto, muitas organizações possuem inventários de dados incompletos ou desatualizados, atrasando os esforços para descobrir quais dados foram violados e quão sensíveis ou confidenciais são. Esses atrasos podem complicar a resposta e aumentar o custo de uma violação.

As equipes de segurança devem garantir que tenham visibilidade abrangente em todos esses ambientes, para que possam monitorar e proteger continuamente os dados, independentemente de onde eles estejam. As organizações podem aplicar gerenciamento de postura de segurança de dados (DSPM) e outras soluções, como gerenciamento de acesso à identidade e ASM, em todos esses ambientes para proteção consistente e abrangente.

As equipes de segurança devem prestar atenção extra a ambientes híbridos e nuvens públicas. Cerca de 40% das violações de dados envolveram dados armazenados em múltiplos ambientes, e quando os dados violados estavam armazenados em nuvens públicas, o custo médio da violação foi o mais alto, chegando a US$ 5,17 milhões. É imperativo que as equipes de segurança obtenham uma compreensão mais profunda dos riscos específicos e controles para cada serviço de nuvem que empregam.

Gerenciar dados em vários ambientes torna-se ainda mais complicado pelo impacto dos dados não gerenciados. Mais de um terço das violações de dados envolvem dados ocultos. As equipes de segurança devem agora assumir que suas organizações possuem fontes de dados não gerenciadas. Dados não criptografados, incluindo dados em cargas de trabalho de IA, aumentam ainda mais o risco. As estratégias de criptografia de dados devem considerar os tipos de dados, seu uso e onde eles estão localizados para reduzir o risco em caso de violação.

Fortaleça as estratégias de prevenção com IA e automação

A adoção de modelos de IA generativa e aplicações de terceiros em toda a organização — assim como o uso contínuo de dispositivos de internet das coisas (IoT) e aplicações SaaS — está expandindo a superfície de ataque, colocando pressão sobre as equipes de segurança.

Aplicar IA e automação que apoiem estratégias de prevenção de segurança — incluindo nas áreas de ASM, red-teaming e gerenciamento de postura — pode ser frequentemente abordado por serviços de segurança gerenciados. Organizações que aplicaram IA e automação para prevenção de segurança viram o maior impacto de seus investimentos em IA no estudo deste ano, em comparação com outras três áreas de segurança: detecção, investigação e resposta. Elas economizaram uma média de US$ 2,22 milhões em comparação com aquelas que não implementaram IA em tecnologias de prevenção.

Adote uma abordagem de segurança primeiro para a IA generativa

Enquanto as organizações avançam rapidamente com a IA generativa, apenas 24% das iniciativas de IA generativa estão sendo protegidas. A falta de segurança ameaça expor dados e modelos de dados a violações, potencialmente minando os benefícios que os projetos de IA generativa pretendem entregar.

À medida que a adoção de IA generativa continua a escalar, as organizações precisam de um framework para proteger dados, modelos e uso de IA generativa, além de estabelecer controles de governança de IA. Elas precisarão proteger os dados de treinamento contra roubo e manipulação. As organizações podem usar a descoberta e classificação de dados para detectar dados sensíveis usados no treinamento ou ajuste fino. Elas também podem implementar controles de segurança de dados em criptografia, gerenciamento de acesso e monitoramento de conformidade.

Com a IA generativa, as organizações enfrentam não apenas o risco de crescimento de dados ocultos, mas também de modelos ocultos. As organizações devem estender o gerenciamento de postura aos próprios modelos de IA para proteger dados sensíveis de treinamento de IA, obter visibilidade do uso de modelos de IA não autorizados ou *modelos ocultos de IA*, e mau uso de IA ou vazamento de dados.

Proteger o desenvolvimento de modelos de IA generativa requer a varredura de vulnerabilidades no pipeline, fortalecer integrações e impor políticas e acesso. Para proteger o uso de modelos de IA generativa, as equipes de segurança devem monitorar inputs maliciosos, como injeções de prompts, e outputs contendo dados sensíveis. Elas também devem implementar soluções de segurança de IA que possam detectar e responder a ataques específicos de IA, como envenenamento de dados, evasão de modelo e extração de modelo. Desenvolver playbooks de resposta para negar acesso, isolar e desconectar modelos comprometidos também é essencial.

Com a expansão dos cenários de ameaças devido à IA generativa e outras iniciativas de TI, é necessário oferecer treinamento de segurança para profissionais não especializados em segurança, incluindo cientistas de dados e engenheiros de dados que trabalham em equipes de IA.

Melhore seu treinamento de resposta cibernética

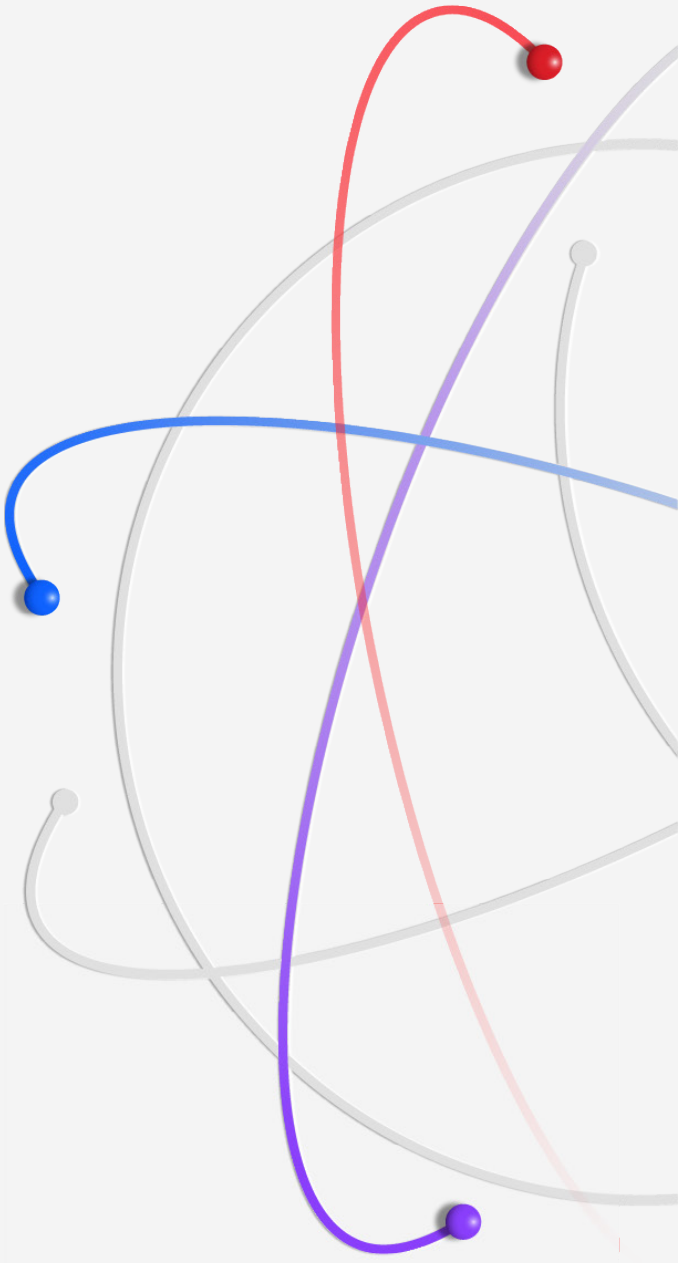
A forma como uma organização reage e se comunica durante e após uma violação — com a liderança empresarial, os órgãos reguladores e os clientes — é mais importante do que nunca. Para melhorar sua capacidade de lidar com ataques de alto impacto, as organizações podem desenvolver seu reflexo para respostas a violações participando de exercícios de simulação de crises em alcance cibernético.

Esses exercícios podem incluir equipes de segurança e líderes empresariais, para que toda a organização melhore sua capacidade de detectar, conter e responder a violações. Os líderes de segurança devem trabalhar com suas funções empresariais em toda a organização e equipes de comunicação com antecedência para elaborar planos de resposta e testá-los. Com a expansão dos cenários de ameaças devido à IA generativa e outras iniciativas de TI, é necessário oferecer treinamento de segurança para profissionais não especializados em segurança. Esses profissionais incluem cientistas de dados e engenheiros de dados que trabalham em equipes de aprendizado de máquina e IA, e aqueles responsáveis pela continuidade das cargas de trabalho de IA em ativos locais e na nuvem.

Ao investir na preparação de resposta, as organizações podem ajudar a reduzir os efeitos dispendiosos e disruptivos das violações de dados, apoiar a continuidade operacional e ajudar a preservar seus relacionamentos com clientes, parceiros e outros stakeholders. Além disso, uma resposta ensaiada tranquiliza os funcionários e reduz o estresse, a angústia e o atrito internamente, à medida que as etapas agudas de um ataque são tratadas, controladas e comunicadas por uma equipe de liderança bem preparada.

Dados demográficos da organização

O estudo deste ano examinou 604 organizações de vários tamanhos em 16 países e regiões geográficas e 17 setores. Esta seção explora o detalhamento das organizações no estudo por região geográfica e setor e define as classificações dos setores.



Dados demográficos geográficos

O estudo de 2024 foi realizado em 16 países e regiões geográficas. Uma nova região adicionada ao estudo este ano foi Benelux, a união econômica da Bélgica, Holanda e Luxemburgo. A Escandinávia foi excluída do estudo.

A ASEAN é uma amostra de um grupo de organizações localizadas em Singapura, Indonésia, Filipinas, Malásia, Tailândia e Vietnã. A América Latina é uma amostra de um grupo de organizações localizadas no México, Argentina, Chile e Colômbia. O Oriente Médio é uma amostra de um grupo de organizações localizadas na Arábia Saudita e nos Emirados Árabes Unidos.

Visão geral do estudo global

Países e regiões	Amostra de 2024	% da amostra total	Anos estudados	Moeda
ASEAN	25	4%	8	Dólar de Singapura (SGD)
Austrália	27	4%	15	Dólar australiano (AUD)
Benelux	32	5%	1	Euro (EUR)
Brasil	45	7%	12	Real brasileiro (BRL)
Canadá	28	5%	10	Dólar canadense (CAD)
França	36	6%	15	Euro (EUR)
Alemanha	47	8%	16	Euro (EUR)
Índia	53	9%	13	Rúpia indiana (INR)
Itália	29	5%	13	Euro (EUR)
Japão	42	7%	13	Iene (JPY)
América Latina	28	5%	5	Peso mexicano (MXN)
Oriente Médio	39	6%	11	Rial da Arábia Saudita (SAR)
África do Sul	24	4%	9	Rand sul-africano (ZAR)
Coreia do Sul	28	5%	7	Won (KRW)
Reino Unido	50	8%	17	Libra esterlina (GBP)
Estados Unidos	71	12%	19	Dólar dos EUA (US$)
Total	604	100%		

Figura 46. Parcela de todas as organizações do estudo

Dados demográficos do setores

A seleção de 17 setores tem sido consistente em vários anos do estudo. Este ano, os quatro principais setores (financeiro, industrial, serviços profissionais e tecnologia) responderam por 47% das 604 organizações estudadas.

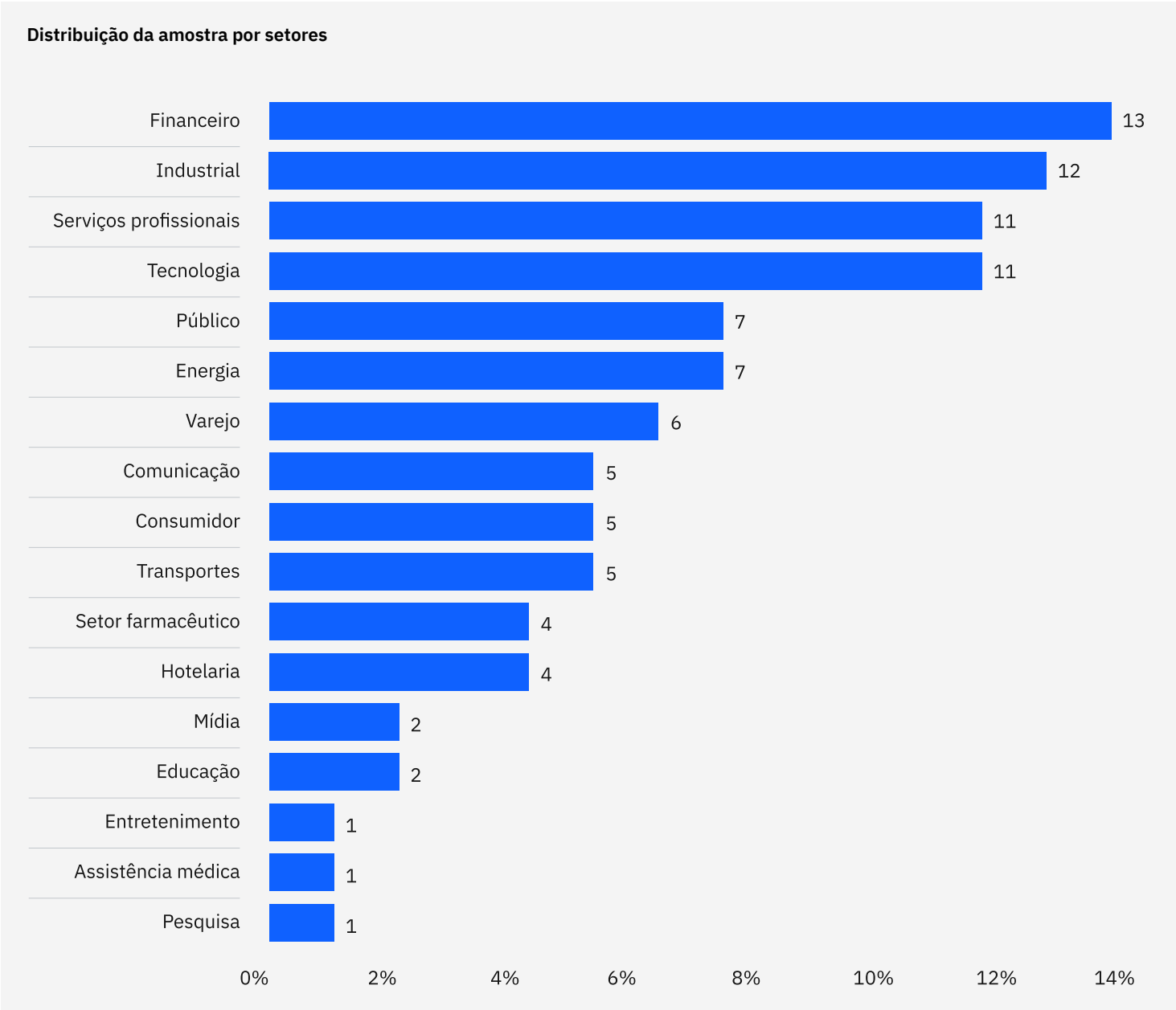


Figura 47. Parcela de todas as organizações do estudo

Definições dos setores

Assistência médica
Hospitais e clínicas

Financeiro
Empresas do setor bancário, de seguro e de investimento

Energia
Empresas de petróleo e gás, empresas de serviços públicos e produtores e fornecedores de energia alternativa

Produtos farmacêuticos
Empresas farmacêuticas, incluindo ciências da vida biomédicas

Industrial
Processamento e engenharia química e empresas de manufatura

Tecnologia
Empresas de software e hardware

Educação
Universidades e faculdades públicas e privadas e empresas de treinamento e desenvolvimento

Serviços profissionais
Serviços profissionais, como empresas jurídicas, contábeis e de consultoria

Entretenimento
Produção de filmes, esportes, jogos e cassinos

Transportes
Companhias aéreas, ferrovias, caminhões e de entrega

Comunicações
Jornais, editoras de livros e agências de relações públicas e publicidade

Consumidor
Fabricantes e distribuidores de produtos de consumo

Mídia
Televisão, satélite, redes sociais e internet

Hotelaria
Hotéis, cadeias de restaurantes e linhas de cruzeiro

Varejo
Lojas físicas e de comércio eletrônico

Pesquisa
Pesquisa de mercado, think tanks e pesquisa e desenvolvimento

Público
Órgãos do governo federal, estadual e municipal e organizações não governamentais

Metodologia de pesquisa

Para preservar a confidencialidade, o instrumento de referência não capturou nenhuma informação específica das empresas. Os métodos de coleta de dados excluíram informações contábeis reais e, em vez disso, dependiam de os participantes estimarem os custos diretos marcando uma variável de intervalo em uma linha numérica. Os participantes foram instruídos a marcar a linha numérica em um ponto entre os limites inferior e superior de um intervalo para cada categoria de custo.

O valor numérico obtido a partir da linha numérica, em vez de uma estimativa pontual para cada categoria de custo apresentada, preservou a confidencialidade e garantiu uma taxa de resposta mais alta. O instrumento de referência também exigia que os entrevistados fornecessem uma segunda estimativa separada para os custos indiretos e de oportunidade.

A fim de manter um conjunto de dados gerenciável para comparação, o relatório incluiu apenas os centros de atividades de custo com um impacto crucial nos custos de violação de dados. Com base em discussões com especialistas, foi escolhido um conjunto fixo de atividades de custo. Depois de coletar as informações de referência, cada instrumento foi cuidadosamente reexaminado para verificar sua consistência e integridade.

O escopo dos fatores de custo da violação de dados foi limitado a categorias conhecidas que se aplicam a um amplo conjunto de operações de negócios que envolvem informações pessoais. Optamos por nos concentrar nos processos de negócios em vez de nas atividades de proteção de dados ou de conformidade com a privacidade porque acreditávamos que o estudo do processo produziria resultados de melhor qualidade.

Como calculamos o custo de uma violação de dados

Para calcular o custo médio de uma violação de dados, excluímos as violações muito pequenas e muito grandes. As violações de dados examinadas no relatório de 2024 variaram entre 2.100 e 113.000 registros comprometidos. Usamos uma análise separada para examinar os custos das megaviolações; essa metodologia é explicada mais detalhadamente na seção "Perguntas frequentes sobre violação de dados" deste relatório.

Usamos o custo baseado em atividades, que identifica as atividades e atribui um custo de acordo com o uso real. Quatro atividades relacionadas a processos geraram uma série de despesas associadas à violação de dados de uma organização: detecção e escalonamento, notificação, resposta pós-violação e perda de negócios.

Detecção e escalonamento
As atividades que permitem que uma organização detecte a violação incluem:

- Atividades forenses e investigativas
- Serviços de avaliação e auditoria
- Gerenciamento de crises
- Comunicações para executivos e diretorias

Notificações
As atividades que permitem que uma organização notifique os titulares dos dados, os órgãos reguladores de proteção de dados e outros terceiros incluem:

- E-mails, cartas, chamadas ou avisos gerais aos titulares dos dados
- Determinação dos requisitos regulatórios
- Comunicação com os órgãos reguladores
- Contratação de um especialista externo

Resposta pós-violação
As atividades para ajudar as vítimas de uma violação a se comunicarem com uma organização e conduzir atividades de reparação às vítimas e órgãos reguladores incluem:

- Help desk e recebimento de comunicações
- Serviços de monitoramento de crédito e proteção de identidade
- Criação de novas contas ou cartões de crédito
- Despesas legais
- Descontos em produtos
- Multas regulatórias

Perda de negócios
As atividades que tentam minimizar a perda de clientes, a interrupção dos negócios e as perdas de receita incluem:

- Interrupção dos negócios e perdas de receita devido ao downtime do sistema
- Custo de perda de clientes e aquisição de novos clientes
- Danos à reputação e diminuição do fundo de comércio

Perguntas frequentes sobre a violação de dados

O que é uma violação de dados?
Uma violação de dados é definida como um evento no qual os registros que contêm informações de identificação pessoal; informações de contas financeiras ou médicas; ou outros dados secretos, confidenciais ou proprietários são potencialmente colocados em risco. Esses registros podem estar em formato eletrônico ou em papel. As violações incluídas no estudo variaram entre 2.100 e 113.000 registros comprometidos.

O que é um registro comprometido?
Um registro é uma informação que revela dados corporativos, governamentais ou financeiros confidenciais ou proprietários, ou identifica um indivíduo cujas informações foram perdidas ou roubadas em uma violação de dados. Exemplos incluem um banco de dados com o nome de um indivíduo, informações de cartão de crédito e outras PII, ou um registro de saúde com o nome do segurado e informações de pagamento.

Como os dados são coletados?
Nossos pesquisadores coletaram dados qualitativos minuciosos em 3.556 entrevistas separadas com indivíduos de 604 organizações que sofreram uma violação de dados entre março de 2023 e fevereiro de 2024. Os entrevistados estavam familiarizados com a violação de dados de sua organização e com os custos associados à resolução da violação. Esses entrevistados incluíram CEOs ou executivos, chefes de operações, controladores ou chefes de finanças, profissionais de TI, líderes de unidades de negócios e gerentes gerais, além de profissionais de gerenciamento de risco e cibersegurança. Por questões de privacidade, não coletamos informações específicas das organizações.

O que está incluído no custo de uma violação de dados?
Coletamos as despesas diretas e indiretas incorridas pela organização. As despesas diretas incluíram a contratação de especialistas forenses, a terceirização do suporte da linha direta e o fornecimento de assinaturas sem custo de monitoramento de crédito e descontos para produtos e serviços futuros. Os custos indiretos incluíram investigações e comunicações internas, juntamente com o valor extrapolado da perda de clientes resultante da rotatividade ou da diminuição das taxas de aquisição de clientes.

Esta pesquisa incluiu apenas eventos diretamente relevantes para a experiência da violação de dados. Regulamentos, como o General Data Protection Regulation (GDPR) e o California Consumer Privacy Act (CCPA), podem incentivar as organizações a aumentarem os investimentos em suas tecnologias de governança de cibersegurança. No entanto, essas atividades não afetaram diretamente o custo de uma violação de dados para os fins desta pesquisa. Para manter a consistência com os anos anteriores, usamos o mesmo método de conversão de moeda em vez de ajustar os custos contábeis.

Como a pesquisa de referência difere da pesquisa por entrevista?
A unidade de análise no relatório do custo das violações de dados foi a organização. Na pesquisa por entrevista, a unidade de análise é o indivíduo. Recrutamos 604 organizações para participar deste estudo.

O custo médio por registro pode ser usado para calcular o custo de violações que envolvem milhões de registros perdidos ou roubados?
Não é coerente com essa pesquisa usar o custo geral por registro como base para calcular o custo de violações únicas ou múltiplas que totalizem milhões de registros. O custo por registro é derivado do nosso estudo de centenas de eventos de violações de dados em que cada evento apresentou um máximo de 113.000 registros comprometidos. Para medir o impacto das megaviolações que envolvem um milhão ou mais de registros, o estudo usa uma simulação com base em uma amostra de 17 eventos desse tamanho.

Por que foram usados métodos de simulação para estimar o custo de uma megaviolação de dados?
O tamanho da amostra de 17 organizações que sofreram uma megaviolação não foi grande o suficiente para permitir uma análise estatisticamente significativa usando os métodos de custo baseados nas atividades do estudo. Para solucionar esse problema, implementamos simulações de Monte Carlo para estimar uma gama de resultados possíveis, ou seja, aleatórios, por meio de tentativas repetidas. No total, realizamos mais de 269.000 testes. A média geral de todas as médias das amostras forneceu um resultado mais provável para cada tamanho de violação de dados, variando de um milhão a 53 milhões de registros comprometidos.

As mesmas organizações são acompanhadas todos os anos?
Cada estudo anual envolve uma amostra diferente de organizações. Para sermos consistentes com os relatórios anteriores, recrutamos e combinamos anualmente organizações com características semelhantes, como o setor da organização, o número de funcionários, a pegada de carbono geográfica e o tamanho da violação de dados. Desde o início dessa pesquisa, em 2005, estudamos as experiências de violações de dados de 6.184 organizações.

Limitações da pesquisa

Nosso estudo usou um método de referência confidencial e exclusivo que foi implementado com sucesso em pesquisas anteriores. No entanto, as limitações inerentes a essa pesquisa de referência precisam ser cuidadosamente consideradas antes de serem tiradas conclusões dos resultados.

Resultados não estatísticos
Nosso estudo se baseou em uma amostra representativa e não estatística de entidades globais. Inferências estatísticas, margens de erro e intervalos de confiança não podem ser aplicados a esses dados, uma vez que nossos métodos de amostragem não eram científicos.

Falta de resposta
O viés da falta de resposta não foi testado; portanto, é possível que as organizações que não participaram sejam substancialmente diferentes em termos de custo subjacente da violação de dados.

Viés do quadro de amostragem
Como nossa amostragem foi feita com base em critérios de julgamento, a qualidade dos resultados foi influenciada pelo grau em que a estrutura representava a população das organizações que estavam sendo estudadas. Acreditamos que o quadro de amostragem atual foi tendencioso em relação a organizações com programas de privacidade ou segurança da informação mais maduros.

Informações específicas das organizações
A referência não capturou informações que identificassem as organizações. Os indivíduos poderiam usar variáveis de resposta categórica para divulgar informações demográficas sobre a categoria e o setor da organização.

Fatores não medidos
Omitimos variáveis das nossas análises, como as principais tendências e as características organizacionais. Não é possível determinar até que ponto as variáveis omitidas podem explicar os resultados da referência.

Resultados dos custos extrapolados
Embora certas verificações e balanços possam ser incorporados ao processo de referência, é sempre possível que os entrevistados não tenham fornecido respostas precisas ou verdadeiras. Além disso, o uso de métodos de extrapolação de custos, em vez de dados de custos reais, pode inadvertidamente introduzir vieses e imprecisões.

Conversões de moedas
A conversão das moedas locais para o dólar dos EUA deflacionou as estimativas de custo total médio em outros países. Para fins de consistência com os anos anteriores, decidimos continuar usando o mesmo método contábil em vez de ajustar o custo. É importante observar que esse problema pode afetar apenas a análise global, pois todos os resultados em nível de país são mostrados nas moedas locais. As taxas de câmbio reais atuais usadas neste relatório de pesquisa foram publicadas pelo Federal Reserve em 4 de março de 2024.

Sobre a IBM e o Ponemon Institute

IBM

A IBM é uma fornecedora líder global de serviços de nuvem híbrida, IA e negócios, ajudando clientes em mais de 175 países a capitalizar sobre insights de seus dados, simplificar processos empresariais, reduzir custos e obter vantagem competitiva em seus setores. Tudo isso é respaldado pelo compromisso lendário da IBM com confiança, transparência, responsabilidade, inclusão e serviço. Para mais informações, visite www.ibm.com/br-pt.

Saiba mais sobre como melhorar sua postura de segurança:

Acesse ibm.com/br-pt/security

Junte-se à conversa na comunidade do IBM Security

Ponemon Institute

Fundado em 2002, o Ponemon Institute é dedicado à pesquisa e educação independentes que avançam práticas responsáveis de gestão de informações e privacidade nos negócios e no governo. Nossa missão é conduzir estudos empíricos de alta qualidade sobre questões críticas que afetam o gerenciamento e a segurança de informações sensíveis sobre pessoas e organizações.

O Ponemon Institute mantém rigorosos padrões de confidencialidade de dados, privacidade e pesquisa ética e não coleta nenhuma informação de identificação pessoal (PII) de indivíduos ou informações identificáveis de empresas em pesquisas empresariais. Além disso, rigorosos padrões de qualidade garantem que os sujeitos não sejam questionados sobre perguntas extrínsecas, irrelevantes ou inadequadas.

Se você tiver perguntas ou comentários sobre este relatório de pesquisa, incluindo pedidos de permissão para citar ou reproduzir o relatório, entre em contato conosco por carta, telefone ou e-mail:

Ponemon Institute LLC
Departamento de pesquisa
1-800-887-3118
research@ponemon.org

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo, SP
IBM Corporation
New Orchard Road
Armonk, NY 10504, EUA

Produzido nos
Estados Unidos da América
Julho de 2024