Estudo do Custo de Violações de Dados 2014: Análise Global

Pesquisa de referência patrocinada pela IBM
Realizada de modo independente pelo Ponemon Institute LLC
Maio de 2014

Relatório de Pesquisa do Ponemon Institute©

Estudo do Custo de Violações de Dados 2014[1]: Análise Global

Ponemon Institute, Maio de 2014

Parte 1. Introdução

A IBM e o Ponemon tem o prazer de apresentar o nono *Estudo do Custo de Violações de Dados: Estudo Global anual.* De acordo com a pesquisa, o custo total médio de uma violação de dados para as empresas participantes cresceu 15%, chegando a US$3,5 milhões[2]. O custo médio pago pela perda ou roubo de um registro que contém informações sensíveis ou confidenciais subiu mais de 9%, ou seja, de US$136 em 2013 para US$145 no estudo deste ano.

Pela primeira vez, nosso estudo examina a probabilidade de uma empresa ter uma ou mais ocorrências de violação de dados nos próximos 24 meses. De acordo com as experiências das empresas que participaram da pesquisa, acreditamos que é possível prever a probabilidade de uma violação de dados com base em dois fatores: quantos registros foram perdidos ou roubados e o segmento de mercado da empresa. As conclusões sugerem que organizações da Índia e do Brasil estão mais propensas a ter uma violação de dados envolvendo pelo menos 10.000 registros. Por outro lado, organizações da Alemanha e da Austrália estão menos propensas a ter uma violação. Em todos os casos, é mais provável que uma empresa tenha uma violação envolvendo 10.000 registros ou menos do que uma superviolação envolvendo mais de 100.000 registros.

No estudo deste ano, participaram 314 empresas representando os 10 países a seguir: Estados Unidos, Reino Unido, Alemanha, Austrália, França, Brasil, Japão, Itália, Índia e, pela primeira vez, a região árabe (Emirados Árabes Unidos e Arábia Saudita). Todas as organizações participantes tiveram uma violação de dados, variando de aproximadamente 2.415 registros[3] comprometidos para pouco mais de 100.000 . Um registro comprometido é definido como um registro que identifica o indivíduo cujas informações foram perdidas ou roubadas em uma violação de dados.

As conclusões revelam que o custo médio *per capita* consolidado da violação de dados (compilado para 10 países e convertido para dólares dos Estados Unidos) varia muito entre os países. Muitas dessas diferenças de custo podem ser atribuídas aos tipos de ataques e ameaças que as organizações enfrentam, bem como aos regulamentos e leis de proteção de dados em seus respectivos países. No estudo global deste ano, a violação de dados média consolidada subiu de US$136 para US$145. Entretanto, organizações da Alemanha e dos Estados Unidos têm, em média, custos muito mais elevados (respectivamente, US$195 e US$201).

O Ponemon Institute realizou seu primeiro estudo *Custo de Violações de Dados* nos Estados Unidos nove anos atrás. Desde então, o estudo foi expandido e passou a incluir o Reino Unido, Alemanha, França, Austrália, Índia, Itália, Japão, Brasil e, pela primeira vez este ano, Emirados Árabes Unidos e Arábia Saudita. Até o momento, 1.279 organizações de negócios e do governo (setor público) participaram do processo de referência desde o início desta série de pesquisa.

Conforme mencionado acima, o estudo deste ano examina os custos incorridos por 314 empresas em 16 segmentos de mercado depois que elas passaram pela perda ou roubo de dados pessoais protegidos. É importante ressaltar que os custos apresentados nesta pesquisa não são hipotéticos, mas vêm de incidentes reais de perda de dados. Baseiam-se nas estimativas de custo fornecidas pelos 1.690 indivíduos entrevistados durante um período de 10 meses nas empresas que estão representadas nesta pesquisa.

Estas são as diferenças mais notáveis entre os países, medidas em dólares dos Estados Unidos:

- **As violações mais caras e menos caras.** As empresas da Alemanha e dos Estados Unidos tiveram as violações de dados mais caras (respectivamente, US$201 e US$195 por registro). Esses países também apresentaram o custo total mais elevado (Estados Unidos: US$5,85 milhões; Alemanha:

[1]Pela primeira vez, a data deste relatório é o ano de publicação, não a data de conclusão do trabalho de campo. Observe que a maioria dos incidentes de violação de dados estudados neste relatório ocorreu no ano-calendário de 2013.
[2]As moedas locais foram convertidas para dólares dos Estados Unidos.
[3]Os termos "custo por registro comprometido" e "custo *per capita*" têm um significado equivalente neste relatório.

US$4,74 milhões). As violações menos caras ocorreram no Brasil e na Índia (respectivamente, US$70 e US$51). No Brasil, o custo médio total para uma empresa foi de US$1,61 milhão; na Índia, foi de US$1,37 milhão.

- **Tamanho das violações de dados.** Em média, as empresas dos Estados Unidos e da região árabe tiveram violações de dados que resultaram no maior número de registros expostos ou comprometidos (29.087 e 28.690 registros, respectivamente). Em média, as empresas do Japão e da Itália apresentaram o menor número de registros violados (18.615 e 19.034 registros, respectivamente).
- **As causas das violações de dados variam entre os países.** As empresas da região árabe e da Alemanha foram as mais propensas a sofrer um ataque malicioso ou criminoso, seguidas por França e Japão. As empresas da Índia foram as mais propensas a sofrer uma violação de dados por falha do sistema ou falha no processo de negócios; as empresas do Reino Unido foram as mais propensas a ter uma violação causada por erro humano.
- **As violações de dados mais caras foram ataques maliciosos e criminosos.** As conclusões consolidadas mostram que ataques maliciosos ou criminosos são os incidentes de violação de dados mais caros nos 10 países. As empresas dos Estados Unidos e da Alemanha apresentam os incidentes de violação de dados mais caros, com custo de US$246 e US$215 por registro comprometido, respectivamente. O Brasil e a Índia tiveram as violações de dados menos caras causadas por invasores maliciosos ou criminosos, com custo *per capita* de US$77 e US$60, respectivamente.
- **Fatores que diminuíram e aumentaram o custo de uma violação de dados.** Ter uma forte postura de segurança, um plano de resposta a incidentes e a nomeação de um CISO reduziram o custo por registro em US$14,14, US$12,77 e US$6,59, respectivamente. Os fatores que aumentaram o custo foram aqueles causados por perda ou roubo de dispositivos (+ US$16,10), envolvimento de terceiros na violação (+ US$14,80), notificação rápida (+ US$10,45) e contratação de consultores (+ US$2,10).
- **O gerenciamento da continuidade de negócios reduziu o custo de uma violação.** Pela primeira vez, a pesquisa revela que o envolvimento do gerenciamento da continuidade de negócios na correção da violação é capaz de reduzir o custo em US$8,98, em média, por registro comprometido.
- **Países que perderam o maior número de clientes após uma violação de dados.** A França e a Itália apresentaram a taxa mais elevada de rotatividade ou perda anormal de clientes após uma violação de dados. Por outro lado, a região árabe e a Índia tiveram a menor taxa de perda anormal de clientes.
- **Países que gastaram mais e menos com detecção e encaminhamento.** Em média, organizações da Alemanha e da França gastaram mais com atividades de detecção e encaminhamento, tais como investigação e avaliação da violação de dados (US$1,3 milhão e US$1,1 milhão, respectivamente). Organizações da Índia e da região árabe gastaram menos com detecção e encaminhamento (respectivamente, US$320.763 e US$353.735).
- **Países que gastaram mais e menos com notificação.** Os custos típicos de notificação incluem atividades de TI associadas à criação de bancos de dados de contatos, determinação de todos os requisitos regulamentares, contratação de especialistas externos e outros esforços para garantir que as vítimas sejam alertadas para o fato de que suas informações pessoais foram comprometidas. Organizações dos Estados Unidos e da Alemanha gastaram mais, em média (respectivamente, US$509.237 e US$317.635). O Brasil e a Índia gastaram menos com notificação (US$53.772 e US$19.841, respectivamente).
- **Sua organização terá uma violação de dados?** Com o intuito de entender o possível risco para as informações sensíveis e confidenciais de uma organização, achamos que seria útil compreender a probabilidade de uma organização ter uma violação de dados. Para isso, extrapolamos uma distribuição de probabilidade subjetiva para toda a amostra de empresas participantes em relação à probabilidade de uma violação de dados materiais ocorrer durante os próximos dois anos. Os resultados mostram que a probabilidade de uma violação de dados materiais envolvendo pelo menos 10.000 registros é superior a 22%. Além dos resultados agregados totais, constatamos que a probabilidade de violação de dados varia consideravelmente por país. A Índia e o Brasil têm a mais alta probabilidade estimada de ocorrência (30%), enquanto a Alemanha tem uma taxa de ocorrência aproximada de 2%.

Perguntas Mais Frequentes sobre o Custo de Violações de Dados

O que é uma violação de dados? Uma violação é definida como um evento em que o nome de um indivíduo, assim como um registro médico e/ou registro financeiro ou cartão de débito, é possivelmente colocado em risco—seja em formato eletrônico ou papel. Em nosso estudo, identificamos três causas principais de violação de dados. São elas: ataque malicioso ou criminoso, falha do sistema ou erro humano. Os custos de uma violação de dados podem variar de acordo com a causa e as medidas de proteção em vigor no momento da violação.

O que é um registro comprometido? Nossa definição de registro são informações que identificam a pessoa física (indivíduo) cujas informações foram perdidas ou roubadas em uma violação de dados. Os exemplos podem incluir o banco de dados de uma empresa de varejo com o nome de um indivíduo associado a informações de cartão de crédito e outras informações de identificação pessoal. Também pode ser o registro do beneficiário de seguro de uma seguradora de saúde, que contém informações médicas e de pagamento. No estudo deste ano, o custo médio da perda ou roubo de um desses registros para a organização é de US$145.

Como os dados são coletados? Os pesquisadores do Ponemon Institute coletaram dados qualitativos abrangentes por meio de 1.690 entrevistas realizadas durante um período de 10 meses. O recrutamento de organizações para o estudo de 2014 começou em janeiro de 2013; as entrevistas foram concluídas em março de 2014. Em cada uma das 314 organizações participantes, conversamos com profissionais de TI, conformidade e segurança de informações que estão informados sobre a violação de dados da organização e os custos associados à resolução da mesma. Por uma questão de privacidade, não coletamos informações específicas da organização.

Como o custo da violação de dados é calculado? Para calcular o custo médio da violação de dados, coletamos as despesas diretas e indiretas incorridas pela organização. As despesas diretas incluem a contratação de peritos forenses, a terceirização do suporte por linha direta e o fornecimento de assinaturas gratuitas de monitoramento de crédito e descontos para produtos e serviços futuros. Os custos indiretos incluem investigações e comunicação internas, bem como o valor extrapolado da perda do cliente resultante da rotatividade ou da diminuição das taxas de aquisição de clientes.

Qual é a diferença entre a pesquisa de referência e a pesquisa de opinião? No estudo *Custo de Violações de Dados*, a unidade de análise é a organização. Na pesquisa de opinião, a unidade de análise é o indivíduo. Recrutamos 314 organizações para participar do estudo. As violações de dados variaram de 2.415 registros comprometidos a pouco mais de 102.000.

O custo médio da violação de dados pode ser utilizado para calcular as consequências financeiras de uma superviolação, como aquelas que envolvem milhões de registros perdidos ou roubados? O custo médio de uma violação de dados em nossa pesquisa não se aplica a violações de dados catastróficas ou superviolações, porque elas não são comuns entre as violações sofridas pela maioria das organizações. A fim de ser representativa da população de organizações globais e tirar conclusões a partir da pesquisa que possam ser úteis para entender os custos em caso de perda ou roubo de informações protegidas, nossa análise não incluiu violações de dados superiores a aproximadamente 100.000 registros comprometidos.

As mesmas organizações são controladas a cada ano? Cada estudo anual envolve uma amostra diferente de empresas. Em outras palavras, não estamos controlando a mesma amostra de empresas com o passar do tempo. Para garantir a consistência, recrutamos e associamos empresas com características semelhantes, tais como o segmento de mercado da empresa, número de funcionários, presença geográfica e o tamanho da violação de dados. Desde que a pesquisa começou em 2005, estudamos as experiências de violação de dados de 1.279 organizações no mundo todo.

Parte 2. Principais Conclusões

Esta seção contém as conclusões detalhadas da pesquisa. Os tópicos são apresentados na seguinte ordem:

- Entendendo o custo da violação de dados
- As causas-raízes de uma violação de dados
- Fatores que influenciam o custo de uma violação de dados
- Tendências na frequência de registros comprometidos e rotatividade ou perda de clientes
- Tendências nos componentes de custo de uma violação de dados
- A probabilidade de uma organização ter uma violação de dados

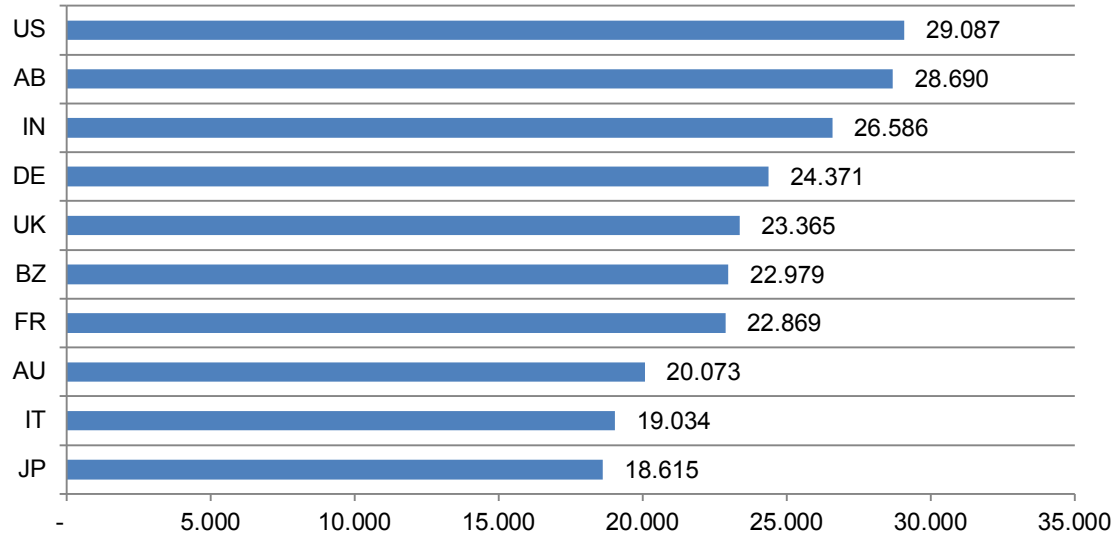
A tabela a seguir relaciona os países, a legenda e a moeda usada neste relatório.

Tabela 1. Legenda do país	Legenda	Casos de referência	Moeda
Austrália	AU	22	Dólar australiano
Brasil	BZ	32	Real
França	FR	27	Euro
Alemanha	DE	30	Euro
Índia	IN	29	Rupia
Itália	IT	23	Euro
Japão	JP	26	Iene
Emirados Árabes Unidos e Arábia Saudita	AB	24	AED/SAR
Reino Unido	UK	40	GBP
Estados Unidos	US	61	Dólar

Entendendo o custo da violação de dados

Número de registros expostos ou comprometidos. A Figura 1 informa o tamanho médio das violações de dados para organizações nos 10 países representados nesta pesquisa. Conforme mostrado, as organizações dos Estados Unidos, região árabe e Índia tiveram o maior número médio de registros perdidos ou roubados.

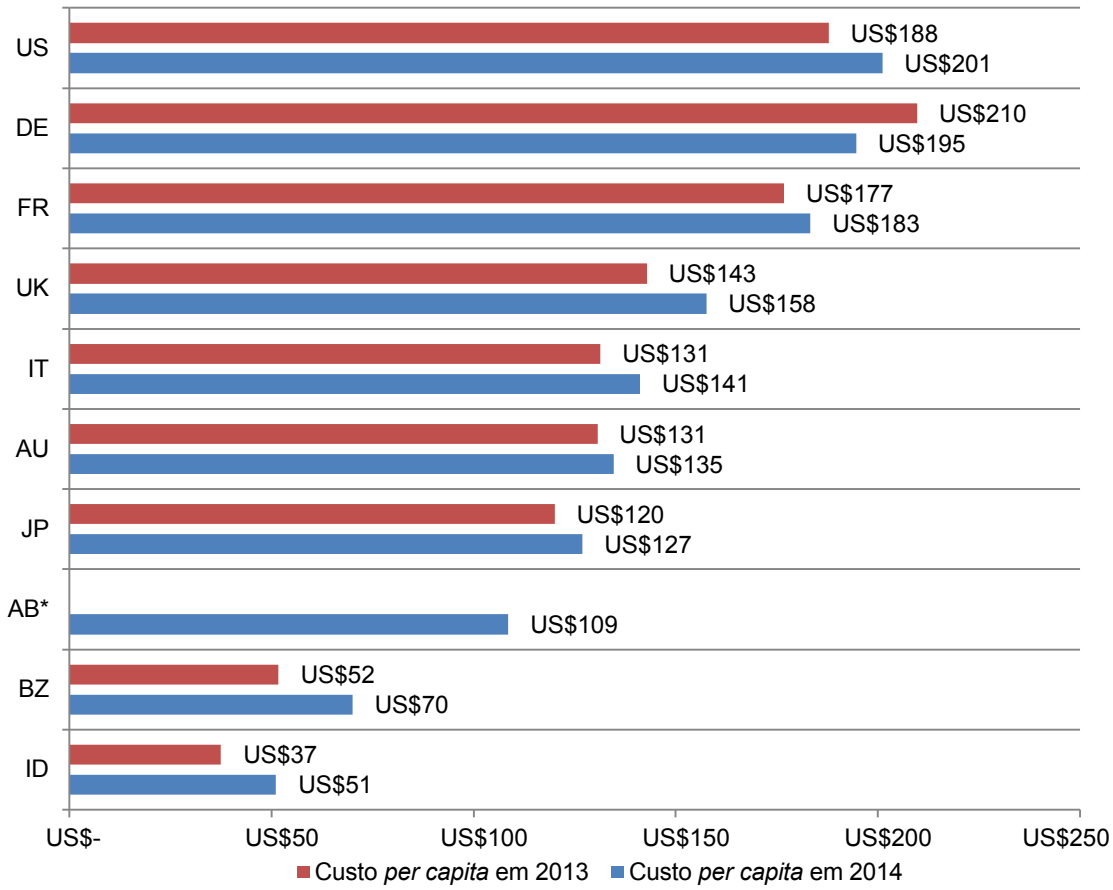
Figura 1. O número médio de registros violados por país



O custo médio *per capita* durante dois anos. A Figura 2 informa o custo médio *per capita* de uma violação de dados (expresso em dólares dos Estados Unidos) para estudos nos 10 países. Conforme mostrado, existe uma variação notável entre as amostras dos países[4]. O custo médio *per capita* consolidado para todos os países foi de US$145 em comparação com o custo médio de US$136 calculado no ano passado (excluindo a região árabe). Os Estados Unidos e a Alemanha tiveram os custos *per capita* mais elevados (respectivamente, US$201 e US$195). A Índia e o Brasil tiveram os custos mais baixos (respectivamente, US$51 e US$70).

Figura 2. O custo médio *per capita* da violação de dados durante dois anos

Medido em US$

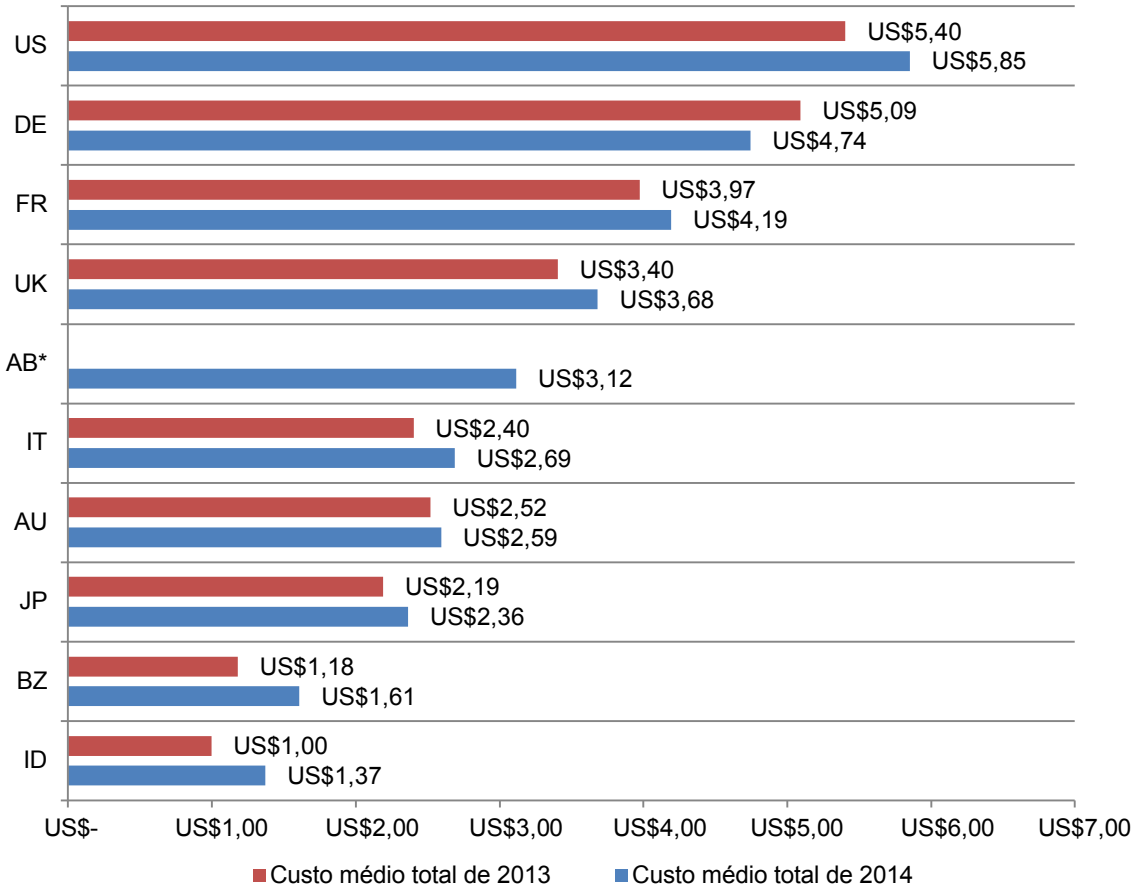


* Não há dados disponíveis para o exercício financeiro de 2013

[4] O custo *per capita* é definido como o custo total da violação de dados dividido pelo tamanho da violação de dados (ou seja, o número de registros perdidos ou roubados).

O custo organizacional médio da violação de dados varia por país. A Figura 3 apresenta o custo médio total da violação de dados para os estudos com 10 países no estudo deste ano. Como é possível ver, a amostra dos Estados Unidos teve o custo médio total mais elevado (superior a US$5,85 milhões), seguida pela Alemanha (US$4,74 milhões). Por outro lado, as amostras de empresas do Brasil e da Índia apresentaram o custo médio total mais baixo (respectivamente, US$1,61 milhão e US$1,37 milhão).

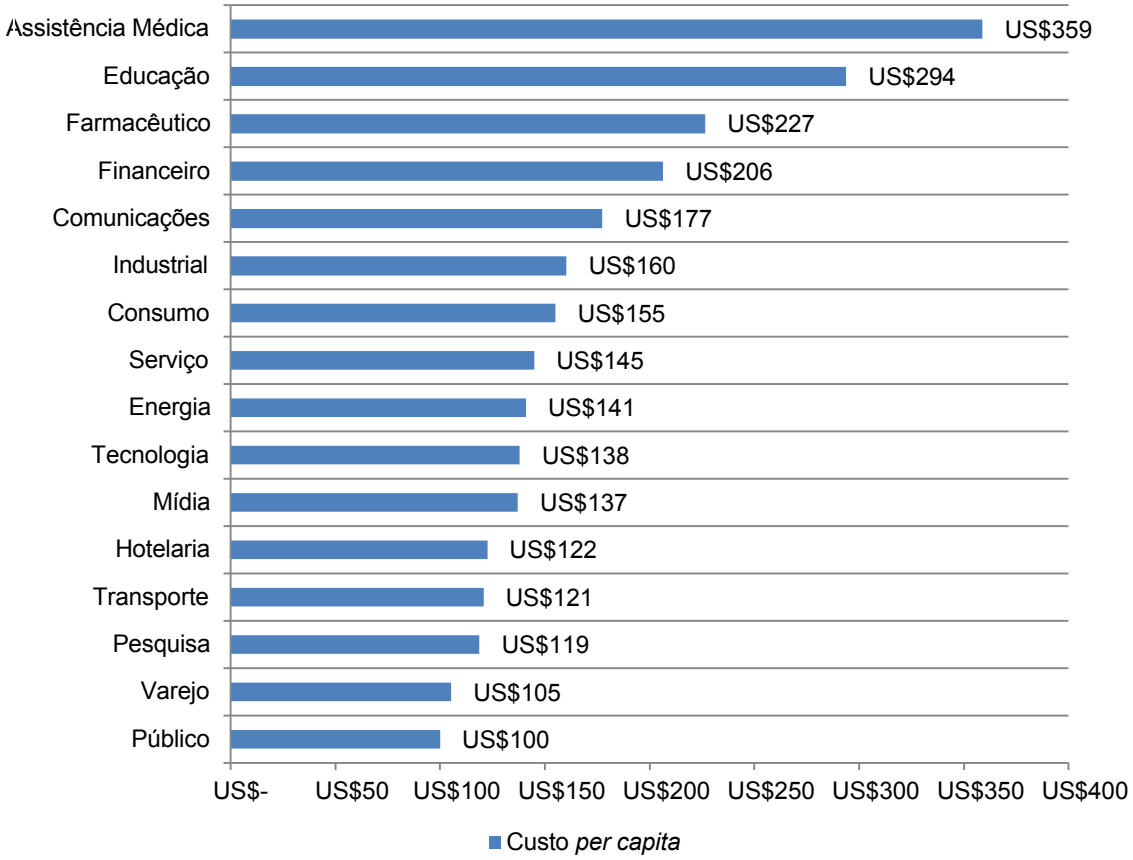
Figura 3. O custo organizacional médio total da violação de dados durante dois anos
Medido em US$ (o US$ 000,000 foi omitido)



* Não há dados disponíveis para o exercício financeiro de 2013.

Alguns segmentos de mercado têm custos de violação de dados mais elevados. A Figura 4 informa os custos *per capita* referentes à amostra consolidada por classificação de segmento de mercado. Segmentos de mercado fortemente regulamentados, como assistência médica, educação, farmacêutico e serviços financeiros, tiveram um custo *per capita* de violação de dados substancialmente acima da média geral (US$145). Organizações do setor público e empresas de varejo tiveram um custo *per capita* muito abaixo do valor médio geral.

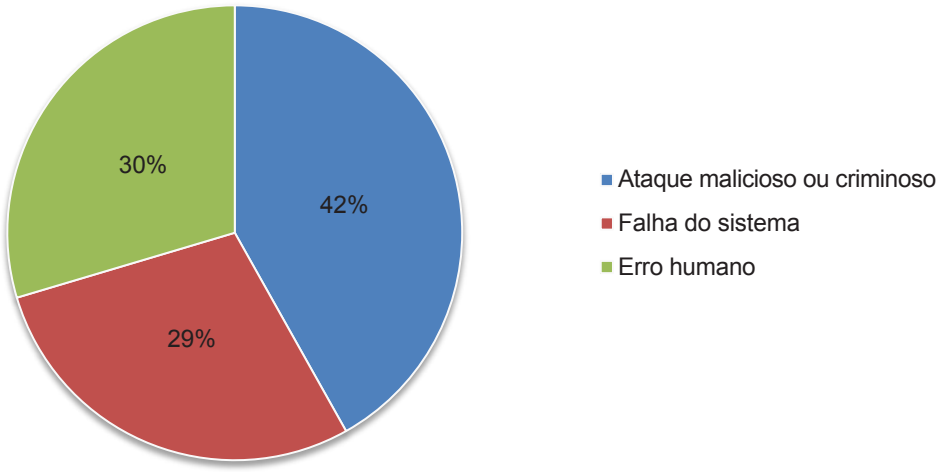
Figura 4. Custo *per capita* por classificação de segmento de mercado
Visualização consolidada (n=314)



As causas-raízes da violação de dados

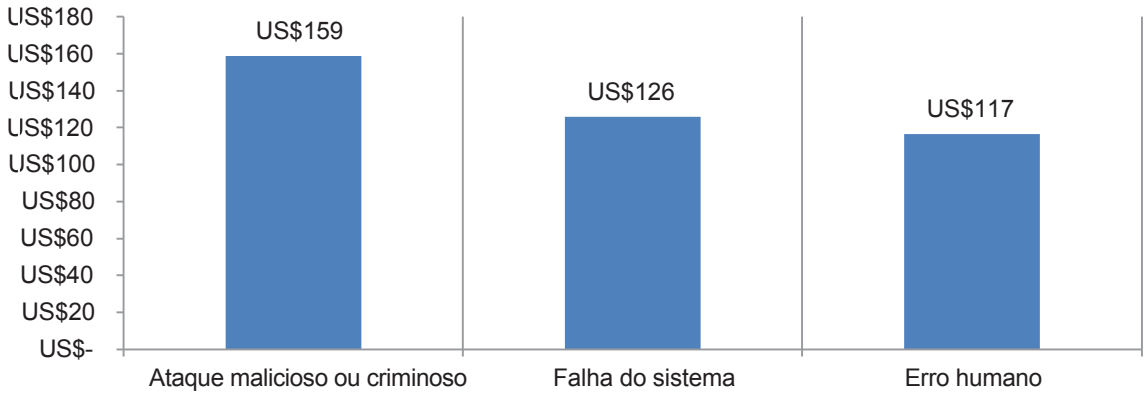
Ataques maliciosos ou criminosos são a causa mais frequente de violações de dados no mundo todo[5]. A Figura 5 oferece um resumo das principais causas-raízes da violação de dados em base consolidada para os 10 países representados na pesquisa. Quarenta e dois por cento dos incidentes envolveram um ataque malicioso ou criminoso; 30% estavam ligados a um funcionário ou contratada negligente (fator humano); e 29% envolveram falhas do sistema, incluindo falhas nos processos de TI e negócios[6].

Figura 5. Distribuição da amostra de referência por causa-raiz da violação de dados
Visualização consolidada (n=314)



Os ataques maliciosos são os mais caros no mundo todo. A Figura 6 mostra o custo *per capita* da violação de dados para as três causas-raízes do incidente de violação, em base consolidada. Esses resultados mostram que o custo de violações de dados causadas por ataques maliciosos ou criminosos para as empresas aumentou de uma média de US$157 (no estudo do ano passado) para US$159. Isso está significativamente acima da média consolidada de US$145 por registro comprometido e do custo *per capita* por violações causadas por falha do sistema e fatores humanos (US$126 e US$117, respectivamente). No ano passado, as falhas do sistema atingiram uma média de US$122; o erro humano continuou igual (US$117).

Figura 6. Custo *per capita* para as três causas-raízes da violação de dados
Visualização consolidada (n=314)
Medido em US$

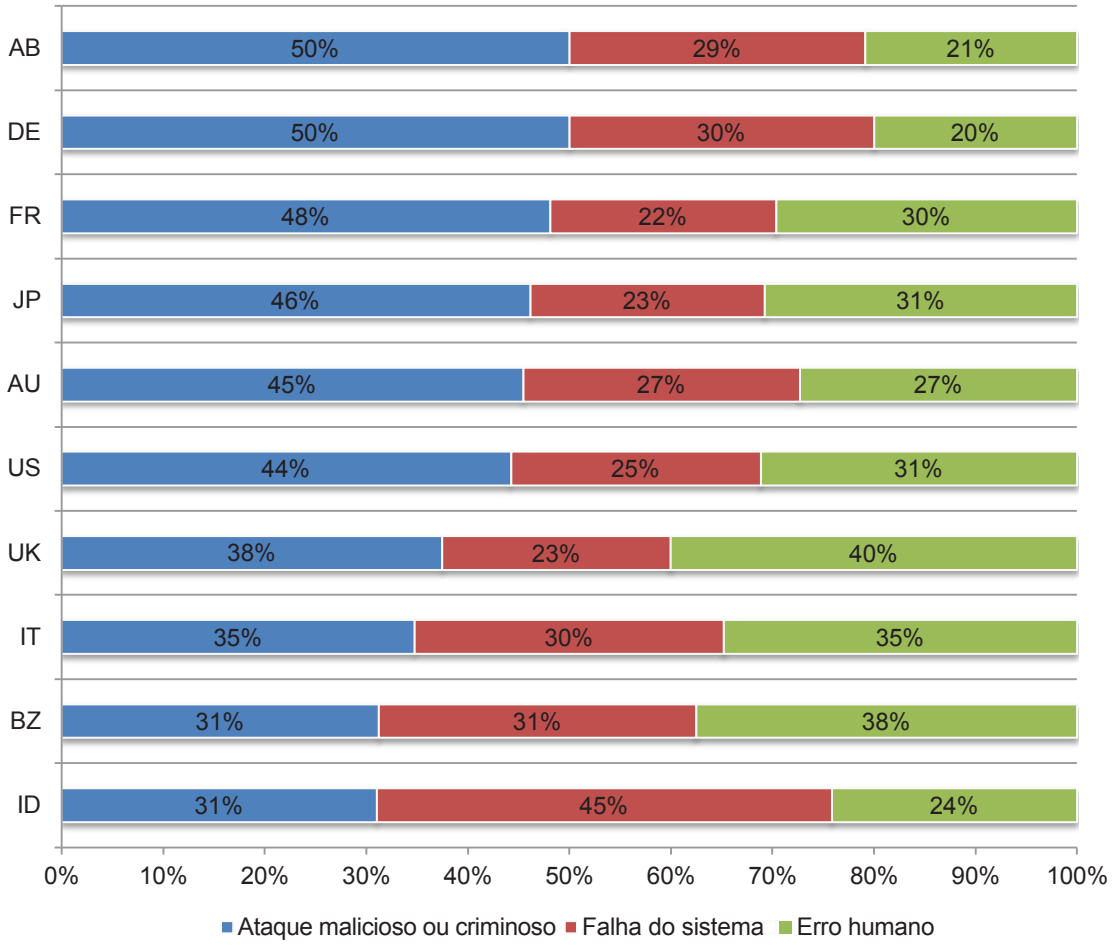


[5] Portadores de informações privilegiadas negligentes são indivíduos que causam uma violação de dados em função de seu descuido, o que é determinado em uma investigação posterior da violação de dados. Ataques maliciosos podem ser causados por hackers ou portadores de informações privilegiadas com intenção criminosa (funcionários, contratadas ou outros terceiros).

[6] Os tipos mais comuns de ataques maliciosos ou criminosos incluem infecções por malware, portadores de informações privilegiadas com intenção criminosa, phishing/engenharia social e injeção de SQL.

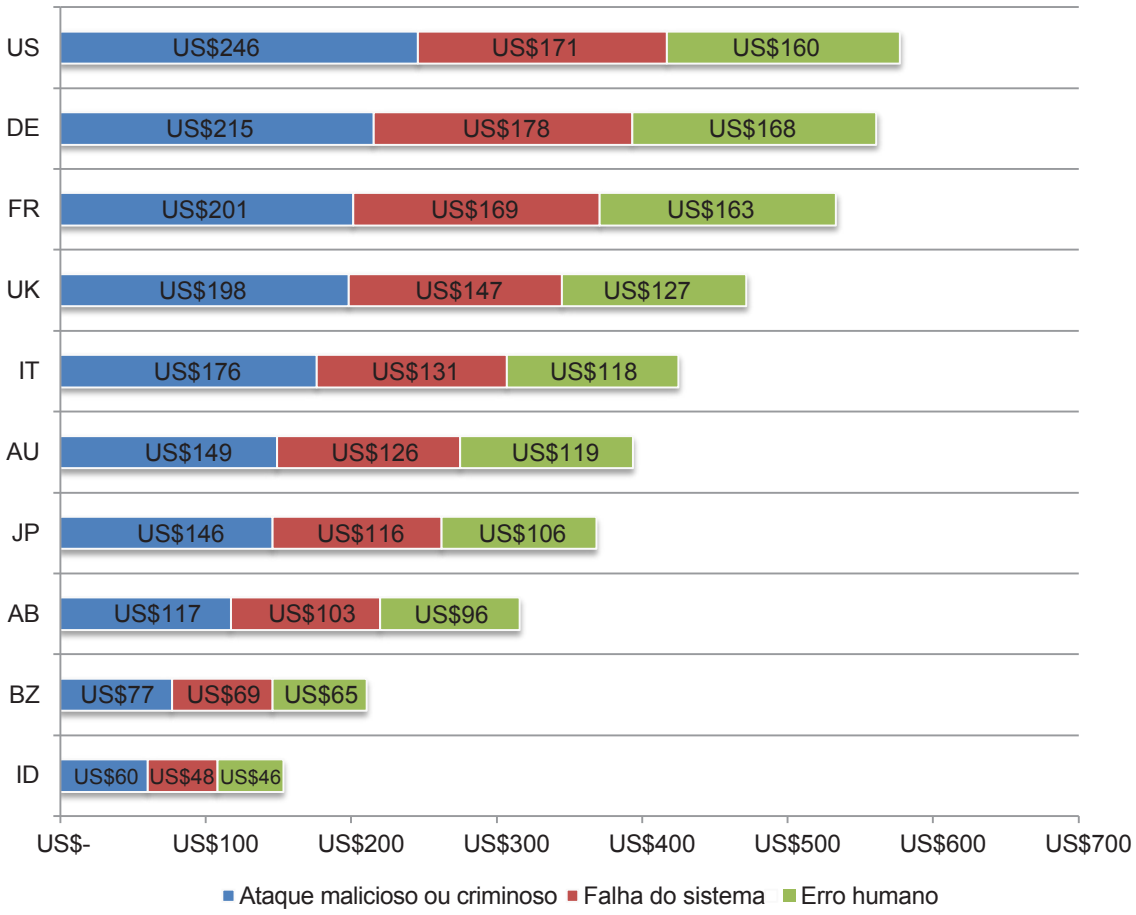
A Figura 7 apresenta as principais causas-raízes da violação de dados conforme as amostras dos 10 países. Com 50%, as empresas da região árabe e da Alemanha foram as mais propensas a sofrer um ataque malicioso ou criminoso. Por outro lado, as empresas da Índia e do Brasil foram as menos propensas a sofrer tais violações de dados. As empresas da Índia foram as mais propensas a sofrer uma violação de dados causada por falha do sistema ou falha no processo de negócios.

Figura 7. Distribuição da amostra de referência por causa-raiz da violação de dados



A Figura 8 apresenta o custo *per capita* da violação de dados por amostra de país para as três causas-raízes. Esses resultados mostram claramente que os custos de violações de dados resultantes de ataques maliciosos ou criminosos foram consistentemente mais elevados do que os custos resultantes de falhas do sistema ou erro humano. Este gráfico também mostra uma grande variação entre as amostras dos países. Ou seja, o custo de um incidente de violação de dados malicioso ou criminoso nos Estados Unidos foi de US$246 por registro comprometido. Na Índia, esse custo *per capita* foi de apenas US$60.

Figura 8. Custo *per capita* para as três causas-raízes da violação de dados
Medido em US$

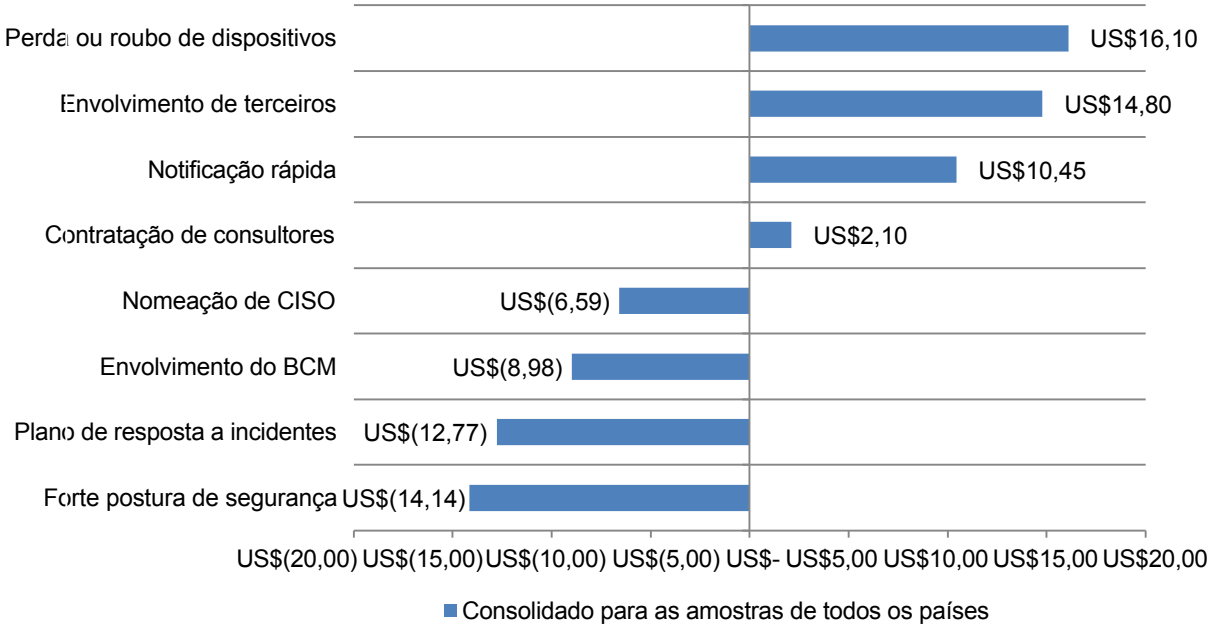


Fatores que influenciam o custo da violação de dados
Visualização consolidada (n=314) medida em US$

Uma forte postura de segurança resulta na maior diminuição do custo da violação de dados. Conforme mostrado na Figura 9, uma forte postura de segurança, o planejamento de resposta a incidentes, o gerenciamento da continuidade de negócios e um CISO com responsabilidades corporativas diminuem o custo *per capita* da violação de dados (mostrado em números negativos). A perda ou roubo de dispositivos, o envolvimento de terceiros no incidente, a notificação rápida e a contratação de consultores aumentam o custo *per capita* da violação de dados (mostrado em números positivos).

Por exemplo, as empresas que tinham uma forte postura de segurança no momento da violação de dados conseguiram reduzir o custo médio por registro para US$131,86 (US$145—US$14,14). No entanto, nos casos em que a violação de dados envolveu perda ou roubo de dispositivos, o custo por registro podia subir para US$161,10 (US$145 + US$16,10).

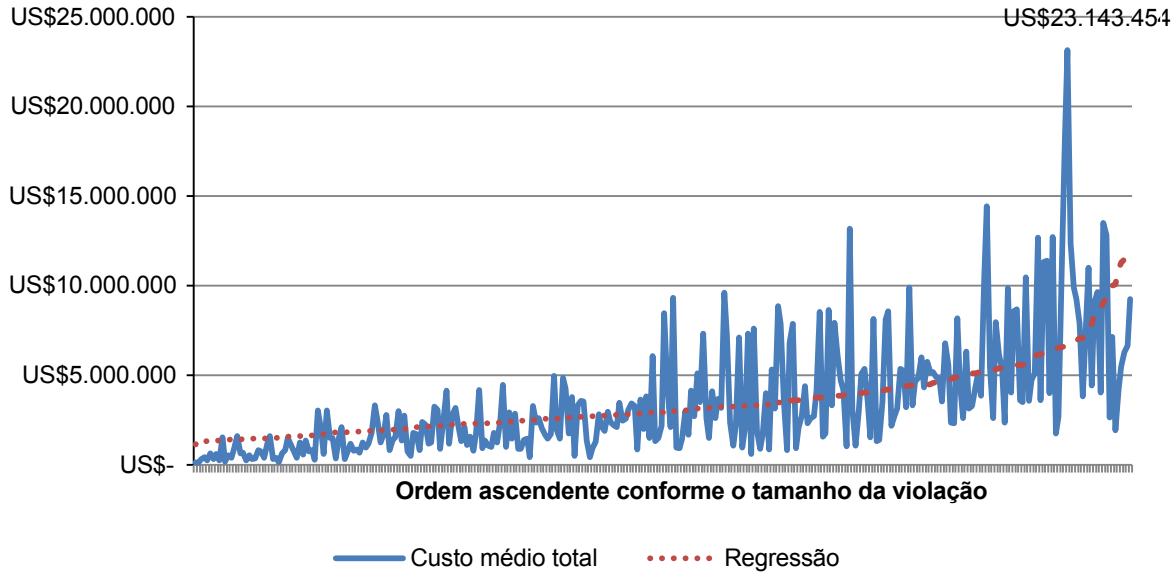
Figura 9. Impacto de oito fatores no custo *per capita* da violação de dados



Tendências na frequência de registros comprometidos e rotatividade de clientes

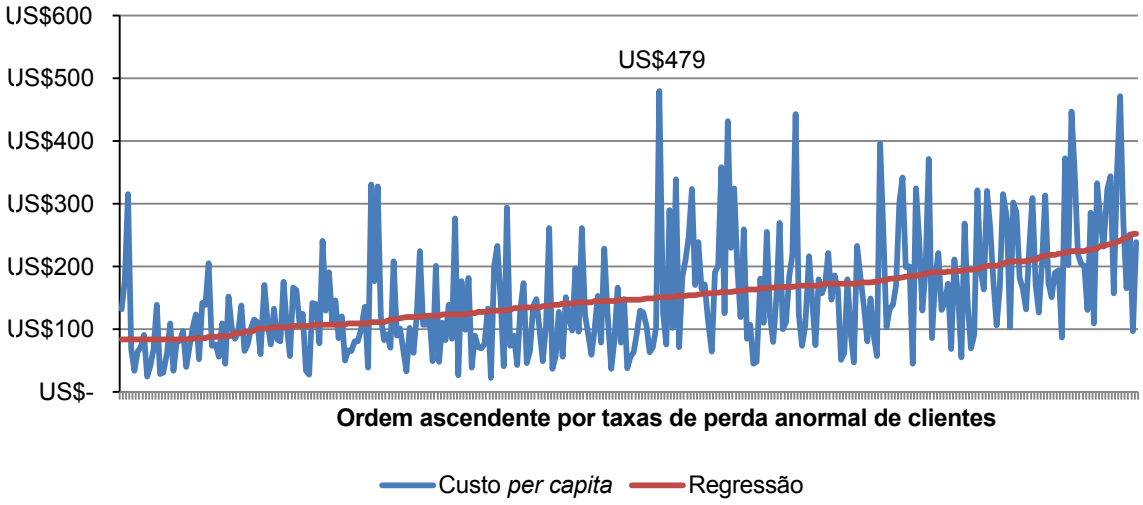
O número de registros perdidos é proporcional ao custo da violação de dados. A Figura 10 mostra a relação entre o custo total da violação de dados e o tamanho do incidente para 314 organizações em ordem ascendente, conforme o tamanho do incidente de violação. A linha de regressão indica que o tamanho do incidente de violação de dados e os custos totais estão relacionados linearmente. No estudo deste ano, o custo variou de US$135.603 a US$23.143.454.

Figura 10. Custo total da violação de dados por tamanho da violação de dados
Regressão = Interceptação + {Tamanho do Evento de Violação} x β, onde β simboliza a inclinação.
Medido em US$



A perda de clientes é proporcional ao custo *per capita* da violação de dados. A Figura 11 mostra a distribuição dos custos *per capita* da violação de dados em taxa ascendente de perda anormal de clientes para 314 organizações. A linha de regressão está subindo, o que sugere que a perda anormal de clientes e os custos *per capita* estão relacionados de forma linear.

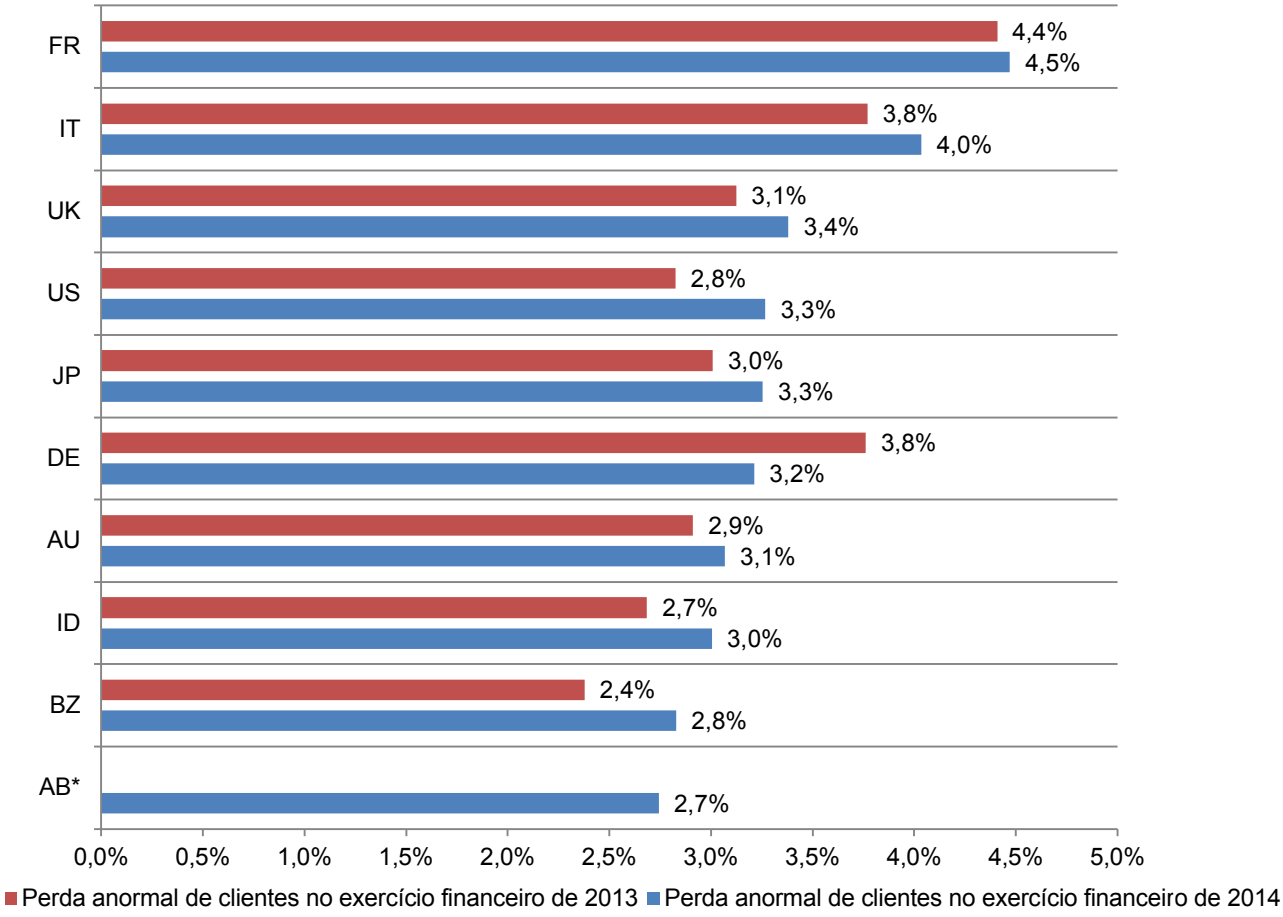
Figura 11. Distribuição de taxas de perda anormal de clientes em ordem ascendente por custos *per capita*
Regressão = Interceptação + {taxa de perda anormal de cliente} x β, onde p simboliza a inclinação.
Medido em US$



Alguns países são mais vulneráveis à perda de clientes. A Figura 12 mostra as taxas anormais médias para os 10 países representados nesta pesquisa. Os resultados de 2014 apresentam diferenças notáveis entre os países. A França continuou apresentando a taxa de perda de clientes mais elevada, seguida pela Itália. A região árabe e o Brasil apresentaram a menor taxa de perda de clientes.

A implicação dessa conclusão é que as organizações de países com altas taxas de perda de clientes conseguiram reduzir significativamente os custos das violações de dados ao enfatizar as atividades de retenção de clientes com o objetivo de preservar a reputação e o valor da marca.

Figura 12. Taxas de perda anormal de clientes durante dois anos por amostra do país

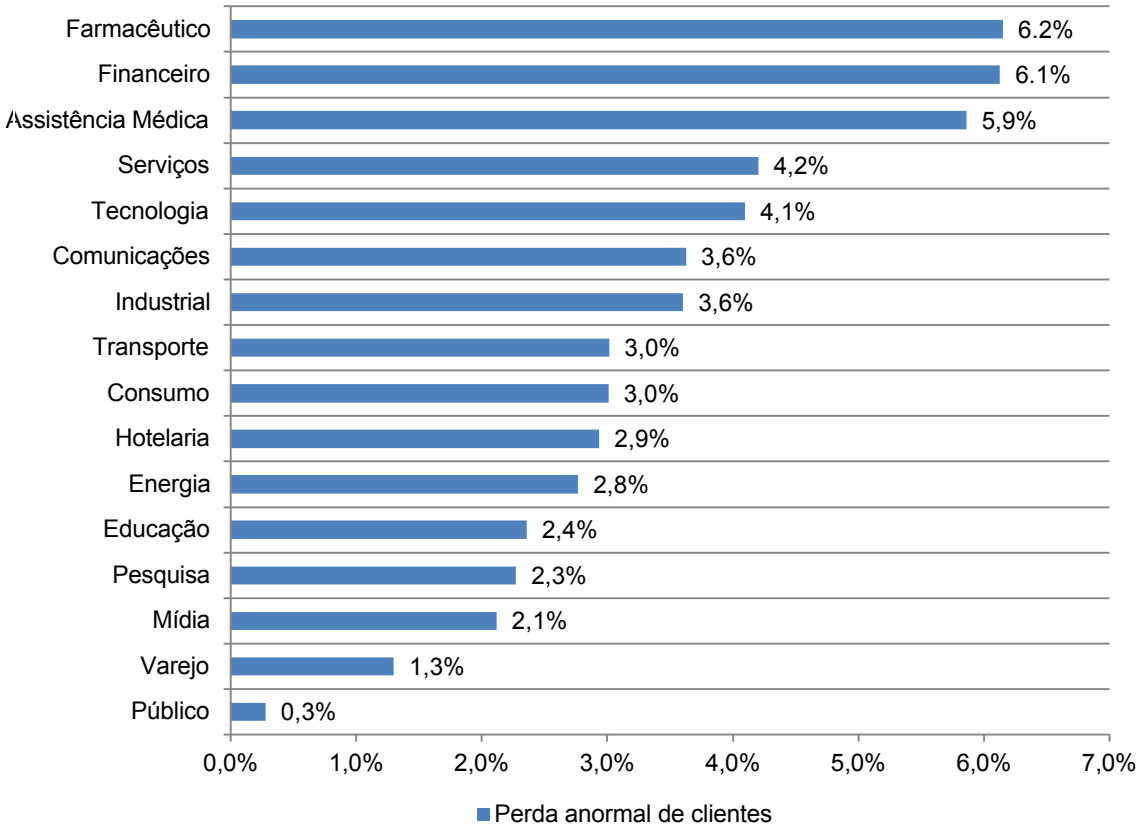


*Não há dados disponíveis para o exercício financeiro de 2013

Alguns segmentos de mercado são mais vulneráveis à perda de clientes. A Figura 13 mostra a taxa de perda anormal de clientes das organizações de referência para o estudo de 2014. Embora o pequeno tamanho da amostra nos impeça de generalizar o efeito do segmento de mercado nas taxas de perda de clientes, organizações farmacêuticas, de serviços financeiros e de assistência médica tendem a apresentar uma perda anormal de clientes relativamente alta; já as empresas do setor público e do varejo tendem a apresentar uma perda anormal de clientes relativamente baixa[7].

Figura 13. Taxas de perda anormal de clientes por classificação de segmento de mercado das empresas de referência

Visualização consolidada (n=314)

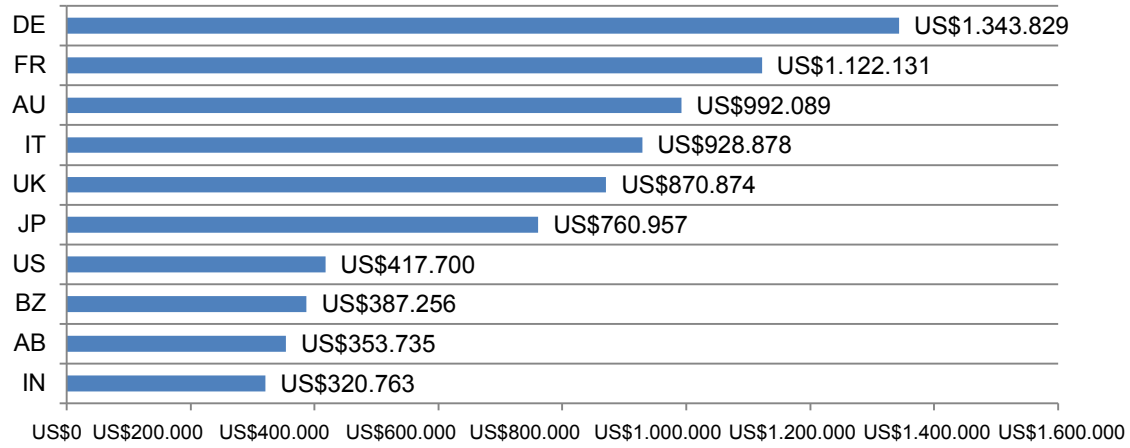


[7] Organizações do setor público utilizam uma estrutura diferente de perda de clientes, uma vez que clientes de organizações do governo normalmente não têm uma opção alternativa.

Tendências nos componentes de custo de uma violação de dados

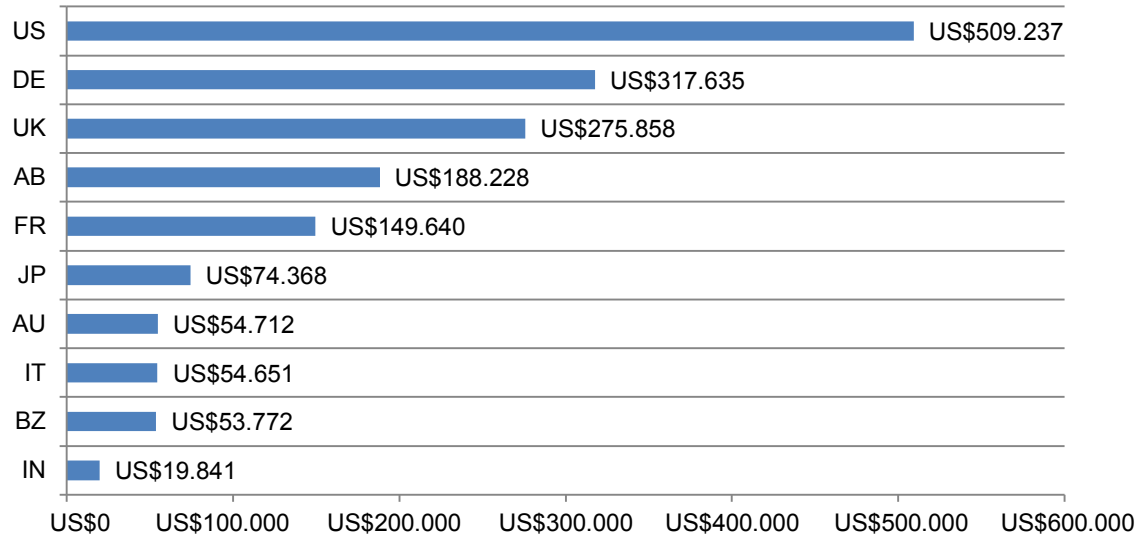
Os custos de detecção e encaminhamento são mais altos na Alemanha. A Figura 14 apresenta os custos associados à detecção e encaminhamento de incidentes de violação de dados em 10 países. Tais custos geralmente incluem atividades forenses e investigativas, serviços de avaliação e auditoria, gerenciamento de equipe de crise e comunicação com a alta gerência e o conselho de administração. Conforme mencionado, as empresas da Alemanha tiveram os custos mais altos de detecção e encaminhamento; a Índia e a região árabe apresentaram os custos mais baixos.

Figura 14. Custos médios de detecção e encaminhamento
Medido em US$



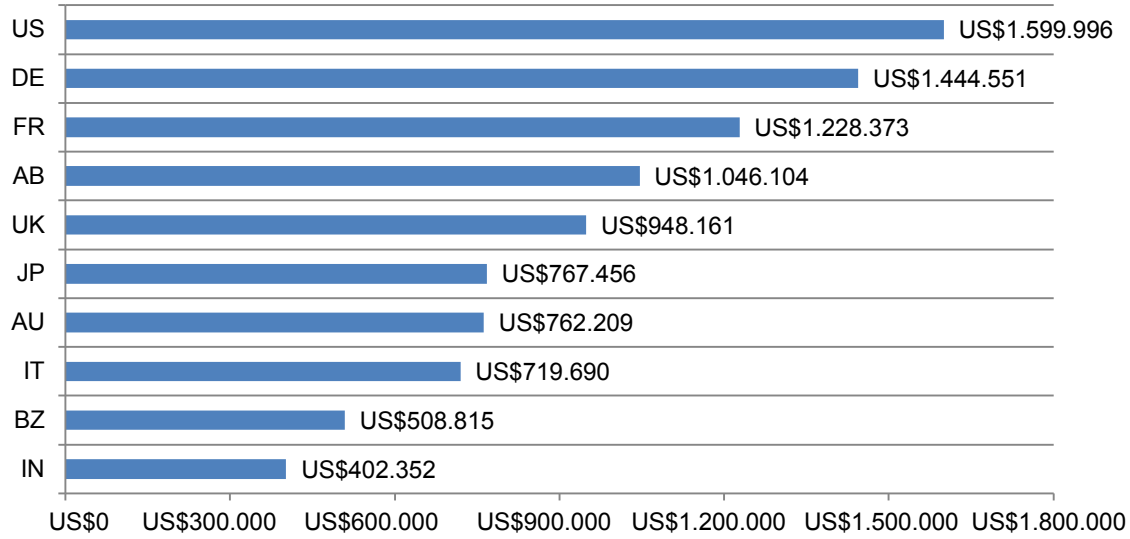
Custos da notificação do impacto conforme as leis de notificação de violações de dados nos Estados Unidos. A Figura 15 revela que as empresas dos Estados Unidos têm um custo significativamente mais alto em relação a notificar as vítimas de uma violação de dados. A Índia e o Brasil têm os custos mais baixos. Os custos de notificação geralmente incluem atividades de TI associadas à criação de bancos de dados de contatos, determinação de todos os requisitos regulamentares, contratação de especialistas externos, despesas postais, contatos secundários em caso de devolução de correspondência ou email e ajuste da comunicação recebida.

Figura 15. Custos médios da notificação
Medido em US$



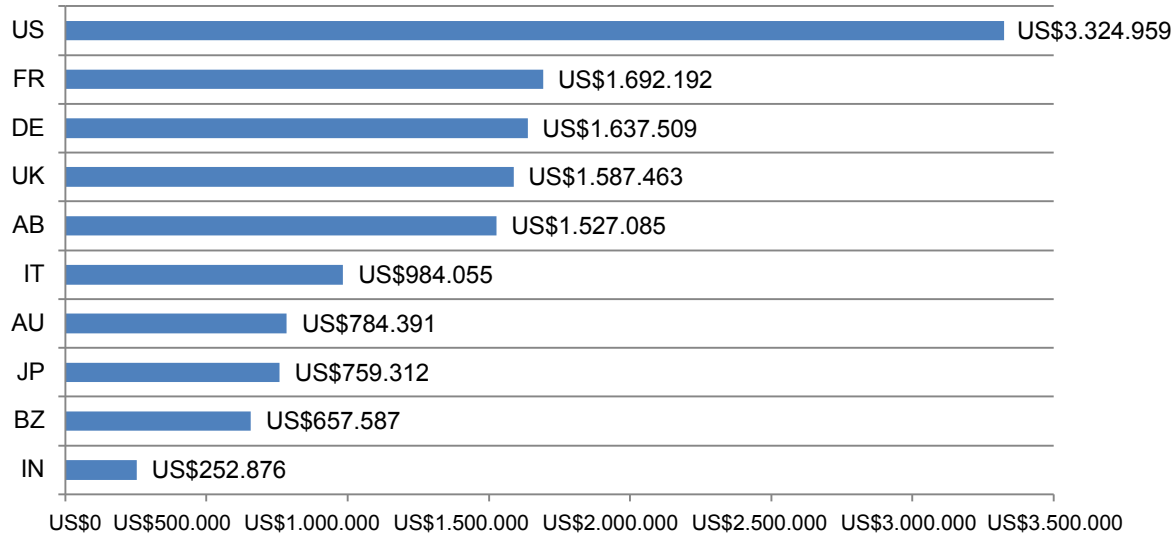
Os custos posteriores à violação de dados são mais altos nos Estados Unidos e na Alemanha. A Figura 16 mostra a distribuição de custos associados às atividades posteriores (após o fato) nos 10 países. Esses custos normalmente incluem atividades de help desk, comunicações recebidas, atividades investigativas especiais, correção, despesas legais, descontos em produtos, serviços de proteção de identidade e intervenções regulamentares. Os custos mais baixos foram encontrados no Brasil e na Índia.

Figura 16. Custos médios posteriores à violação de dados
Medido em US$



As organizações dos Estados Unidos apresentam custos de perda de negócios mais elevados. Os custos de perdas de negócios incluem rotatividade anormal de clientes, aumento das atividades de aquisição de clientes, perdas de reputação e diminuição do fundo de comércio. O custo de perda de negócios mais alto foi uma média de US$3,3 milhões; o mais baixo foi de US$252.876 na Índia.

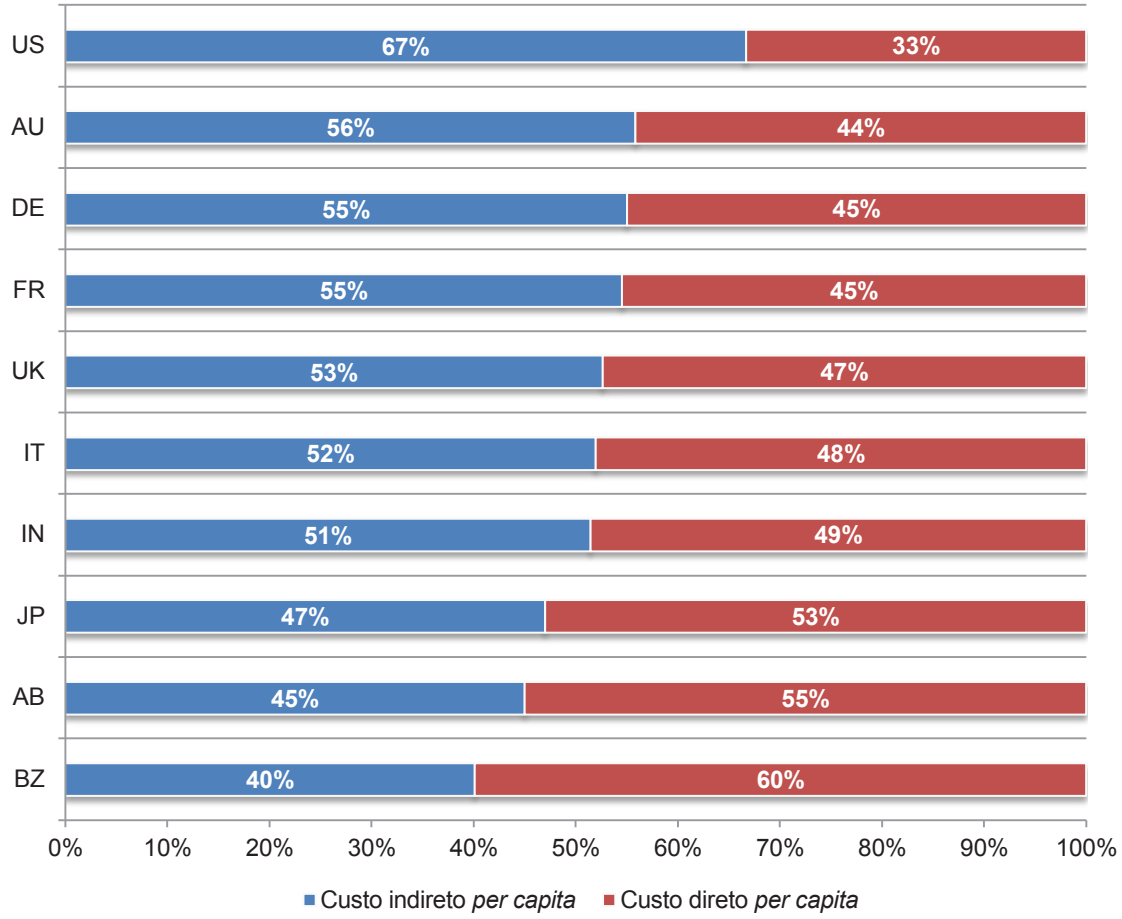
Figura 17. Custos médios de perda de negócios
Medido em US$



A proporção de custos diretos e indiretos da violação de dados varia conforme o país. Os custos diretos se referem ao desembolso de despesas diretas para realizar determinada atividade, como a contratação de peritos forenses, a contratação de um escritório de advocacia ou a prestação de serviços de proteção de identidade para as vítimas. Os custos indiretos incluem o tempo, esforço e outros recursos organizacionais usados durante a resolução da violação de dados. Incluem a utilização de funcionários existentes para ajudar nos esforços de notificação de violações de dados ou na investigação do incidente. Os custos indiretos também incluem a perda de fundo de comércio e a perda de clientes.

A Figura 18 informa os componentes diretos e indiretos de uma violação de dados em base de porcentagem para os 10 países. Conforme mostrado, as empresas dos Estados Unidos têm os custos indiretos mais altos. O Brasil e a região árabe apresentam os custos diretos mais altos.

Figura 18. Porcentagem de custos diretos e indiretos de violações de dados *per capita*

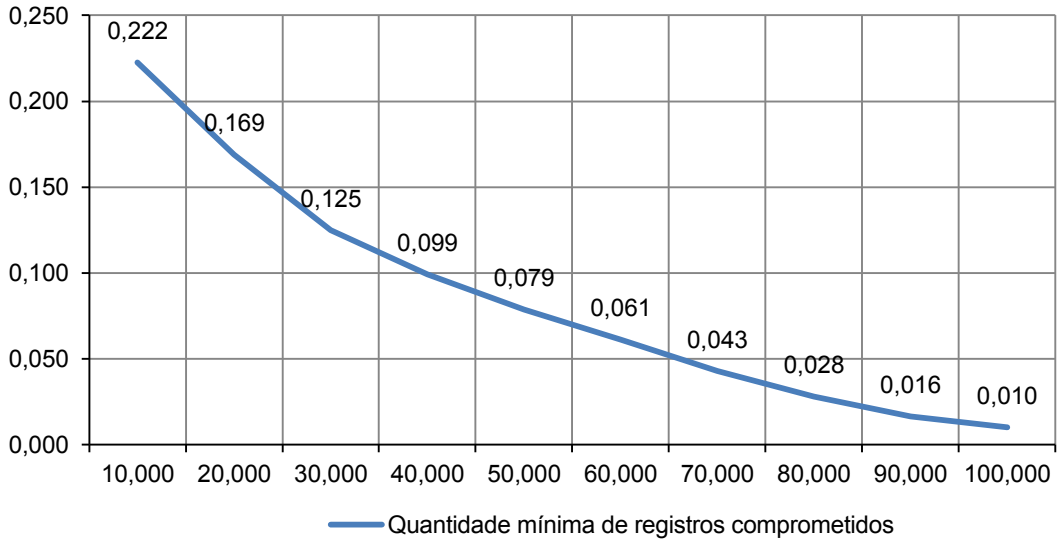


A probabilidade de que uma organização terá uma violação de dados

É mais provável que as empresas tenham uma pequena violação de dados do que uma superviolação. Pela primeira vez, nossa pesquisa fornece uma análise da probabilidade de uma ou mais ocorrências de violação de dados nos próximos 24 meses. De acordo com as experiências das organizações em nossa pesquisa, acreditamos que é possível prever a probabilidade de uma violação de dados com base em dois fatores: quantos registros foram perdidos ou roubados e o segmento de mercado da empresa.

A Figura 19 mostra as probabilidades subjetivas de incidentes de violação envolvendo uma quantidade mínima de 10.000 a 100.000 registros comprometidos[8]. Como é possível ver, a probabilidade de uma violação de dados diminui continuamente à medida que o tamanho aumenta. Embora a probabilidade de uma violação de dados envolvendo pelo menos 10.000 registros esteja estimada em aproximadamente 22% durante um período de 24 meses, as chances de uma violação de dados envolvendo 100.000 registros é inferior a 1%.

Figura 19. Probabilidade de uma violação de dados envolvendo uma quantidade mínima de 10.000 a 100.000 registros

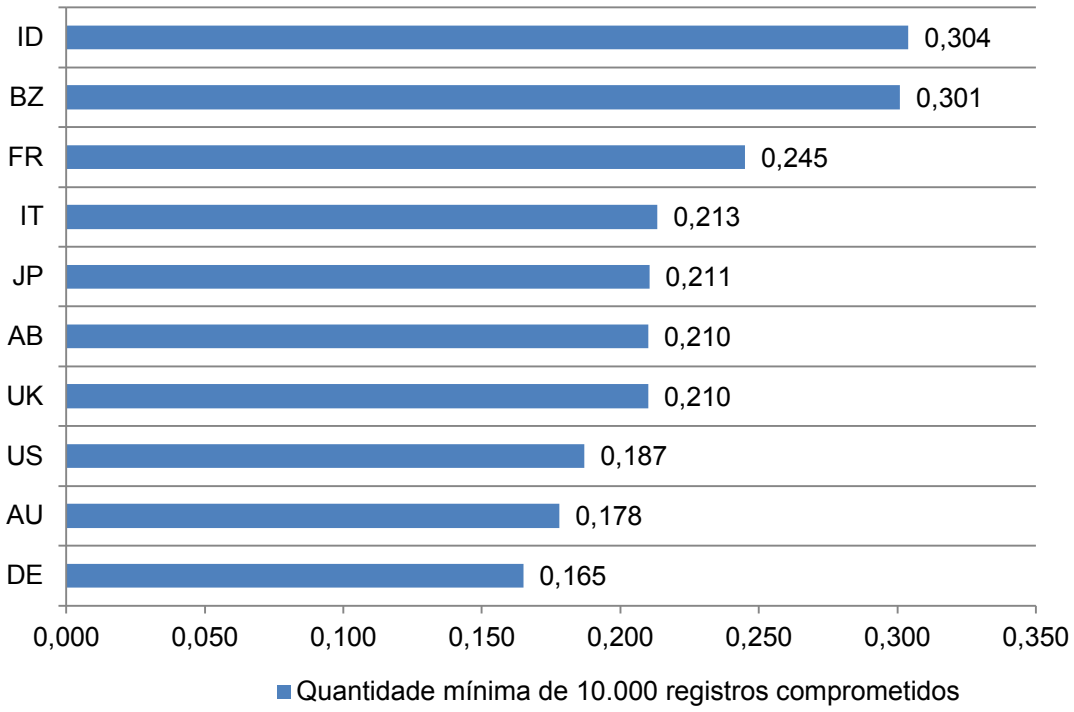


[8] As probabilidades estimadas foram obtidas a partir dos entrevistados da amostra usando uma técnica de estimação pontual. Os principais indivíduos que participaram das entrevistas de avaliação de custo (como o CISO ou o CPO) forneceram sua estimativa de probabilidade de violação de dados para 10 níveis de incidentes de violação de dados (variando de 10.000 a 100.000 registros perdidos ou roubados). A escala de tempo utilizada nessa tarefa de estimação foi o período de 24 meses seguinte. Uma distribuição de probabilidade agregada foi extrapolada para cada uma das 314 empresas participantes.

As organizações de alguns países são mais propensas a sofrer uma violação de dados. A Figura 20 resume a probabilidade de uma violação de dados envolvendo pelo menos 10.000 registros para os 10 países que participaram da pesquisa. Embora o pequeno tamanho da amostra nos impeça de generalizar as diferenças entre os países, a probabilidade estimada de uma violação de dados materiais varia consideravelmente entre eles.

A Índia e o Brasil parecem ter a probabilidade estimada de ocorrência mais elevada. A Alemanha e a Austrália têm a menor probabilidade.

Figura 20. Probabilidade de uma violação de dados envolvendo uma quantidade mínima de 10.000 registros por segmento de mercado



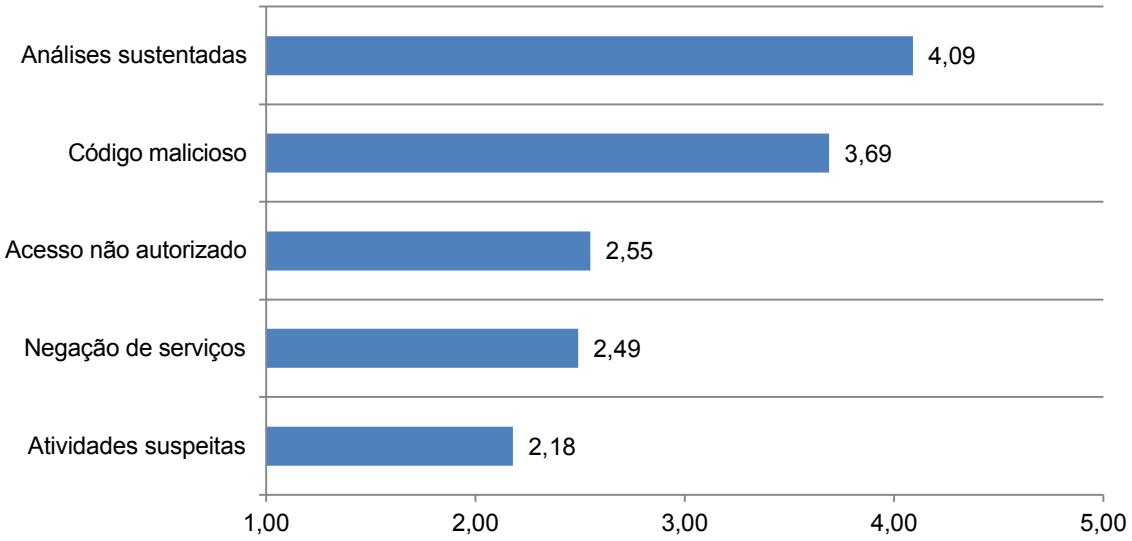
Parte 3. Conclusões de Segurança Global

O *Estudo do Custo de Violações de Dados* deste ano revela que a causa mais comum de uma violação de dados (à exceção da Índia) é um ataque interno malicioso ou um ataque criminoso. No estudo deste ano, perguntamos às empresas representadas na pesquisa o que mais as preocupa em relação aos incidentes de segurança, quais investimentos estão fazendo e a existência de uma estratégia de segurança.

De acordo com as conclusões, o valor ideal a investir durante os próximos 12 meses para executar a estratégia de segurança da organização é de US$14 milhões, em média. Todavia, no próximo período de 12 meses, as empresas preveem que terão, em média, cerca de metade desse valor, ou seja, US$7 milhões.

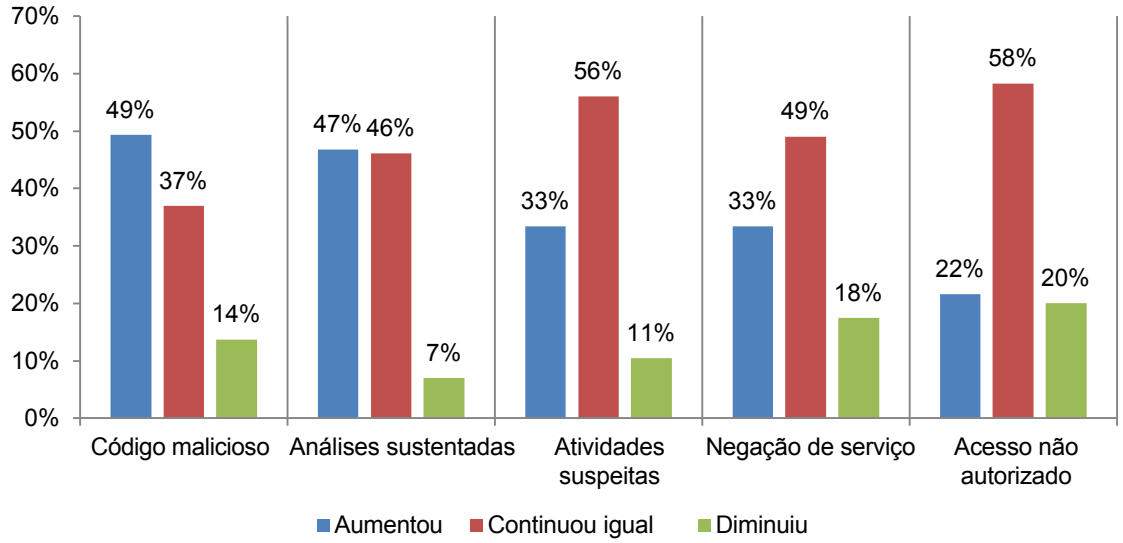
A seguir, apresentamos uma análise consolidada das principais conclusões para os 10 países. Conforme mostrado na Figura 21, as análises sustentadas e o código malicioso são considerados as maiores ameaças à segurança de uma organização. As menos ameaçadoras são atividades suspeitas e negação de serviço.

Figura 21. Tipos de incidentes de segurança com base na gravidade da ameaça
1 = o menos grave até 5 = o mais grave
Visualização consolidada (n=314)



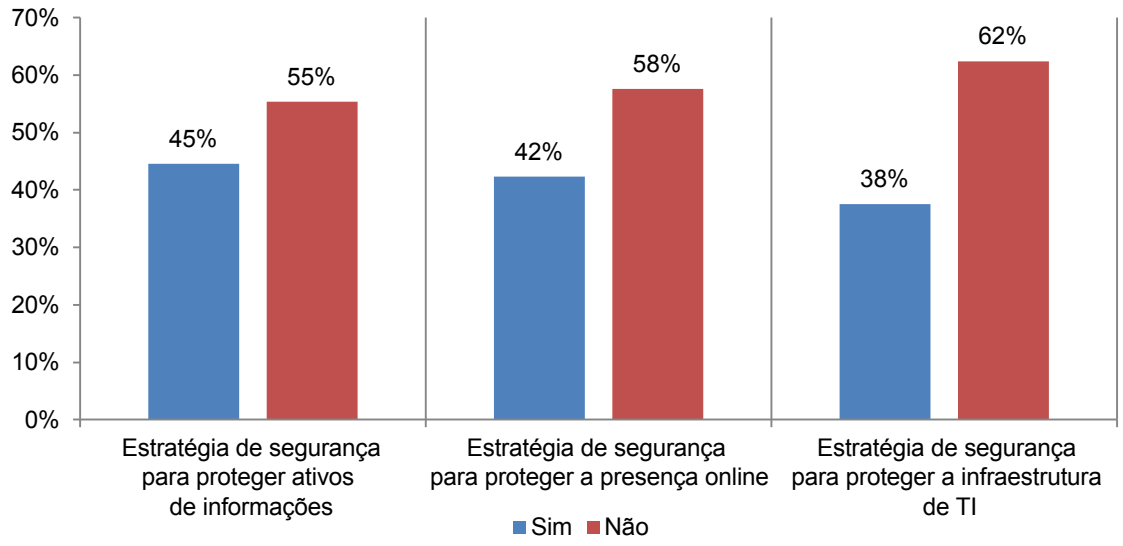
Por que o código malicioso e as análises sustentadas são uma preocupação. A Figura 22 mostra por que essas ameaças são as maiores preocupações para a segurança de TI. De acordo com 49% das empresas, o código malicioso deve aumentar; 47% acreditam que as análises sustentadas se tornarão um problema maior. Somente 22% acreditam que o acesso não autorizado aumentará em atividade; 20% acham que, na verdade, ele diminuirá.

Figura 22. Mudanças nas ameaças de segurança durante o próximo ano
Visualização consolidada (n=314)



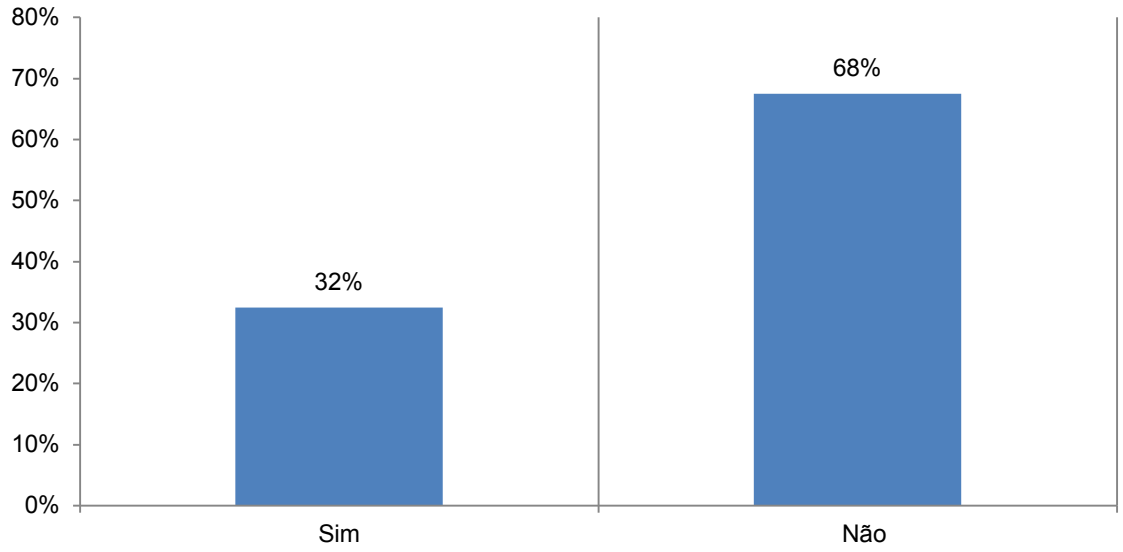
As empresas precisam melhorar sua abordagem estratégica em relação às ameaças. Conforme mostrado na Figura 23, estratégias destinadas a proteger a presença online, ativos de informações e a infraestrutura não existem para a maioria das empresas representadas nesta pesquisa. É mais provável que existam estratégias para proteger os ativos de informações. Conforme discutido acima, o orçamento para executar a estratégia de segurança da organização e sua missão é muito inferior ao que consideram necessário. Isso poderia explicar tais conclusões.

Figura 23. Estratégia de segurança atual
Visualização consolidada (n=314)



Cerca de um terço das empresas estão incorporando o seguro cibernético como parte de sua estratégia de gerenciamento de risco. Segundo a Figura 24, 32% das organizações que participaram da pesquisa têm uma apólice de seguro cibernético para gerenciar o risco de ataques e ameaças. Dentre aquelas que têm seguro cibernético, 54% estão satisfeitas com a cobertura.

Figura 24. A organização tem uma apólice de seguro cibernético ou de proteção contra a violação de dados?
Visualização consolidada (n=314)



Uma conclusão interessante é o papel importante que o seguro cibernético pode desempenhar não apenas no gerenciamento do risco de uma violação de dados, mas na melhoria da postura de segurança da empresa. Foi sugerido que ter seguro incentiva as empresas a relaxarem em relação à segurança, mas nossa pesquisa sugere o contrário. As empresas com boas práticas de segurança estão mais propensas a comprar um seguro.

Parte 4. Como calculamos o custo da violação de dados

Para calcular o custo da violação de dados, utilizamos uma metodologia de custo chamada de custo baseado em atividades (ABC). Essa metodologia identifica atividades e atribui um custo de acordo com o uso real. As empresas que participaram dessa pesquisa de referência precisaram estimar o custo para todas as atividades realizadas com o objetivo de resolver uma violação de dados.

As atividades típicas de descoberta e resposta imediata à violação de dados incluem o seguinte:

- Realizar investigações e análises forenses para determinar a causa-raiz da violação de dados
- Determinar as prováveis vítimas da violação de dados
- Organizar a equipe de resposta a incidentes
- Conduzir a comunicação e a sensibilização por meio de relações públicas
- Preparar documentos de notificação e outras divulgações necessárias para as vítimas da violação de dados e reguladores
- Implementar procedimentos de central de atendimento e treinamento especializado

Estas são as atividades típicas realizadas após a descoberta de uma violação de dados:

- Serviços de auditoria e consultoria
- Serviços jurídicos para defesa
- Serviços jurídicos para conformidade
- Serviços gratuitos ou com desconto para as vítimas da violação
- Serviços de proteção de identidade
- Perda de negócios de clientes com base no cálculo da perda ou rotatividade de clientes
- Custos da aquisição de clientes e do programa de fidelidade

Depois que a empresa estima uma faixa de custo para essas atividades, os custos são categorizados como diretos, indiretos e de oportunidade, conforme definido abaixo:

- *Custo direto*—o desembolso de despesas diretas para realizar determinada atividade.

- *Custo indireto*—a quantidade de tempo, esforço e outros recursos organizacionais utilizados, mas não como desembolso direto de dinheiro.

- *Custo de oportunidade*—o custo resultante de oportunidades de negócios perdidas como consequência dos efeitos da reputação negativa depois que a violação foi informada às vítimas (e revelada ao público pela imprensa).

Nosso estudo também examina as principais atividades relacionadas a processos que orientam uma série de despesas associadas à detecção, resposta, contenção e correção da violação de dados de uma organização. Os custos referentes a cada atividade são apresentados na seção Principais Conclusões (Parte 2). Os quatro centros de custo são:

- Detecção ou descoberta: Atividades que permitem que uma empresa detecte, de forma razoável, a violação de dados pessoais em risco (em armazenamento) ou em movimento.

- Encaminhamento: Atividades necessárias para informar a violação das informações protegidas às pessoas adequadas dentro de um período de tempo especificado.

- Notificação: Atividades que permitem que a empresa notifique os sujeitos dos dados de que informações pessoais foram perdidas ou roubadas; pode ser por meio de carta, telefonema de saída, email ou notificação geral.

- Posterior à violação de dados: Atividades para ajudar as vítimas de uma violação a se comunicar com a empresa para fazer perguntas adicionais ou obter recomendações a fim de minimizar possíveis danos. As atividades posteriores à violação de dados também incluem monitoramento do relatório de crédito ou a nova emissão de uma nova conta (ou cartão de crédito).

Além das atividades relacionadas a processos acima, a maioria das empresas tem custos de oportunidade associados ao incidente de violação, que resultam da diminuição da confiança por parte de clientes atuais ou futuros. Portanto, a pesquisa do nosso Instituto mostra que a publicidade negativa associada a um incidente de violação de dados causa efeitos na reputação que podem resultar em taxas de rotatividade ou perda anormal de clientes, assim como na diminuição da taxa de aquisições de novos clientes.

Para extrapolar esses custos de oportunidade, é utilizado um método de estimação de custo que se baseia no "valor vitalício" de um cliente médio, conforme definido para cada organização participante.

- Rotatividade de clientes existentes: O número estimado de clientes que provavelmente encerrarão seu relacionamento como resultado do incidente de violação. A perda incremental é a rotatividade anormal atribuível ao incidente de violação. Esse número é uma porcentagem anual, baseada em estimativas fornecidas pela gerência durante o processo de entrevista de referência[9].

- Diminuição da aquisição de clientes: O número estimado de clientes-alvo que não terão um relacionamento com a organização como consequência da violação. Esse número é fornecido como uma porcentagem anual.

Reconhecemos que a perda de dados que não são de clientes, como registros de funcionários, poderá não afetar a perda ou rotatividade de clientes de uma organização[10]. Nesses casos, espera-se que a categoria de custo de negócios seja menor quando as violações de dados não envolvem dados de clientes ou consumidores (incluindo informações sobre a transação de pagamento).

[9]Em vários casos, a rotatividade é parcial, ou seja, as vítimas da violação continuam seu relacionamento com a organização que sofreu a violação, mas o volume de atividades dos clientes acaba diminuindo. Esse declínio parcial é percebido especialmente em determinados segmentos de mercado—como serviços financeiros ou entidades do setor público—em que a rescisão é cara ou economicamente inviável.

[10]Neste estudo, informações sobre cidadãos, pacientes e estudantes foram consideradas dados de clientes.

Parte 5. Características organizacionais e métodos de referência

A Figura 25 mostra a distribuição das organizações de referência conforme sua classificação principal de segmento de mercado. No estudo deste ano, 16 segmentos de mercado estão representados.
O maior setor é o de serviços financeiros, que inclui bancos, seguros, gerenciamento de investimentos e processadores de pagamento.

Figura 25. Distribuição da amostra de referência por segmento de mercado
Visualização consolidada (n=314)

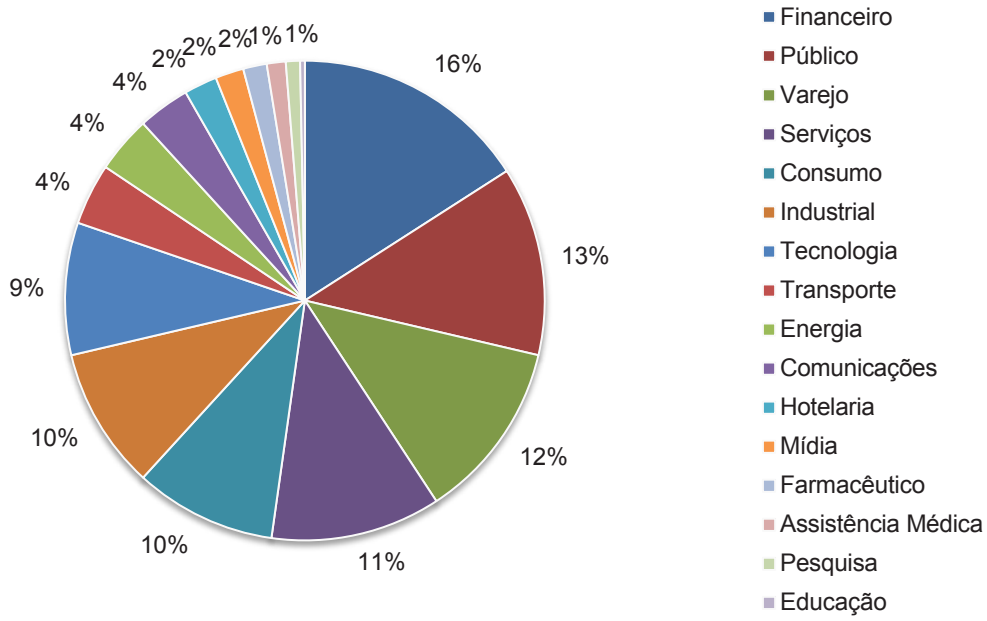
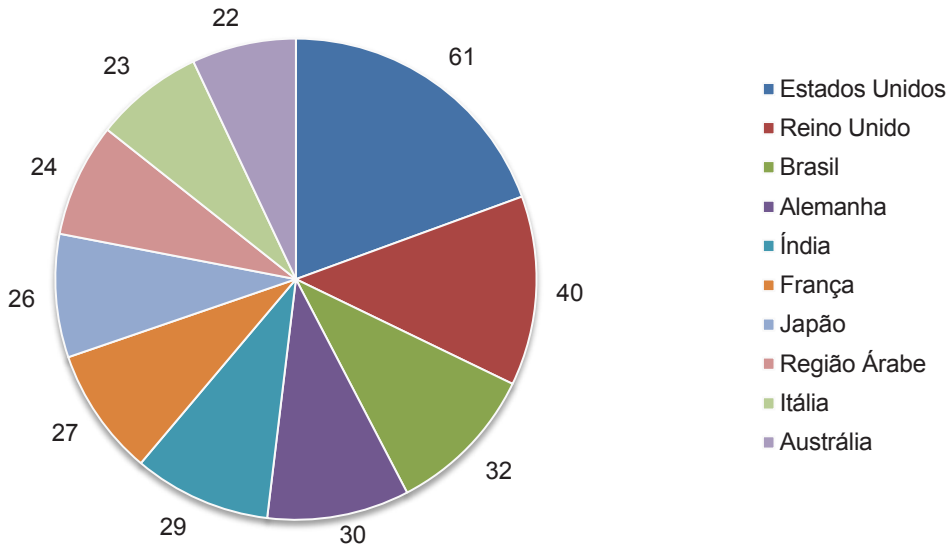


Figura 26. Tamanhos das amostras para os estudos em 10 países



Os métodos de coleta de dados não incluíram informações de contabilidade reais, mas utilizaram a estimação numérica baseada no conhecimento e experiência de cada participante. Em cada categoria, a estimação de custo foi um processo em duas fases. Em primeiro lugar, o instrumento de referência exigiu que os indivíduos classificassem as estimativas de custo direto para cada categoria de custo, marcando um intervalo variável definido no seguinte formato de linha de números.

Como usar a linha de números: A linha de números fornecida em cada categoria de custo da violação de dados é uma maneira de obter sua melhor estimativa para a soma de desembolsos de dinheiro, mão de obra e gastos adicionais incorridos. Marque apenas um ponto em algum lugar entre os limites inferior e superior indicados acima. É possível reconfigurar os limites inferior e superior da linha de números a qualquer momento durante o processo de entrevista.

Insira sua estimativa de custos diretos aqui para [categoria de custo apresentada]

LL	_____|_____	UL

O valor numérico obtido a partir da linha de números (em vez de uma estimativa pontual para cada categoria de custo apresentada) preservou a confidencialidade e assegurou uma taxa de resposta mais alta. O instrumento de referência também exigiu que os profissionais fornecessem uma segunda estimativa para custos indiretos e de oportunidade, separadamente.

Para manter o processo de referência em um tamanho gerenciável, os itens foram cuidadosamente limitados aos centros de atividades de custo que consideramos essenciais para a medição de custos da violação de dados. Com base nas discussões com especialistas informados, o conjunto final de itens incluiu um conjunto fixo de atividades de custo. Após a coleta das informações de referência, cada instrumento foi examinado novamente com cuidado em termos de consistência e completude.

Para fins de confidencialidade completa, o instrumento de referência não capturou informações específicas da empresa. Os materiais dos sujeitos não continham códigos de rastreamento ou outros métodos que pudessem associar as respostas às empresas participantes.

O escopo dos itens de custo da violação de dados contidos em nosso instrumento de referência foi limitado a categorias de custo conhecidas que se aplicam a um amplo conjunto de operações de negócios encarregadas do manuseio de informações pessoais. Acreditamos que um estudo focado no processo de negócios—não em atividades de proteção de dados ou conformidade com a privacidade—produziria resultados de melhor qualidade.

Parte 6. Limitações

Nosso estudo utiliza um método de referência confidencial e exclusivo que foi implementado com sucesso em pesquisas anteriores. Contudo, esta pesquisa de referência possui limitações inerentes que precisam ser consideradas com cuidado antes de tirar conclusões.

- Resultados não estatísticos: Nosso estudo utiliza uma amostra representativa e não estatística de entidades globais que sofreram uma violação envolvendo a perda ou roubo de registros de clientes ou consumidores durante os últimos 12 meses. Inferências estatísticas, margens de erro e intervalos de confiança não podem ser aplicados a esses dados, uma vez que nossos métodos de amostragem não são científicos.
- Ausência de resposta: As conclusões atuais se baseiam em uma pequena amostra representativa de referências. Neste estudo global, 314 empresas concluíram o processo de referência. O viés de ausência de resposta não foi testado. Por isso, é possível que as empresas que não participaram sejam substancialmente diferentes em termos de custo subjacente de violação de dados.
- Viés de estrutura de amostragem: Como nossa estrutura de amostragem é de julgamento, a qualidade dos resultados é influenciada pelo grau em que a estrutura é representativa da população de empresas estudada. Acreditamos que a estrutura de amostragem atual está predisposta a empresas com programas mais maduros de privacidade ou segurança de informações.
- Informações específicas da empresa: As informações de referência são sensíveis e confidenciais. Assim, o instrumento atual não captura informações que identificam a empresa. Também permite que indivíduos utilizem variáveis de resposta categórica para divulgar informações demográficas sobre a categoria da empresa e do segmento de mercado.
- Fatores não avaliados: Para manter o script de entrevista conciso e focado, decidimos omitir outras variáveis importantes de nossas análises, tais como principais tendências e características organizacionais. Não é possível determinar até que ponto as variáveis omitidas poderiam explicar os resultados de referência.
- Resultados de custo extrapolados: A qualidade da pesquisa de referência se baseia na integridade das respostas confidenciais fornecidas pelos entrevistados das empresas participantes. Embora alguns controles possam ser incorporados no processo de referência, sempre existe a possibilidade de que os entrevistados não forneceram respostas corretas ou verdadeiras. Além disso, o uso de métodos de extrapolação de custo (em vez de dados de custo real) pode introduzir viés e imprecisões de modo acidental.

Se você tiver perguntas ou comentários sobre este relatório de pesquisa ou se quiser obter cópias adicionais do documento (incluindo permissão para citar ou reutilizar o relatório), entre em contato com carta, telefone ou email:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49686 USA
1.800.887.3118
research@ponemon.org

Cópias completas dos relatórios de todos os países estão disponíveis em www.ibm.com/services/costofbreach.

Ponemon Institute LLC

Promovendo o Gerenciamento Responsável de Informações

O Ponemon Institute dedica-se à pesquisa independente e a uma educação que promove práticas responsáveis de gerenciamento de informações e privacidade nos negócios e no governo. Nossa missão é realizar estudos empíricos de alta qualidade sobre questões críticas que afetam o gerenciamento e a segurança de informações sensíveis a respeito de pessoas e organizações.

Como membro do **Council of American Survey Research Organizations (CASRO),** nós mantemos padrões rigorosos de confidencialidade de dados, privacidade e pesquisa ética. Não coletamos informações de indivíduos que possam identificá-los pessoalmente (nem informações identificáveis de empresas em nossa pesquisa de negócios). Além disso, temos rigorosos padrões de qualidade para assegurar que os sujeitos não precisem responder a perguntas estranhas, irrelevantes ou inadequadas.

SELQ3Q27-BRPT-QQ