Relatório Global de Impacto Cibernético 2015

Patrocinado por Aon Risk Solutions

Realizado de forma independente por Ponemon Institute LLC Data de publicação Abril de 2015

Relatório Global de Impacto Cibernético 2015

Ponemon Institute, abril de 2015

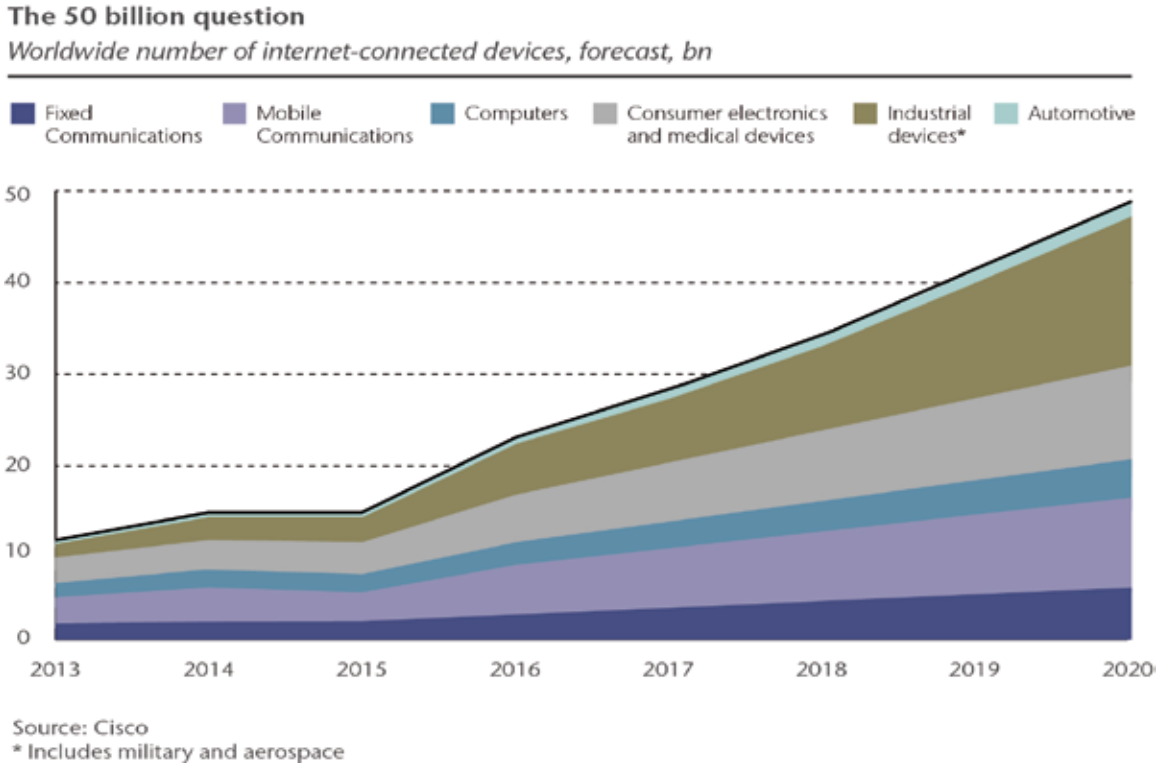
Parte 1. Introdução

O Ponemon Institute tem o prazer de apresentar o Relatório Global de Impacto Cibernético 2015, patrocinado por Aon Risk Services. O objetivo da pesquisa é compreender como as empresas qualificam e quantificam o risco financeiro sofrido por seus ativos tangíveis e intangíveis em caso de incidente de segurança ou privacidade de rede.

As economias passam por uma transformação rápida e aguda, passando historicamente de produtos tangíveis e serviços de trabalho manual para a dependência de ativos de tecnologia e informação. Computação em nuvem, dispositivos móveis, mídias sociais, análises de "big data" e a explosão da "internet das coisas" são parte dessa transformação digital. A figura 1 mostra a projeção do crescimento do uso de dispositivos conectados à internet, que deve atingir 50 bilhões de dispositivos em 2020. Ou seja, apenas cinco anos.

Figura 1. O maravilhoso mundo dos dispositivos conectados à internet

Previsão do número de dispositivos conectados à internet no mundo todo, em bilhões



Como as empresas qualificam e quantificam o impacto dessa exposição sobre suas demonstrações financeiras? Nossa meta é comparar o impacto sobre as demonstrações financeiras de exposições a riscos à propriedade e à rede. Uma melhor compreensão do impacto relativo sobre as demonstrações financeiras ajudará as empresas a alocar recursos e definir a quantidade adequada de recursos de transferência de risco (seguro) para mitigar o impacto causado por exposições a riscos à rede.

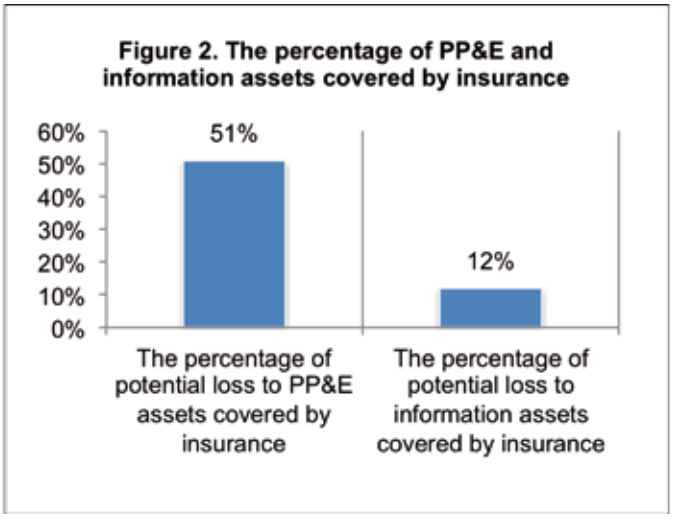
As exposições a riscos à rede podem incluir, de forma geral, violações da privacidade e segurança de informações pessoalmente verificáveis, roubo de propriedade intelectual da empresa, confisco de contas bancárias online, desenvolvimento e disseminação de vírus de computador, publicação de informações comerciais

confidenciais na internet, avarias robóticas e transtornos na infraestrutura crítica de um país.[1]

A pesquisa envolveu 2.243 participantes de 37 países das seguintes regiões: América do Norte, Europa, Oriente Médio e África ("EMEA"), Ásia, Pacífico, Japão ("APJ") e América Latina ("LATAM").2 Os participantes tinham envolvimento nas atividades de gestão de risco cibernético das suas respectivas empresas, bem como atividades de gestão de risco empresarial.

A maior parte dos participantes é ou da área de finanças, tesouraria e contabilidade (37%) ou de gestão de riscos (17%). Outros participantes trabalham em conformidade corporativa/ auditoria (14%) e gerência geral (14%).

Todos os participantes têm algum grau de conhecimento dos riscos cibernéticos enfrentados por sua empresa. No contexto desta pesquisa, risco cibernético significa qualquer risco ou dano financeiro, perturbação ou dano à reputação de uma empresa devido a algum tipo de falha em seus sistemas de tecnologia da informação.[3]



Como mostra a Figura 2, apesar de o dano potencial médio a ativos de informação (US$ 617 milhões) ser comparável ao dano potencial médio a Propriedade, Planta & Equipamentos ("PP&E") ($648 milhões), há entre eles uma diferença significativa na cobertura de seguro.

Algumas das principais mensagens da pesquisa:

- Os ativos de informação são insuficientemente segurados contra roubo ou destruição com base em valor, dano máximo provável ("DMP") e probabilidade de ocorrência de incidente, embora o DMP possa exceder US$ 200 milhões.

- Há diferença na divulgação de danos substanciais a PP&E e a ativos de informação. Entre os participantes, 50% declaram que sua empresa divulgaria o dano a PP&E em suas demonstrações financeiras em uma nota de rodapé. No entanto, 34% dos participantes dizem que danos substanciais a ativos de informação não requerem divulgação.

- Apesar do risco, as empresas relutam em comprar cobertura de seguro cibernético. 52% dos participantes acreditam que a exposição da sua empresa ao risco cibernético aumentará ao longo dos próximos 24 meses. Apenas 19%, porém, declaram que sua empresa tem cobertura de seguro cibernético.

- 37% das empresas participantes sofreram violação de dados ou falha(s) de segurança substancial ou consideravelmente perturbador pelo menos uma vez nos últimos dois anos, sendo que o impacto econômico médio foi de US$ 2,1 milhões.

---

[1] Embora alguns riscos à rede, também chamados riscos cibernéticos, não sejam ainda totalmente seguráveis em mercados tradicionais de seguros (como o valor de segredos comerciais) e outros riscos cibernéticos possam ser seguráveis com apólices distintas (como propriedade, responsabilidade civil geral, crime, etc.), é útil compreender os riscos relativos em termos do impacto sobre as demonstrações financeiras na gestão da empresa.

[2] Os achados regionais são publicados em relatórios separados

[3] Fonte: Institute of Risk Management

Parte 2. Principais achados

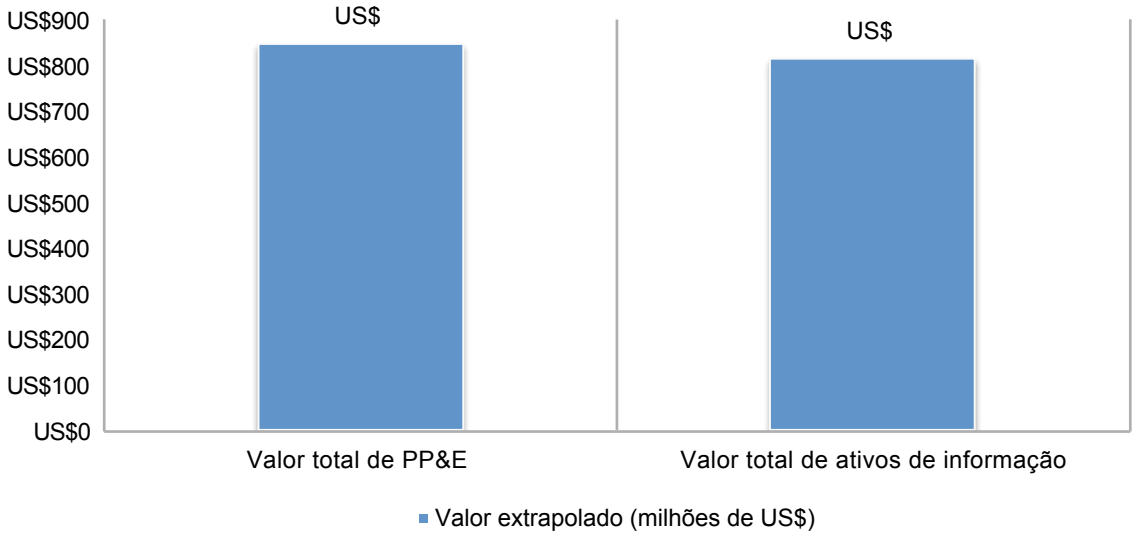
A versão completa e auditada dos achados se encontra no anexo deste relatório. Organizamos o relatório nos seguintes tópicos:

- Diferenças entre a valoração e o DMP de PP&E e de ativos de informação.
- A experiência das empresas com o risco cibernético
- A percepção do impacto financeiro de exposições cibernéticas

Diferenças entre a valoração e o DMP de PP&E e de ativos de informação.

As empresas atribuem a PP&E4 valor ligeiramente mais alto do que a ativos de informação. De acordo com a Figura 3, em média, o valor total de PP&E, incluindo todos os ativos imobilizados e sistemas de controle supervisório e de aquisição de dados ("SCADA") e sistemas de controle industrial é de aproximadamente US$ 848 milhões para as empresas representadas nesta pesquisa. O valor médio total de ativos de informação, que incluem registros de clientes, registros de funcionários, relatórios financeiros, dados analíticos, código fonte, modelos, métodos e outras propriedades intelectuais, é US$ 815 milhões, ligeiramente mais baixo do que aquele atribuído a PP&E.

Figura 3. Valor total de PP&E e de ativos de informação
Valor extrapolado

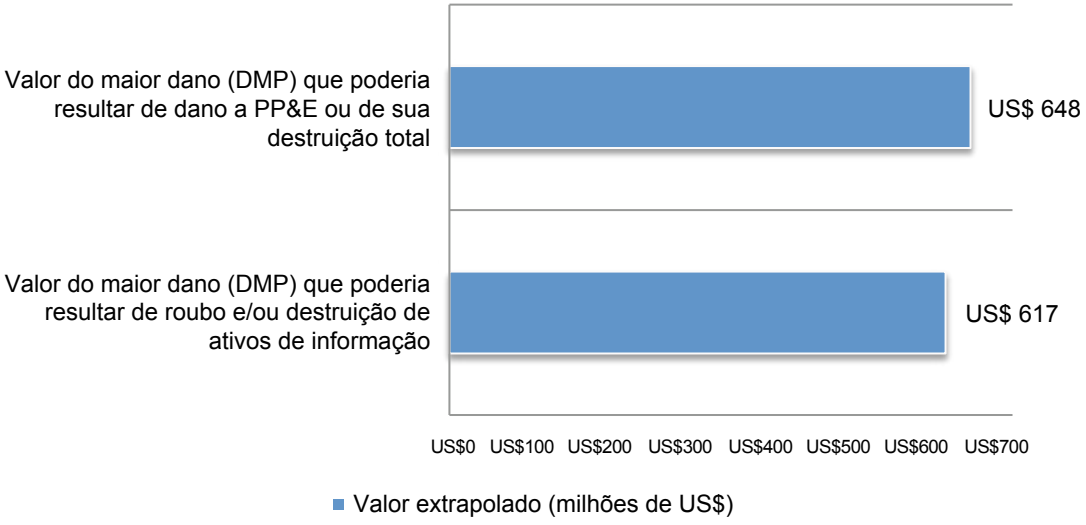


[4] Pediu-se aos participantes que identificassem, em relação aos ativos de PP&E, as causas raízes dos danos (ou seja, perigos), que incluem incêndios, inundações, eventos climáticos, terremotos e outros desastres naturais ou provocados pelo homem.

O valor do dano máximo provável (DMP)5 é maior para PP&E. As empresas estimam que o valor do DMP do maior prejuízo que pudesse resultar de dano a PP&E ou de sua destruição total é de aproximadamente US$ 648 milhões, em média. Essa estimativa pressupõe o funcionamento normal de recursos passivos de proteção tais como paredes corta-fogo e materiais inflamáveis, bem como o funcionamento adequado de sistemas ativos de supressão, como sprinklers, pisos elevados, etc.

No caso de roubo ou destruição de ativos de informação, o maior dano possível é de aproximadamente US$ 617 milhões em média, de acordo com a Figura 4. Essa estimativa pressupõe o funcionamento normal de soluções passivas de proteção cibernética tais como controles de perímetro, ferramentas de prevenção de perda de dados, criptografia de dados e sistemas de gestão de acessos, entre outros.

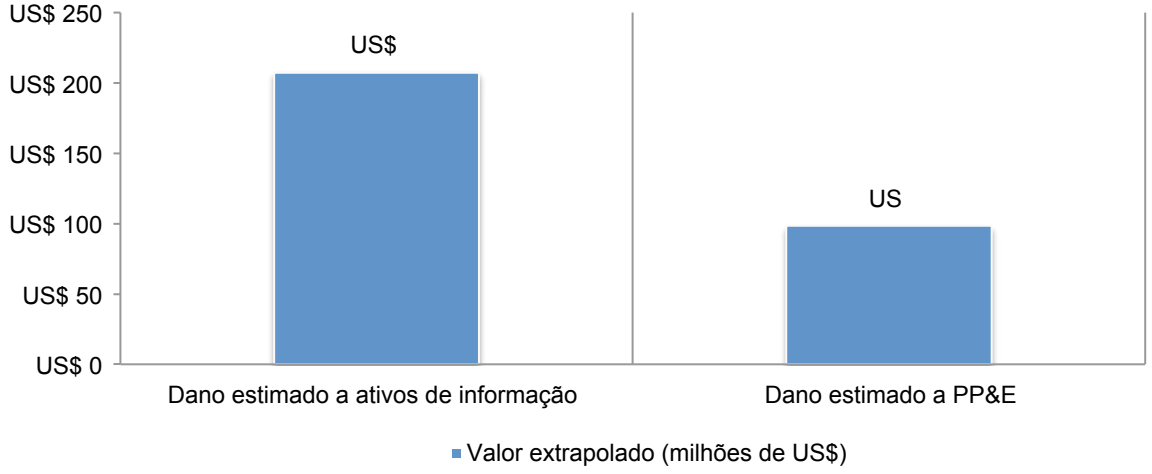
Figura 4. Valor de PP&E e de ativos de informação



[5] O dano máximo provável (DMP) é definido como o maior dano que poderia resultar de um desastre, pressupondo o funcionamento normal de recursos passivos de proteção (como paredes corta-fogo, materiais inflamáveis, etc.) e o funcionamento adequado da maior parte (talvez não de todos) dos sistemas ativos de supressão (como sprinklers).

Qual o impacto da ruptura dos negócios causada por danos a PP&E e a ativos de informação? De acordo com a Figura 5, a ruptura dos negócios tem maior impacto sobre os ativos de informação (US$ 207 milhões)[6] do que sobre PP&E (US$ 98 milhões). Isso sugere que a natureza fundamental do DMP varia consideravelmente na forma como atinge ativos intangíveis e tangíveis. Neste estudo, a ruptura dos negócios representa apenas 15% do DMP para PP&E. Por outro lado, a ruptura dos negócios representa 34% do DMP para ativos de informação.

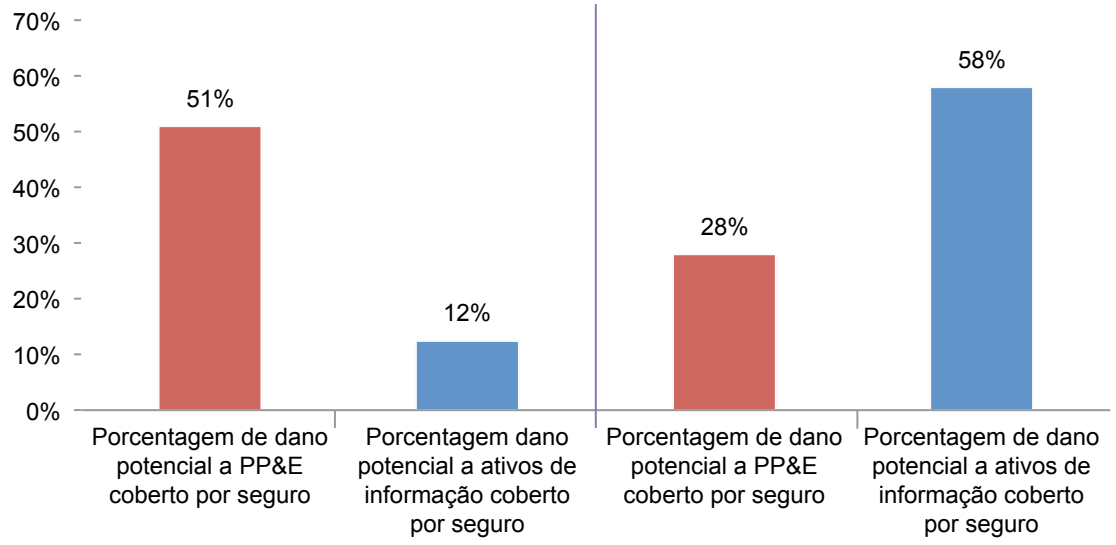
Figura 5. Impacto da ruptura dos negócios sobre ativos de informação e PP&E



[6] Embora os resultados da pesquisa sugiram Dano Máximo Provável na casa dos US$ 200 milhões, cada vez mais empresas estão usando análises de plataforma de decisões sobre riscos e modelagem cibernética para sugerir danos potenciais acima de US$ 500 milhões e de até mais de US$ 1 bilhão e procurar cotações de seguros com limites de prêmios e apólices com termos para tais quantias.

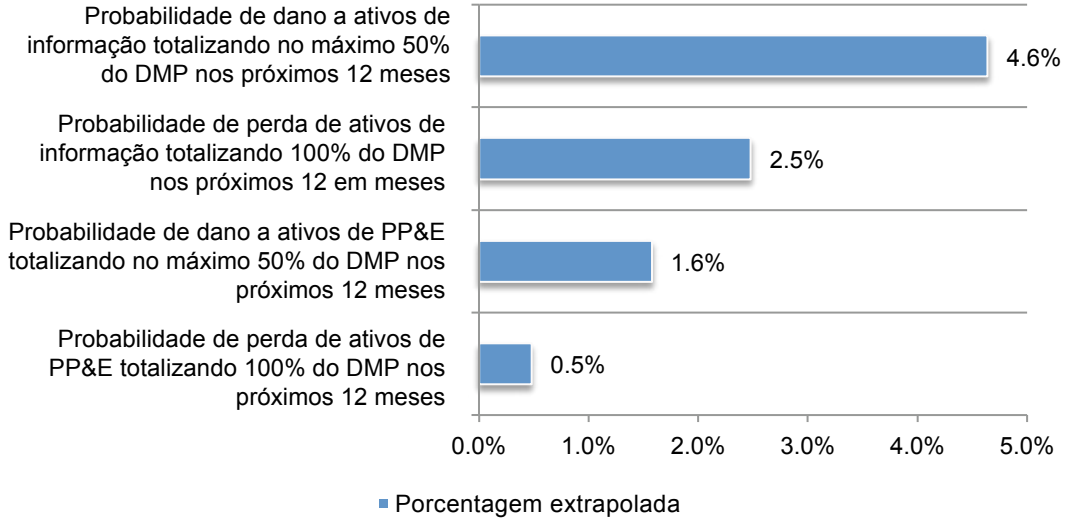
Há uma diferença significativa entre a cobertura de seguros de PP&E e de ativos de informação. Em média, aproximadamente 51% dos ativos de PP&E são cobertos por seguro e aproximadamente 28% de ativos PP&E são autossegurados (Figura 6).[7] Uma média de apenas 12% dos ativos de informação são cobertos por seguro. O autosseguro é mais frequente em ativos de informação: 58%.

Figura 6. Porcentagem de PP&E e de ativos de informação cobertos por seguro
Valor extrapolado



A probabilidade de dano é maior com ativos de informação do que com PP&E. Segundo a estimativa das empresas, a probabilidade de dano a ativos de informação totalizando no máximo 50% do DMP nos próximos 12 meses é de 4,6%, e totalizando até 100% do DMP é de 2,5%, como mostra a Figura 7. A probabilidade de um dano a PP&E totalizando no máximo 50% do DMP é uma média de 1,6%, e totalizando até 100% do DMP é de 0,5%.

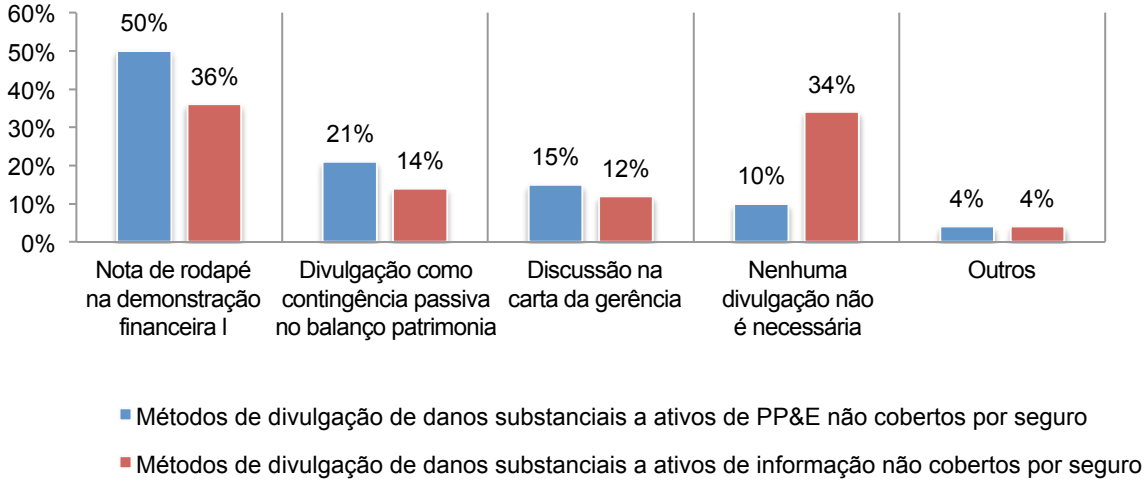
Figura 7. Probabilidade de dano a PP&E e a ativos de informação totalizando mais de 50% e 100% do DMP nos próximos 12 meses



[7] As porcentagens não somam 100% porque são valores extrapolados das questões 3, 4, 10 e 11. Esses resultados estão expostos nos achados completos auditados no anexo deste relatório

Também há diferença em divulgação de danos substanciais a PP&E e a ativos de informação. A Figura 8 mostra de que forma as empresas divulgariam um dano substancial. De acordo com 50% dos participantes, suas empresas divulgariam dano substancial a ativos de PP&E que não fossem cobertos por seguro em suas demonstrações financeiras, seguidos pelos 21% que afirmam que divulgariam tal dano como contingência passiva no balanço patrimonial (como, por ex., FASB 5). 36% declaram que divulgariam dano substancial a ativos de informação em nota de rodapé do demonstrativo financeiro, mas 34% não acreditam ser necessário divulgar tal informação.

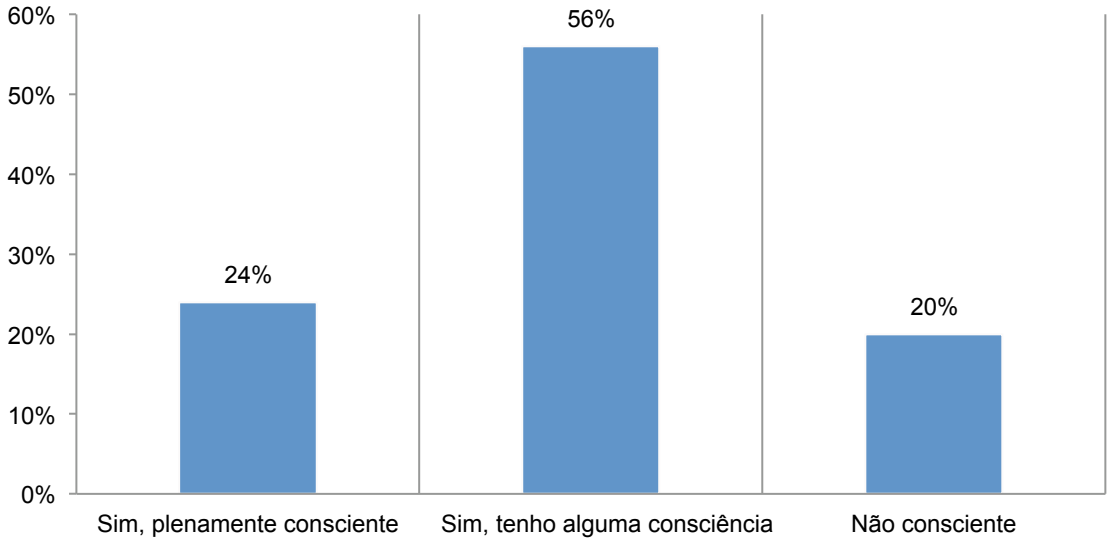
Figura 8. Como sua empresa divulgaria dano substancial a PP&E e a ativos de informação?



A experiência das empresas com o risco cibernético

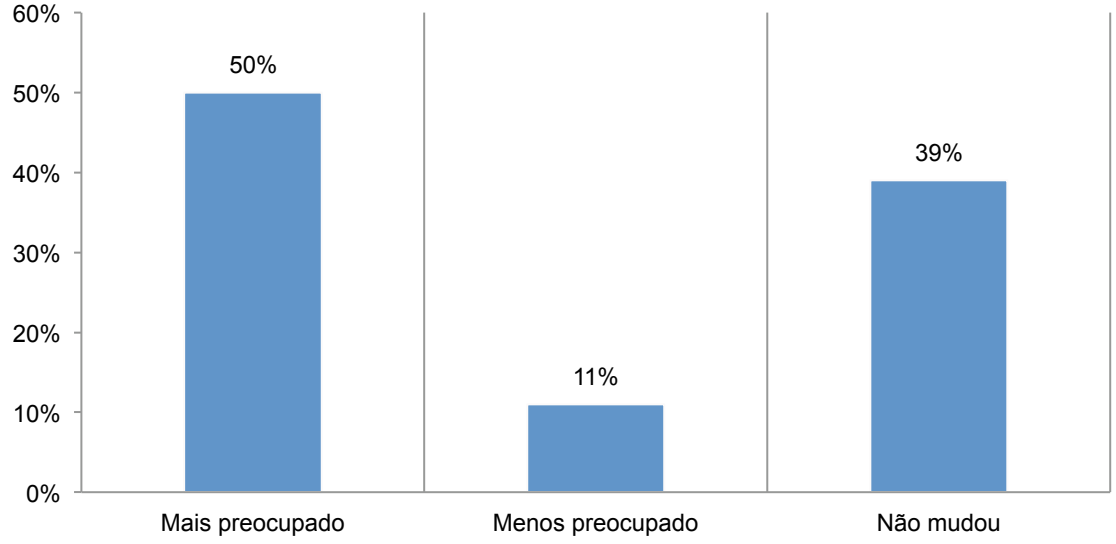
O grau de conscientização sobre as consequências econômicas e legais de violações de dados ou exploits de segurança internacionais é baixo. Como se vê na Figura 9, apenas 24% dos participantes têm total consciência das consequências que podem advir de uma violação de dados ou falha(s) de segurança em outros países em que sua empresa opera, e 20% declaram não ter consciência disso.

Figura 9. Grau de conscientização sobre as consequências econômicas e legais de violações de dados ou exploits de segurança internacionais é baixo.



37% das empresas representadas neste estudo sofreram falha(s) de segurança ou violação de dados substancial ou significativamente perturbadora[8] uma vez ou mais nos últimos 24 meses. A média do impacto financeiro total desses incidentes foi US$ 2,1 milhões[9]. De acordo com a Figura 10, 50% desses participantes dizem que o incidente deixou suas empresas mais preocupadas com a responsabilidade cibernética (*cyber liability*).

Figura 10. O que mudou na preocupação da sua empresa com responsabilidade cibernética após o falha(s) de segurança ou a violação de dados?



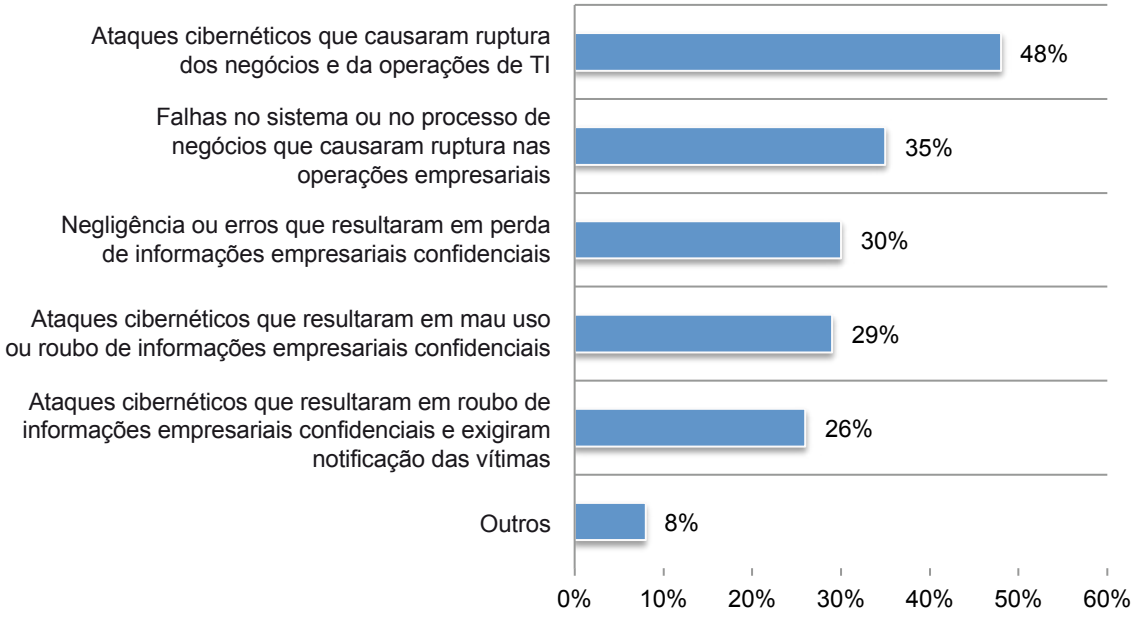
[8] No contexto deste estudo, o termo "substancialidade" leva em consideração quantias gastas em danos ao próprio segurado, potencial responsabilidade civil perante terceiros, valor do tempo perdido, custos de ações judiciais, danos à reputação e perda de receita. Trata-se, portanto, de uma acepção mais ampla do que a definição de "substancialidade" de acordo com as exigências GAAP e SEC.

[9] Inclui todos os custos, inclusive despesas diversas como honorários de consultores e advogados, custos indiretos tais como perdas de produtividade, diminuição da receita, ações judiciais, rotatividade de clientes e danos à reputação.

A Figura 11 mostra, em porcentagens, o tipo de incidente de segurança das empresas representadas nesta pesquisa. O tipo mais comum de incidente foi ataque cibernético que causou ruptura nos negócios e em operações de TI (48% dos participantes), seguido por falha no sistema ou no processo de negócios como causa da ruptura nas operações empresariais (35% dos participantes).

Incidentes envolvendo perda ou roubo de ativos de informação não foram tão prevalentes entre as causas de ruptura dos negócios. Ataques cibernéticos que resultaram em mau uso ou roubo de informações empresariais confidenciais (como propriedades intelectuais) e roubo de informações empresariais confidenciais que tenha exigido notificação ocorreram em 29% e 26% dos participantes, respectivamente. Segundo 30% dos participantes, o incidente de segurança foi provocado por negligência ou erros que resultaram em perda de informações empresariais confidenciais.

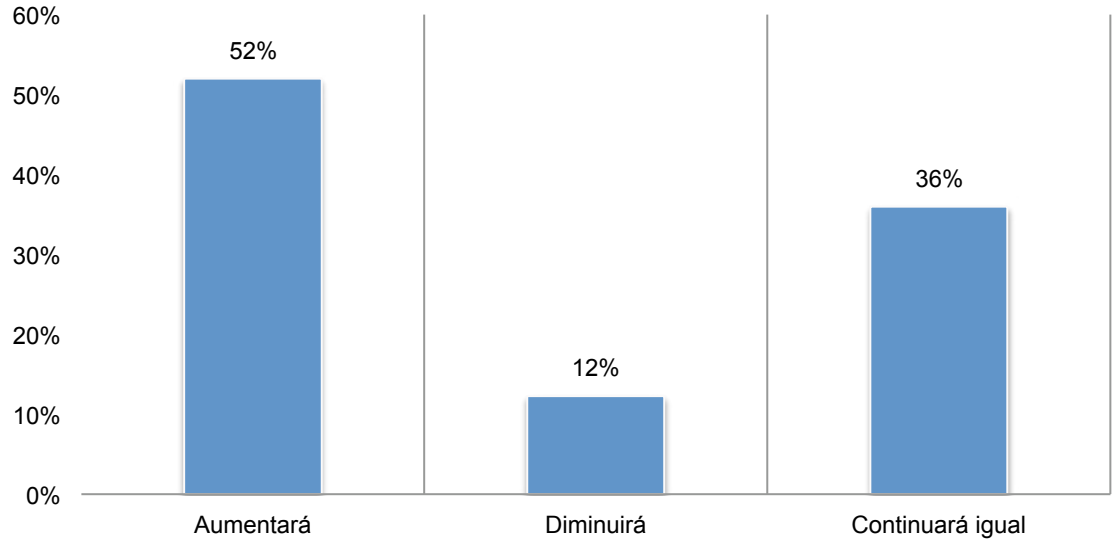
Figura 11. Que tipo de violação de dados ou falha(s) de segurança ocorreu na sua empresa? Pode-se dar mais uma resposta



Percepções do impacto financeiro de exposições cibernéticas

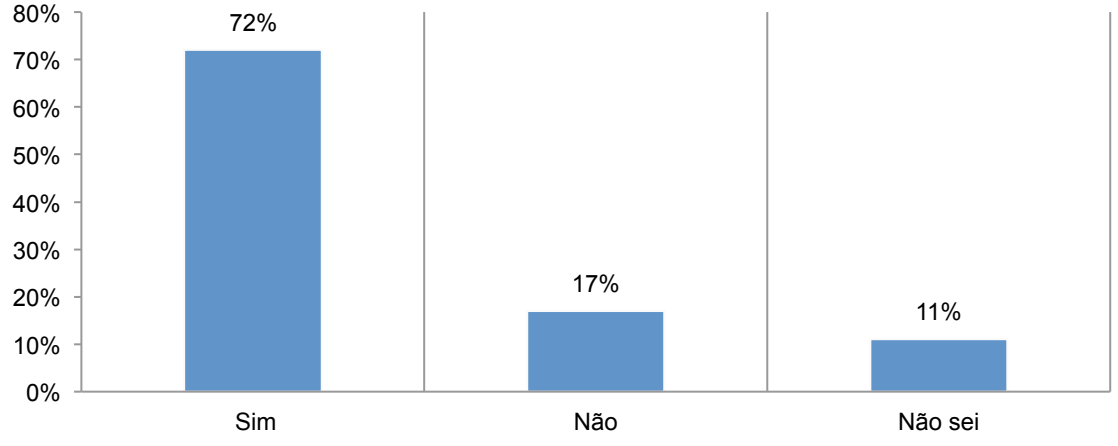
Embora a exposição das empresas ao risco cibernético deva aumentar, a maior parte dos participantes (54%) diz não ter planos de adquirir seguro cibernético. De acordo com a Figura 12, 52% dos participantes acreditam que a exposição da sua empresa ao risco cibernético aumentará, e 36% dizem que se manterá igual. Apenas 12% dos participantes esperam que tal risco diminua.

Figura 12. A exposição da sua empresa ao risco cibernético aumentará, diminuirá ou se manterá igual nos próximos dois anos?



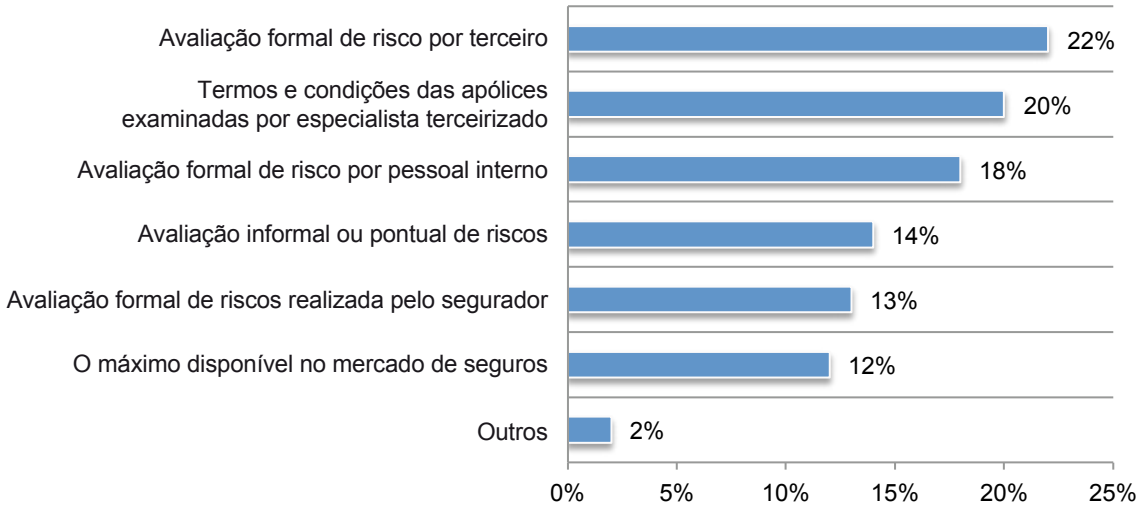
Apesar do risco cibernético, apenas 19% dos participantes declaram que suas empresas atualmente têm cobertura de seguro cibernético com limite médio de US$ 13 milhões. Como mostra a Figura 13, 72% dos participantes acreditam que isso é suficiente em relação a termos e condições da cobertura, exclusões, retenções, limites e segurança financeira do segurador.

Figura 13. A cobertura de seguro cibernético da sua empresa é suficiente?



De acordo com a Figura 14, a adequação da cobertura é determinada, principalmente, por terceiros. 32% dos participantes dizem que um terceiro realizou uma avaliação formal de risco, e 20% afirmam que um especialista terceirizado examinou os termos e condições da apólice. Em seguida vem uma avaliação formal de risco realizada por pessoal interno (18% dos participantes). 14% dizem ter passado por avaliação formal ou pontual de risco e 13% dizem ter passado por avaliação formal de risco realizada pelo segurador.

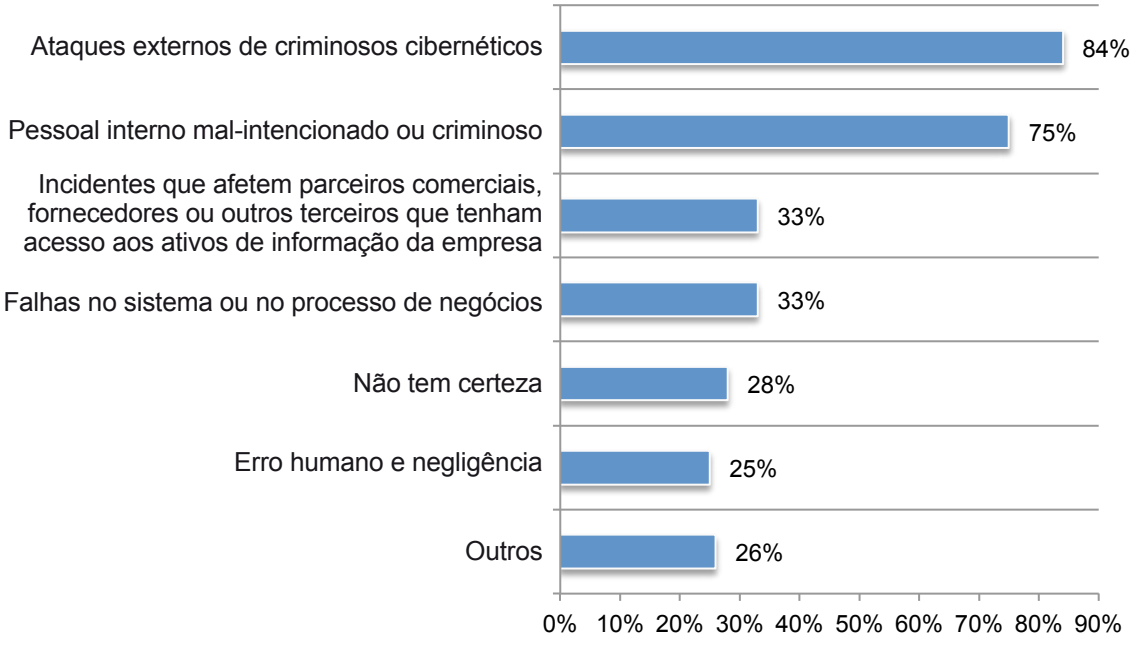
Figura 14. Como as empresas determinam a adequação da cobertura



A Figura 15 trata de incidentes cobertos por seguro cibernético. A maior parte dos incidentes cobertos são ataques externos de criminosos cibernéticos (84% dos participantes), pessoal interno mal-intencionado ou criminoso (75% dos participantes) e incidentes que afetaram parceiros comerciais, fornecedores ou outros terceiros que tenham acesso aos ativos de informação da empresa (33% dos participantes).

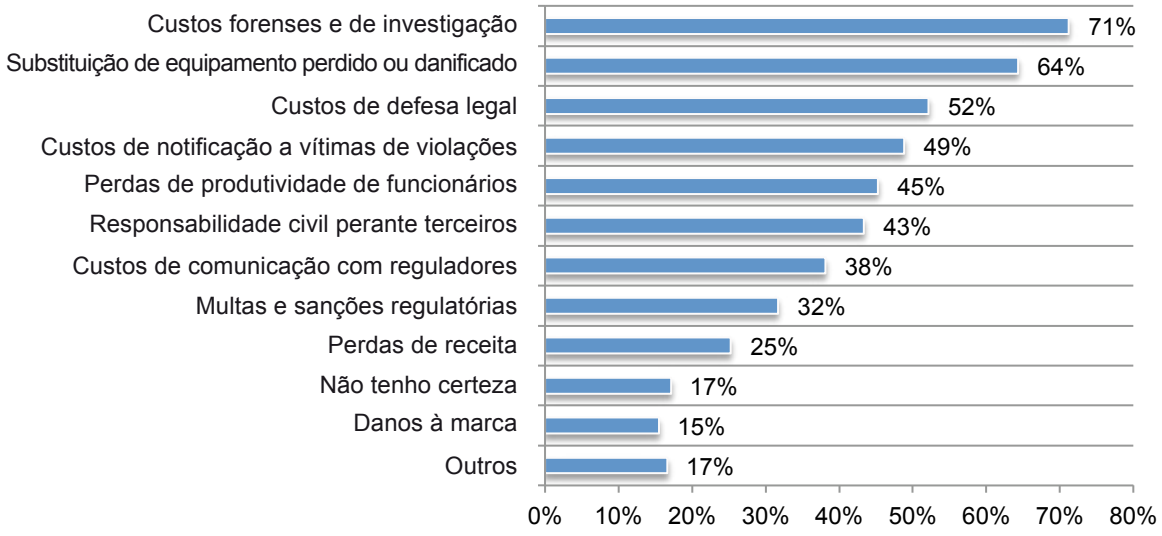
Embora as falhas no sistema ou no processo de negócios sejam a causa mais frequente de violação de dados ou exploits, 33% dos participantes declaram que tais incidentes estão cobertos por seu seguro cibernético. 38% não sabem quais incidentes estão cobertos.

Figura 15. Tipos de incidentes cobertos por seguro cibernético.
Pode-se dar mais de uma resposta



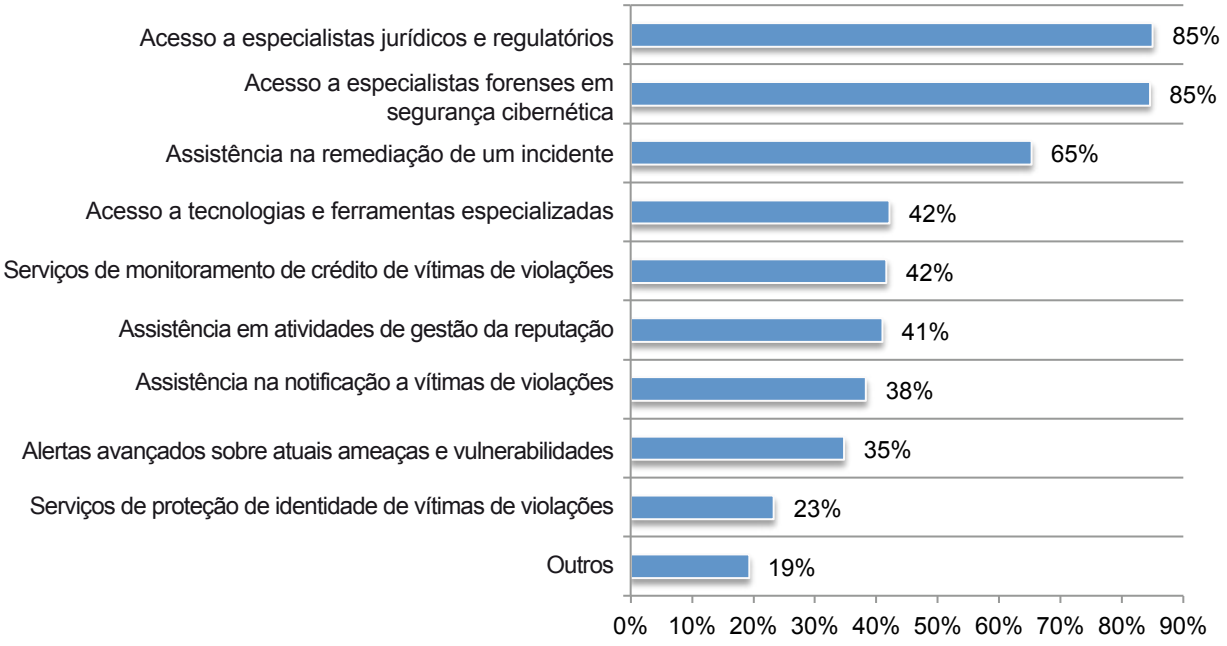
As Figuras 16 e 17 mostram a cobertura e os serviços fornecidos por seguradoras. Os cinco principais custos cobertos são custos forenses e de investigação (71% dos participantes), substituição de equipamento perdido ou danificado (64%) custos de defesa legal (52%), custos de notificação a vítimas de violações (4%) e perdas de produtividade de funcionários (45%). 17% dos participantes não têm certeza da cobertura oferecida.

Figura 16. Cobertura oferecida pela seguradora
Pode-se dar mais de uma resposta



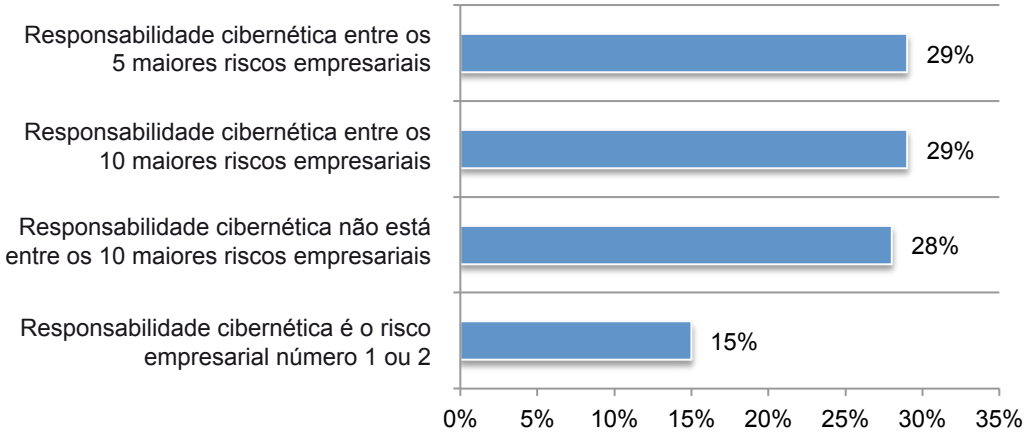
Outros serviços fornecidos: acesso a especialistas jurídicos e regulatórios (85% dos participantes) e especialistas forenses em segurança cibernética (85%), assistência na remediação de um incidente (65%) e acesso a tecnologias e ferramentas especializadas (42%). 42% dos participantes dizem receber serviços de monitoramento de crédito de vítimas de violações.

Figura 17. Outros serviços fornecidos pelo segurador de seguro cibernético
Pode-se dar mais de uma resposta



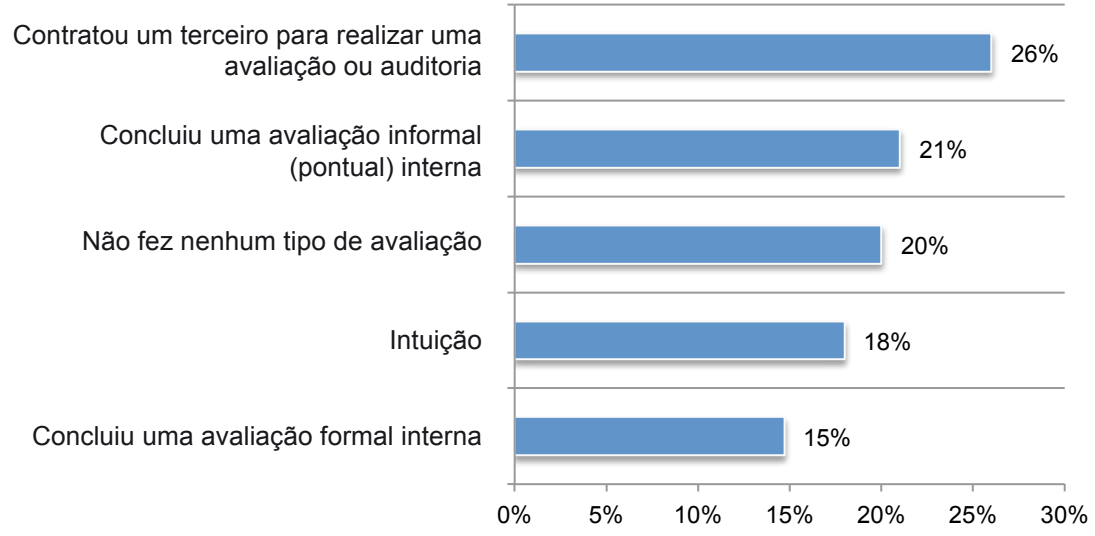
A responsabilidade cibernética está entre os dez principais riscos enfrentados pelas empresas. Como se vê na Figura 18, 72% dos participantes consideram o risco cibernético um dos dez principais riscos empresariais. O risco cibernético é o risco empresarial número um ou número dois para 15 % dos participantes, está entre os cinco primeiros para 29% dos participantes e entre os dez primeiros para outros 29%. 28% dos participantes acreditam que tal risco não está entre os dez principais riscos enfrentados por suas empresas.

Figura 18. Qual a posição do risco cibernético em relação a outros riscos empresariais?



De acordo com 26% dos participantes, sua empresa contratou um terceiro para realizar uma avaliação ou auditoria para determinar o risco cibernético, e 21% disseram que foi feita uma avaliação informal (pontual) interna (Figura 19). Apenas 15% dos participantes afirmam que sua empresa concluiu uma avaliação formal interna, e 18% dizem que sua empresa usa a intuição.

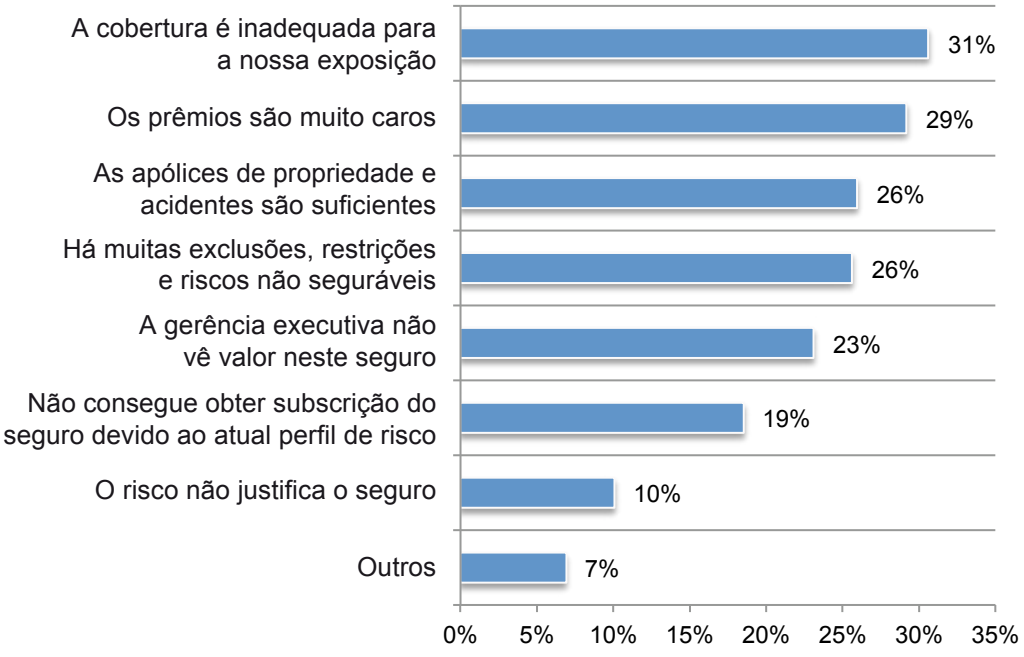
Figura 19. Como vocês determinam o nível de risco cibernético da sua empresa?



A aquisição de seguro cibernético aumentará por preocupação com exploits de segurança e violação de dados? 54% dos participantes não têm planos de adquirir seguro cibernético. 13% dos participantes dizem que suas empresas adquirirão seguro cibernético nos próximo 12 meses; para 22% isso ocorrerá dentre de dois anos e, para 18%, esse prazo será maior do que dois anos.

De acordo com a Figura 20, os principais motivos para não adquirir seguro cibernético são: a cobertura é inadequada para sua exposição (31%); os prêmios são muito caros (29%); as apólices de propriedade e acidentes são suficientes (26%); há muitas exclusões, restrições e riscos não seguráveis (26%).

Figura 20. Quais são os principais motivos para sua empresa não adquirir seguro cibernético?
Pode-se dar mais uma resposta



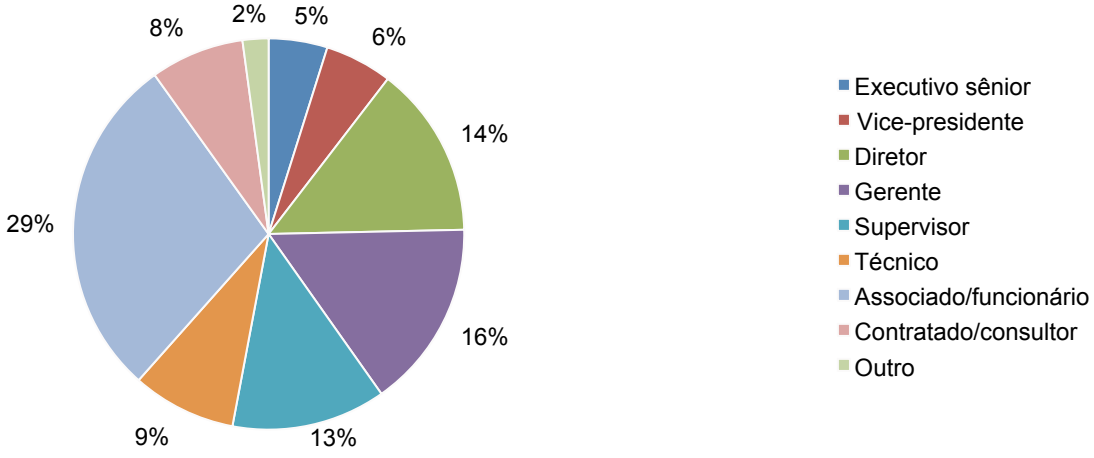
Parte 3. Métodos

O *sampling frame* global foi composto de 60,121 profissionais envolvidos com as atividades de gestão de risco cibernético e gestão de risco empresarial. Como mostra a Tabela 1, 2.525 participantes concluíram a pesquisa. O filtro removeu 282 pesquisas. A amostra final foi de 2.243 pesquisas (ou taxa de resposta de 3,7%).

Tabela 1. Resposta da amostra	**Freq**	**Pct%**
Sampling frame total	60.121	100,0%
Total de retornos	2.525	4,2%
Pesquisas rejeitadas ou eliminadas no filtro	282	0,5%
Amostra final	2.243	3,7%

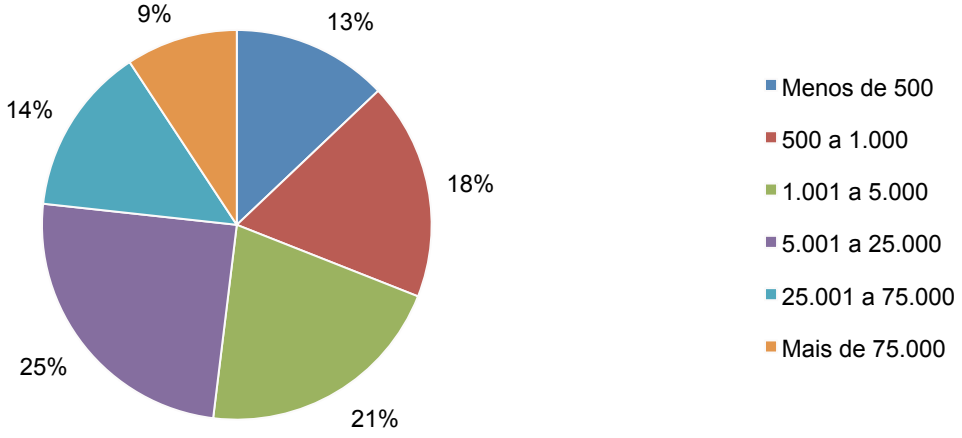
Gráfico de pizza 1 mostra a posição atual ou o nível hierárquico dos participantes. Mais da metade (53%) declaram estar em cargo de no nível de supervisão ou acima.

Gráfico de pizza 1 Posição atual ou o nível hierárquico



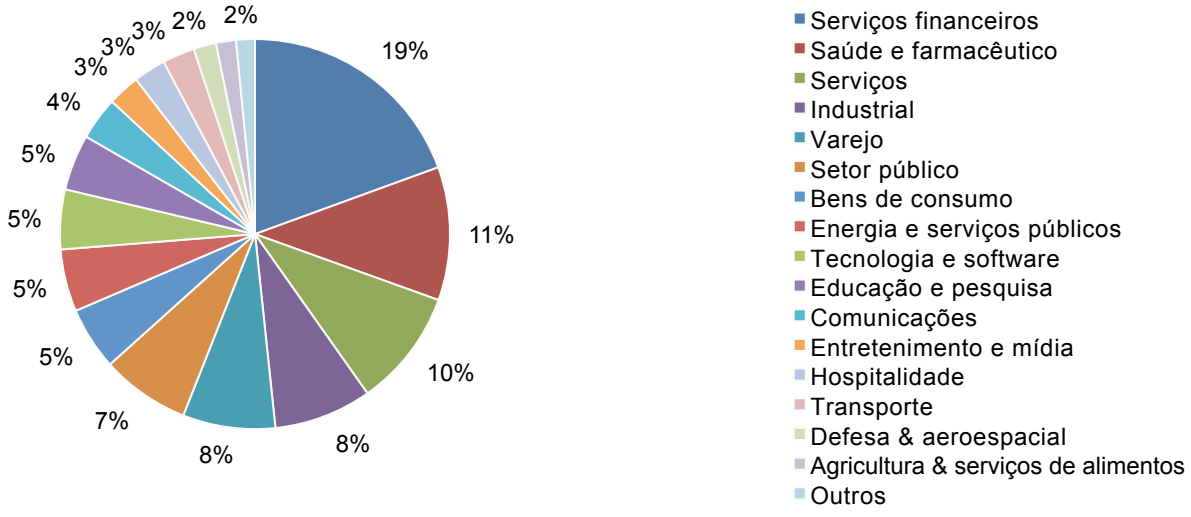
De acordo com o Gráfico de pizza 2, 69% dos participantes são de empresas com mais de 1.000 funcionários globalmente.

Gráfico de pizza 2 Número de funcionários da empresa no mundo todo



O Gráfico de pizza 3 mostra a classificação primária de segmento das empresas. Nele, vê-se que o setor com maior presença é o de serviços financeiros (19%), seguido por saúde e farmacêutico (11%) e serviços (10%).

Gráfico de pizza 3 Segmento primário



Parte 4. Advertência

A pesquisa tem limitações inerentes que precisam ser consideradas cuidadosamente antes que se façam inferências a partir dos achados. Os itens abaixo são limitações específicas que são inerentes à maior parte das pesquisas online.

Viés de não respostas: Os presentes achados se baseiam em uma amostra de retornos de pesquisa. Enviamos pesquisas para um número representativo de pessoas, o que resulta em um grande número de pesquisas respondidas utilizáveis. Apesar dos testes de não resposta, sempre é possível que indivíduos que não participem sejam substancialmente diferentes, em termos de crenças subjacentes, daqueles que completaram o instrumento.

Viés de sampling frame: A precisão se baseia nas informações de contato e no grau em que a lista representa bem os indivíduos envolvidos com a gestão dos riscos cibernéticos e empresarias das suas empresas. Reconhecemos também que os resultados podem ficar enviesados por eventos externos, tais como cobertura da imprensa. Reconhecemos, além disso, o viés causado por remunerar os sujeitos por concluir a pesquisa dentro de um prazo determinado.

Resultados autorreportados: A qualidade da pesquisa se baseia na integridade de respostas confidenciais recebida dos sujeitos. Embora se possam incorporar freios e contrapesos ao processo de pesquisa, sempre há a possibilidade de que um sujeito não forneça respostas precisas.

Anexo: Resultados detalhados da pesquisa

As tabelas abaixo dão a frequência ou frequência percentual de respostas a todas as perguntas da pesquisa que é parte deste estudo. Todas as respostas à pesquisa foram obtidas em fevereiro de 2015.

Resposta à pesquisa	GLOBAL
Sampling frame	60.121
Total de retornos	2.525
Amostra final	2.243
Taxa de respostas	3,7%

Perguntas do filtro

F1. Qual seu nível de familiaridade com os riscos cibernéticos que sua empresa enfrenta atualmente?	GLOBAL
Tenho muita familiaridade	14%
Tenho familiaridade	34%
Tenho alguma familiaridade	52%
Não tenho familiaridade	0%
Total	100%

F2. Você está envolvido nas atividades de gestão de riscos financeiros da sua empresa?	GLOBAL
Sim, tenho envolvimento significativo	24%
Sim, tenho algum significativo	76%
Não tenho envolvimento	0%
Total	100%

F3. Você está envolvido nas atividades de gestão de riscos empresariais da sua empresa?	GLOBAL
Sim, tenho envolvimento significativo	29%
Sim, tenho algum significativo	71%
Não tenho envolvimento	0%
Total	100%

F4. Qual das alternativas abaixo melhor descreve seu cargo?	GLOBAL
Gestão de riscos	17%
Finanças, tesouraria e contabilidade	37%
Conformidade corporativa/auditoria	14%
Segurança/segurança da informação	13%
Gerência geral	14%
Jurídico	5%
Nenhuma das anteriores	0%
Total	100%

As perguntas abaixo se referem à propriedade, plantas e equipamentos da sua empresa (PP&E)

P1: Qual o valor total do PP&E da sua empresa, incluindo todos os ativos imobilizados mais os sistemas SCADA e sistemas de controle industrial? Pressuponha um valor baseado no custo de substituição total (e não no custo histórico).	GLOBAL
Menos de US$ 1 milhão	8%
US$ 1 milhão a US$ 10 milhões	15%
US$ 11 milhões a US$ 50 milhões	12%
US$ 51 milhões a US$ 100 milhões	24%
US$ 101 milhões a US$ 500 milhões	22%
US$ 501 milhões a US$ 1 bilhão	11%
US$ 1 bilhão a US$ 10 bilhões	4%
Mais de US$ 10 bilhões	4%
Total	100%
Valor extrapolado	847.55

P2a. Qual o valor do maior dano (DMP) que poderia resultar de dano a PP&E ou de sua destruição total? A resposta deve ser dada pressupondo-se o funcionamento normal de recursos passivos de proteção tais como paredes corta-fogo e materiais inflamáveis, bem como o funcionamento adequado de sistemas ativos de supressão, como sprinklers e pisos elevados, entre outros.	GLOBAL
Menos de US$ 1 milhão	10%
US$ 1 milhão a US$ 10 milhões	15%
US$ 11 milhões a US$ 50 milhões	16%
US$ 51 milhões a US$ 100 milhões	25%
US$ 101 milhões a US$ 500 milhões	19%
US$ 501 milhões a US$ 1 bilhão	9%
US$ 1 bilhão a US$ 10 bilhões	5%
Mais de US$ 10 bilhões	2%
Total	100%
Valor extrapolado	647.99

P2b. Qual o valor do maior dano (DMP) sofrido pela sua empresa devido à ruptura dos negócios? A resposta deve ser dada pressupondo-se o funcionamento normal de recursos passivos de proteção tais como paredes corta-fogo e materiais inflamáveis, bem como o funcionamento adequado de sistemas ativos de supressão, como sprinklers e pisos elevados, entre outros.	GLOBAL
Menos de US$ 1 milhão	21%
US$ 1 milhão a US$ 10 milhões	29%
US$ 11 milhões a US$ 50 milhões	24%
US$ 51 milhões a US$ 100 milhões	18%
US$ 101 milhões a US$ 500 milhões	6%
US$ 501 milhões a US$ 1 bilhão	1%
US$ 1 bilhão a US$ 10 bilhões	0%
Mais de US$ 10 bilhões	0%
Total	100%
Valor extrapolado	98.28

P3: Que porcentagem desse dano potencial a ativos de PP&E está coberta por seguro?	GLOBAL
Menos de 5%	6%
5% a 10%	8%
11% a 20%	5%
21% a 30%	7%
31% a 40%	8%
41% a 50%	10%
51% a 60%	17%
61% a 70%	12%
71% a 80%	12%
81% a 90%	9%
91% a 100%	6%
Total	100%
Valor extrapolado	51%

Página 21Relatório Global de Impacto Cibernético 2015, patrocinado	GLOBAL
Menos de 5%	14%
5% a 10%	16%
11% a 20%	14%
21% a 30%	16%
31% a 40%	11%
41% a 50%	12%
51% a 60%	5%
61% a 70%	6%
71% a 80%	3%
81% a 90%	1%
91% a 100%	0%
Total	100%
Valor extrapolado	28%

P5: Qual a probabilidade de que sua empresa sofra dano a ativos de PP&E totalizando no máximo 50% do DMP nos próximos 12 meses?	GLOBAL
Menos de 0,1%	25%
0,1% a 0,5%	20%
0,6% a 1,0%	14%
1,1% a 2,0%	12%
2,1% a 3,0%	15%
3,1% a 4,0%	6%
4,1% a 5,0%	5%
5,1% a 10,0%	1%
Mais de 10,0%	3%
Total	100%
Valor extrapolado	1.58%

P6: Qual a probabilidade de que sua empresa sofra dano a ativos de PP&E totalizando no máximo 100% do DMP nos próximos 12 meses?	GLOBAL
Menos de 0,1%	70%
0,1% a 0,5%	15%
0,6% a 1,0%	8%
1,1% a 2,0%	3%
2,1% a 3,0%	2%
3,1% a 4,0%	0%
4,1% a 5,0%	1%
5,1% a 10,0%	1%
Mais de 10,0%	1%
Total	100%
Valor extrapolado	0.48%

P7: Na sua opinião, como sua empresa divulgaria nas demonstrações financeiras um dano substancial a ativos de PP&E que não estivesse coberto por seguro?	GLOBAL
Divulgariam tal dano como contingência passiva no balanço patrimonial (como, por ex., FASB 5)	21%
Em nota de rodapé do demonstrativo financeiro	50%
Discussão na carta da gerência	15%
Nenhuma das anteriores - a divulgação não é necessária	10%
Outros	4%
Total	100%

As perguntas abaixo se referem aos ativos de informação da sua empresa.

P8. Qual é o valor total de ativos de informação, incluindo registros de clientes, registros de funcionários, relatórios financeiros, dados analíticos, código fonte, modelos, métodos e outras propriedades intelectuais Pressuponha um valor baseado no custo de substituição total (e não no custo histórico). Tal valor pode ser uma quantificação precisa ou uma estimativa.	GLOBAL
Menos de US$ 1 milhão	10%
US$ 1 milhão a US$ 10 milhões	14%
US$ 11 milhões a US$ 50 milhões	14%
US$ 51 milhões a US$ 100 milhões	20%
US$ 101 milhões a US$ 500 milhões	17%
US$ 501 milhões a US$ 1 bilhão	18%
US$ 1 bilhão a US$ 10 bilhões	5%
Mais de US$ 10 bilhões	4%
Total	100%
Valor extrapolado	814.76

P9a. Qual o valor do maior dano (DMP) que poderia resultar de roubo e/ou destruição de ativos de informação? A resposta deve ser dada pressupondo-se o funcionamento normal de recursos passivos de proteção cibernética tais como controles de perímetro, ferramentas de prevenção de perda de dados, criptografia de dados e sistemas de gestão de acessos e identidade, entre outros.	GLOBAL
Menos de US$ 1 milhão	10%
US$ 1 milhão a US$ 10 milhões	17%
US$ 11 milhões a US$ 50 milhões	14%
US$ 51 milhões a US$ 100 milhões	26%
US$ 101 milhões a US$ 500 milhões	17%
US$ 501 milhões a US$ 1 bilhão	9%
US$ 1 bilhão a US$ 10 bilhões	6%
Mais de US$ 10 bilhões	2%
Total	100%
Valor extrapolado	617.06

P9b. Qual o valor do maior dano (DMP) sofrido pela sua empresa devido à ruptura cibernética dos negócios? A resposta deve ser dada pressupondo-se o funcionamento normal de soluções passivas de proteção cibernética tais como controles de perímetro, ferramentas de prevenção de perda de dados, criptografia de dados e sistemas de gestão de acessos e identidade, entre outros.	GLOBAL
Menos de US$ 1 milhão	23%
US$ 1 milhão a US$ 10 milhões	23%
US$ 11 milhões a US$ 50 milhões	24%
US$ 51 milhões a US$ 100 milhões	12%
US$ 101 milhões a US$ 500 milhões	10%
US$ 501 milhões a US$ 1 bilhão	5%
US$ 1 bilhão a US$ 10 bilhões	2%
Mais de US$ 10 bilhões	0%
Total	100%
Valor extrapolado	207.34

P10: Que porcentagem dano potencial a ativos de informação está coberta por seguro?	GLOBAL
Menos de 5%	32%
5% a 10%	43%
11% a 20%	9%
21% a 30%	6%
31% a 40%	3%
41% a 50%	2%
51% a 60%	2%
61% a 70%	1%
71% a 80%	1%
81% a 90%	1%
91% a 100%	0%
Total	100%
Valor extrapolado	12%

P11: Que porcentagem de dano potencial a ativos de informação está autossegurada?	GLOBAL
Menos de 5%	5%
5% a 10%	6%
11% a 20%	2%
21% a 30%	2%
31% a 40%	3%
41% a 50%	7%
51% a 60%	18%
61% a 70%	20%
71% a 80%	24%
81% a 90%	9%
91% a 100%	4%
Total	100%
Valor extrapolado	58%

P12: Qual a probabilidade de que sua empresa sofra dano a ativos de informação totalizando no máximo 50% do DMP nos próximos 12 meses?	GLOBAL
Menos de 0,1%	7%
0,1% a 0,5%	9%
0,6% a 1,0%	6%
1,1% a 2,0%	7%
2,1% a 3,0%	9%
3,1% a 4,0%	13%
4,1% a 5,0%	14%
5,1% a 10,0%	21%
Mais de 10,0%	14%
Total	100%
Valor extrapolado	4.64%

P13. Qual a probabilidade de que sua empresa sofra dano a ativos de informação totalizando no máximo 100% do DMP nos próximos 12 meses?	GLOBAL
Menos de 0,1%	14%
0,1% a 0,5%	11%
0,6% a 1,0%	9%
1,1% a 2,0%	12%
2,1% a 3,0%	18%
3,1% a 4,0%	12%
4,1% a 5,0%	18%
5,1% a 10,0%	6%
Mais de 10,0%	0%
Total	100%
Valor extrapolado	2.48%

P14. Na sua opinião, como sua empresa divulgaria nas demonstrações financeiras um dano substancial a ativos de informação que não estivesse coberto por seguro?	GLOBAL
Divulgariam tal dano como contingência passiva no balanço patrimonial (FASB 5)	14%
Em nota de rodapé do demonstrativo financeiro	36%
Discussão na carta da gerência	12%
Nenhuma das anteriores - a divulgação não é necessária	34%
Outros	4%
Total	100%

Parte 2. Outras perguntas

P15. Você tem consciência das consequências econômicas e legais de violações de dados ou exploits de segurança nos outros países em que sua empresa opera?	GLOBAL
Sim, tenho total consciência.	23%
Sim, tenho alguma consciência.	56%
Não tenho consciência	20%
Total	100%

P16a. Sua empresa sofreu falha(s) de segurança ou violação de dados substancial ou significativamente perturbadora uma vez ou mais nos últimos 24 meses? Consulte a definição de "substancialidade" exposta acima.	GLOBAL
Sim	37%
Não [pular para P17]	63%
Total	100%

P16b. Em caso afirmativo, qual das alternativas abaixo melhor descreve as violações de dados ou exploits de segurança sofridos pela sua empresa nos últimos 24 meses? Selecione todas os itens aplicáveis.	GLOBAL
Ataques cibernéticos que causaram ruptura dos negócios e das operações de TI (como negação de ataques de serviços)	48%
Ataques cibernéticos que resultaram em roubo de informações empresariais confidenciais, exigindo por isso notificação às vítimas	26%
Ataques cibernéticos que resultaram em mau uso ou roubo de informações empresariais confidenciais, tais como propriedades intelectuais	29%
Negligência ou erros que resultaram em perda de informações	30%
Falhas no sistema ou no processo de negócios que causaram ruptura nas operações empresariais (como atualizações de software)	35%
Outros	8%
Total	177%

P16c. Em caso afirmativo, qual foi o impacto financeiro total das violações de dados ou exploits de segurança sofridos pela sua empresa nos últimos 24 meses? Inclua todos os custos, inclusive despesas diversas como honorários de consultores e advogados, custos indiretos tais como tais como perdas de produtividade, diminuição da receita, ações judiciais, rotatividade de clientes e danos à reputação.	GLOBAL
Zero	5%
Menos de US$ 10.000	13%
US$ 10.000 a US$ 100.000	12%
US$ 100.001 a US$ 250.000	18%
US$ 250.001 a US$ 500.000	19%
US$ 500.001 a US$ 1.000.000	13%
US$ 1.000.000 a US$ 5.000.000	10%
US$ 5.000.001 a US$ 10.000.000	5%
US$ 10.000.001 a US$ 25.000.000	2%
US$ 25.000.001 a US$ 50.000.000	2%
US$ 50.000.001 a US$ 100.000.000	0%
Mais de US$ 100.000.000	0%
Total	100%
Valor extrapolado	2,099,656

P16d. Em caso afirmativo, o que mudou na preocupação da sua empresa com responsabilidade cibernética após tal falha(s) de segurança ou a violação de dados?	GLOBAL
Mais preocupada	50%
Menos preocupada	11%
Nenhuma alteração	39%
Total	100%

P17. Você acredita que a exposição da sua empresa ao risco cibernético aumentará, diminuirá ou se manterá igual nos próximos dois anos?	GLOBAL
Aumentará	52%
Diminuirá	12%
Continuará igual	36%
Total	100%

P18a. Do ponto de vista do risco empresarial, qual a posição do risco cibernético em relação a outros riscos empresariais? Escolha a melhor alternativa.	GLOBAL
A responsabilidade cibernética é o risco empresarial número 1 ou 2 para minha empresa	15%
A responsabilidade cibernética está entre os 5 maiores riscos empresariais para minha empresa	29%
A responsabilidade cibernética está entre os 10 maiores riscos empresariais para minha empresa	29%
Responsabilidade cibernética não está entre os 10 maiores riscos empresariais para minha empresa	28%
Total	100%

P18b. Como vocês determinam o nível de risco cibernético da sua empresa?	GLOBAL
Concluiu uma avaliação formal interna	20%
Concluiu uma avaliação informal (pontual) interna	21%
Contratou um terceiro para realizar uma avaliação ou auditoria	26%
Intuição	18%
Não fez nenhum tipo de avaliação	15%
Total	100%

P19a. Sua empresa tem cobertura de seguro cibernético?	GLOBAL
Sim	19%
Não [pular para P20a]	81%
Total	100%

P19b. Em caso afirmativo, que limite você adquire?	GLOBAL
Menos de US$ 1 milhão	24%
US$ 1 milhão a US$ 5 milhões	32%
US$ 6 milhões a US$ 20 milhões	35%
US$ 21 milhões a US$ 100 milhões	5%
Mais de US$ 100 milhões	4%
Total	100%
Valor extrapolado	12.70

P19c. A cobertura de seguro cibernético da sua empresa é suficiente em relação a termos e condições da cobertura, exclusões, retenções, limites e segurança financeira do segurador?	GLOBAL
Sim	72%
Não	17%
Não tem certeza	11%
Total	100%

P19d. Como sua empresa determina o nível de cobertura que considera adequado?	GLOBAL
Avaliação formal de riscos por pessoal interno	18%
Avaliação formal de risco realizada pelo segurador	13%
Avaliação formal de riscos por terceiro	22%
Avaliação informal ou pontual de riscos	14%
Termos e condições das apólices examinadas por especialista terceirizado	20%
O máximo disponível no mercado de seguros	12%
Outros	2%
Total	100%

P19e. Que tipos de incidentes o seguro cibernético da sua empresa cobre? Selecione todas os itens aplicáveis.	GLOBAL
Ataques externos de criminosos cibernéticos	84%
Pessoal interno mal-intencionado ou criminoso	75%
Falhas no sistema ou no processo de negócios	33%
Erro humano e negligência	25%
Incidentes que afetem parceiros comerciais, fornecedores ou outros terceiros que tenham acesso aos ativos de informação da sua empresa	33%
Outros	26%
Não tem certeza	28%
Total	304%

P19f. Que cobertura tal seguro oferece à sua empresa? Selecione todas os itens aplicáveis.	GLOBAL
Custos forenses e de investigação	71%
Custos de notificação a vítimas de violações	49%
Custos de comunicação com reguladores	38%
Perdas de produtividade de funcionários	45%
Substituição de equipamento perdido ou danificado	64%
Perdas de receita	25%
Custos de defesa legal	52%
Multas e sanções regulatórias	32%
Responsabilidade civil perante terceiros	43%
Danos à marca	15%
Outros	17%
Não tem certeza	17%
Total	469%

P19g. Além da cobertura de custos, que outros serviços o segurador de seguro cibernético oferece à sua empresa no caso de falha(s) de segurança ou violação de dados? Marque todas as alternativas aplicáveis.	GLOBAL
Acesso a especialistas forenses em segurança cibernética	85%
Acesso a especialistas jurídicos e regulatórios	85%
Acesso a tecnologias e ferramentas especializadas	42%
Alertas avançados sobre atuais ameaças e vulnerabilidades	35%
Assistência na remediação de um incidente	65%
Assistência na notificação a vítimas de violações	38%
Serviços de proteção de identidade de vítimas de violações	23%
Serviços de monitoramento de crédito de vítimas de violações	42%
Assistência em atividades de gestão da reputação	41%
Outros	19%
Total	475%

P20a. Sua empresa pretende comprar seguro cibernético?	GLOBAL
Sim, nos próximos 12 meses	13%
Sim, nos próximos 24 meses	22%
Sim, em mais de 24 meses	18%
Não	46%
Total	100%

P20b. Em caso negativo, 1uais são os principais motivos para sua empresa não pretender adquirir seguro cibernético?	GLOBAL
Os prêmios são muito caros	29%
A cobertura é inadequada para a nossa exposição	31%
Há muitas exclusões, restrições e riscos não seguráveis	26%
O risco não justifica o seguro	10%
As apólices de propriedade e acidentes são suficientes	26%
A gerência executiva não vê valor neste seguro	23%
Não consegue obter subscrição do seguro devido ao atual perfil de risco	19%
Outros	7%
Total	170%

P21. Quem na sua empresa tem mais responsabilidade pela gestão do risco cibernético? Escolha os dois principais.	GLOBAL
CEO/conselho administrativo	4%
Diretor financeiro (CFO)	6%
Líderes da unidade de negócios (LOB)	15%
Diretor de informação	30%
Diretor de segurança da informação	15%
Gestão de riscos	13%
Compras	6%
Diretor jurídico	7%
Conformidade/auditoria	4%
Outros (selecione)	1%
Total	100%

Parte 3. Cargo e características hierárquicas

D1. Que nível melhor descreve seu cargo atual?	GLOBAL
Executivo sênior	5%
Vice-presidente	6%
Diretor	14%
Gerente	16%
Supervisor	13%
Técnico	9%
Associado/funcionário	29%
Contratado/consultor	8%
Outros	2%
Total	100%

D2. Qual o número de funcionários da sua empresa no mundo todo?	GLOBAL
Menos de 500	13%
500 a 1.000	18%
500 a 5.000	21%
5.001 a 25.000	25%
25.001 a 75.000	14%
Mais de 75.000.	9%
Total	100%

D3. Qual das alternativas abaixo melhor descreve a principal área de atuação da sua empresa?	GLOBAL
Agricultura & serviços de alimentos	2%
Comunicações	4%
Bens de consumo	5%
Defesa e aeroespacial	2%
Educação e pesquisa	5%
Energia e serviços públicos	5%
Entretenimento e mídia	3%
Serviços financeiros	19%
Saúde e farmacêutico	11%
Hospitalidade	3%
Industrial	8%
Outros	2%
Setor público	7%
Varejo	8%
Serviços	10%
Tecnologia e software	5%
Transporte	3%
Total	100%

AGRADECIMENTO

Agradecemos a revisão e contribuição de Adam Kalinich, aluno do Curso 18C do Massachusetts Institute of Technology: "Matemática e ciência da computação."

Ponemon Institute

Promovendo a gestão responsável de informações

O Ponemon Institute se dedica à educação e pesquisa independente, promovendo práticas responsáveis de gestão de privacidade e informação nas empresas e nos governos. Nossa missão é realizar estudos empíricos de alta qualidade sobre questões cruciais que afetam a gestão e a segurança de informações individuais e empresariais sensíveis.

Como membro do **CASRO, Conselho norte-americano de empresas de pesquisa**, observamos normas rígidas de confidencialidade de dados, privacidade e ética em pesquisa. Não coletamos informações pessoalmente verificáveis de indivíduos (ou, em pesquisas corporativas, nenhuma informação que identifique a empresa). Além disso, seguimos rígidos padrões de qualidade para garantir que os sujeitos não tenham que responder perguntas alheias ao tema, irrelevantes ou impróprias.