Estudo sobre o custo da violação de dados 2015: Brasil

Pesquisa de referência patrocinada pela IBM conduzida de forma independente pelo Instituto Ponemon LLC Maio de 2015

Relatório de Pesquisa do Instituto Ponemon

Estudo sobre o custo de violação de dados 2015[1]: Brasil

Instituto Ponemon, maio de 2015

Parte 1. Introdução

A IBM e o Instituto Ponemon têm o prazer de apresentar o *Custo de violação de dados 2015: Brasil,* nosso terceiro estudo de referência anual sobre o custo de incidentes de violação de dados para empresas localizadas no Brasil. A pesquisa revela que o custo médio[2] da violação de dados por registro aumentou significativamente de R$157 (Reais) para R$175. O custo total da violação de dados organizacional aumentou de R$3,60 milhões para R$3,96 milhões.

Visão geral do Estudo do Brasil

- 34 empresas participaram
- R$3,9 milhões é o custo total médio da violação de dados
- 10% de aumento no custo total da violação de dados
- R$175 é o custo médio por registro perdido ou furtado
- 11% de aumento no custo por registro perdido ou furtado

A série de pesquisa sobre *Custo de violação de dados* foi lançada há 10 anos atrás nos Estados Unidos e no Brasil há três anos. Desde então, expandimos o estudo para incluir o Reino Unido, a França, a Alemanha, a Itália, a Índia, a Austrália, o Japão e os Emirados Árabes e a Arábia Saudita (região árabe). Este ano, pela primeira vez, conduzimos nossa pesquisa de custo de violação de dados no Canadá. Até o momento, 97 organizações brasileiras participaram no processo de benchmarking.

O estudo deste ano examina os custos incorridos por 34 empresas brasileiras de 12 diferentes setores industriais seguindo a perda ou o furto de dados pessoais protegidos e a notificação de vítimas de violação conforme necessários por várias leis. É importante observar que os custos apresentados nesta pesquisa não são hipotéticos, mas são de incidentes reais de perda de dados. Os custos são baseados em estimativas fornecidas pelas pessoas entrevistadas por um período de dez meses nas empresas representadas nessa pesquisa.

O número de registros violados por incidente este ano variou de 4.300 registros a 88.120. O número médio de registros violados era de 22.902. Não incluímos organizações que tinham mais de 100 mil violações de dados, porque elas não eram representativas da maioria das violações de dados e incluí-las no estudo distorceria os resultados.

As descobertas e implicações para organizações a seguir são as mais interessantes:

O custo, total e por registro, da violação de dados organizacional aumentou. De acordo com as descobertas de referência, o custo médio para organizações que tinham uma violação de dados aumentou em média de R$157 por registro comprometido em 2014 para R$175 em 2015. O custo médio total de violação de dados em 2014 era R$3,60 milhões. O estudo deste ano revelou um aumento para R$3,96.

As medidas revelam por que os custos de violação de dados aumentaram. O custo médio total e o custo por registro de uma violação de dados aumentaram em até 10% e 11%, respectivamente. Entretanto, o índice de cancelamento anormal diminuiu 15%, indicando que as empresas estão fazendo um trabalho melhor ao reter clientes depois de uma violação de dados. O tamanho médio de violação de dados ou número de registros perdidos ou furtados aumentou 2%.

Certos segmentos de mercado tiveram custos de violação de dados mais altos. Os serviços de comunicações, energia e financeiros tiveram um custo de violação de dados substancialmente acima da média geral de R$175. As empresas de transporte, setor público (governo) e de bens de consumo tiveram um custo por registro bem abaixo do valor médio geral.

[1] Pela primeira vez, esse relatório é datado no ano de publicação em vez de na data de conclusão de campo. Observe que a maioria dos dados dos incidentes de violação de dados estudados no relatório atual aconteceu no ano de 2013.

[2] Os termos "custo por registro" e registro comprometido por custo têm significado equivalente nesse relatório.

Os ataques maliciosos eram a causa raiz principal de violações de dados e são os mais onerosos.[3]
Trinta e oito por cento de incidentes envolviam um ataque malicioso ou criminoso. A negligência do funcionário ou contratado representa 32 por cento de todas as violações e as falhas do sistema somam 30 por cento de todas as violações de dados. De acordo com nossa pesquisa, as empresas que passaram por um incidente malicioso tinham um custo de violação de dados por registro de R$202. As empresas que passaram por falhas do sistema tinham um custo médio de R$167. A negligência do funcionário ou o erro humano custaram uma média de R$150

Certos fatores podem reduzir o custo da violação de dados. O uso abrangente de criptografia, os planos de resposta de incidente, o envolvimento do gerenciamento de continuidade de negócios, o treinamento do funcionário, o compromisso de um CISO, o envolvimento do comitê e a proteção de seguros diminuíram o custo por registro da violação de dados. Entretanto, o erro ou envolvimento de terceiros, os dispositivos perdidos ou furtados, a pressa em notificar e o engajamento de consultores aumentou o custo por registro da violação de dados.

Quanto mais registros perdidos, maior o custo da violação de dados. As empresas que tinham uma violação de dados envolvendo menos de 10.000 registros tinham uma violação de dados de R$1,2 milhões e violações de dados envolvendo 50.000 ou mais registros e tinham uma média de R$6,65 milhões.

Certos segmentos de mercado são mais vulneráveis para o índice de cancelamento. Os setores financeiro, organizações de serviços, farmacêutico, comunicações e energia passaram por um índice de cancelamento relativamente alto e anormal e o setor público (governo), as empresas de varejo e indústria passaram por uma taxa de cancelamento anormal muito baixa.

Os custos de detecção e procedimentos para escalar aumentaram significativamente. Esses custos geralmente incluem atividades forenses e investigativas, serviços de avaliação e auditoria, gerenciamento de equipe de crise e comunicações com a gerência executiva e o comitê de diretores. Os custos médios de detecção e procedimentos para escalar aumentaram de R$0,87 milhões em 2014 para R$1,09 milhões em 2015.

Os custos de notificação diminuíram. Os custos de notificação incluem atividades de TI associadas à criação de bancos de dados de contato, determinação de todos os requisitos regulamentares, engajamento de especialistas externos, dispêndios postais, contatos secundários para retornos de correio ou emails e configuração de comunicação de entrada. O custo médio de notificação deste ano diminuiu de R$0,12 milhões para R$0,11 milhões.

Os custos de pós-violação de dados continuam a aumentar. Os custos de pós-violação de dados geralmente incluem atividades de help desk, comunicações de entrada, atividades investigativas especiais, atividades de correção, dispêndios legais, descontos de produto, serviços de proteção de identidade e intervenções regulamentares. Os antigos custos médios de pós-resposta aumentaram de R$1,14 milhões em 2014 para R$1,23 em 2015.

Os custos de negócios perdidos aumentaram. Esses custos incluem a rotatividade anormal de clientes, as atividades de aquisição do cliente aumentadas, as perdas de reputação e o fundo de comércio diminuído. O custo médio de negócios perdidos para organizações de referência aumentou de R$1,47 milhões em 2014 para R$1,53 em 2015.

Ambos os custos diretos e indiretos da violação de dados aumentaram significativamente. Ambos os custos diretos e indiretos de uma violação de dados aumentaram até R$9. O custo direto por registro comprometido aumentou de R$63 para R$72. O custo indireto elevou-se de R$94 por registro para R$103. [3]

[3]Pessoas internas negligentes são pessoas que causam uma violação de dados devido a sua falta de cuidado, conforme determinado em uma investigação de pós-violação de dados. Nesse estudo, os hackers ou criminosos internos (funcionários, contratados ou outros terceiros) geralmente são responsáveis por ataques maliciosos ou criminosos.

Perguntas mais frequentes do custo de violação de dados

O que é uma violação de dados? Uma violação é definida como um evento no qual o nome de uma pessoa mais o registro médico e/ou um registro financeiro ou cartão de débito é possivelmente colocado em risco - seja no formato eletrônico ou papel. Em nosso estudo, identificamos três causas principais de violação de dados. Esses são um 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 proteções a postos no momento da violação de dados.

O que é um registro comprometido? Definimos um registro como informações que identificam a pessoa natural (indivíduo) cujas informações foram perdidas ou furtadas em uma violação de dados. Os exemplos podem incluir o banco de dados da empresa de varejo com o nome de uma pessoa associado a informações de cartão de crédito e outras informações de identificação pessoal. Ou poderia ser o registro de uma seguradora de saúde do segurado com informações médicas e de pagamento. No estudo deste ano, o custo médio para a organização se um desses registros for perdido ou furtado é de R$175.

Como você coleta os dados? Os pesquisadores do Instituto Ponemon coletaram dados qualitativos aprofundados por meio de entrevistas conduzidas por um período de dez meses. O recrutamento de organizações para o estudo de 2015 começou em janeiro de 2014 e as entrevistas foram concluídas em março de 2015. Em cada uma das 34 organizações participantes, falamos com os profissionais de TI, conformidade e segurança da informação cientes da violação de dados de suas organizações e custos associados à resolução da violação. Para fins de privacidade, não coletamos informações específicas da organização.

Como você calcula o custo da violação de dados? Para calcular o custo médio da violação de dados, coletamos ambos as despesas diretas e indiretas incorridas pela organização. As despesas diretas incluem o engajamento de especialistas forenses, a terceirização do suporte de linha direta e o fornecimento de assinaturas de monitoramento de crédito gratuito e descontos de produtos e serviços futuros. Os custos indiretos incluem investigações internas e comunicação, bem como o valor extrapolado da perda do cliente resultante da rotatividade ou taxas de aquisição do cliente diminuídas.

Como a pesquisa de referência difere da pesquisa de opinião? A unidade de análise no estudo *Custo de violação de dados* é a organização. Na pesquisa de opinião, a unidade de análise é a pessoa. Recrutamos 34 organizações a participarem deste estudo. As violações de dados variaram de uma taxa baixa de 4.300 a uma taxa alta de 88.120 registros comprometidos.

O custo médio da violação de dados pode ser usado para calcular as consequências financeiras de uma mega violação, como aquelas que envolvem milhões de registros perdidos ou furtados? O custo médio de uma violação de dados em nossa pesquisa não se aplica a violações de dados enormes ou catastróficas, porque não são típicas das violações que a maioria das organizações passam. Para sermos representantes da população das organizações brasileiras e tirar conclusões da pesquisa que pode ser útil ao entender os custos quando as informações protegidas são perdidas ou furtadas, não incluímos as violações de dados de mais de 100 mil registros comprometidos em nossa análise.

Você está controlando as mesmas organizações todo ano? Cada estudo anual envolve uma amostra diferente de empresas. Em outras palavras, não estamos controlando a mesma amostra de empresas ao longo do tempo. Para sermos consistentes, recrutamos e combinamos empresas com características semelhantes, como o segmento de mercado da empresa, o número de funcionários, a área de cobertura geográfica e o tamanho da violação de dados. Desde o começo dessa pesquisa em 2013, estudamos as experiências de violação de dados de 97 organizações localizadas nas organizações do Brasil.

Parte 2. Principais descobertas

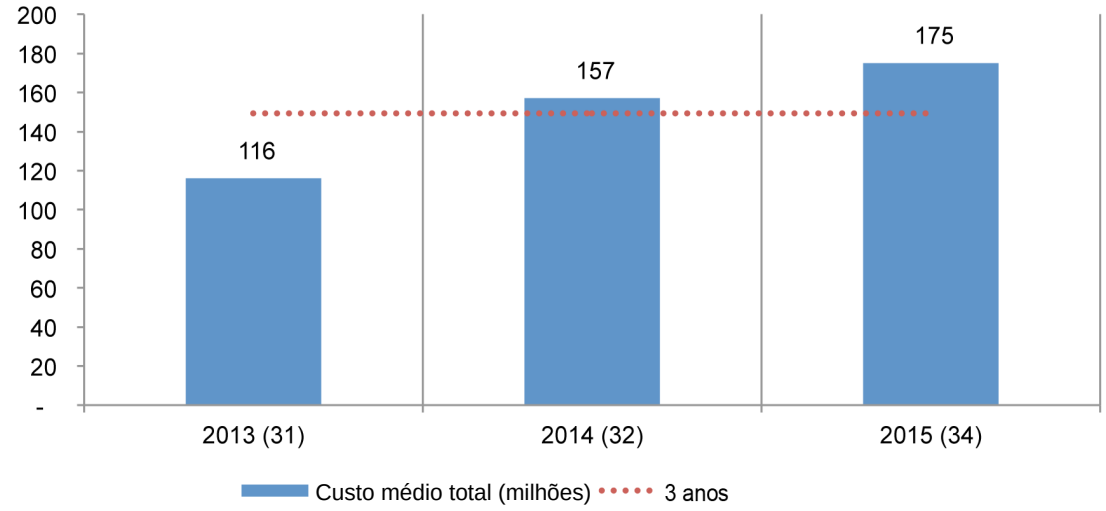
Nesta seção, fornecemos as descobertas detalhadas desta pesquisa. Os tópicos são apresentados na ordem a seguir:

- Entender o custo da violação de dados
- As causas raíz da violação de dados
- Fatores que influenciam o custo da violação de dados
- Tendências na frequência de registros comprometidos e rotatividade do cliente
- Tendências nos componentes de custo da violação de dados
- Recomendações sobre como minimizar o risco e as consequências de uma violação de dados

Entender o custo da violação de dados

O custo da violação de dados aumentou significativamente. A Figura 1 relata o custo médio por registro de uma violação de dados para 34 empresas brasileiras em 2015.[4] De acordo com as descobertas da referência, o custo médio para as organizações que tinham uma violação de dados aumentou de uma média de R$157 por registro comprometido para R$175.

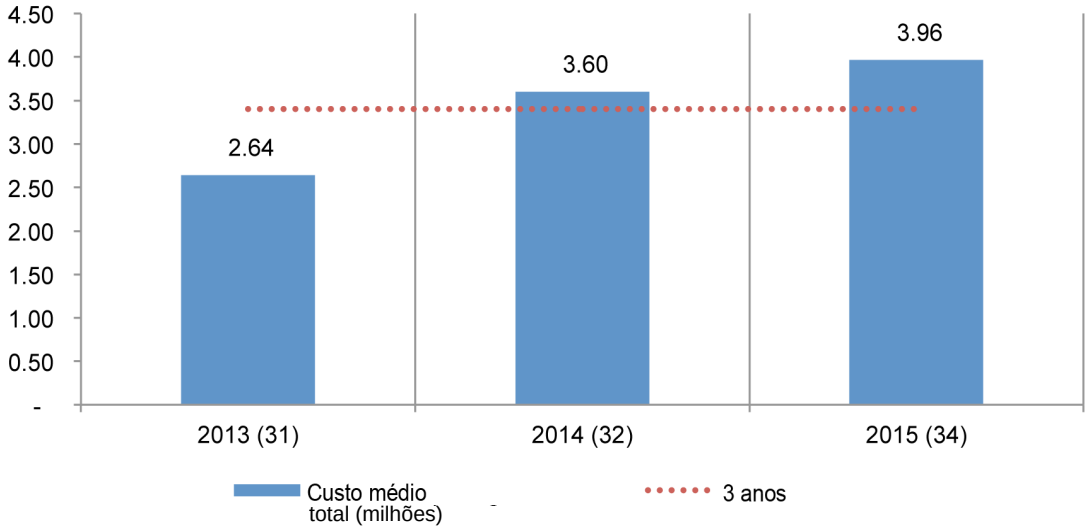
Figura 1. O custo médio por registro da violação de dados durante três anos
O número entre parênteses define o tamanho de amostra de referência
Valores em Reais (R$)



[4]O custo por registro é definido como o custo total da violação de dados dividido pelo tamanho da violação de dados em termos do número de registros perdidos ou furtados.

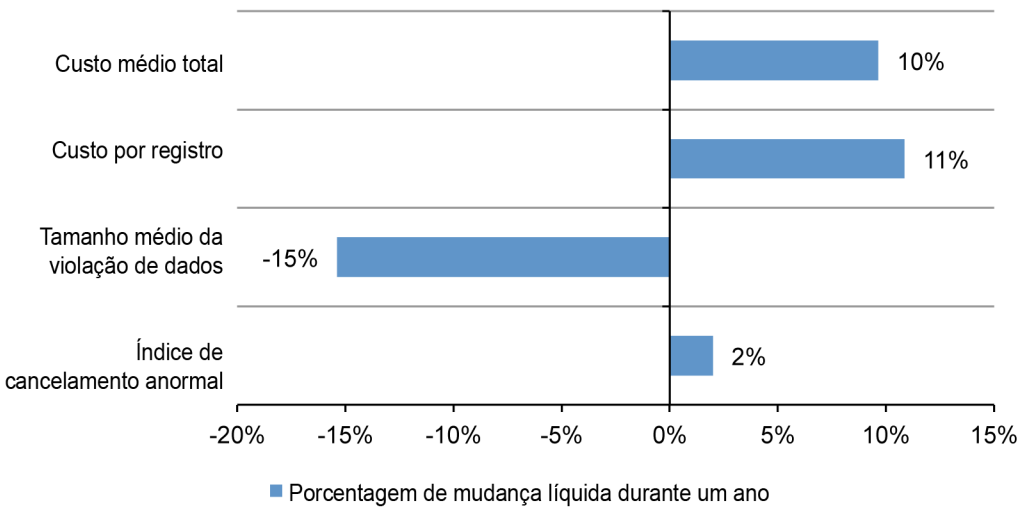
O custo médio total organizacional da violação de dados aumentou. A Figura 2 mostra o custo médio total da violação de dados para 32 empresas brasileiras em 2014 era de R$ 3,60 milhões. O estudo deste ano de 34 empresas revelou um aumento para R$ 3,96 milhões.

Figura 2. O custo médio total organizacional da violação de dados durante três anos
Medido em milhões de reais (R$)



As medidas revelam por que os custos de violação de dados aumentaram. A Figura 3 relata aumentos no custo médio total e no custo por registro de uma violação de dados em até 10% e 11%, respectivamente. O tamanho médio da violação de dados ou o número de registros perdidos ou furtados aumentou 2 por cento. Entretanto, o índice de cancelamento anormal diminuiu 15 por cento. No contexto dessa pesquisa, o índice de cancelamento anormal é definido como maior que a perda esperada dos clientes no curso normal dos negócios.

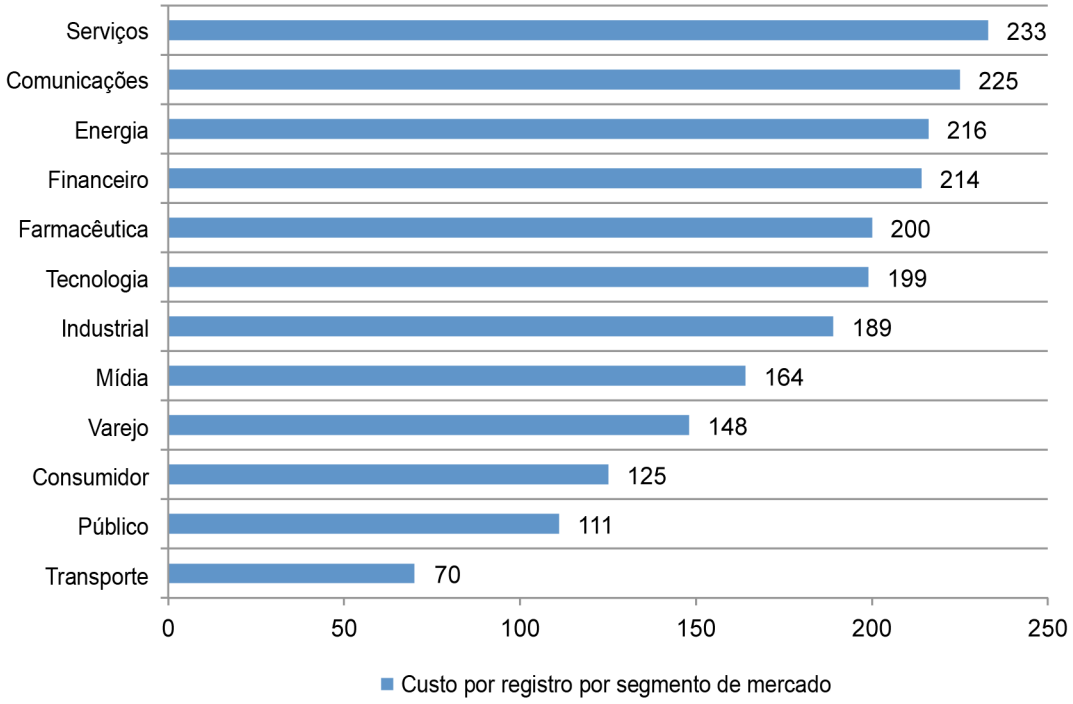
Figura 3. Medidas de custo de violação de dados
A mudança líquida é definida como a diferença entre os resultados de 2015 e 2014



Certos segmentos de mercado tiveram custos de violação de dados mais altos. A Figura 4 relata os custos por registro para o estudo de 2015 pela classificação de segmento de mercado.

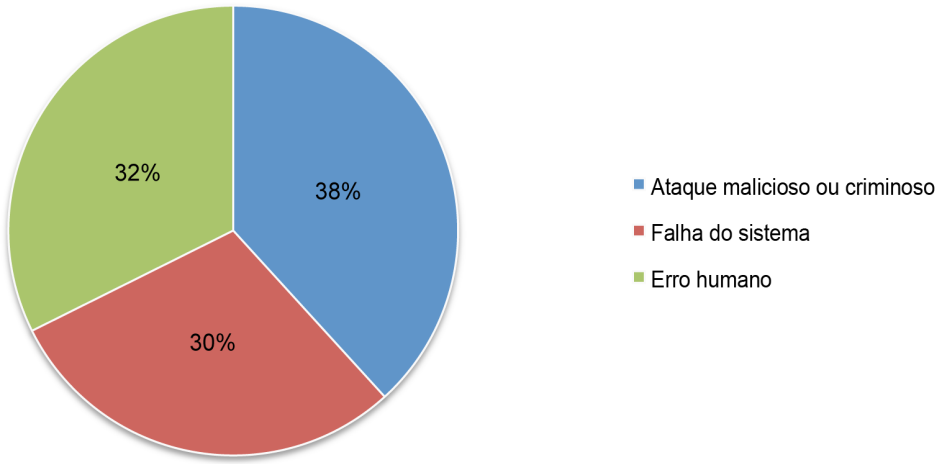
Embora um tamanho de amostra pequeno nos impeça de generalizar diferenças de custo de segmento de mercado, serviços, comunicações, serviços de energia e financeiros tiveram um custo por registro de violação de dados substancialmente acima da média geral de R$175. As empresas de transporte, setor público (governo) e de consumo tiveram um custo por registro bem abaixo do valor médio geral.

Figura 4. Custo por registro por classificação de segmento de mercado de empresas referenciadas
Medido em reais (R$)



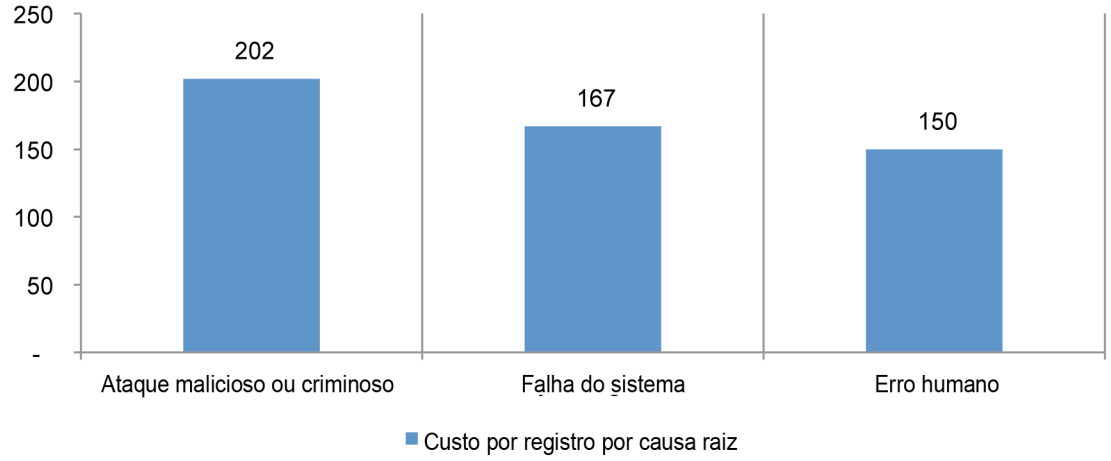
Os ataques maliciosos eram a causa raiz principal de violações de dados.[5] A Figura 5 fornece um resumo das causas raiz principais da violação de dados para todas as 34 organizações. Trinta e oito por cento de incidentes envolviam um ataque malicioso ou criminoso. A negligência do funcionário ou contratado representa 32 por cento de todas as violações de dados e as falhas do sistema somam 30 por cento de todas as violações de dados.

Figura 5. Distribuição da amostra de referência por causa raiz da violação de dados



Os ataques maliciosos são mais dispendiosos. A Figura 6 relata o custo por registro de violação de dados para as três causas raiz do incidente de violação. De acordo com nossa pesquisa, as empresas que passaram por um incidente malicioso tinham um custo de violação de dados por registro de R$202. As empresas que passaram por falhas do sistema tinham um custo médio de R$167. A negligência do funcionário ou o erro humano custam uma média de R$150.

Figura 6. Custo por registro para três causas raiz da violação de dados
Medido em reais (R$)



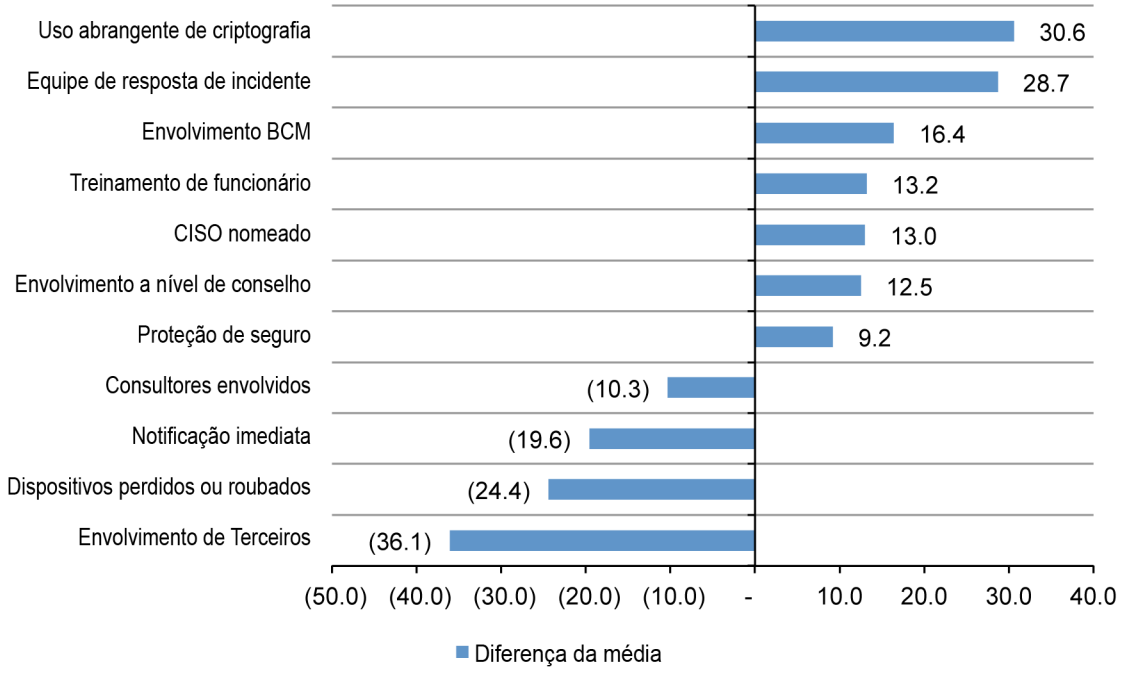
Pessoas internas negligentes são pessoas que causam uma violação de dados devido a sua falta de cuidado, conforme determinado em uma investigação de pós-violação de dados. Nesse estudo, os hackers ou criminosos internos (funcionários, contratados ou outros terceiros) geralmente são responsáveis por ataques maliciosos ou criminosos.

Fatores que influenciam o custo da violação de dados

Conforme mostrado na Figura 7, o uso abrangente de criptografia, os planos de resposta de incidente, o envolvimento do gerenciamento de continuidade de negócios, o treinamento do funcionário, o apontamento de um CISO, o envolvimento do comitê e a proteção de seguros diminuíram o custo por registro da violação de dados.

Entretanto, o envolvimento de terceiros, dispositivos perdidos ou furtados, a pressa em notificar e o engajamento dos consultores aumentou o custo por registro da violação de dados. Assim, o uso abrangente de criptografia reduziu o custo médio da violação de dados de R$175 para R$144,4 (custo diminuído = R$30,6). Por outro lado, um erro de terceiros aumentou o custo médio para R$211,10 (custo aumentado = R$36,1).

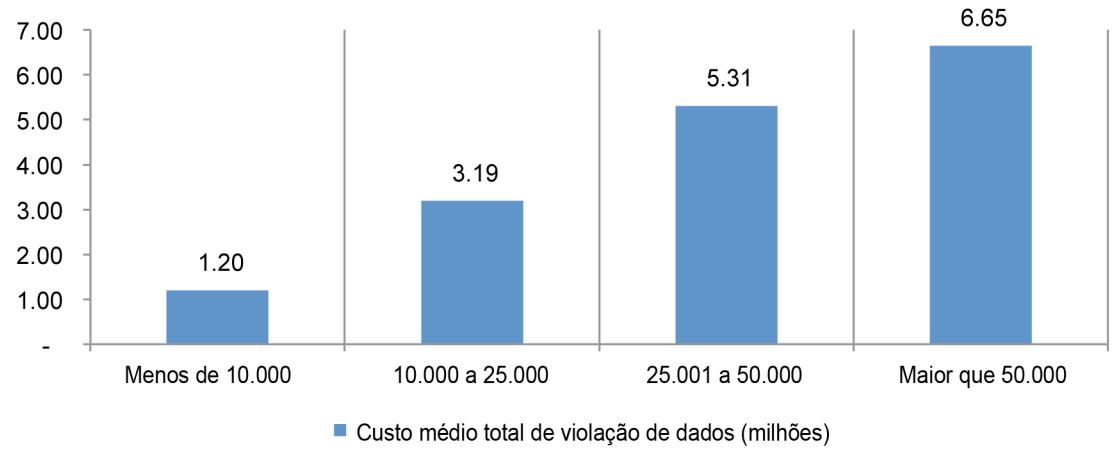
Figura 7. Impacto de 11 fatores no custo por registro da violação de dados
Medido em reais (R$)



Tendências na frequência de registros comprometidos e rotatividade do cliente

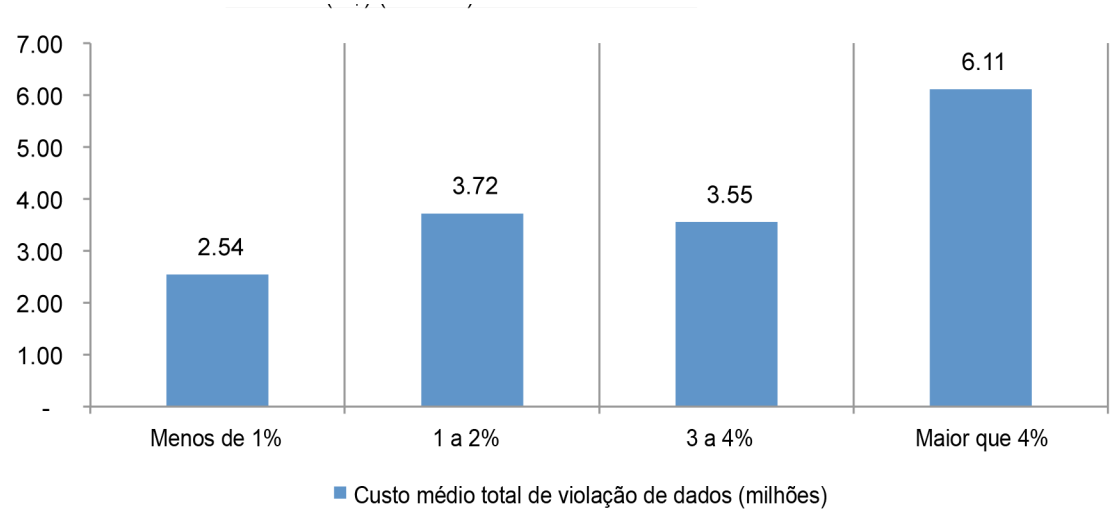
Quanto mais registros perdidos, maior o custo da violação de dados. A Figura 8 mostra o relacionamento entre o custo total da violação de dados e o tamanho do incidente para 34 empresas com referência em ordem crescente pelo tamanho do incidente da violação. As empresas que tinham uma violação de dados envolvendo menos de 10.000 registros tinham uma média de custo por registro de R$1,20 e as violações de dados envolvendo 50.000 ou mais registros tinham uma média de custo por registro de R$6,65.

Figura 8. Custo total de violação de dados por tamanho
Medido em milhões de reais (R$)



Quanto maior o índice de cancelamento, maior o custo por registro de violação de dados. A Figura 9 relata a distribuição dos custos de violação de dados por registro em taxa crescente de índice de cancelamento anormal. O custo por registro mais alto como um resultado do índice de cancelamento do cliente é de R$6,11 para índices de cancelamento maiores que 4% e o menor é R$2,54 para índices menores que 1%

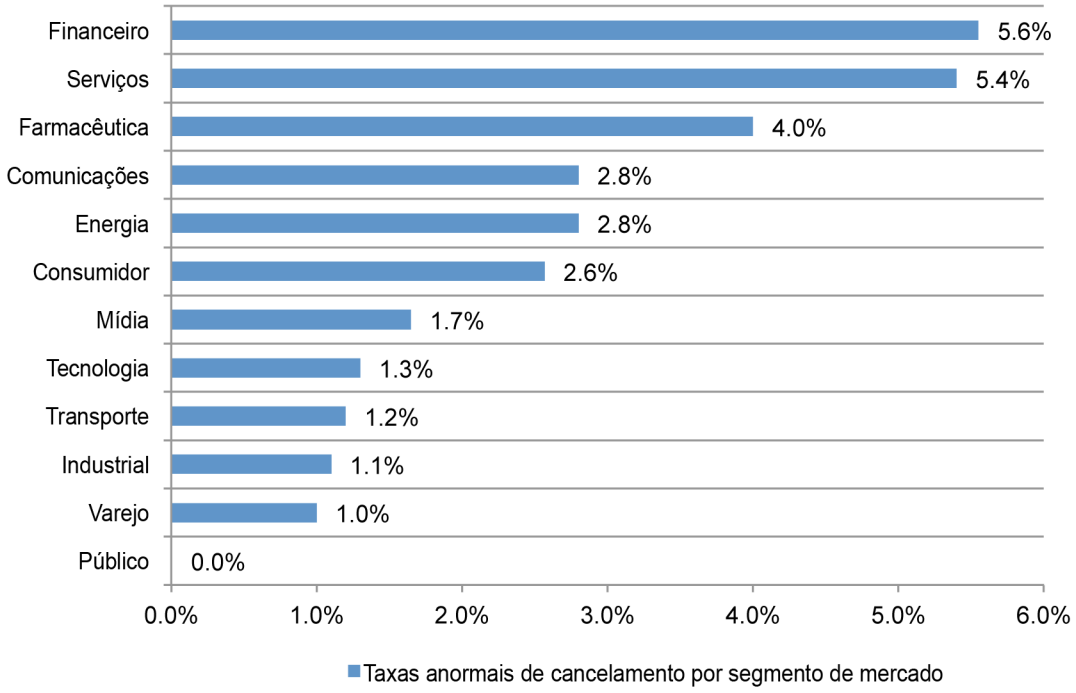
Figura 9. Custo total de violação de dados por taxa de cancelamento anormal
Medido em milhões de reais (R$)



Certos segmentos de mercado são mais vulneráveis ao índice de cancelamento. A Figura 10 relata a taxa de cancelamento anormal de organizações com referência para o estudo atual. Embora o tamanho de amostra pequeno nos impeça de generalizar o efeito do segmento de mercado nas taxas de cancelamento anormal, nossos resultados mostram a variação marcada - em que, os setores financeiro, organizações de serviços, farmacêutico, comunicações e energia passaram por um índice de cancelamento relativamente alto e anormal e o setor público (governo), as empresas de varejo e indústria passaram por uma taxa de cancelamento anormal muito baixa.[6]

A implicação dessas descobertas é que os segmentos de mercado com as mais altas taxas de cancelamento poderiam reduzir significativamente os custos de uma violação de dados enfatizando na retenção de clientes e atividades para preservar a reputação e o valor da marca.

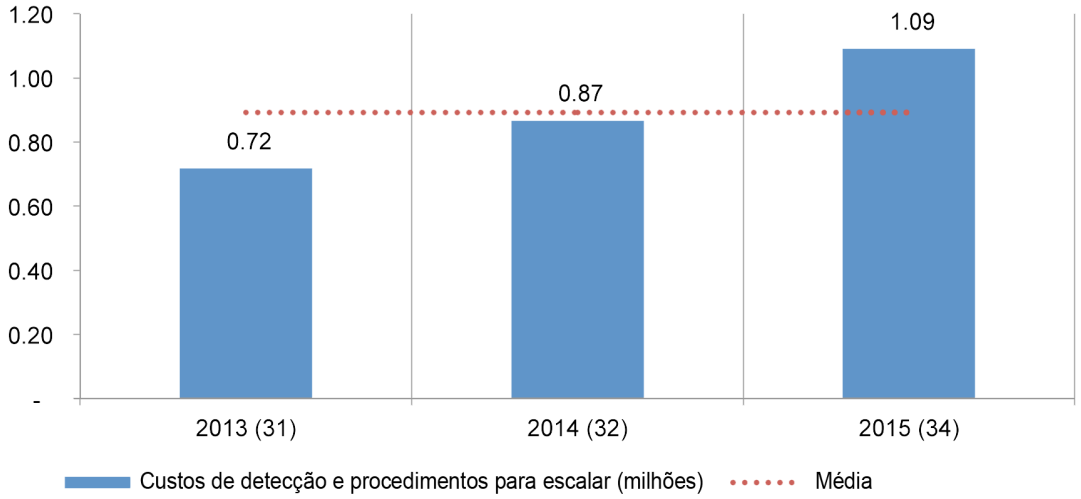
Figura 10. Taxas anormais de cancelamento pela classificação de segmento de mercado de empresas referenciadas



[6]As organizações do setor público utilizam uma estrutura de índice de cancelamento diferente uma vez que os clientes das organizações do governo geralmente não têm uma opção alternativa.

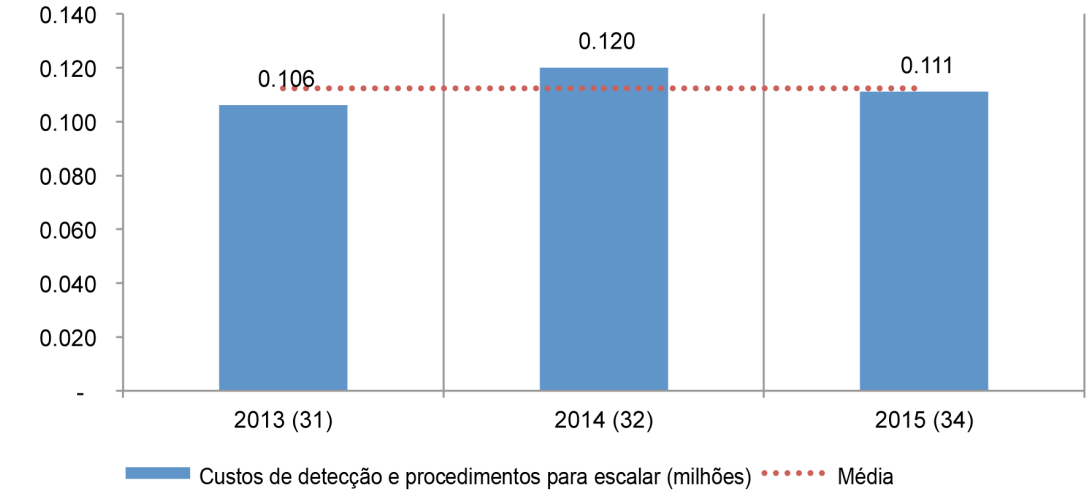
Os custos de detecção e procedimentos para escalar aumentaram significativamente. A Figura 11 mostra os custos associados à detecção e ao aumento de incidentes de violação de dados. Esses custos geralmente incluem atividades forenses e investigativas, serviços de avaliação e auditoria, gerenciamento de equipe de crise e comunicações com a gerência executiva e o comitê de diretores. Conforme observado, os custos médios de detecção e procedimentos para escalar aumentaram de R$0,87 milhões para R$1,09 milhões.

Figura 11. Custos médios de detecção e procedimentos para escalar durante três anos
Medido em milhões de reais (R$)



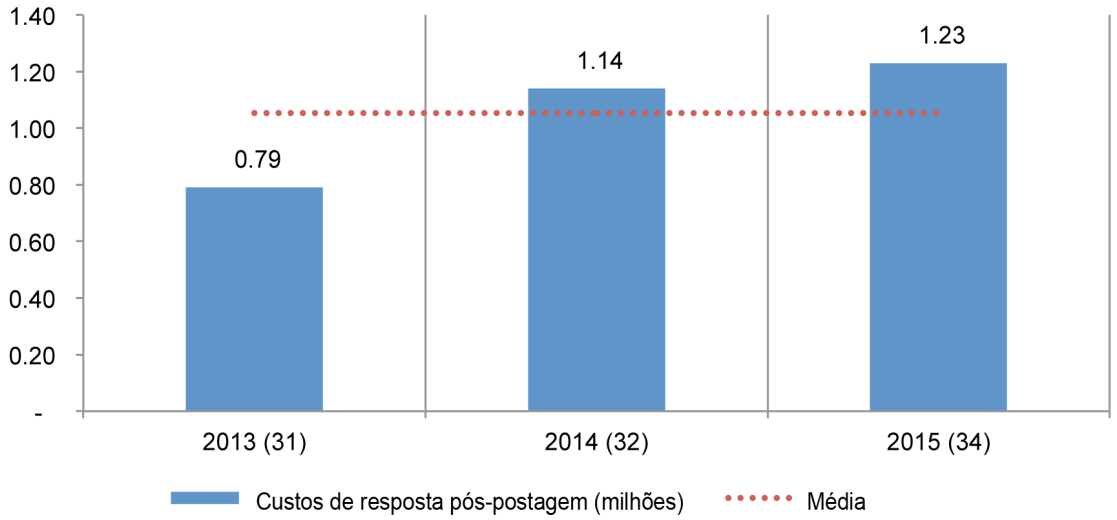
Os custos de notificação diminuíram. A Figura 12 relata os custos associados a atividades de notificação. Esses custos incluem atividades de TI associadas à criação de bancos de dados de contato, determinação de todos os requisitos regulamentares, engajamento de especialistas externos, dispêndios postais, contatos secundários para retornos de correio ou emails e configuração de comunicação de entrada. O custo médio de notificação deste ano diminuiu de R$0,12 milhões para R$0,11 milhões.

Figura 12. Custos médios de notificação durante três anos
Medido em milhões de reais (R$)



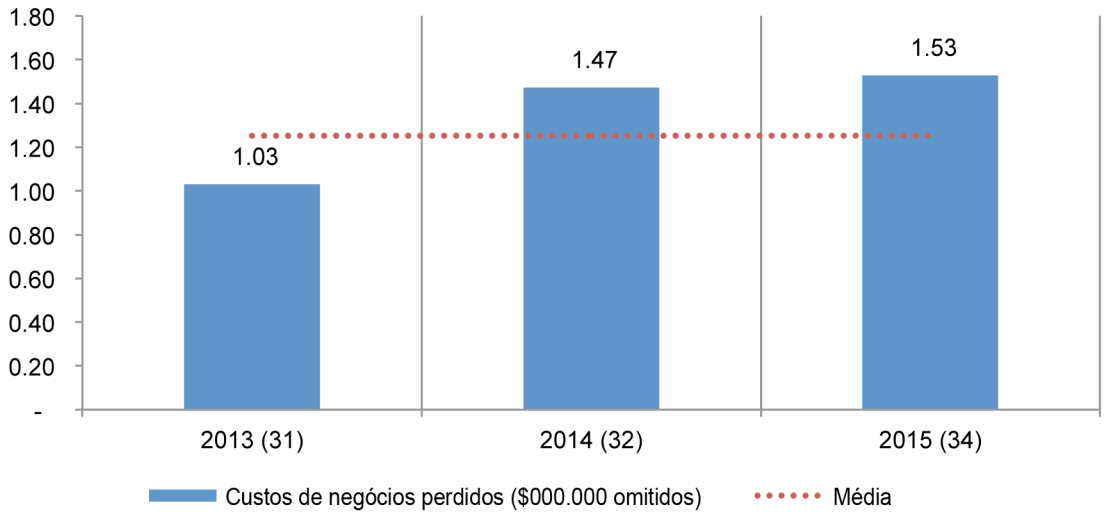
Os custos de pós-violação de dados continuam a aumentar. A Figura 13 mostra os custos associados a pós-atividades antigas (após o fato). Esses custos geralmente incluem atividades de help desk, comunicações de entrada, atividades investigativas especiais, atividades de correção, dispêndios legais, descontos de produto, serviços de proteção de identidade e intervenções regulamentares. Os antigos custos médios de pós-resposta aumentaram de R$1,14 milhões em 2014 para R$1,23 em 2015.

Figura 13. Custos médios de resposta pós-resposta durante 3 anos
Medido em milhões de reais (R$)



Os custos de negócios perdidos aumentaram. A Figura 14 relata os custos de negócios perdidos associados a incidentes de violação de dados pelos quais as empresas brasileiras passaram. Esses custos incluem a rotatividade anormal de clientes, as atividades de aquisição do cliente aumentadas, as perdas de reputação e o fundo de comércio diminuído. O custo médio de negócios perdidos para organizações de referência aumentou de R$1,47 milhões em 2014 para R$1,53 em 2015

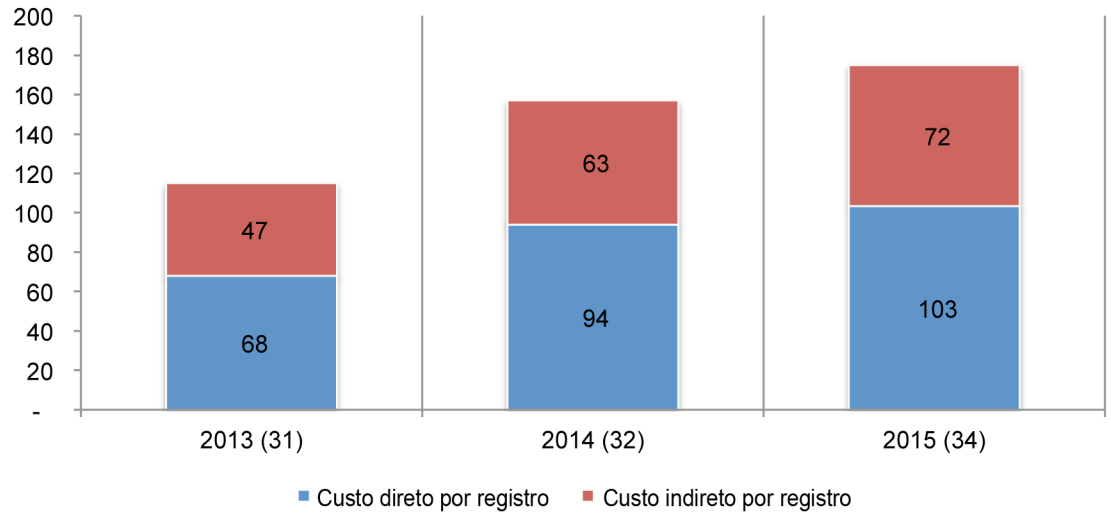
Figura 14. Custos médios de negócios perdidos durante três anos
Medido em milhões de reais (R$)



Ambos os custos diretos e indiretos da violação de dados aumentaram significativamente. Os custos diretos referem-se às despesas diretas para realizar uma determinada atividade, como engajar especialistas forenses, contratar um escritório de advocacia ou oferecer serviços de proteção de identidade a vítimas. Os custos indiretos incluem o tempo, o esforço e outros recursos organizacionais gastos. Isso inclui usar funcionários existentes para ajudar nos esforços de notificação de violação de dados ou na investigação do incidente. Os custos indiretos também incluem a perda de ágio e o índice de cancelamento do cliente.

A Figura 15 relata os componentes de custo direto ou indireto de uma violação de dados por registro. Ambos os custos aumentaram até R$9. O custo direto por registro comprometido aumentou de R$63 para R$72. O custo indireto elevou-se de R$94 por registro para R$103.

Figura 15. Tendências em custos diretos e indiretos de uma violação de dados durante três anos
Medido em reais (R$)



Recomendações sobre como minimizar o risco e as consequências de uma violação de dados

As empresas que participam de nosso estudo anual relatam que suas violações de dados eram mais altas no custo médio total e no custo por registro. Concluímos que o investimento em melhorar suas práticas de proteção de dados é importante. O uso abrangente de criptografia, o plano de resposta de incidente a postos, o envolvimento do gerenciamento de continuidade de negócios na correção da violação de dados, o treinamento de funcionários, o apontamento de um CISO com responsabilidade em toda a empresa, o envolvimento do nível de comitê e a proteção de seguros parecem todos reduzir custos de violação de dados para empresas brasileiras.

Esperamos que esse estudo ajude a entender o que os custos potenciais de uma violação de dados poderiam ser e como melhor alocar recursos para a prevenção, detecção e resolução de uma violação de dados. O estudo revela especificamente as consequências financeiras graves de atos maliciosos ou criminosos. Essas violações de dados podem provar serem as mais dispendiosas.

Além de medir as atividades de custo específicas em relação ao vazamento de informações pessoais, relatamos na Tabela 1 as medidas preventivas implementadas pelas empresas após a violação de dados. As medidas mais populares ou etapas tomadas são: procedimentos manuais adicionais e controles (44 por cento), uso expandido de criptografia (44 por cento), sistemas de segurança e inteligência (35 por cento) e soluções de gerenciamento de identidade e acesso (35 por cento).

Os maiores aumentos do último ano envolviam o uso expandido da criptografia (+11 por cento) e a implementação de sistemas de inteligência de segurança (+7 por cento). As maiores reduções envolviam o uso de procedimentos manuais adicionais e controles (-11 por cento) e soluções de segurança de endpoint (-5 por cento).

Tabela 1. Medidas preventivas e controles implementados após o incidente de violação	2013	2014	2015
Procedimentos manuais adicionais e controles	52%	55%	44%
Treinamento e programas de reconhecimento	40%	43%	40%
Soluções de gerenciamento de identidade e acesso	27%	31%	35%
Certificação ou auditoria de segurança	26%	25%	23%
Uso expandido de criptografia	25%	33%	44%
Fortalecimento de controles de perímetro	19%	26%	23%
Soluções de prevenção de perda de dados (DLP)	19%	27%	23%
Soluções de segurança de endpoint	18%	30%	25%
Sistemas de inteligência de segurança	15%	28%	35%
Outras práticas de controle do sistema	11%	9%	6%

*Observe que uma empresa pode estar implementando mais de uma medida preventiva.

A Tabela 2 resume 11 categorias de custo geral por porcentagem durante dois anos. Os dois custos mais altos são os negócios do cliente perdidos e as investigações e forense. Os custos permaneceram mais baixos desde o ano passado. Entretanto, as investigações e a forênsica aumentaram 3 por cento.

Parte 3. Observações e descrição sobre empresas participantes

Tabela 2. Mudanças de custo durante 3	2013	2014	2015
Investigações e forênsica	24%	26%	29%
Auditoria e serviços de consultoria	15%	12%	13%
Custos de contato de saída	3%	2%	1%
Custos de contato de entrada	3%	2%	1%
Relações públicas/comunicações	3%	3%	2%
Serviços legais - defesa	6%	7%	5%
Serviços legais - conformidade	5%	6%	5%
Serviços gratuitos ou descontados	7%	5%	4%
Serviços de proteção de identidade	1%	1%	2%
Negócios perdidos do cliente	25%	27%	29%
Custo de aquisição do cliente	8%	9%	9%
Total	100%	100%	100%

Parte 3. Como calculamos o custo da violação de dados

Para calcular o custo da violação de dados, usamos uma metodologia onerosa chamada Custo baseado em atividade (CBA). Essa metodologia identifica atividades e designa um custo de acordo com o uso real. As empresas que participam desta pesquisa de referência são solicitadas a estimarem o custo para todas as atividades em que elas se engajam para resolver a violação de dados.

Atividades típicas para descoberta e resposta imediata à violação de dados incluem o seguinte:

- Conduzir investigações e forênsica para determinar a causa raiz da violação de dados
- Determinar as prováveis vítimas da violação de dados
- Organizar a equipe de resposta de incidente
- Conduzir o alcance da comunicação e de relações públicas
- Preparar os documentos de aviso e outras divulgações necessárias para vítimas de violação de dados e reguladores
- Implementar procedimentos de call center e treinamento especializado

As atividades a seguir são atividades típicas conduzidas em consequência de descobrir a violação de dados:

- Auditoria e serviços de consultoria
- Serviços legais para defesa
- Serviços legais para conformidade
- Serviços gratuitos ou descontados para vítimas de violação
- Serviços de proteção de identidade
- Negócios perdidos de cliente com base no cálculo de índice de cancelamento ou rotatividade do cliente
- Custos de programa de aquisição e lealdade do cliente

Uma vez que a empresa estimar um intervalo de custos para essas atividades, categorizamos os custos como diretos, indiretos e oportunidade conforme definido abaixo:

- *Custo direto* - a despesa direta para realizar uma determinada atividade.
- *Custo indireto* - a quantia de tempo, esforço e outros recursos organizacionais gastos, mas não como despesa de dinheiro direta.
- *Custo de oportunidade* - o custo resultante de oportunidades de negócios perdidas como uma consequência de efeitos de reputação negativa após a violação ter sido relatada a vítimas (e revelada publicamente à mídia).

Nosso estudo também considera as principais atividades relacionadas ao processo que orientam uma variedade de custos associados à detecção, resposta, retenção e correção de violação de dados da organização. Os custos para cada atividade são apresentados na seção Descobertas principais (Parte 2). Os quatro centros de custos são:

- Detecção ou descoberta: Atividades que permitem que uma empresa detecte razoavelmente a violação de dados pessoais em risco (em armazenamento) ou em movimento.
- Escala: Atividades necessárias para relatar a violação de informações protegidas à equipe apropriada em um período especificado.
- Notificação: atividades que permitem que a empresa notifique assuntos de dados com uma letra, chamada de telefone de saída, email ou aviso geral de que as informações pessoais foram perdidas ou furtadas.
- Pós violação de dados: Atividades para ajudar as vítimas de uma violação a comunicarem-se com a empresa para fazer perguntas adicionais ou obter recomendações a fim de minimizar possíveis danos. As atividades de pós-violação de dados também incluem o monitoramento de relatório de crédito ou a nova emissão de uma nova conta (ou cartão de crédito).

Além das atividades relacionadas a processo acima, a maioria das empresas passa por custos de oportunidade associados ao incidente de violação, que resulta da confiança diminuída por clientes presentes e futuros. Desta forma, a pesquisa do nosso Instituto mostra que apublicidade negativa associada ao incidente de violação de dados causa efeitos de reputação que podem resultar em taxas de rotatividade ou cancelamento anormais, bem como uma taxa diminuída para novas aquisições do cliente.

Para extrapolar os custos desta oportunidade, usamos um método de estimativa de custo que conta com o valor de tempo de vida de um cliente médio conforme definido para cada organização participante.

- Número estimado de clientes existentes: O número estimado de clientes que provavelmente terminarão seu relacionamento como resultado do incidente de violação. A perda incremental é a rotatividade anormal atribuível ao incidente de violação. Este número é uma porcentagem anual, que é baseada em estimativas fornecidas pelo gerenciamento durante o processo de entrevista de referência.[7]

- Aquisição de cliente diminuída: 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 do não cliente, como registros de funcionários, não podem impactar o índice de cancelamento ou rotatividade da organização.[8] Nestes casos, esperaríamos que a categoria de custo de negócios fosse inferior quando as violações de dados não envolvem os dados do cliente ou consumidor (incluindo informações transacionais de pagamento).

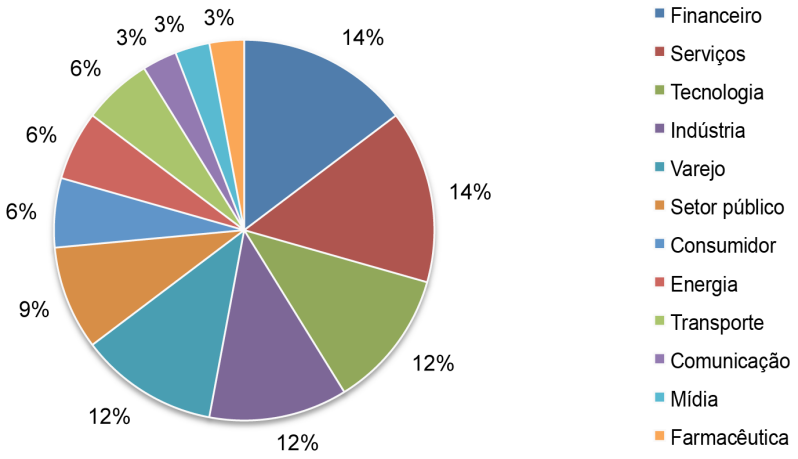
[7]Em várias instâncias, a rotatividade é parcial, em que as vítimas da violação ainda continuavam seu relacionamento com a organização violada, mas o volume da atividade do cliente realmente sofre declínio. Esse declínio parcial é especialmente notável em certos segmentos de mercado, como serviços financeiros ou entidades do setor público, onde a rescisão é onerosa ou economicamente inexequível.

[8]Nesse estudo, consideramos informações do cidadão, paciente e aluno como dados do cliente.

Parte 4. Características organizacionais e métodos de referência

A Figura 16 mostra a distribuição de organizações de referência por sua classificação de segmento de mercado primária. No estudo deste ano, 12 segmentos de mercado são representados. O maior setor são os serviços financeiros, que incluem bancos, seguro, administração de investimento e processadores de pagamento.

Figura 16. Distribuição da amostra de referência por segmento de mercado



Todas as organizações participantes passaram por um ou mais incidentes de violação de dados em algum momento durante o ano passado. Nosso instrumento de referência capturou informações descritivas dos profissionais de TI, conformidade e segurança da informação sobre o impacto total sobre o custo de uma violação que envolve a perda ou furto de informações do cliente ou consumidor. Também foi preciso que esses profissionais estimassem custos de oportunidade associados a atividades do programa.

Os componentes de custo de violação de dados estimados foram capturados em um formulário de classificação. Na maioria dos casos, o pesquisador conduziu entrevistas de acompanhamento para obter fatos adicionais, incluindo taxas de cancelamento anormais estimadas que resultaram do evento de violação mais recente da empresa envolvendo 1.000 ou mais registros comprometidos[99]

Os métodos de coleta de dados não incluíram informações de contabilidade reais, mas em vez disso confiaram na estimativa numérica baseada no conhecimento e experiência de cada participante. Dentro de cada categoria, a estimativa de custo era um processo de dois estágios. Primeiro, o instrumento de referência necessitava que as pessoas classificassem estimativas de custo direto para cada categoria de custo marcando uma variável de intervalo definida no formato de linha de número a seguir.

Como usar a linha de número: A linha de número fornecida em cada categoria de custo de violação de dados é uma forma de obter sua melhor estimativa para a soma de despesas de dinheiro, mão de obra e custos adicionais incorridos. Marque apenas um ponto em algum lugar entre os limites inferiores e superiores configurados acima. É possível reconfigurar os limites inferiores e superiores da linha de número a qualquer momento durante o processo de entrevista.

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

LL	I	UL

[9] Nossos critérios de amostragem apenas incluíam empresas que passaram por uma violação de dados entre 1.000 e 100.000 registros perdidos ou furtados em algum momento durante os últimos 12 meses. Excluímos incidentes de violação de dados catastróficos para evitar o enviesamento de descobertas de amostra geral.

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

Para manter o processo de benchmarking a um tamanho gerenciável, limitamos cuidadosamente os itens apenas para aqueles centros de atividades de custo que consideramos cruciais para a medida de custo de violação de dados. Com base nas discussões com especialistas qualificados, o conjunto final de itens incluía um conjunto fixo de atividades de custo. Mediante a coleta das informações de referência, cada instrumento era reexaminado cuidadosamente para consistência e totalidade.

Para fins de confidencialidade completa, o instrumento de referência não capturou nenhuma informação específica da empresa. Os materiais do assunto não continham códigos de rastreamento ou outros métodos que poderiam vincular resposta a empresas participantes.

O escopo dos itens de custo de violação de dados contidos em nosso instrumento de referência era limitado para categorias de custo conhecidas que se aplicavam a um amplo conjunto de operações de negócios que manipulavam informações pessoais. Acreditamos que um estudo focado no processo de negócios - e não em atividades de conformidade de privacidade ou proteção de dados - resultariam numa melhor qualidade de resultados.

Parte 5. Limitações

Nosso estudo usa um método de referência confidencial e proprietário que foi implementado com sucesso em uma pesquisa anterior. Entretanto, existem limitações inerentes a esta pesquisa de referência que precisam ser consideradas cuidadosamente antes de tirar conclusões das descobertas.

- Resultados não estatísticos: Nosso estudo se baseia em uma amostra representativa e não estatística de entidades baseadas em brasileiros que passam por uma violação envolvendo a perda ou furto de registros do cliente ou consumidor durante os últimos 12 meses. As inferências estatísticas, margens de erro e intervalos de confiança não podem ser aplicados a esses dados que nossos métodos de amostragem não serem científicos.

- Não resposta: As descobertas atuais são baseadas em uma pequena amostra representativa de referências. Trinta e duas empresas concluíram o processo de referência. O viés de não resposta não foi testado, portanto, sempre é possível que as empresas que não participaram sejam substancialmente diferentes em termos de custo de violação de dados subjacentes.

- Viés de quadro de amostragem: Como nosso quadro de amostragem é julgador, a qualidade de resultados é influenciada pelo grau ao qual o quadro é representativo da população de empresas que estão sendo estudadas. Acreditamos que o quadro de amostragem atual seja tendencioso em relação às empresas com uma privacidade mais madura ou com programas de segurança de informações implementados.

- Informações específicas da empresa: As informações de referência são sensíveis e confidenciais.
  Assim, o instrumento atual não captura informações de identificação da empresa. Ele também permite que as pessoas usem variáveis de resposta categórica para divulgar informações demográficas sobre a empresa e categoria do segmento de mercado.

- Fatores não medidos: Para manter o script da entrevista conciso e focado, decidimos omitir outras variáveis importantes de nossas análises, como tendências líderes e características organizacionais. Na medida em que as variáveis omitidas puderem ser explicadas, resultados de referência não podem ser determinadas.

- Resultados de custo extrapolados: A qualidade da pesquisa de referência é baseada na integridade das respostas confidenciais fornecidas pelos participantes em empresas participantes. Embora certas verificações e saldos possam ser incorporados no processo de referência, sempre existe a possibilidade de que os participantes não forneceram respostas precisas ou confiáveis. Além disso, o uso dos métodos de extrapolação de custo em vez dos dados de custo reais pode levar, de maneira inadvertida, as imprecisões.

Se você tiver dúvidas ou comentários sobre este relatório de pesquisa ou se gostaria de obter cópias adicionais do documento (incluindo a permissão para citar ou reutilizar esse relatório), entre em contato por 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 de todos os relatórios do país estão disponíveis em
www.ibm.com/security/data-breach

Ponemon Institute LLC
Antecipando o gerenciamento de informações responsáveis

O Instituto Ponemon é dedicado à pesquisa e educação independentes que antecipa informações responsáveis e práticas de gerenciamento de privacidade no negócio e no governo. Nossa missão é conduzir a alta qualidade, os estudos empíricos sobre problemas críticos que afetam o gerenciamento e a segurança de informações sensíveis sobre pessoas e organizações.

Como um membro do **Council of American Survey Research Organizations (CASRO),** conservamos a confidencialidade de dados estrita, privacidade e padrões de pesquisa éticos. Não coletamos informações de identificação pessoal de pessoas (ou informações de identificação de empresas em nossa pesquisa de negócios). Além disso, temos padrões de qualidade estritos para assegurar que as pessoas não recebam perguntas estranhas, irrelevantes ou impróprias.