Risco para Reputação Corporativa e TI

Como a continuidade de negócios, o suporte técnico e a segurança possibilitam moldar a reputação e o valor de sua empresa

Considerações do Estudo

IBM Global Reputational Risk and IT de 2012

Risco para reputação corporativa e TI:

Como a segurança, a continuidade de negócios e o suporte técnico podem moldar a reputação e o valor de sua empresa é um estudo da IBM que investiga como as organizações pelo mundo estão gerenciando suas reputações na atual era digital. A TI é parte integral da organização e falhas nesta área podem resultar em dano à imagem das empresas. Este relatório foi criado pela Economist Intelligence Unit, que também realizou a pesquisa online e realizou entrevistas em nome da IBM.

Gostaríamos de agradecer a todos os executivos que participaram da pesquisa e concederam entrevistas, por seu tempo e insight valiosos.

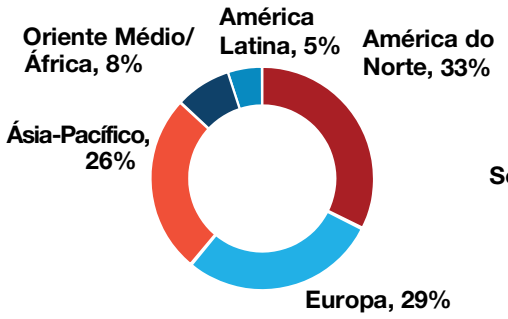
Sobre a pesquisa

A pesquisa, realizada em junho de 2012 pela Economist Intelligence Unit, incluiu respostas de 427 executivos seniors de todo o mundo. Dos quais 42% são executivos em cargos de chefia.

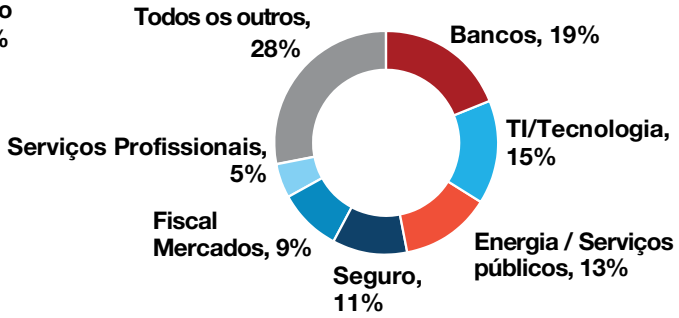
As empresas com receita menor que 500 milhões de dólares correspondem a 37% dos entrevistados e 52% são empresas com receita de mais de 1 bilhão de dólares. A pesquisa engloba diversos segmentos de mercado, incluindo bancos (19%), TI e tecnologia (15%), energia e serviços públicos (13%), e seguro (11%).

Economist Intelligence Unit | The Economist

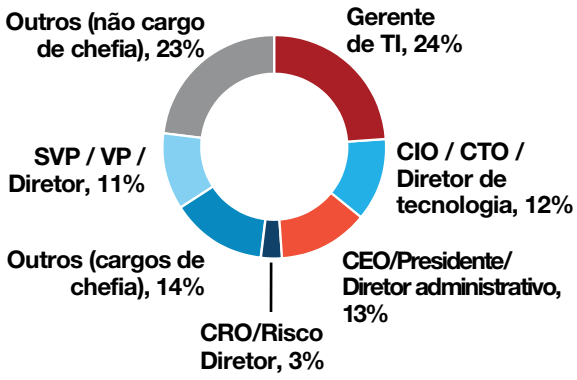
Entrevistados: 427



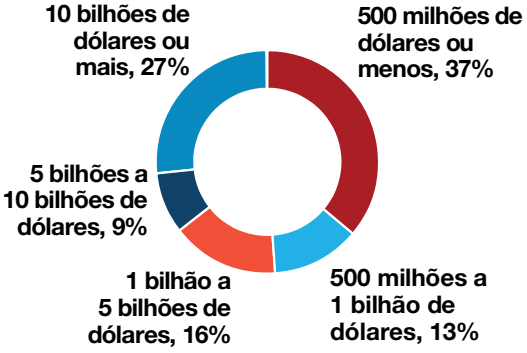
Segmentos de mercado: 23*



Cargos: 15*



Tamanho das empresas: 5



*Principais categorias de entrevistados

A pesquisa do estudo IBM Global Reputational Risk and IT de 2012, realizada pela Economist Intelligence Unit, reuniu informações de 427 executivos de nível sênior de todo o mundo.

Uma reputação impecável

Os líderes de negócios normalmente têm uma boa compreensão do valor da reputação de suas organizações. Uma reputação forte gera confiança para as partes interessadas. Se uma empresa é confiável, os clientes comprarão e recomendarão seus produtos; possíveis investidores e funcionários desejarão fazer parte dela; e comunidades acolherão suas operações.

Entretanto, a triste realidade é que as reputações corporativas estão se tornando cada vez mais difíceis de gerenciar na era digital e elas podem ser facilmente prejudicadas por diversos fatores – entre eles as falhas de TI. Com sites de mídia social como o Facebook e o Twitter com mais de 950 milhões e 500 milhões de usuários respectivamente, existe agora uma alternativa altamente visível e imediata para as comunicações de uma empresa no que diz respeito à sua reputação.

Em resposta, mais organizações têm introduzido o risco reputacional como uma categoria distinta em suas estruturas de gerenciamento de risco corporativo. Nossa pesquisa mostra que as empresas começarão a prestar mais atenção às relações entre falhas de TI e danos reputacionais. Agora, elas notam como os executivos tentam proteger suas marcas do que poderia discutivelmente ser chamado de "um erro previsível".

Com base neste estudo com 427 executivos de nível sênior de todo o mundo, três forças principais suportam as reputações corporativas: provisão do melhor produto ou serviço possível, envolvimento do cliente e status de parceiro confiável. Considerando como as empresas têm se tornado cada vez mais dependentes da tecnologia para cumprir com todos os três – sem mencionar a administração dos negócios – o consenso é claro: o risco de TI pode prejudicar a produtividade das empresas, as relações com o cliente e consequentemente a confiança.

"A TI é como o coração que bombeia sangue para todo o corpo, por isso, qualquer falha pode ameaçar a sobrevivência de toda a organização".

– Gerente de TI, empresa francesa de TI e tecnologia

A falha na continuidade de negócios é um dos riscos relacionados à TI mais prováveis de prejudicar as reputações corporativas. Entretanto, o estudo descobriu que outras ameaças de TI – que não necessariamente interrompem as operações – são consideradas tão ou mais perigosas que a continuidade de negócios na lista de fatores de riscos reputacionais. Em especial, os executivos consideram o roubo de dados/cibercrime como sendo a ameaça mais perigosa, muito mais que as falhas de sistema. As tecnologias emergentes, como a nuvem, o Bring Your Own Device (BYOD) e as mídias sociais tornam o problema mais complexo. O controle sobre estas novas tecnologias é menor do que outras ameaças de TI, pois as organizações não tiveram tempo para se adaptar totalmente a elas e, no caso de BYOD e mídia social, porque elas estreitam o limite entre ferramentas pessoais e profissionais.

Jaideep Jain, um parceiro de negócios de TI com uma empresa global de mercadorias de consumo na Índia disse que grandes empresas, em especial, têm sido relativamente lentas na adoção de tecnologias como a nuvem e o BYOD. "Estas ameaças são compreendidas, mas não temos dados para quantificar os riscos. Além disso, pelo fato de estarmos nos aproximando destas tecnologias com cautela, a chance de ocorrer um incidente é baixa". Ademais, o Sr. Jain acrescenta que é preciso que haja um incidente ou uma adversidade em um teste de invasão para realmente voltar o foco a uma nova vulnerabilidade de TI.

Este relatório descreve como as organizações do mundo todo estão buscando proteger suas reputações ao se adaptar às mudanças atuais do ambiente de negócios e do panorama de TI.

Prevenção

Os executivos passaram a acompanhar mais de perto as implicações reputacionais das falhas de TI. Os entrevistados no estudo disseram que a TI exerce uma influência particularmente forte na satisfação do cliente, na conformidade e na reputação da marca (ver Figura 1).

Figura 1. Percentual de entrevistados que consideram elementos de negócios "muito" afetados pelos riscos de TI.

Os executivos também identificaram três responsabilidades fundamentais da função de TI em que os riscos reputacionais são maiores:

- Segurança (84%)
- Continuidade de Negócios (77%)
- Suporte Técnico (68%)

É fácil entender por que os executivos acreditam que a segurança está mais fortemente relacionada ao risco reputacional do que as funções de TI como continuidade de negócios ou suporte técnico. Suponhamos, por exemplo, que um banco de dados de clientes de uma empresa seja violado e os números de cartão de crédito dos clientes tenham sido roubados. A reputação desta empresa certamente seria afetada. De maneira similar, os entrevistados no estudo indicam que o roubo de dados/cibercrime (61%) é uma ameaça reputacional maior que falhas no sistema (44%), o que reforça a visão de que a segurança é preocupação mais importante para os executivos atualmente (ver Figura 2).

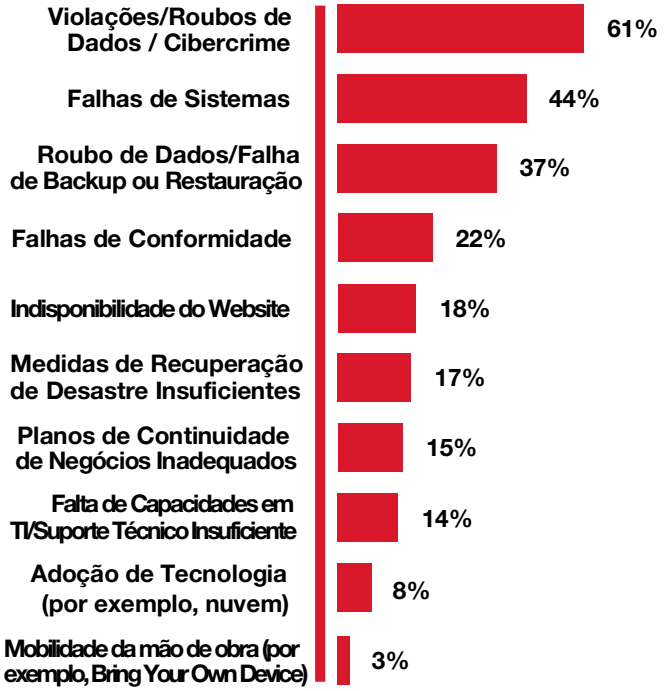


Figura 2. Riscos de TI de maior ameaça à reputação.

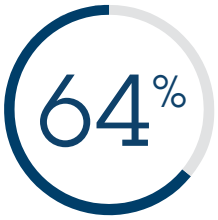
Embora o suporte técnico ocupe o terceiro lugar entre as principais responsabilidades de TI em termos de possível ameaça à reputação de uma empresa, ele ocupa o primeiro lugar na lista de falhas com tempo de recuperação de seis a 24 meses. Apenas 12% dos entrevistados disseram que eles tiveram falhas graves de suporte técnico recentes, mas a intensidade do risco é elevada pelos tempos de recuperação relativamente longos após um incidente desta natureza. A intensidade do risco pode ser ainda maior à medida que a empresa adota novas tecnologias como a nuvem e as mídias sociais.

"Subestimar o custo do risco reputacional sai muito mais caro do que o custo da proteção. É melhor ser proativo do que reativo".

– Gerente de TI, empresa de energia e serviços públicos dos EUA.

Um dos problemas identificados pelas descobertas do estudo é que muitas empresas adotam uma abordagem reativa ao gerenciamento de risco de TI. Normalmente, eles dedicam recursos a riscos como roubo de dados e cibercrime, falhas de sistema e falhas no backup de dados em que ocorreram falhas graves no passado. Entretanto, eles prestam menos atenção a riscos emergentes que ainda não causaram danos graves à reputação.

No entanto, os executivos estão tentando enxergar além do retrovisor. Dentre aproximadamente dois terços dos entrevistados no estudo que disseram que suas empresas se concentrarão mais em gerenciar sua reputação no futuro, quase a metade (43%) afirmou que isso é impulsionado pelo crescimento da tecnologia e da mídia social, enquanto apenas 20% citaram experiências adversas anteriores como o principal fator. As empresas não só estão mais preocupadas em encontrar pontos cegos em sua estrutura de gerenciamento de risco, mas também estão dedicando os recursos necessários para suportar seu gerenciamento de risco de TI. Três quartos dos entrevistados disseram que seu orçamento em TI aumentará nos próximos 12 meses devido às preocupações com reputação e 18% disseram que o aumento será de mais de 20%. Segundo um entrevistado no estudo dos EUA, "Subestimar o custo do risco reputacional sai muito mais caro do que o custo da proteção. É melhor ser proativo do que ser reativo".



dizem que sua empresa se concentrará mais em gerenciar sua reputação no futuro

dos entrevistados disseram que seu orçamento em TI aumentará nos próximos 12 meses devido às preocupações com reputação

Indo mais adiante, a avaliação de possíveis pontos cegos e novas tecnologias provavelmente será acelerada pelo uso de casos de estudo e análise de cenários ao invés de esperar por um incidente direto. "Para usar novas tecnologias como a nuvem, é preciso confiança", disse Andrea MacIntosh, diretora de qualidade da Alpha Technologies na Colúmbia Britânica, Canadá. "Como você cria confiança? Demonstrando desempenho ou vendo como organizações comparáveis estão usando-a com sucesso. Acho que há muitos dados de referência para empresas como a nossa, mas como qualquer tecnologia nova, é preciso ser cauteloso".

Cinco características de empresas altamente confiáveis.

Para fins deste estudo, uma organização "bem sucedida" é uma em que os entrevistados identificaram como tendo uma reputação "excelente". Curiosamente, apenas 30% incluíram suas próprias empresas nestes termos. Não obstante a propensão inerente ao processo de autoavaliação, uma análise do desempenho reputacional relativo revela que estas organizações compartilham uma abordagem comum de relacionar fortes capacidades de gerenciamento de risco em TI com uma compreensão sólida de como riscos específicos nesta área podem ameaçar a reputação. Embora esta lista não seja detalhada, estas características foram classificadas na seguinte lista de cinco fatores essenciais para o sucesso.

1 Integração do Risco Reputacional e de TI

Notavelmente, uma grande maioria (83%) dos executivos que caracterizaram suas empresas como tendo excelente reputação disseram que sua empresa possui o gerenciamento integrado de risco reputacional e de TI (ver Figura 3). Ainda assim, o fato de que quase dois terços (64%) daqueles que avaliaram a reputação de suas firmas como igual ou pior do que a de seus concorrentes também disseram que a TI foi integrada ao gerenciamento de risco reputacional mostra que isso não é o suficiente para garantir o sucesso.

2 Mapeamento das Ameaças de TI para os Principais Elementos de Reputação

Organizações de sucesso percebem relações maiores entre ameaças de TI e os principais elementos de reputação. A correlação é especialmente forte entre a TI, a satisfação do cliente e a reputação da marca.

3 Forte Capacidade de Gerenciamento de Risco de TI

Aproximadamente 84% das empresas com excelente reputação disseram que possuem uma capacidade de gerenciamento de risco de TI forte ou muito forte (ver Figura 3). Isso se compara a menos de 30% das empresas com reputações descritas como igual ou pior que a de seus concorrentes. Conforme esperado, uma reputação excelente e capacidades fortes de gerenciamento de risco de TI também significam que a empresa sofre menos incidentes reputacionais graves. Por exemplo, em caso de roubo de dados/cibercrime, aproximadamente 80% dos entrevistados no estudo que avaliam o gerenciamento de risco em TI de sua empresa como "muito forte" dizem poder se recuperar em seis meses ou menos, comparados a quase metade daqueles com um gerenciamento de risco de TI "fraco".

4 Financiamento para o gerenciamento de risco de TI

Firmas bem-sucedidas possuem funções de gerenciamento de risco em TI bem financiadas (ver Figura 3). A proporção de entrevistados que afirmaram ter o financiamento adequado para o gerenciamento de risco em TI para sua empresa é de 78% para aqueles com reputações excelentes, 59% para aqueles com reputações muito boas e 36% para o restante.

5 Controle Rigoroso de Cadeia de Fornecimento

Firmas bem-sucedidas tem maior probabilidade do que outros para relatar que elas exigem rigorosamente que seus fornecedores e parceiros da cadeia de fornecimento obedeçam aos mesmos níveis de controle exigidos internamente (ver Figura 3). A proporção de entrevistados que disse fazer isso é de 58% para aqueles avaliados como excelente, 38% para os avaliados como muito bom e 33% para o restante.

Empresas maiores geralmente são mais bem equipadas que empresas menores para gerenciar riscos de TI. Isso explica a maior proporção de grandes empresas com reputações excelentes. Entretanto, organizações de todos os tamanhos tiveram sucesso em gerenciar os riscos de TI para contribuir na criação de excelentes reputações.

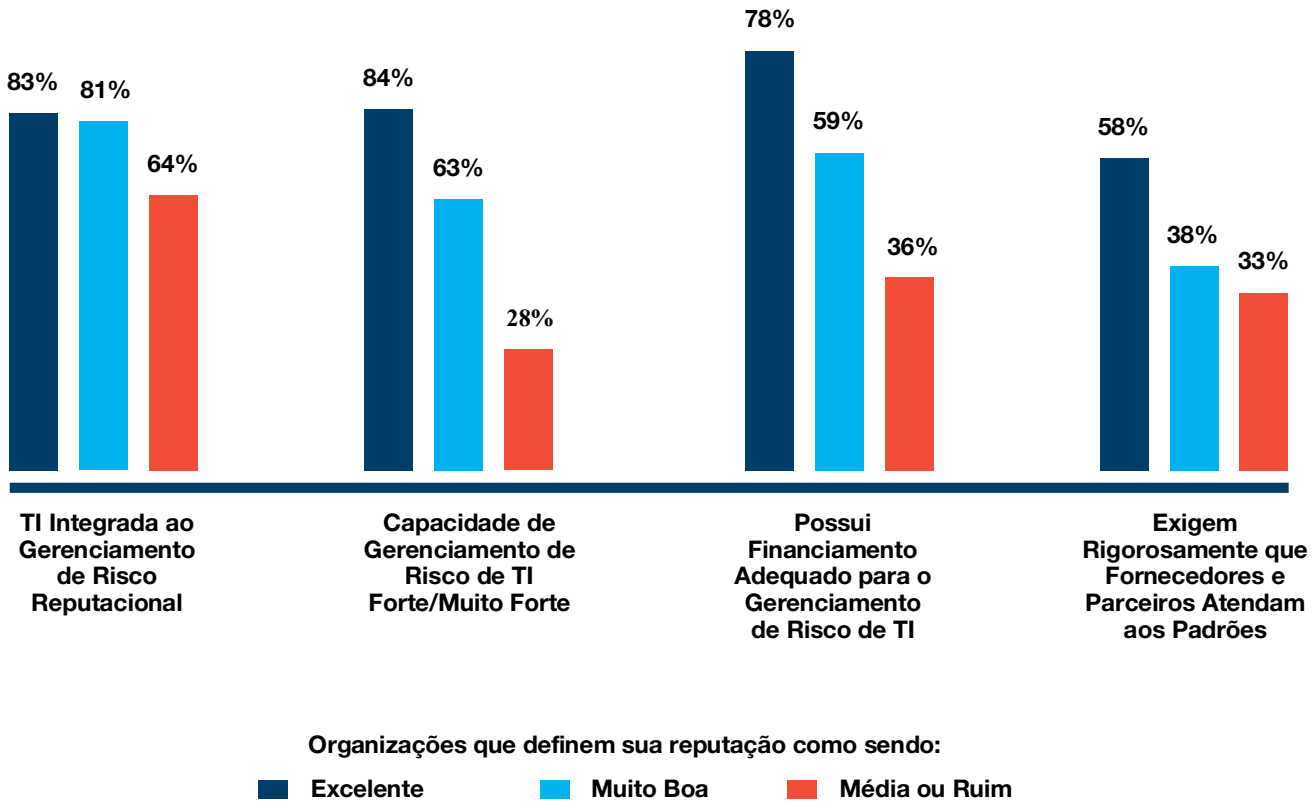


Figura 3. Elementos importantes de risco de TI e como eles são normalmente implementados por empresas com força reputacional variável. O estudo descobriu uma relação direta entre o financiamento de TI e o sucesso do gerenciamento de risco reputacional.

Muitas empresas insistem que suas cadeias de fornecimento fortalecem seus controles para gerenciar riscos reputacionais relacionados à TI. A proporção de executivos dizendo que suas empresas exigem rigorosamente dos fornecedores e parceiros o mesmo nível de controle varia de 67% para roubo de dados/cibercrime a 32% para riscos de mobilidade da mão de obra (ver Figura 4).

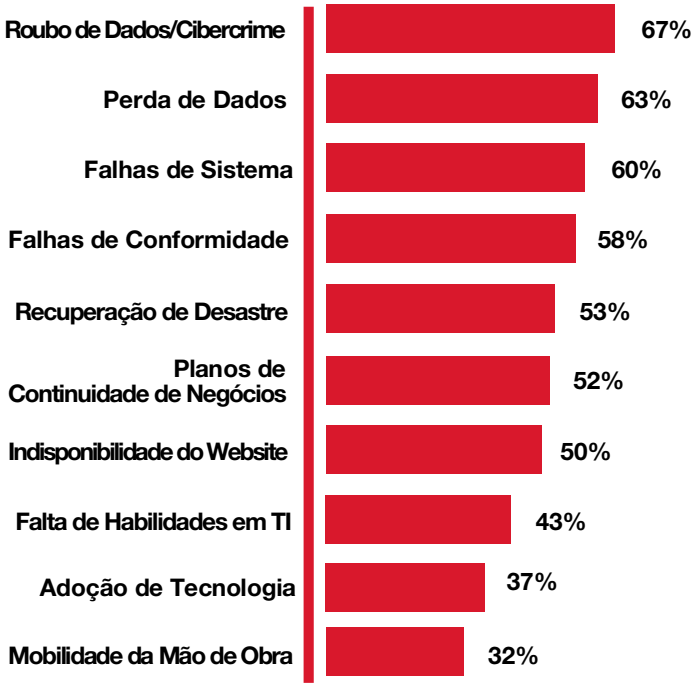


Figura 4. Percentual de entrevistados que exige rigorosamente de seus parceiros da cadeia de fornecimento a aplicação do mesmo nível de controle interno de risco em TI de suas organizações.

Andrea MacIntosh, cuja empresa fornece soluções industriais de energia, explica que a falha em uma das soluções de reserva de energia da Alpha pode possivelmente paralisar o serviço de telefonia de emergência de uma provedora de telecomunicações dos EUA, o que dispararia um desastre regulatório e de conformidade. Isso seria um caso de um produto da Alpha ocasionando uma falha de TI para um cliente. Se a Alpha tivesse uma falha de TI própria, que se tornasse amplamente conhecida (por meio de um blog sobre o segmento de mercado de energia), a Sra. MacIntosh disse que esse evento poderia ter um impacto na reputação da Alpha e "poderíamos perder a confiança de possíveis clientes". A Sra. MacIntosh afirma que o reconhecimento desta conexão está crescendo: "Estamos recebendo cada vez mais solicitações de nossos clientes por detalhes de nossa infraestrutura de TI e de segurança junto com auditorias in loco, como parte do processo de qualificação de fornecedor".

"Estamos recebendo cada vez mais solicitações de nossos clientes por detalhes de nossa infraestrutura de TI e de segurança junto com auditorias in loco, como parte do processo de qualificação de fornecedor".

– Andrea MacIntosh, Diretora de Qualidade, Alpha Technologies, Canadá

Abordagens de Cima para Baixo e de Baixo para Cima para Gerenciar Riscos Reputacionais Relacionados à TI

A grande maioria (mais de 80%) dos executivos em nosso estudo disse que o CEO é o maior responsável pela reputação de sua empresa, seguido pelo CFO (31%), pelo CIO (27%), pelo CRO (23%) e pelo CMO (22%). Particularmente, quase dois terços disseram que a responsabilidade é compartilhada entre mais de um cargo de chefia (ver Figura 5).

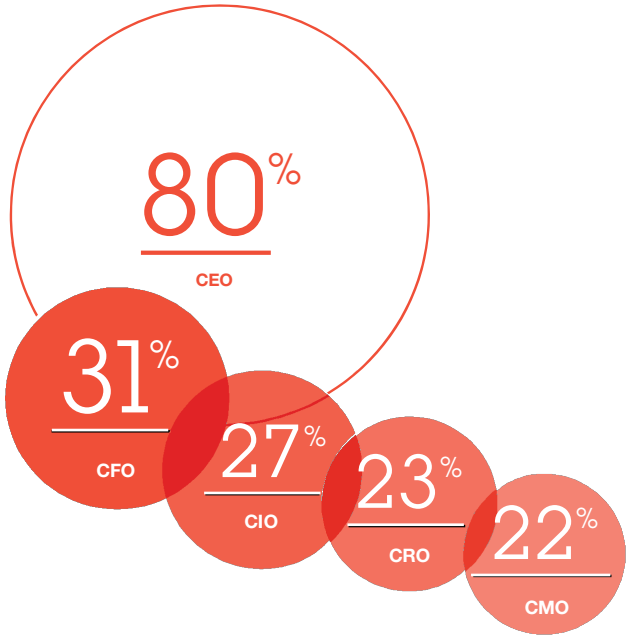


Figura 5. Quem controla? O CEO é o líder óbvio quando os entrevistados escolheram entre os três cargos mais altos com maior responsabilidade pelo gerenciamento do risco reputacional.

Isso é consistente com tendências mais amplas de maior responsabilidade nos cargos de chefia para o gerenciamento de risco integrado de toda a empresa. Em um estudo de 2011 [1] patrocinado pela IBM e realizado pela Economist Intelligence Unit (EIU), de 391 executivos de nível sênior, 71% dos entrevistados disseram que os executivos em cargos de chefia estavam "muito envolvidos" na estratégia geral de gerenciamento de riscos e 88% disse que esperavam aumentar este nível de envolvimento. Embora os executivos sugiram que as estratégias mais bem sucedidas aparecem quando gerentes de risco com especialidades diferentes colaboram para fornecer perfis de risco integrados ao gerenciamento sênior. Quase três quartos dos participantes do estudo disseram que as exposições aos riscos de TI são escaladas aos cargos de chefia de forma eficaz.

Um estudo[2] de 2005 da EIU descobriu que os gerentes de marketing têm pouca participação no gerenciamento do risco reputacional e que sua função era limitada em grande parte à função de comunicações como os "olhos e ouvidos" da empresa no que tange ameaças reputacionais. Conforme seguimos em direção aos resultados do estudo de 2012, quase um quarto dos entrevistados disseram que seu Diretor Executivo de Marketing é um dos três principais executivos corporativos responsáveis pela reputação da empresa. Esta expansão do papel da função do marketing sugere uma necessidade de maior colaboração entre os CIOs e os CMOs conforme as empresas empregam tecnologias para analisar milhões de dados de marketing que contêm insights ocultos sobre a reputação de uma empresa.

Protegendo a Reputação por meio da Comunicação

Enquanto os especialistas em TI são responsáveis pela recuperação técnica após um incidente, eles precisam trabalhar juntamente com seus parceiros de marketing, comunicações e relações públicas para se comunicar claramente com as partes interessadas após uma falha. Executivos de TI experientes dizem que estas mensagens precisam ser diretas e totalmente honestas, especialmente em um ambiente em que a mídia explora qualquer fraude corporativa. O Sr. Jain disse que a melhor proteção é criar uma reputação de ser transparente e se comunicar de forma eficaz com as partes interessadas. Em seguida, ele disse "Se houver um incidente, é importante reconhecer o engano e falar claramente como ele foi corrigido e o que está sendo feito no momento sobre o engano". Ele destacou que uma resposta rápida é essencial: "Se você demorar para se comunicar com o público, você permite que eles cheguem a conclusões próprias".

Comunicações para convencer as partes interessadas de que as causas de uma falha de TI foram solucionadas podem reduzir drasticamente o tempo necessário para restaurar a confiança, mas o dano que uma falha específica de TI pode causar às partes interessadas aumenta o esforço necessário. Por exemplo, indisponibilidade de websites podem causar pequenos inconvenientes aos clientes e são fáceis de explicar. Aproximadamente 78% dos entrevistados no estudo disseram que eles se recuperam de tais incidentes em menos de seis meses. Por outro lado, é necessário um tempo muito maior para se recuperar de danos reputacionais causados por cibercrimes, em parte pelo fato de estes causarem danos graves às partes interessadas e também por ser mais difícil passar a mensagem de que o problema foi totalmente solucionado.

Gerenciamento de Risco e a Mídia Social

A mídia social aparece com destaque em conversas entre executivos, tanto em entrevistas quanto em respostas ao estudo, sobre por que eles estão ficando cada vez mais preocupados com a proteção da reputação de suas empresas. Como as redes sociais são baseadas na tecnologia, há uma tendência a agregá-la aos riscos técnicos relacionados à TI. Entretanto, os canais de mídia social não são riscos por si só; pelo contrário, eles são amplificadores da reputação de uma organização (para melhor ou para pior). Isso significa que eles devem ser avaliados como parte da combinação geral de comunicação de uma organização.

"A comunidade [de mídia social] está falando sobre sua participação, e é preciso decidir que tipo de posição vai tomar. Do contrário, as pessoas o farão para você".

- David Boroevich, Vice Presidente de Marketing, Alpha Technologies, Canadá

As mídias sociais avançaram além de sua função inicial, que era permitir comunicações entre consumidores. Blogs voltados a negócios especializados e comunidades técnicas têm um impacto cada vez maior em empresas business-to-business (B2B). Na verdade, "social" pode não ser mais um termo adequado para descrever as interações ponto a ponto entre membros da comunidade. Em qualquer evento, a necessidade de mitigar

o possível dano reputacional causado pelas comunicações aceleradas é um desafio diferente de usar a mídia social eficazmente para envolver partes interessadas. Este estudo sugere que as estratégias para lidar com a questão ainda estão em estágio inicial. Apenas 19% dos entrevistados no estudo disseram que sua empresa possui um plano de recuperação de desastres que inclui o uso destas ferramentas de mídia social.

"Eu era cético quanto ao valor da mídia social em nosso negócio", disse David Boroevich, Vice Presidente de Marketing da Alpha Technologies, uma empresa B2B que oferece soluções industriais de energia. "Temos pessoas trabalhando nisso, mas pensamos que isso é mais um trabalho 'extra'; tem que fazer parte de nosso programa".

Ele acrescenta que, até mesmo em segmentos de mercado especializados, "a comunidade está falando sobre sua participação e é preciso decidir que tipo de posição vai tomar. Do contrário, as pessoas o farão para você".

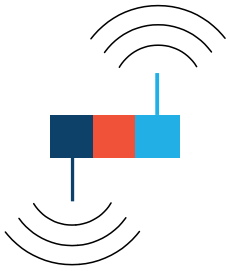
Melhores Práticas para Aperfeiçoar o Desempenho do Gerenciamento de Risco

Líderes de negócios interessados em aperfeiçoar o desempenho de seu gerenciamento de risco reputacional podem aprender com as melhores práticas identificadas pelos executivos que participaram deste estudo. As estratégias eficientes incluem:

- **Ser proativo e não reativo.** Estar preparado para investir no desenvolvimento de estratégias abrangentes de gerenciamento de risco reputacional que incluem controles robustos dos riscos de TI – especialmente daqueles relacionados à segurança, à continuidade de negócios e ao suporte técnico – bem como outros riscos reputacionais.
- **Criar uma organização em que os gerentes de TI colaborem com outros especialistas em gerenciamento de risco.** Juntos, eles deverão ser responsáveis por apresentar um perfil abrangente de todos os riscos reputacionais da empresa à alta gerência.
- **Faça análise de cenário, especialmente com tecnologia nova e emergente.** Não espere a ocorrência de um incidente. Existem diversos casos de estudo para serem usados como base para um planejamento hipotético.
- **Avalie os riscos em toda a cadeia de fornecimento.** Falhas por conta de um fornecedor em pós-produção pode ser tão catastrófico quanto um problema interno, e os controles de risco podem ser harmonizados entre os principais responsáveis. Da mesma forma, empresas de B2B devem colaborar com os clientes para assegurar que todos os riscos relevantes sejam bem gerenciados.

"A tecnologia é um amplificador para tudo, tanto para melhor quanto para pior. Se nós a usamos, temos que gerenciá-la rigorosamente".

- CIO, Empresa de serviços profissionais de Barbados



Conclusão

Organizações de todos os portes estão prestando mais atenção às ameaças provenientes do atual ambiente digital contra as suas reputações. Esta preocupação está refletida em abordagens para toda a empresa mais integradas ao gerenciamento de risco liderado pelos executivos em cargos de chefia e na maior atenção dada aos impactos diretos causados pelos riscos de TI. Estes incluem riscos gerados pelo uso de novas tecnologias. A segurança tem delimitado a continuidade de negócios como a conexão mais importante entre os riscos de TI e a reputação.

As descobertas do estudo de 2012, *Global IT Reputational Risk and IT* , demonstram a importância de gerenciar riscos de TI dentro do contexto de riscos reputacionais que ameaçam a organização. Quando isso acontecer, as empresas podem aproveitar a confiança e o suporte de suas principais partes interessadas, que impulsionam o desempenho dos negócios.

Para obter mais informações

Para saber mais sobre como a IBM pode ajudá-lo a proteger a reputação de sua organização ao fortalecer o gerenciamento de risco de TI, entre em contato com um representante da IBM ou visite as seguintes páginas.

Para segurança e gerenciamento de risco de TI, visite:
ibm.com/services/security

Para continuidade de negócios e gerenciamento de risco de TI, visite:
ibm.com/services/continuity

Para suporte técnico e gerenciamento de risco de TI, visite:
ibm.com/services/techsupport

Veja o infográfico de TI e risco reputacional da IBM em:
ibm.co/repriskinfographic

Entre na discussão

Sua opinião é importante! Participe da extensão de nossa pesquisa de TI e risco reputacional de 2012. Basta ler o código de resposta rápida aqui ou visitar **ibmrisksurvey.com**

Suas informações serão adicionadas à maior pesquisa já realizada sobre este assunto tão importante. Você receberá a nova análise e o novo relatório sobre as descobertas da pesquisa no início de 2013. Muito obrigado pela sua participação.

IBM Corporation
Global Technology Services
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América
Setembro de 2012

[1] *Principais Tendências Impulsionando a Resiliência e o Risco dos Negócios Globais: Descobertas do Estudo Global Business Resilience and Risk de 2011 da IBM* Setembro de 2011

[2] *Reputação: Risco dos riscos.* Economist Intelligence Unit. Dezembro de 2005

Recicle

RLW03009-USEN-02