Seis regras para o gerenciamento efetivo de riscos da TI e de reputação

Como gerenciar riscos da TI e de reputação para proteger e melhorar o valor da marca e seu posicionamento competitivo

Implicações do IBM Global Reputational Risk and IT Study de 2013

Sobre o estudo

O IBM Global Reputational Risk and IT Study é um dos maiores estudos já realizados para examinar a relação entre riscos da TI e de reputação.

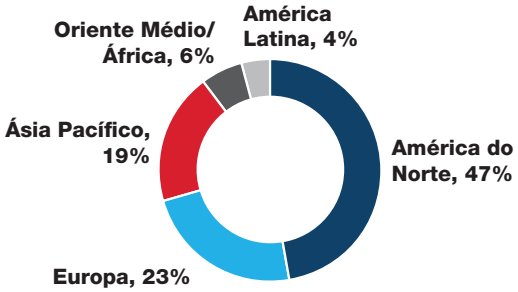
O grupo inicial de 427 entrevistados participou de uma pesquisa realizada pela Economist Intelligence Unit em nome da IBM. 175 entrevistados adicionais participaram do estudo online em um website IBM.

Todos os participantes responderam a questões elaboradas especialmente para fornecer um quadro detalhado da relação entre riscos de reputação e da TI nos negócios atuais.

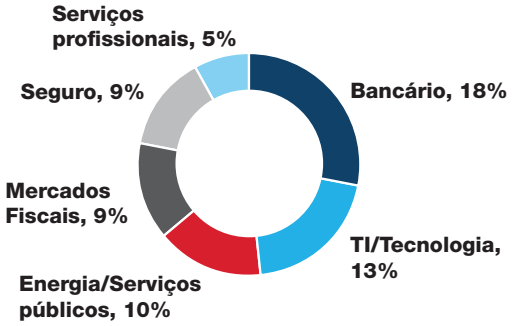
Gostaríamos de agradecer a todos os executivos que participaram da pesquisa por seu tempo e insights valiosos.

Para uma análise detalhada dos resultados da pesquisa, certifique-se de ler o relatório IBM Global Reputational Risk and IT Study de 2012

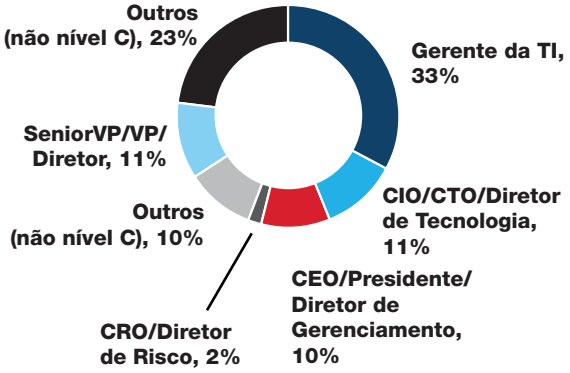
Entrevistados: 602



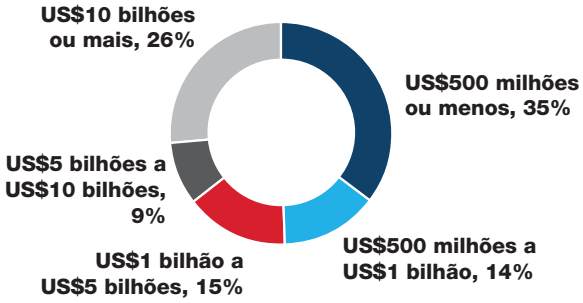
Segmentos de mercado: 23*



Cargos: 15*



Tamanho das empresas: 5



*Principais categorias das respostas exibidas

A relação entre os riscos de reputação e a TI

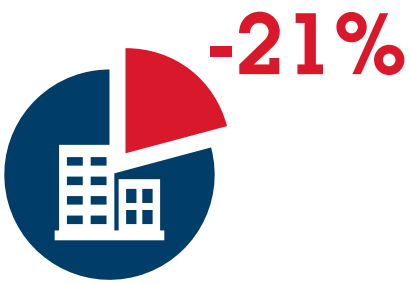
Quando, em 2005, o mundo corporativo começou a prestar atenção no conceito de riscos de reputação,[1] o foco das organizações centrava-se nas questões de negócios, tais como a conformidade e os delitos financeiros. Atualmente, como evidenciado pelos resultados do IBM Global Reputational Risk and IT Study, o foco foi alterado para incluir os impactos na reputação dos riscos da TI.

Virtualmente, toda empresa é dependente de tecnologia para interações e processos essenciais de negócios. Enquanto uma falha da TI pode levar de 10 minutos a 10 horas para se recuperar, o impacto na reputação pode ser sentido por meses ou mesmo anos.

Fatores fortemente afetados pelo risco da TI

O prejuízo na reputação causado por falhas da TI, como a violação de dados, as falhas de sistema e a perda de dados, possui agora uma etiqueta de preço. De acordo com análise realizada pelo Ponemon Institute, o valor econômico de reputação de uma empresa diminui em uma média de 21% como um resultado de uma violação da TI de dados de cliente – ou o equivalente a uma média de US$332 milhões. [2]

O custo real dos danos à reputação



O valor econômico de reputação de uma empresa diminui a uma média de 21% como um resultado de uma violação da TI de dados do cliente.

Fonte: Ponemon Institute[2]

A questão, agora, não é se os riscos da TI afetam sua reputação corporativa, mas sim, o que se pode fazer para prevenir e reduzir efetivamente esses riscos. Contando com as melhores práticas das principais empresas do IBM Global Reputational Risk and IT Study e com o conhecimento dos especialistas de gerenciamento de risco da TI da IBM, esse artigo fornece conselhos práticos e recomendações que lhe permitirão, junto com outros em sua organização, avaliar o gerenciamento de risco da TI e de reputação com um novo olhar crítico e informado e realizar as alterações necessárias para proteger a valiosa reputação da sua empresa.

Seis regras para o gerenciamento efetivo de riscos da TI e de reputação

Uma análise das respostas do estudo da IBM revelou correlações distintas entre as iniciativas tomadas pelas organizações de forma a proteger suas reputações de ramificações de falhas da TI e a eficácia geral de seus esforços de gerenciamento de riscos da TI e de reputação.

Com base nessa análise e no padrão que se revelou entre as organizações mais confiáveis em suas habilidades para prevenir e reduzir o risco de reputação relacionado à TI, há seis iniciativas chave que a IBM recomenda como parte dos esforços de toda empresa:

1. Colocar alguém no comando. A responsabilidade de decisão para o risco de reputação, incluindo itens relacionados à TI, deve recair sobre uma pessoa.

2. Estabelecer a relação entre a conformidade e a reputação. É essencial confrontar as estratégias de gerenciamento de riscos de reputação e da TI com os requisitos de conformidade.

3. Reavaliar o impacto da mídia social. Além de reconhecer o seu potencial para o impacto negativo de reputação, a mídia social deve se alavancada em prol dos seus atributos positivos.

4. Manter-se alerta quanto a sua cadeia de fornecedores. As organizações devem exigir e verificar a adesão aos padrões corporativos dos fornecedores terceirizados.

5. Evitar a complacência. As organizações devem avaliar continuamente os resultados de gerenciamento de risco da TI e de reputação em relação à estratégia de encontrar e eliminar lacunas potenciais.

6. Financiar correções; investir em prevenção. Para melhor mitigar o risco de reputação, as empresas necessitam financiar os sistemas de TI críticos como parte de seus negócios essenciais.

Qual a importância do risco de reputação?

O risco de reputação refere-se à possibilidade de sua empresa perder potencial ou negócios existentes devido à sua confiabilidade ter sido contestada. Participantes de um estudo recente do Ponemon Institute estabeleceram valores econômicos para suas marcas ou reputação corporativas, variando de menos de US$1 milhão para mais de US$10 bilhões, com a média aproximando-se de US$1,56 bilhões.[3]

Muitas empresas atribuem alto valor à reputação corporativa e à sua proteção e seus relatórios anuais contêm seções especiais tratando desse tópico. Com a difusão do uso das mídias sociais e de outras fontes de notícias e de comunicação instantâneas, a reputação de uma empresa nunca esteve tão vulnerável.

Coloque alguém no comando

Quando se pedia para escolher os três cargos mais responsáveis para gerenciar o risco de reputação, uma nítida maioria (80%) dos entrevistados no IBM Global Reputational Risk and IT Study escolhia o CEO (Chief Executive Officer). Atribuíram-se responsabilidades também ao CFO (Chief Financial Officer), ao CIO (Chief Information Officer), ao CRO (Chief Risk Officer) e ao CMO (Chief Marketing Officer), embora em números significativamente menores.

Qual é a principal preocupação do nível C?

CEO	Falha na conformidade
CIO	Tempo de inatividade e integridade de dados
CRO	Medidas insuficientes de recuperação de desastre
CFO	Impacto financeiro dos riscos da TI
CMO	Reputação da marca
CISO	Violação de dados e segurança cibernética
Chief Digital Officer	Risco de reputação

Embora a maioria das organizações atribua a responsabilidade por risco de reputação ao CEO, esta talvez não seja uma escolha eficaz. Os CEO já possuem uma série de responsabilidades; a consequência de se adicionar o risco de reputação a eles pode comprometer a atenção diária e detalhada que é requerida. O CRO pode ser uma opção melhor para muitas organizações e já faz parte do nível C em muitas organizações financeiras.

Porém, visto que as responsabilidades do CRO geralmente abrangem as fontes de riscos tradicionais, bem como os novos riscos relacionados à TI, o CRO pode ainda não ter os recursos necessários para conceder ao risco de reputação a atenção que merece.

Empresas de visão vanguardista estão começando a nomear os CDO (Chief Digital Officers). O CDO é o responsável por todo e qualquer aspecto relacionado à presença digital da empresa. Acrescentando um CDO ao nível C, damos ao risco de reputação e da TI a ênfase e a prioridade essenciais no atual mundo conduzido pela tecnologia.

O surgimento do Chief Digital Officer

Responsável por qualquer aspecto relacionado à presença digital de uma empresa, o CDO está na linha de frente dos esforços de gerenciamento de riscos de reputação e da TI de uma organização.

O CDO é um membro relativamente recente do nível C e muitas empresas já nomearam alguém para essa posição. Aquelas que nomearam um CDO escolheram, geralmente, um indivíduo de dentro da organização que possuía um forte conhecimento de tecnologia e de negócios. O CIO e o CMO estão geralmente no topo da pequena lista de candidatos.

Prevê-se que, como a conscientização e a preocupação acerca do risco de reputação e da TI continuam aumentando, o CDO fará parte do nível C para um número significativo de organizações.

Estabeleça a relação entre a conformidade e a reputação.

A conformidade é geralmente vista como um risco discreto e separado, com o CFO detendo a responsabilidade pelos processos e estratégias envolvidos. Na realidade, a conformidade e a reputação estão intrinsecamente ligadas – como atestam as notícias recentes e os preços das ações.

Os riscos da TI também possuem um grande papel a ser desempenhado na conformidade. Por exemplo, no estudo da IBM, 87% dos entrevistados do segmento bancário disseram que as falhas da TI apresentam consequências graves para a conformidade, especialmente o arquivamento e a proteção de dados que são essenciais para responder eficientemente às exigências legais ou regulatórias.

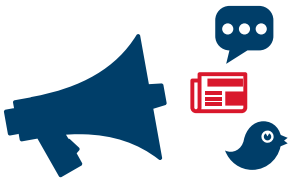
Reavalie o impacto da mídia social

A mídia social acrescentou uma dimensão inteiramente nova para avaliar e gerenciar o risco de reputação. No passado, eles eram avaliados e mitigados com base na sua probabilidade e no seu potencial impacto (2 dimensões). Agora, graças à mídia social, a equação do risco de reputação necessita levar em consideração a velocidade (terceira dimensão).
No mercado conectado atual, os clientes e outras partes interessadas ficam sabendo dos incidentes de reputação relacionados à TI quase que instantaneamente.
A resposta de uma empresa precisa ser igualmente imediata.

Entretanto, o impacto da mídia social sobre a reputação de uma organização não é completamente negativo. A mídia social fornece valiosos novos canais para o envolvimento do cliente, o que é essencial para melhorar a reputação de uma empresa. A mídia social também pode ser utilizada como uma fonte de informações instantâneas para clientes e funcionários em caso de um evento de reputação relacionado à TI, ajudando a reduzir as repercussões daquele e até mesmo a reconstruir a reputação.

O risco de reputação precisa ser avaliado em três dimensões

Probabilidade	**1** em **7**? **1** em **100**?
Impacto	**Grave** Moderado Leve
Velocidade	NOVO



Uma estratégia robusta de risco da TI e de reputação necessita reconhecer o poder de reputação da mídia social e requer táticas para alavancá-la para proteger e melhorar a reputação da empresa.

Mantenha-se alerta quanto à sua cadeia de fornecedores

A cadeia de suprimentos de uma empresa – incluindo vendedores, parceiros e fornecedores terceirizados – é geralmente o seu elo de reputação mais fraco. Apenas 28% dos entrevistados para o IBM Global Reputation and IT Risk Study, por exemplo, indicaram que eles, muito categoricamente, exigem às suas cadeias de suprimentos a aplicação do mesmo nível de controle de risco da TI que suas empresas fazem internamente.

"Uma entrega importante estava no laptop de um contratante, e ele foi roubado. Perdemos o prazo de um cliente importante e perdemos os arquivos fonte de todo o trabalho."

– Chief Marketing Officer, empresa de ensino americana

As implicações de reputação nos relacionamentos das cadeias de suprimentos são duas. Na primeira, os dados corporativos confidenciais que são compartilhados com terceiros podem estar comprometidos se estes não tiverem proteções robustas de resiliência e segurança da TI no local. Na segunda, os principais fornecedores que não protegerem adequadamente os seus próprios sistemas e dados podem ter um nível muito alto de tempo de inatividade, levando a interrupções nos ciclos de produção ou na disponibilidade do produto, o que reflete negativamente tanto na corporação quanto no parceiro.

Para serem mais efetivas, as organizações não só precisam exigir que seus parceiros alcancem seus níveis de gerenciamento de risco de reputação e da TI, mas também precisam verificar a adesão a esses padrões por meio de auditorias regulares e de outros métodos de apresentação de relatórios.

Evite complacência

A análise cruzada das respostas do estudo revelam que as empresas, em geral, estão mais confiantes do que mostra a realidade nas suas habilidades de gerenciar o risco de reputação relacionado à TI – estão com brechas e despreparadas aos danos de reputação não previstos por elas.

Enquanto 62% dos entrevistados do estudo classificaram a habilidade geral de gerenciar riscos da TI como forte ou muito forte, uma porcentagem significativa também relatou a falta de ferramentas básicas de gerenciamento de risco, como a proteção de firewall, o controle de identidade e de acesso, os testes regulares de invasão e o acesso às mais recentes inteligências de segurança.

Empresas não possuem medidas essenciais para mitigação dos riscos da TI

57% das empresas não estão realizando testes de invasões

63% das empresas não possuem acesso à inteligência de segurança mais recente

Todas essas ferramentas básicas de gerenciamento de risco da TI devem estar em vigor em todas as empresas, já que representam o mínimo necessário para gerenciamento de risco de reputação e da TI. Particularmente, testes de invasões e acesso à inteligência de segurança mais recente apresentam uma baixa taxa de implementação. Sem testes de invasões constantes, uma organização não consegue saber quão seguras estão as interações entre os funcionários e entre a empresa e seus clientes. Sem acesso à inteligência de segurança mais recente, uma organização pode deixar seus dados de negócios mais críticos expostos a hackers ou malwares sem saber que existe uma ameaça.

É absolutamente essencial que a estratégia de gerenciamento de risco de reputação e da TI de uma organização mapeie táticas de implementação mensuráveis e concretas. Organizações também devem desempenhar análises regulares de lacunas para garantir que tanto estratégias como táticas evoluam para abordar os riscos em constante mudança.

Retificação de verbas; invista em prevenção

A maioria dos entrevistados no IBM Global Reputation and IT Risk Study relatou como adequados tanto o volume de financiamento da TI atual alocado para gerenciamento de risco de reputação quanto os aumentos antecipados em financiamento. Entretanto, este pode ser outro exemplo de complacência.

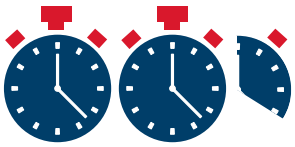
Quando organizações reportam uma grande habilidade de gerenciar riscos da TI, mas não possuem as ferramentas de gerenciamento básicas, é possível inferir que o que está sendo relatado como adequado pode ser, na verdade, inadequado. Quando o CIO não é parte integral do processo de gerenciamento de risco de reputação, a organização pode não ter uma ideia clara do quanto inadequados são seus processos e controles.

Custo do tempo de inatividade do sistema

US$181.770

por hora

Custo do tempo de inatividade do datacenter



US$418.017

por evento

Custo de um evento de interrupção de negócios

Fonte: The Aberdeen Group[4]

Ao determinar qual é de fato o financiamento da TI adequado, as organizações também precisam considerar os custos de um financiamento inadequado – prevenção versus cura. O Aberdeen Group relata que o custo de uma hora de tempo de inatividade de um datacenter para uma organização típica do segmento é de US$181.770, e o custo total de um evento de interrupção de negócios é de US$418.017.5 Multiplique isso por uma média de 2,3 eventos por ano e o custo chega a quase US$1 milhão.

"Subestimar o custo de risco de reputação excede muito o custo de proteção. Pró-ação é preferível à reação."

– Diretor de finanças de um banco norte-americano

As organizações precisam tratar sistemas de TI críticos como parte de seus negócios principais, e não como centros de custos cujo financiamento pode crescer ou diminuir de acordo com a necessidade de investir em outra parte do negócio. A TI contribui comprovadamente para a reputação positiva de uma empresa – e falhas da TI podem causar danos de reputação significativos. Esforços de gerenciamento de risco da TI completamente financiados e investimentos na viabilidade contínua desses esforços podem prevenir a perda de milhões de dólares na renda quando apenas uma falha da TI é evitada. Além disso, a redundância e a diversidade podem eliminar pontos únicos de falhas e aumentar os resultados gerais do controle de risco de reputação.

Os benefícios da terceirização

Pesquisas recentes conduzidas pela Forrester Consulting para a IBM examinaram as razões pelas quais um número crescente de organizações está utilizando terceirização ou parceiros de serviços gerenciados para gerenciar seus esforços de segurança e resiliência da TI e o resultado dessa decisão.

Enquanto os custos permanecem o principal fator motivador na decisão de terceirizar, organizações que terceirizam gerenciamento de risco de reputação e da TI estão percebendo benefícios adicionais, incluindo ROI mais rápido, cobertura 24 horas, acesso consistente a habilidades especializadas e – talvez o mais importante – testes mais frequentes e bem-sucedidos. Na verdade, organizações de TI que terceirizam gerenciamento de risco de reputação e da TI frequentemente descobrem que estão mais confiantes com sua habilidade de prevenir problemas que afetam a reputação corporativa.

Outro benefício importante, mas frequentemente negligenciado, da terceirização: prioridade, foco e financiamento para não ser transferido para outros projetos com urgência imediata, mas com menor importância geral para a empresa. Organizações menores, em particular, devem considerar terceirizar gerenciamento de risco de reputação e da TI. Além de economizar dinheiro, a terceirização pode fornecer à organização conhecimento e recursos, o que seria impossível de replicar internamente.

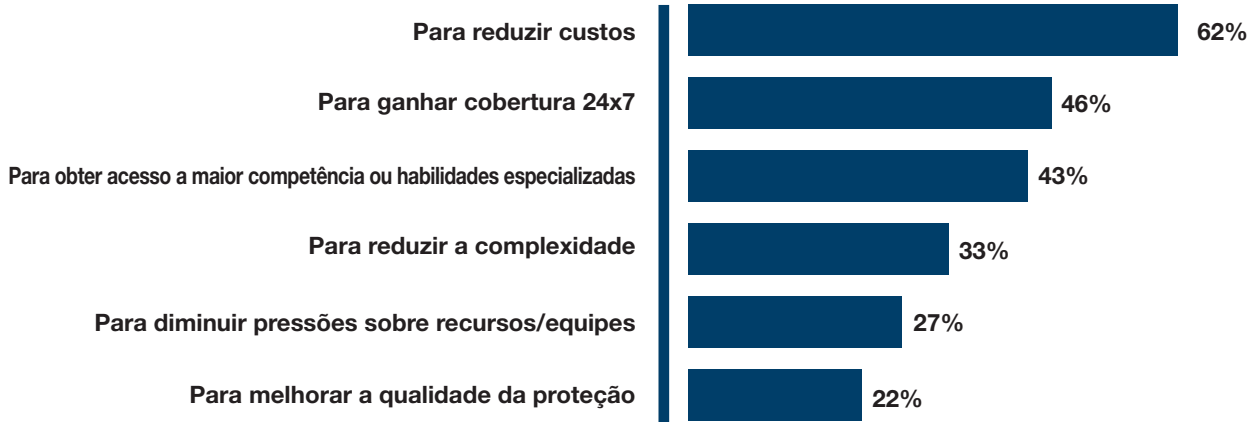
O valor de um olhar objetivo

Uma consultoria externa pode fornecer uma visão objetiva e completa do risco de reputação e da TI que pode estar faltando atualmente nas organizações.

Um consultor experiente pode tratar de:

- **Falhas de responsabilidade**
- **Falhas estratégicas e táticas**
- **Viabilidade das estratégias atuais**
- **Integração do gerenciamento de risco da TI com estratégias gerais de gerenciamento de risco de reputação**

Por que as organizações estão terceirizando a TI?



Fonte: Forrester Consulting[6]

Como a IBM pode ajudar

Quando planejada e implementada de maneira eficiente, sua estratégia de risco de reputação e da TI pode se tornar uma vantagem competitiva vital. Quando você se protege e minimiza o risco de reputação com sucesso, é possível aprimorar o valor da marca sob o olhar de clientes, parceiros e analistas. Além disso, sua organização pode melhor atrair novos clientes, manter clientes existentes e gerar maior renda.

A IBM pode ajudá-lo a proteger sua reputação com um robusto portfólio de segurança da TI, continuidade e resiliência de negócios e soluções de suporte técnico. Você pode começar com a avaliação de risco de segurança da TI ou com um teste de invasão realizada por especialistas da IBM. Para continuidade e resiliência de negócios, é possível começar com o workshop CORE (Continuous Operations Risk Evaluation) e continuar com os serviços de resiliência com base em nuvem. Nossas soluções de suporte técnico alcançam desde suporte de software básico até suporte técnico personalizado.

O que torna as soluções IBM eficientes é nosso alcance global com um toque local. Isso inclui:

- Mais de 160 centros de resiliência de negócios em 70 países; mais de 50 anos de experiência
- Mais de 9.000 clientes que se recuperaram de desastres, com a IBM fornecendo 100% de recuperação para clientes que declararam um desastre
- Uma rede global de 33 centros de operações de segurança, pesquisa e de desenvolvimento de soluções; 133 países monitorados
- 15.000 pesquisadores, desenvolvedores e especialistas no assunto trabalhando em iniciativas de segurança em todo o mundo.

Avalie seus esforços de risco de reputação e da TI

Sua organização está exposta, ciente ou capaz? Responda algumas perguntas e a ferramenta online fácil e rápida da IBM fornecerá uma avaliação geral de seus esforços de gerenciamento de risco de reputação e da TI, juntamente com a pontuação nas principais categorias e sugestões para melhorias. ibmriskindex.com

Para mais informações

Para saber mais sobre como a IBM pode auxiliar na reputação de sua empresa ao fortalecer o gerenciamento de risco da TI, entre em contato com o seu representante IBM ou com seu Parceiro de Negócios IBM, ou acesse os sites:

Para saber mais sobre o IBM Global Reputational Risk and IT Study
ibm.com/services/riskstudy

Para utilizar o Reputational Risk and IT Index para avaliar seus esforços, acesse:
ibmriskindex.com

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo – SP
Brasil

A home page da IBM pode ser encontrada em:
ibm.com

[1] Pesquisa do Google Trends para "reputational risk," em fevereiro de 2012.

[2,3] "Reputation Impact of a Data Breach: U.S. Study of Executives & Managers," patrocinado pela Experian® Data Breach Resolution Ponemon Institute, novembro de 2011.

[4,5] "Datacenter Downtime: How Much Does It Really Cost?" Aberdeen Group, fevereiro de 2012.

[6] "The Convergence of Reputational Risk and IT Outsourcing, " Forrester Consulting, setembro de 2012.

Por favor, recicle.

RLW03018-BRPT-01