Estudo sobre o Custo da Violação de Dados de 2015:

Impacto do Gerenciamento da Continuidade de Negócios

Pesquisa de referência patrocinada pela IBM
e conduzida de forma independente pelo Ponemon Institute LLC
em junho de 2015

Relatório de Pesquisa do Ponemon Institute©

2015[1]:
Impacto do Gerenciamentoda Continuidade de Negócios

Ponemon Institute, junho de 2015

Parte 1. Introdução

O *Estudo sobre o Custo da Violação de Dados de 2015 é um estudo global,* patrocinado pela IBM,que quantifica o impacto econômico das violações de dados e observa tendências de custo ao longo do tempo. Acreditamos que um melhor entendimento do custo, das causas principais e dos fatores que influenciam o custo ajudará as organizações na determinação da quantia apropriada de investimento e dos recursos necessários para evitar ou minimizar as consequências de um ataque.

O custo médio per capita da violação de dados varia bastante entre os países. Muitas dessas diferenças de custo podem ser atribuídas aos tipos de ataques e ameaças enfrentados pelas organizações, bem como aos regulamentos e às leis de proteção de dados em seus respectivos países. No estudo global deste ano, o custo médio per capita da violação de dados aumentou de 145 para 154 dólares. O custo total de uma violação de dados aumentou de 3,5 para 3,8 milhões de dólares.[2]

O estudo desse ano envolveu 350 empresas em 16 segmentos de mercado, representando os países a seguir: Estados Unidos, Reino Unido, Alemanha, Austrália, França, Brasil, Japão, Itália, Índia, região Árabe e, pela primeira vez, Canadá. Todas as organizações participantes passaram por uma violação de dados, variando de uma violação pequena de aproximadamente 3.000 até aproximadamente 100.000 registros comprometidos[3]. Definimos um registro comprometido como um que identifica o indivíduo cujas informações foram perdidas ou roubadas em uma violação de dados.

Uma conclusão importante desta pesquisa anual é um melhor entendimento dos fatores que podem minimizar as consequências financeiras de uma violação de dados. Este relatório especial analisa o impacto positivo que um programa de gerenciamento de continuidade de negócios (*Business Continuity Management* - BCM) pode ter sobre as consequências financeiras e de reputação de uma violação de dados.[4]

O Impacto dos Programas de Gestão de Continuidade de Negócios no Custo de uma Violação de Dados

- 9% de redução no custo per capita da violação de dados
- 27% de redução no tempo médio para identificar uma violação de dados
- 41% de redução no tempo médio para conter uma violação de dados
- 28% de diminuição na probabilidade de uma violação de dados nos próximos 2 anos

Muitas empresas possuem uma função ou equipe de BCM que está envolvida na gestão de risco, recuperação de desastre e gestão de crise corporativas. Cerca de 50 por cento das empresas neste estudo agora estão envolvendo especialistas de BCM quando elas passam por uma violação de dados. Como resultado de ter esses especialistas e processos de BCM estabelecidos, a resolução da violação de dados é mais eficiente e menos cara.

[1]Este relatório é datado com o ano de publicação e não com a data de conclusão do trabalho de campo. Observe que a maioria dos incidentes de violação de dados estudados no relatório atual aconteceram no ano calendário de 2014.
[2]As moedas locais foram convertidas para dólares americanos.
[3]Os termos "custo por registro comprometido" e "custo per capita" têm significado equivalente neste relatório.
[4]As equipes de BCM que oferecem suporte ao processo de resposta a incidentes incluem profissionais na função de recuperação de desastres.

Conclusões importantes sobre a importância da BCM na redução das consequências de uma violação de dados:

- **O custo da violação de dados é linearmente proporcional ao tempo médio necessário para identificação e o tempo médio para contenção do incidente de violação de dados.** Nossas descobertas sugerem que o envolvimento de BCM resulta em um tempo médio significativamente menor para identificação e contenção do incidente de violação de dados. Especialmente, as empresas sem envolvimento de BCM experimentaram uma média de 234 dias para identificar a violação. Em comparação, as empresas com envolvimento de BCM experimentaram uma média de 178 dias para identificar a violação. De maneira semelhante, aquelas sem envolvimento de BCM experimentaram uma média de 83 dias para contenção versus 55 dias para contenção da violação para aquelas com envolvimento da BCM.

- **O envolvimento de BCM no planejamento e na execução da resposta ao incidente de violação de dados é muito significativo**. Das 350 empresas participantes deste estudo global, 174 relataram que possuem envolvimento de BCM na resolução das consequências de uma violação de dados. A maioria dessas empresas (63 por cento) avalia o envolvimento da BCM como muito significativo.

- **O custo da violação de dados é mais elevado se o BCM não faz parte do planejamento e da execução da resposta a incidentes de violação de dados**. O custo médio por registro perdido ou roubado pode ser superior a 161 dólares. Com o envolvimento de BCM, o custo médio pode ser tão baixo quanto 147 dólares.

- **A probabilidade de ter uma violação de dados no futuro é maior para empresas que não envolvem o BCM como parte de seu planejamento de resposta a incidentes**. As descobertas revelam que se o BCM não está envolvida no planejamento de violação de dados, a probabilidade de ter uma violação de dados em algum momento nos próximos 2 anos é de 27,9 por cento. Ao passo que, se há BCM envolvido, essa probabilidade cai para 21,1 por cento.

- **A Alemanha e o Japão possuem a maior porcentagem de empresas que envolvem as equipes de BCM de suas empresas para ajudar no planejamento e na execução da resposta a incidentes de violação de dados.** Os países com o menor envolvimento de BCM são o Brasil e a região Árabe. Com a exceção da Itália, todos os países aumentaram o nível de envolvimento de BCM no processo de gestão de incidentes de violação de dados.

- **O BCM minimiza interrupções nas operações de negócios quando ocorre uma violação de dados**. De acordo com as descobertas, 80 por cento das empresas sem envolvimento de BCM tiveram uma interrupção relevante nas operações de negócios. Isto diminui para 55 por cento para empresas envolvendo o BCM.

- **O envolvimento de BCM melhora a resiliência das operações de TI**. 74 por cento das empresas sem envolvimento de BCM disseram que tiveram uma interrupção relevante em suas operações de TI. Isso diminui para 52 por cento daquelas com envolvimento de BCM que disseram que as operações de TI foram interrompidas de maneira relevante.

- **O BCM pode proteger a reputação de uma empresa após uma violação de dados**. Menos da metade das empresas nesta pesquisa com envolvimento de BCM (45 por cento) disseram que sua reputação ou marca foi negativamente impactada devido a uma violação de dados. No entanto, 55 por cento das empresas sem envolvimento de BCM disseram que a marca e a reputação de sua organização foram afetadas.

Parte 2. Principais Descobertas

A tabela a seguir lista 11 países, legenda, tamanhos de amostra e moedas usados neste estudo global. Ela também mostra o número de anos do relatório anual para cada país, variando de um ano para o Canadá a 10 anos para os Estados Unidos.

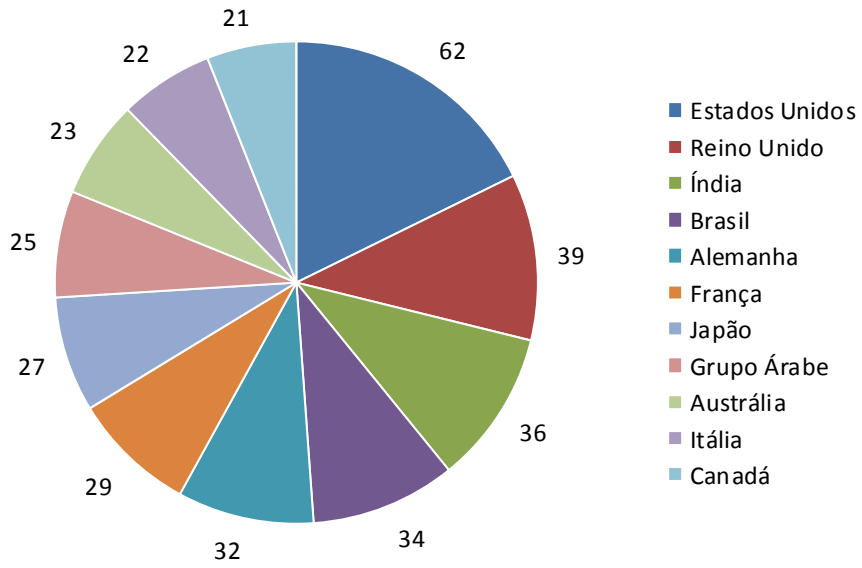
Tabela 1. Estudo Global em Resumo

Legenda	Países	Amos	Porcentagem	Moeda	Anos de
AB	Grupo Árabe*	25	7%	Dirham do	2
AU	Austrália	23	7%	Dólar	6
BZ	Brasil	34	10%	Real	3
CA	Canadá	21	6%	Dólar	1
DE	Alemanha	32	9%	Euro	7
FR	França	29	8%	Euro	6
ID	Índia	36	10%	Rúpia	4
IT	Itália	22	6%	Euro	4
JP	Japão	27	8%	Iene	4
UK	Reino Unido	39	11%	Libra	8
US	Estados Unidos	62	18%	Dólar	10
	Total	350	100%		

*AB é uma amostra combinada das empresas localizadas na Arábia Saudita e nos Emirados Árabes Unidos

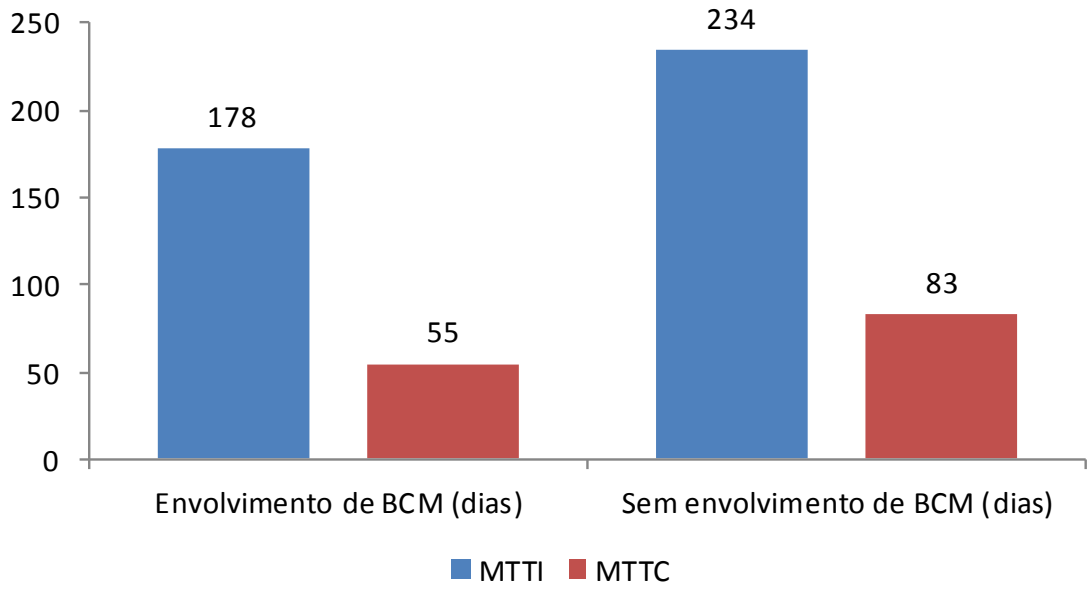
O gráfico a seguir mostra a distribuição das 350 organizações participantes em 11 países. Como pode ser visto, os EUA representam o maior segmento com 62 organizações e o Canadá a menor amostra com 21 organizações.

Gráfico de Setores 1. Frequência das amostras de referência por país
Visão consolidada (n = 350)



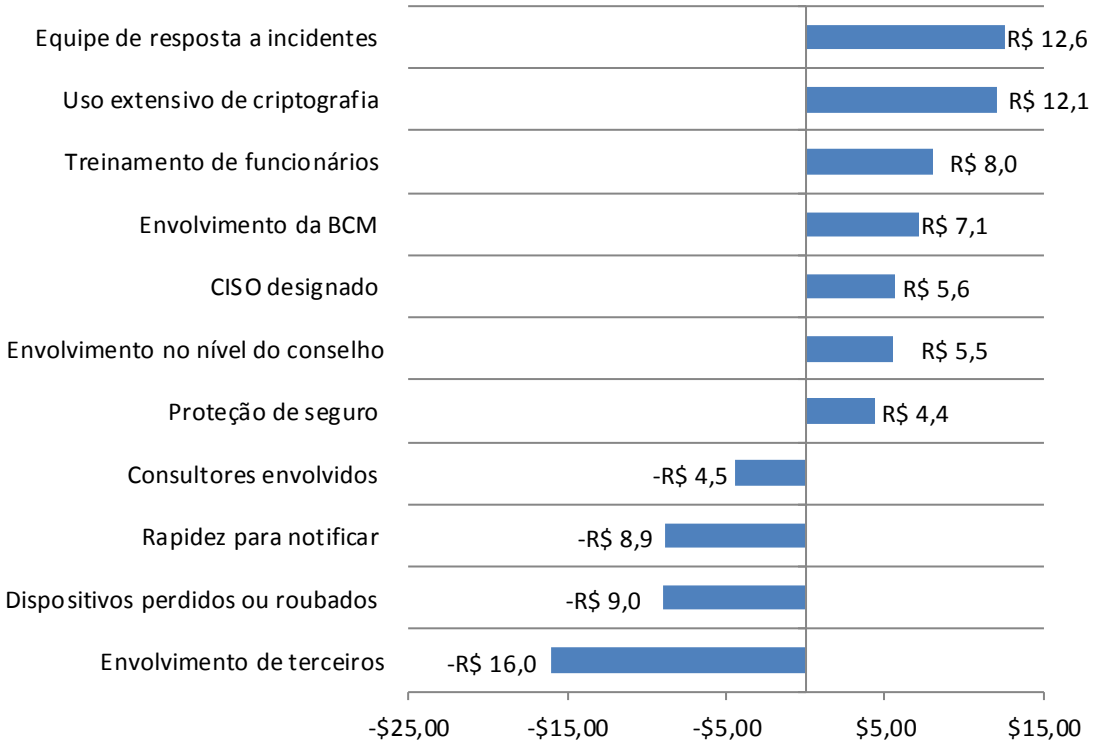
O custo da violação de dados está linearmente relacionado ao tempo médio necessário para identificar e ao tempo médio para conter o incidente de violação de dados. No estudo desse ano, mostramos que o tempo médio para identificação (MTTI) e o tempo médio para contenção (MTTC) da violação de dados estavam linearmente relacionados aos custos da violação de dados. A Figura 1 mostra uma outra inter-relação interessante. Ou seja, tanto o número de dias para identificação quanto o número de dias para contenção do incidente de violação de dados são substancialmente menores para as organizações que envolveram o BCM. A diferença percentual no MTTI e no MTTC é de 27 por cento e 41 por cento, respectivamente.

Figura 1. MTTI e MTTC para organizações que envolvem ou não envolvem o BCM no processo de resposta a incidentes
Diferença percentual para MTTI = 27%; diferença percentual para MTTC = 41%
Visão consolidada (Ano fiscal de 2015 = 350, Ano fiscal de 2014 = 315)



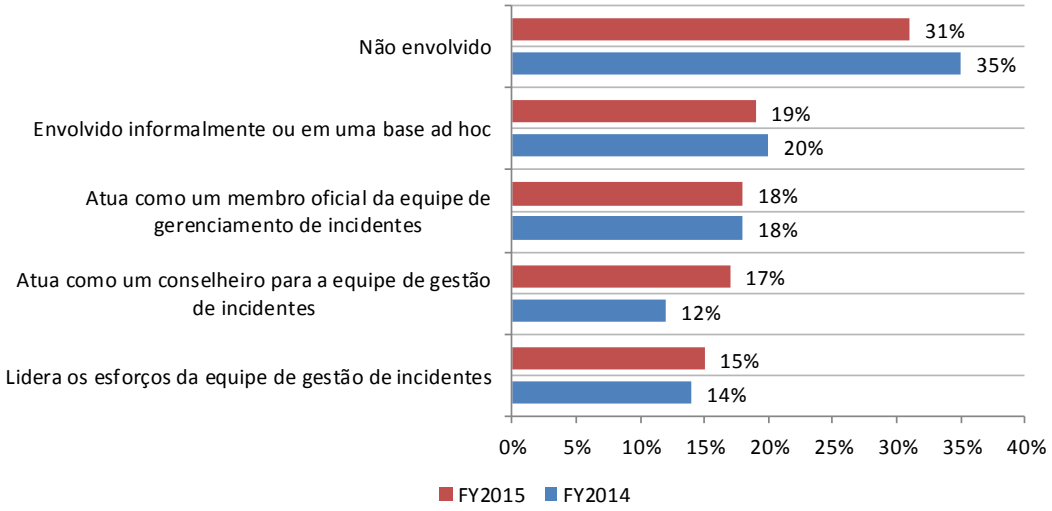
Fatores que influenciam o custo da violação de dados. No contexto desta análise, números positivos são economias de custo incrementais e números negativos são aumentos de custo incrementais definidos para cada um dos 11 fatores. Conforme mostrado na Figura 2, a existência de uma equipe competente de resposta a incidentes resulta em uma grande diminuição do custo per capita da violação de dados. A gestão de continuidade de negócios diminui o custo da violação de dados em uma média de 7,1 dólares por registro comprometido.

Figura 2. Impacto dos 11 fatores no custo per capita da violação de dados
Medidos na visão consolidada em US$ (n = 350)



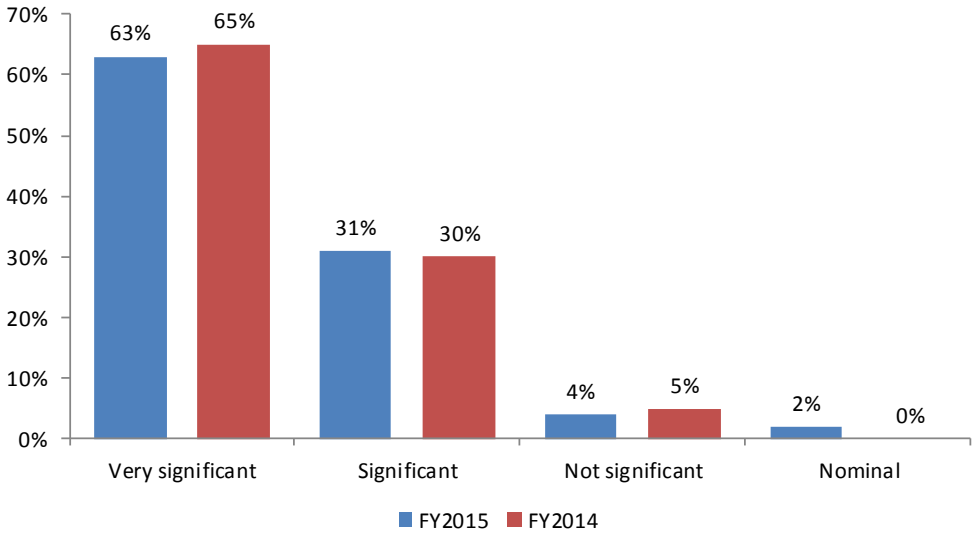
Contribuição de BCM para o planejamento da resposta a incidentes. A Figura 3 fornece um resumo do envolvimento do BCM no planejamento e na execução da resposta a incidentes de violação de dados. Das 350 empresas neste estudo global, 174 ou 50 por cento tiveram envolvimento de BCM. As 176 empresas restantes não envolveram sua equipe de BCM ou envolveram o BCM apenas em uma base ad hoc. A análise do último ano mostrou que 45 por cento das empresas envolveram o BCM na resposta a incidentes de violação de dados.

Figura 3. Como o BCM contribui com o processo de resposta a incidentes de violação de dados?
Visão consolidada (Ano fiscal de 2015 = 350, Ano fiscal de 2014 = 315)



A Figura 4 mostra o nível de envolvimento do BCM no planejamento e na execução da resposta a incidentes. Para o estudo deste ano, 63 por cento das empresas avaliam esse envolvimento como muito significativo. Outros 31 por cento avaliam o envolvimento deBCM como significativo. O estudo do último ano mostrou uma avaliação de 65 e 30 por cento do envolvimento de BCM como muito significativo ou significativo, respectivamente.

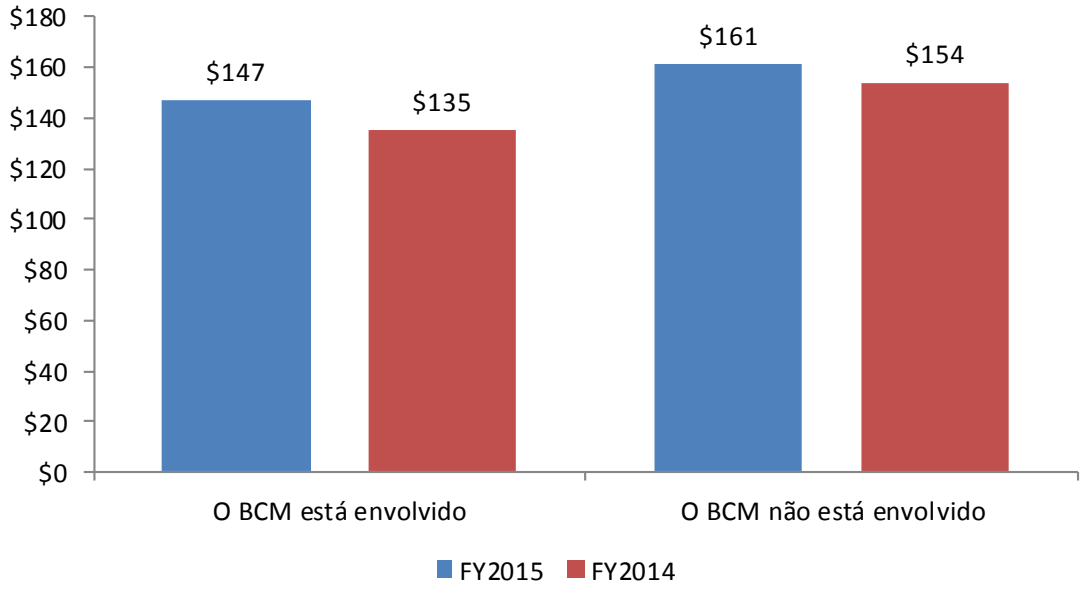
Figura 4. O que melhor descreve a contribuição do BCM com o processo de resposta a incidentes?
Visão consolidada (Ano fiscal de 2015 = 350, Ano fiscal de 2014 = 315)



O BCM reduz o custo per capita da violação de dados. A Figura 5 apresenta o custo médio per capita da violação de dados para as empresas que envolvem a equipe de BCM no planejamento e na execução da resposta a incidentes e aquelas que não envolvem, ao longo de dois anos. Tais empresas que envolvem o BCM experimentam um custo per capita inferior ao daquelas que não envolvem . Este ano, a diferença percentual no custo per capita da violação de dados entre empresas que envolvem e não envolvem o BCM é de 9 por cento. A diferença percentual no último ano foi de 13 por cento.

Figura 5. Custo per capita da violação de dados para empresas com ou sem envolvimento do BCM

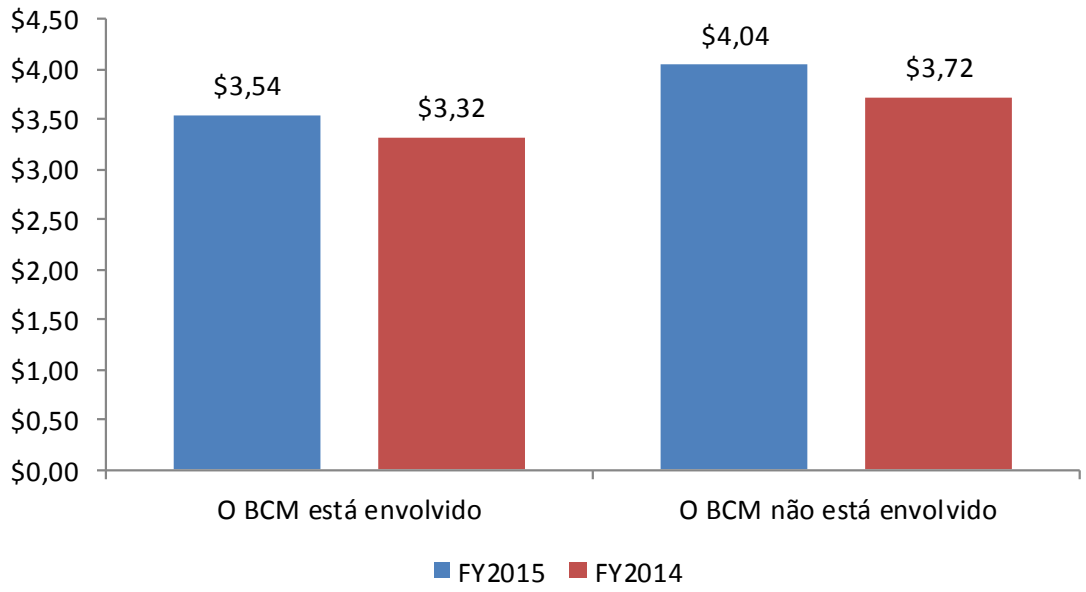
diferença percentual no ano fiscal de 2015 = 9%; diferença percentual no ano fiscal de 2014 = 13%
Visão consolidada (Ano fiscal de 2015 = 350, Ano fiscal de 2014 = 315)



A Figura 6 apresenta o custo total da violação de dados para as empresas que envolvem a equipe de BCM no planejamento e na execução da resposta a incidentes e aquelas que não o fazem ao longo de dois anos. Semelhante ao mostrado acima, essas empresas que envolvem o BCM experimentam um custo total mais baixo do que aqueles que não envolvem o BCM. A diferença percentual no custo total entre as empresas que envolvem e não envolvem o BCM é de 13 por cento. No último ano, esta diferença percentual foi de 11 por cento.

Figura 6. Custo per capita da violação de dados para empresas com ou sem envolvimento de BCM

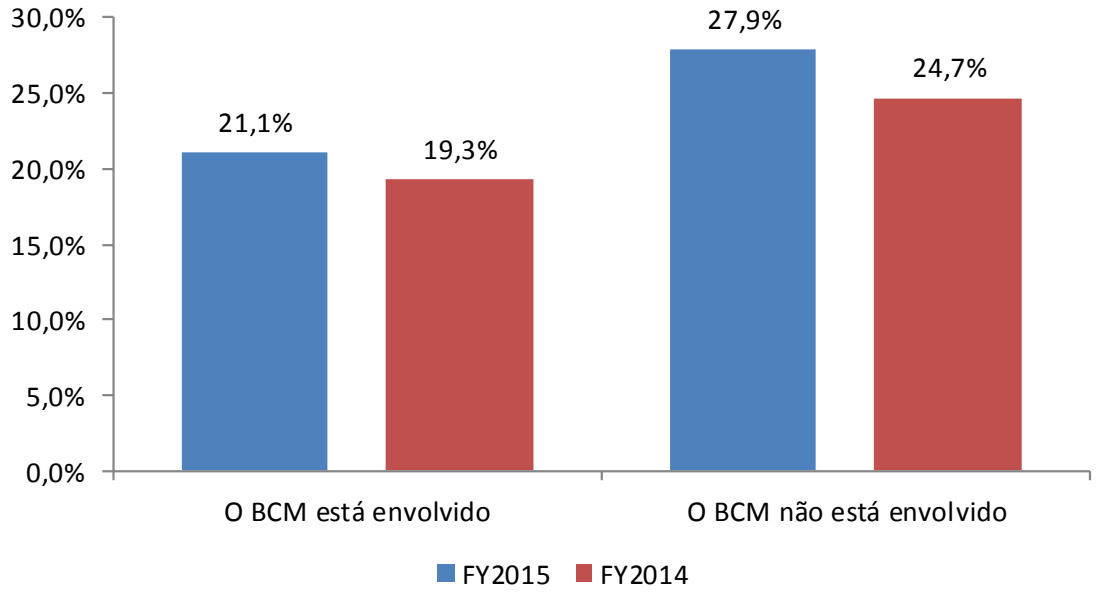
Diferença percentual no ano fiscal de 2015 = 13%; diferença percentual no ano fiscal de 2014 = 11%
Visão consolidada (Ano fiscal de 2015 = 350, Ano fiscal de 2014 = 315)
(Milhões)



O BCM reduz a probabilidade de uma violação de dados. A Figura 7 apresenta a probabilidade média de violação de dados envolvendo um mínimo de 10.000 ou mais registros ao longo dos próximos 24 meses para empresas que envolvem a equipe de BCM e aquelas que não envolvem.

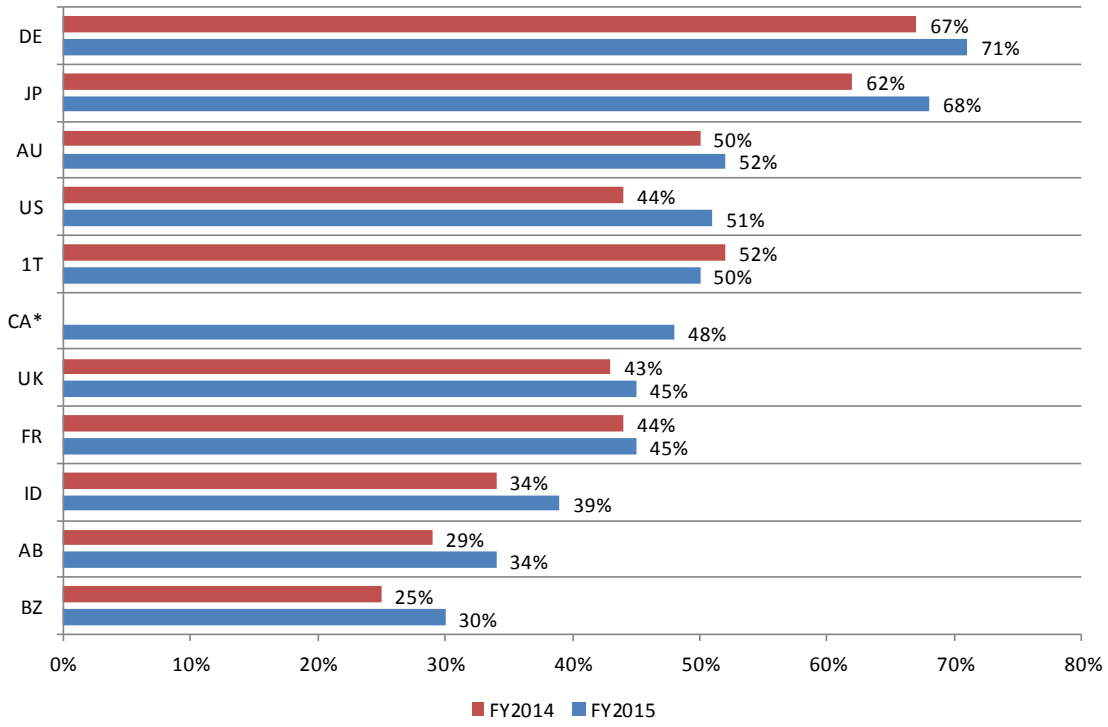
Claramente, as organizações que envolvem o BCM experimentam uma menor probabilidade de incorrência do que aquelas que não envolvem oBCM. Este padrão se aplica tanto aos resultados de 2014 quanto aos de 2015. Especificamente, a diferença percentual na probabilidade de uma futura violação de dados entre as empresas que envolvem e não envolvem o BCM é de 28 por cento neste ano. No último ano, a diferença percentual foi de 25 por cento.

Figura 7. Probabilidade de uma violação de dados importante para empresas com ou sem envolvimento do BCM
Diferença percentual no ano fiscal de 2015 = 28%; diferença percentual no ano fiscal de 2014 = 25%
Visão consolidada (Ano fiscal de 2015 = 350, Ano fiscal de 2014 = 315)



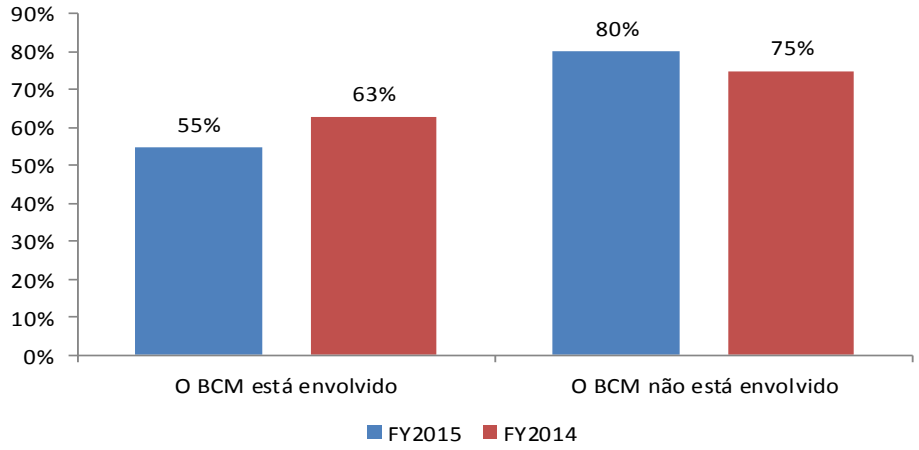
Alemanha e Japão têm maior probabilidade de envolver BCMs ao lidar com violações de dados.
A Figura 8 mostra o percentual de envolvimento da equipe de BCM no planejamento e na execução de incidentes para amostras de 11 países. Semelhante ao último ano, a Alemanha (DE) tem a mais alta taxa de envolvimento de BCM com 71 por cento das empresas alemãs relatando que possuem uma equipe de BCM. Em contraste, apenas 30 por cento das empresas do Brasil (BZ) possuem envolvimento de BCM. É interessante notar que com uma exceção (a Itália), todos os países experimentaram um aumento líquido no envolvimento de BCM no decorrer do último ano.

Figura 8. Taxa de participação de BCM por amostra de país
*Dados históricos não estão disponíveis
(ano fiscal de 2015 = 350, ano fiscal de 2014 = 315)



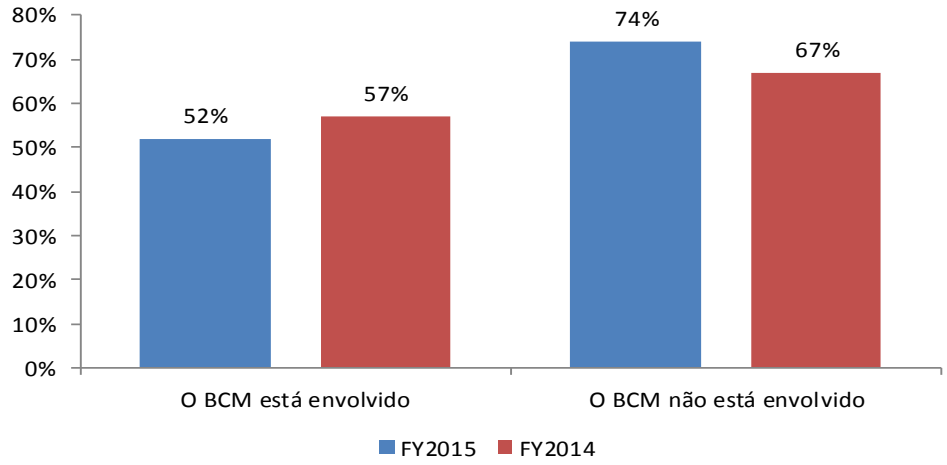
O BCM minimiza interrupções nas operações de negócios quando ocorre uma violação de dados. A Figura 9 revela diferenças entre empresas com ou sem envolvimento de BCM com relação a interrupções importantes nos processos de negócios. Conforme relatado para o ano fiscal de 2015, 80 por cento das empresas sem envolvimento de BCM disseram que o incidente de violação de dados causou uma interrupção relevante nos processos de negócios. No entanto, 55 por cento das empresas com envolvimento de BCM tiveram uma interrupção relevante. Um padrão semelhante é aplicável aos resultados do ano fiscal de 2014.

Figura 9. O incidente de violação de dados causou uma interrupção relevante nos processos de negócios?
Visão consolidada (Ano fiscal de 2015 = 350, Ano fiscal de 2014 = 315)



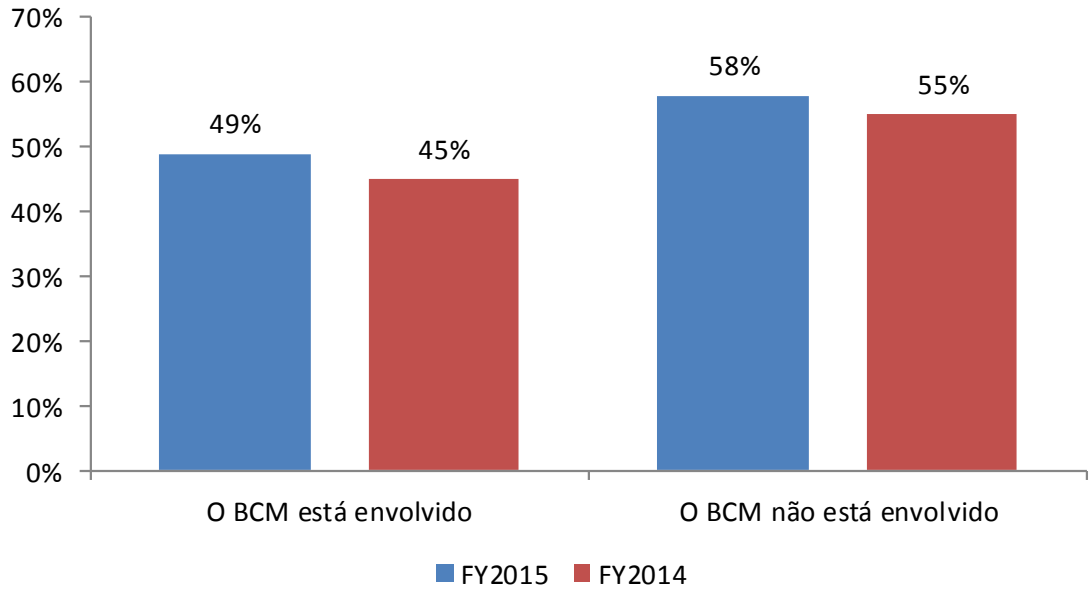
O envolvimento de BCM melhora a resiliência das operações de TI. Semelhante ao mostrado acima, a Figura 10 mostra diferenças entre empresas com ou sem envolvimento de BCM com relação a interrupções importantes nas operações de TI. Conforme relatado para o ano fiscal de 2015, 74 por cento das empresas sem envolvimento de BCM disseram que o incidente de violação de dados causou uma interrupção relevante nas operações de TI. Em contraste, 52 por cento das empresas com envolvimento de BCM disseram que o incidente causou uma interrupção relevante. Um padrão semelhante é aplicável aos resultados do ano fiscal de 2014.

Figura 10. O incidente de violação de dados causou uma interrupção relevante nas operações de TI?
Visão consolidada (Ano fiscal de 2015 = 350, Ano fiscal de 2014 = 315)



O BCM pode proteger a reputação de uma empresa após uma violação de dados. A Figura 10 também mostra diferenças entre empresas que envolvem o BCM versus aquelas que não envolvem. No estudo deste ano, 55 por cento das empresas que não envolvem o BCM disseram que a violação de dados teve um impacto negativo importante sobre a reputação e a marca. Em contraste, 45 por cento das empresas que envolvem o BCM disseram que o incidente teve um impacto negativo na reputação ou marca da organização. Um padrão semelhante é aplicável aos resultados do ano fiscal de 2014.

Figura 10. A violação de dados teve um impacto negativo importante na reputação da organização?
Visão consolidada (Ano fiscal de 2015 = 350, Ano fiscal de 2014 = 315)



Parte 3. Como calculamos o custo da violação de dados

Para calcular o custo da violação de dados, usamos uma metodologia de custo denominada custo baseado em atividade (ABC). Esta metodologia identifica atividades e atribui um custo de acordo com o uso real. As empresas participando desta pesquisa de referência são solicitadas a estimar o custo de todas as atividades realizadas para resolver a violação de dados.

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

- Condução de investigação e análise forense para determinar a causa raiz da violação de dados
- Determinação das prováveis vítimas da violação de dados
- Organização da equipe de resposta a incidentes
- Condução de comunicação e divulgação de relações públicas
- Preparação de documentos de aviso e outras divulgações exigidas para as vítimas da violação de dados e os reguladores
- Implementação de procedimentos de call center e treinamento especializado

A seguir estão atividades típicas conduzidas após a descoberta da violação de dados:

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

Uma vez que a empresa estima uma variação de custos para essas atividades, categorizamos os custos como diretos, indiretos e de oportunidade, conforme definido abaixo:

- *Custo direto* - o gasto direto de despesas para realizar uma determinada atividade.
- *Custo indireto* - a quantidade de tempo, esforço e outros recursos organizacionais gastos, mas não como um gasto direto de dinheiro.
- *Custo de oportunidade* - o custo resultante da perda de oportunidades de negócios como uma consequência dos efeitos negativos de reputação após a violação ter sido relatada para as vítimas (e revelada publicamente nos meios de comunicação).

Nosso estudo também analisa as principais atividades relacionadas com o processo que impulsionam uma variedade de despesas associadas com a detecção, resposta, contenção e correção da violação de dados de uma organização. Os custos para cada atividade são apresentados na seção Principais Descobertas (Parte 2). Os quatro centros de custo são:

- Detecção ou descoberta: atividades que permitem que uma empresa detecte razoavelmente a violação de dados pessoais tanto em risco (em armazenamento) como em andamento.
- Procedimentos para escalar: atividades necessárias para relatar a violação de informações protegidas para o pessoal apropriado dentro de um período de tempo especificado.
- Notificação: atividades que permitem que a empresa notifique os assuntos de dados com uma carta, telefonema de saída, e-mail ou aviso geral de que informações pessoais foram perdidas ou roubadas.
- Pós-violação de dados: atividades para ajudar as vítimas de uma violação a se comunicarem com a empresa para fazer perguntas adicionais ou obter recomendações para minimizar os possíveis danos. As atividades pós-violação de dados também incluem o monitoramento de relatórios de crédito ou nova emissão de uma nova conta (ou cartão de crédito).

Além das atividades relacionadas ao processo acima, a maioria das empresas experimentam custos de oportunidade associados ao incidente de violação, o que resulta da diminuição de confiança por parte dos clientes atuais e futuros. Consequentemente, a pesquisa de nosso Instituto mostra que a publicidade negativa associada a um incidente de violação de dados causa efeitos de reputação que podem resultar em taxas anormais de rotatividade ou perda, bem como em uma diminuição na taxa de aquisição de novos clientes.

Para extrapolar esses custos de oportunidade, nós usamos um método de estimativa de custo que depende do "valor de vida útil" de um cliente médio, conforme definido para cada organização participante.

- Rotatividade dos clientes existentes: o número estimado de clientes que provavelmente irão encerrar seu relacionamento como resultado do incidente de violação. A perda incremental é a rotatividade anormal atribuível ao incidente de violação. Este número é um percentual anual, que é baseado nas estimativas fornecidas pela administração durante o processo de entrevista da referência.[5]
- Diminuição na aquisição de clientes: o número estimado de clientes-alvo que não terão um relacionamento com a organização como uma consequência da violação. Este número é fornecido como um percentual anual.

Reconhecemos que a perda de dados que não são do cliente, tais como registros de funcionários, podem não causar impacto[6] na perda ou na rotatividade de uma organização. Nestes casos, podemos esperar a categoria de custos do negócio sendo menor quando violações de dados não envolvem dados de clientes ou consumidores (incluindo informações de transações de pagamento em andamento).

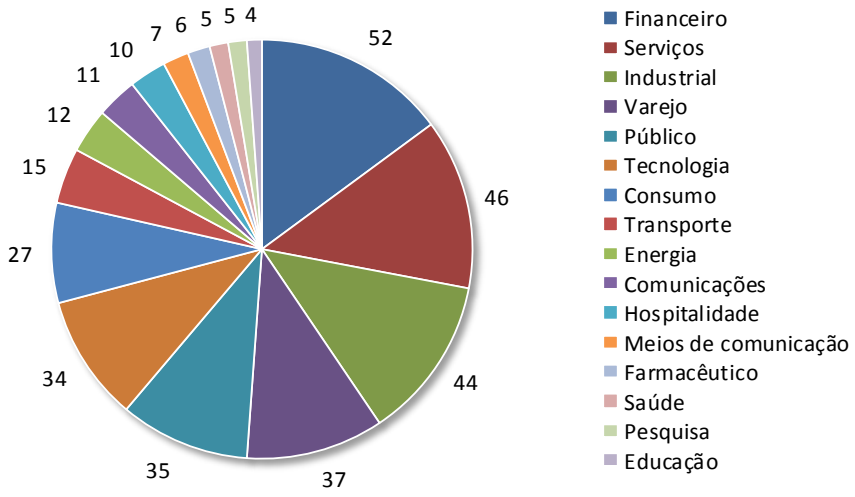
[5]Em vários casos, a rotatividade é parcial, em que as vítimas da violação continuam seu relacionamento com a organização violada, mas o volume de atividades do cliente realmente diminui. Esta diminuição parcial é especialmente notável em determinados segmentos de mercado - tais como serviços financeiros ou entidades do setor público - nos quais o encerramento é dispendioso ou economicamente inviável.

[6]Neste estudo, consideramos informações de cidadãos, pacientes e alunos como dados do cliente..

Parte 4. Características organizacionais e métodos de referência

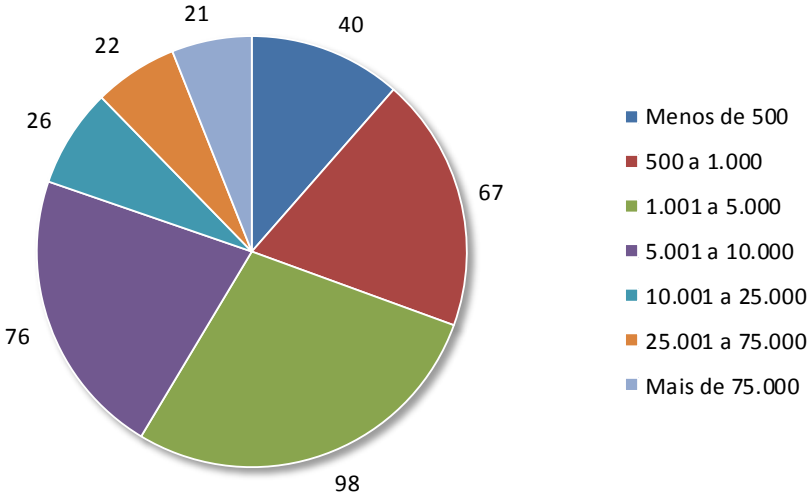
O Gráfico de Setores 2 mostra a distribuição das organizações de referência por sua classificação primária de segmento de mercado. No estudo deste ano, são representados 16 segmentos de mercado. O maior setor é o de serviços financeiros, que inclui bancos, processadores de seguros, gestão de investimentos e pagamentos.

Gráfico de setores 2. Distribuição de amostras de referência por segmento de mercado
Visão consolidada (n = 350)



O Gráfico de Setores 3 mostra a distribuição das organizações de referência por número total de pessoas. Os maiores segmentos incluem empresas com mais de 1.000 funcionários.

Gráfico de Setores 3. Número global de pessoas das empresas participantes
Visão consolidada (n = 350)



Os métodos de coleta de dados não incluíram informações contábeis reais, mas sim contaram com estimativas numéricas baseadas no conhecimento e na experiência de cada participante. Dentro de cada categoria, a estimativa de custo foi composta por um processo com dois estágios. Em primeiro lugar, o instrumento de referência solicitou que os indivíduos avaliassem as estimativas de custos diretos para cada categoria de custos ao marcar um intervalo variável definido no formato de linha de números a seguir.

Como usar a linha de números: A linha de números fornecida sob cada categoria de custo da violação de dados é uma maneira de obter a sua melhor estimativa para a soma dos gastos em dinheiro, da mão de obra e das despesas gerais incorridas. Marque apenas um ponto em algum lugar entre os limites inferior e superior definidos acima. Você pode redefinir os limites inferior e superior da linha números a qualquer momento durante o processo de entrevista.

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

LI		LS

O valor obtido 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 os custos indiretos e de oportunidade, separadamente.

Para manter o processo de benchmarking gerenciável, nós limitamos cuidadosamente os itens apenas aos centros de atividade de custo que consideramos cruciais para a avaliação dos custos da violação de dados. Com base em discussões com especialistas experientes, o conjunto final de itens incluiu um conjunto fixo de atividades de custo. Após a coleta das informações de referência, cada instrumento foi reexaminado cuidadosamente para garantir consistência e totalidade.

Com o propósito de garantir confidencialidade total, o instrumento de referência não capturou qualquer informação específica da empresa. Os materiais sujeitos não continham códigos de rastreamento ou outros métodos que poderiam vincular 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 custos conhecidas que se aplicavam a um amplo conjunto de operações de negócios que manipulam informações pessoais. Acreditamos que um estudo com foco nos processos de negócios - e não em atividades de proteção de dados ou de conformidade de privacidade - renderia resultados com melhor qualidade

Parte 5. Limitações

Nosso estudo utiliza um método de referência confidencial e com direitos de propriedade que foi implementado
com sucesso em uma pesquisa anterior. No entanto, há limitações inerentes à esta pesquisa de referência
que precisam ser cuidadosamente consideradas ao tirar conclusões das descobertas.

- Resultados não estatísticos: nosso estudo é baseado em uma amostra representativa e não estatística de entidades globais experimentando uma violação envolvendo a perda ou o roubo de registros do cliente ou consumidor nos últimos 12 meses. Inferências estatísticas, margens de erro e intervalos de confiança não podem ser aplicados a estes dados já que nossos métodos de amostragem não são científicos.

- Não resposta: as descobertas atuais são baseadas em uma pequena amostra representativa das referências. Neste estudo global, 350 empresas concluíram o processo de referência. O viés de não resposta não foi testado, portanto, é sempre possível que as empresas que não participaram sejam substancialmente diferentes em termos de custo de violação de dados subjacente.

- Viés da estrutura de amostra: como a nossa estrutura de amostragem está relacionada a julgamento, a qualidade dos resultados é influenciada pelo grau em que a estrutura é representativa da população de empresas sendo estudadas. Acreditamos que a estrutura de amostragem atual está inclinada na direção de empresas com programas de privacidade ou segurança de informações com mais maturidade.

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

- Fatores não avaliados: para manter o roteiro da entrevista conciso e focado, decidimos omitir outras variáveis importantes de nossas análises, tais como principais tendências e características organizacionais. A medida em que as variáveis omitidas podem explicar os resultados de referência não pode ser determinada.

- Resultados de custo extrapolados: a qualidade da pesquisa de referência é baseada na integridade das respostas confidenciais fornecidas pelos entrevistados nas empresas participantes. Embora alguns pontos e contrapesos possam ser incorporadas no processo de referência, sempre há a possibilidade de que os entrevistados não tenham fornecido respostas precisas ou verdadeiras. Além disso, o uso de métodos de extrapolação de custos em vez de dados de custos reais pode, inadvertidamente, introduzir inclinações e imprecisões.

Se você tiver dúvidas ou comentários sobre este relatório de pesquisa ou gostaria de obter cópias adicionais do documento (incluindo permissão para citar ou reutilizar este relatório), entre em contato por carta, telefonema ou e-mail:

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 estão disponíveis em
www.ibm.com/security/data-breach

Ponemon Institute

Promovendo a Gestão Responsável de Informações

O Ponemon Institute é dedicado à investigação e educação que promovem práticas responsáveis de gestão de informações e privacidade dentro de empresas e do governo. Nossa missão é conduzir estudos empíricos e de alta qualidade sobre problemas críticos que afetam a gestão e a segurança de informações sensíveis sobre pessoas e organizações.

Como um membro do **Council of American Survey Research Organizations (CASRO),** nós defendemos padrões éticos restritos de confidencialidade de dados, privacidade e pesquisa. Nós não coletamos qualquer informação pessoalmente identificável de indivíduos (ou informações que podem identificar a empresa em nossa pesquisa de negócios). Além disso, temos padrões de qualidade rigorosos para garantir que não sejam feitas perguntas estranhas, irrelevantes ou impróprias aos entrevistados.