

A woman with short hair, wearing a white blouse and a necklace, is standing and speaking to two colleagues. One colleague is a woman with long braids, and the other is an older man with grey hair. They are in an office environment with a laptop and papers on a desk.

**ECONOMIST
IMPACT**

Redefinição de riscos: passar da reação à antecipação

Patrocinado por



Índice

- 3** Sobre a pesquisa e agradecimentos
- 4** Prefácio da Iron Mountain
- 5** Sumário executivo
- 8** Introdução
- 9** Gestão de riscos — tendências e percepções
- 13** A gestão do risco em quatro pilares
 - Evolução do local de trabalho
 - Cibersegurança e governança de dados
 - Sustentabilidade
 - Eficiência operacional
- 22** Desafios para a gestão de riscos
 - Medição
 - Recursos
 - Coordenação
- 26** Conclusão

Sobre a pesquisa e agradecimentos

“Redefinição de riscos: passar da reação à antecipação” é um programa de pesquisa conduzido pela *Economist Impact* e patrocinado pela Iron Mountain que examina os principais fatores internos e externos que moldam a abordagem de risco das organizações e o papel que os executivos, a tecnologia e a configuração institucional desempenham na gestão de riscos. Ela também alavancou dados de entrevistas a especialistas e um inquérito personalizado a 656 executivos de sectores principais na Austrália, Brasil, Canadá, França, Alemanha, Hong Kong, Índia, México, Nova Zelândia, Singapura, Reino Unido e EUA.

Gostaríamos de agradecer aos seguintes especialistas pelo seu tempo e partilha de conhecimentos:

- Simeon Fishman, vice-presidente executivo e CRO da *The Clearing House*
- Sophie Heading, responsável pelos riscos globais no *World Economic Forum*
- Dr Witold J Henisz, vice-reitor e diretor da faculdade da Iniciativa para o Ambiente, o Social e a Governança (*Environment, Social, and Governance Initiative*) da Wharton School

O *briefing* foi elaborado por uma equipe de pesquisadores, editores e designers da *Economist Impact*, incluindo:

- Monica Ballesteros — diretora de projeto
- Durukhshan Esmati — gestora de projeto
- Kathleen Harrington — analista
- Alasdair Ross — escritor
- Amanda Simms — editora
- EMC Design Ltd — designer

A *Economist Impact* é o único responsável pelo conteúdo deste relatório. As conclusões e opiniões aqui expressadas não refletem necessariamente as opiniões do nosso patrocinador, parceiros nem dos especialistas entrevistados.

Prefácio da Iron Mountain

Nos últimos três anos, muitas organizações sofreram transformações significativas em resposta a ameaças emergentes e a fatores de perturbação globais. Esta evolução exigiu que todos nós nos tornássemos mais resilientes, passando de medidas reativas para uma antecipação proativa. Ao criarem resiliência contra potenciais ameaças futuras, em vez de se limitarem a responder a ameaças conhecidas, as organizações são capazes de se adaptar a riscos imprevistos e de aproveitar oportunidades emergentes.

Há mais de 70 anos, a Iron Mountain capacita clientes em todo o mundo a reduzir os riscos à sua marca, reputação e situação financeira, além da capacidade de atender clientes, pacientes ou cidadãos de forma eficaz. Com isto em mente, temos o prazer de patrocinar o mais recente estudo da Economist Impact, que explora a mudança de percepções da gestão de riscos organizacionais.

Como descobrirá no presente relatório, mais de 90% das organizações estão a dar maior ênfase à gestão do risco devido às recentes perturbações globais e económicas. Em termos de riscos emergentes, o relatório destaca as preocupações constantes com a cibersegurança. Outro é a proliferação de tecnologias emergentes, com a inteligência artificial generativa, por exemplo, a criar novos riscos e a expandir a capacidade dos gestores de riscos para detetar essas ameaças ao mesmo tempo. Embora a proteção dos ativos físicos continue a ser crucial para a nossa organização, reconhecemos que todos estão agora mais vulneráveis às ciberameaças, pelo

que acompanhámos o mercado para proteger os dados dos clientes num espaço digital.

Os resultados do relatório mostram também que os executivos estão a prestar mais atenção aos riscos ambientais do que em anos anteriores. No que diz respeito à sustentabilidade, o nosso caminho para as emissões líquidas zero centra-se na redução da utilização de energia, na eletrificação dos nossos sistemas e veículos, na instalação de sistemas de energia renovável e na aquisição de energia verde para reduzir a exposição ao aumento dos preços dos combustíveis fósseis e às regulamentações locais em matéria de emissões. Ao perseguirmos os nossos próprios objetivos ambientais, sociais e de governação, e ao apoiarmos os nossos clientes na concretização dos seus, não só atenuamos os riscos associados à evolução da regulamentação, às alterações climáticas e à desigualdade social, como também criamos novas oportunidades.

Estamos entusiasmados com os resultados do inquérito que mostram que os executivos estão a gerir o risco e a criar resiliência de forma mais proativa. Este é o cerne da nossa missão. As informações baseadas em dados contidas no presente relatório dão-nos uma visão mais aprofundada da forma como nos podemos preparar melhor, a nós e aos nossos clientes, para o futuro.

Larry Jarvis
Vice-Presidente Sénior, Diretor de Segurança da Informação
Iron Mountain

Sumário executivo



A gestão de riscos está cada vez mais integrada na estrutura organizacional e cada vez mais representada nos níveis sêniores. Os gerentes de risco recolhem dados sobre potenciais ameaças e coordenam a resposta da organização. Porém, à medida que essas ameaças evoluem a um ritmo acelerado, é fundamental que a disciplina avance no sentido de antecipar os riscos que ainda não estão no radar da organização. Isto no lugar de se limitar a dar resposta aos acontecimentos conforme estes ocorrerem.

A *Economist Impact*, patrocinada pela Iron Mountain, realizou uma pesquisa primária para observar como os executivos percebem os principais fatores internos e externos que moldam a abordagem das organizações em relação ao risco e o papel que os executivos, a tecnologia e a estrutura institucional desempenham na gestão de riscos. Ela também alavancou dados de entrevistas com especialistas e uma enquete personalizada a 656 executivos das principais indústrias (serviços financeiros, cuidados de saúde e ciências da vida, energia e sector público) na Austrália, Brasil, Canadá, França, Alemanha, Hong Kong, Índia, México, Nova Zelândia, Singapura, Reino Unido e EUA.

Os gestores de riscos estão avançando no sentido de compreender de modo mais profundo como os riscos se propagam como torrentes na organização toda. Por exemplo, saber em que medida um encerramento ou uma violação da segurança de um fornecedor crucial pode afetar as operações, as receitas e a reputação da organização. A sensibilização para os riscos contingentes está aumentando, mas ainda há margem para melhorias.

Redefinição de riscos: passar da reação à antecipação

Uma gestão de riscos holística e de antecipação, que dê resposta às ameaças emergentes, deve ser conduzida a partir do topo da organização, com uma resposta ao risco sistematicamente coordenada que seja aceita e “assumida” por todos os colaboradores. Além da organização, a sensibilização para o risco deve ser assimilada por parceiros, fornecedores e distribuidores.

As tecnologias digitais emergentes, como o *machine learning* e a inteligência artificial (IA), prometem expandir o conjunto de ferramentas do gerente de riscos, detetando padrões nos dados que os analistas humanos podem falhar. No entanto, os atacantes também têm acesso a estas tecnologias, que podem ser utilizadas para encontrar vulnerabilidades ou lançar ataques de *phishing* mais persuasivos. Estas tecnologias emergentes têm de ser cuidadosamente monitorizadas à medida que as suas verdadeiras implicações se tornam mais claras.

Analizamos quatro áreas nas quais a evolução das práticas está transformando o panorama da gestão de riscos:

Evolução do local de trabalho: os colaboradores de uma organização são simultaneamente o seu maior ativo e a sua maior vulnerabilidade, o que se reflete nos esforços e recursos que as organizações dedicam ao seu recrutamento, retenção e formação. A digitalização colocou os colaboradores mais próximos dos processos críticos, aumentando o risco e acelerando o ritmo no qual este se manifesta. Todavia, a mudança para o teletrabalho tornou as fronteiras digitais da organização mais permeáveis. Atrair e reter colaboradores está também sendo mais difícil, enquanto uma geração adota uma abordagem do trabalho mais orientada para os valores. A enquete sugere que os gestores de risco estão acompanhando estas tendências emergentes; 96% dos entrevistados indicam que a sua organização desenvolveu novas políticas e procedimentos de gestão da mão de obra, tal como o trabalho híbrido.

Cibersegurança e governança de dados: a informática não só sustenta uma nova leva de ganhos de produtividade, como também cria novas fontes de risco. A informação flui de forma mais rápida e abrangente do que nunca e, criticamente, de modo mais rápido do que a reação humana. Com o risco contingente também aumentando devido ao surgimento de organizações enormes, dispersas e multinacionais, a proteção da presença digital de uma entidade contra danos acidentais

ou maliciosos tornou-se uma questão de sobrevivência. O lançamento de modelos de IA generativa de código aberto trouxe subitamente para o horizonte e para a sala de reuniões um risco há muito antecipado, embora os impactos desta tecnologia nascente continuem a ser difíceis de prever. Os gestores podem responder melhor a este ambiente em mudança concentrando-se incansavelmente nas três áreas principais dos riscos de dados: a governança, a segurança e a privacidade.

Sustentabilidade: as alterações climáticas ameaçam o nosso futuro, mas os seus efeitos já se fazem sentir. As condições meteorológicas extremas estão sendo cada vez mais intensas e frequentes, enquanto a biodiversidade está sob crescente ameaça. Há também impactos catastróficos no comércio e nas infraestruturas. Portanto, as organizações estão concentradas em manter cadeias de abastecimento diversificadas e flexíveis. Embora se concentrem na resiliência, estas também são pressionadas pelos intervenientes a fim de ajudarem a resolver os problemas subjacentes: o esgotamento dos recursos, a degradação ambiental e as emissões perigosas. A ausência de ação no que respeita a estas questões poderá ter graves repercussões. Este fato é reconhecido pela grande maioria dos entrevistados, tendo 80% salientado a importância dos indicadores de risco para a reputação.

Redefinição de riscos: passar da reação à antecipação

Eficiência operacional: apesar das organizações enfrentarem uma maré crescente de riscos provenientes do exterior, os gerentes de riscos devem continuar a se concentrar nas ameaças mais próximas de casa, independentemente se a origem destas são as pessoas, os processos ou os requisitos regulamentares. As organizações caíram na armadilha de encarar a função de riscos como um centro de custos que coloca obstáculos à obtenção de lucros. Os gestores de risco melhoram a sua capacidade de fornecer à administração métricas que proporcionem o equilíbrio entre os custos de manutenção de práticas de risco sólidas com as potenciais perdas decorrentes de uma falha. A forma como os riscos operacionais se manifestam varia muito entre organizações e setores, mas a enquete sugere que os gerentes de risco reconhecem a importância do investimento nesta área.

Embora a disciplina da gestão de riscos esteja evoluindo em sintonia com a mutação do cenário de ameaças, há desafios consideráveis que carecem de ser enfrentados. Entre estes estão:



Medição: ainda que os custos de implementação de um sistema de gestão de riscos sejam claros, o mesmo não pode ser dito sobre a medição dos seus benefícios. Parte do papel da função é garantir que potenciais ameaças não se materializem, mas avaliando o custo de algo, que mesmo não tenha acontecido, é problemático. Apesar do investimento ser imediato, os benefícios podem se acumular ao longo dos anos, aumentando o desafio da medição. A chave está na criação de métricas que associem os riscos a objetivos organizacionais mensuráveis.

Recursos: as organizações tendem a financiar a função de riscos refletindo o panorama do passado, em vez de se prepararem para o futuro. Numa altura em que estão surgindo novos riscos e os antigos estão evoluindo, isto costuma deixar o esforço de gestão de riscos subfinanciado, com falta de pessoal e, potencialmente, pouco qualificado.

Coordenação: uma função de riscos orientada para o futuro, eficiente e resiliente exige uma sensibilização e coordenação únicas em toda a estrutura da empresa no lugar de funções tradicionais isoladas. Também requer uma liderança descendente e uma colaboração e execução ascendentes, e deve se estender para além da organização, com o propósito de incluir os seus parceiros, fornecedores e outras partes interessadas.

Introdução

Não há certeza nas operações das organizações. A possibilidade de algo correr mal em cada empresa e em cada ponto da sua cadeia de valor está sempre presente. Desde uma recessão nos principais mercados, passando pela interrupção de fornecimentos críticos, até às ações maliciosas de um colaborador descontente, os riscos que são difíceis de prever ou evitar, prejudicam os resultados e os objetivos das organizações. Os danos podem variar desde uma pequena irritação até os casos extremos, como a falência e a prisão.

Evitar estas ameaças é uma disciplina sofisticada e de rápida evolução. É complicado pelo fato dos riscos mudarem ao longo do tempo em termos de intensidade, natureza e âmbito. Durante e imediatamente após a crise financeira de 2008-2009, o risco de ficar sem acesso ao crédito era a preocupação principal. Na pandemia da COVID-19, o foco foi colocado na continuidade das atividades, uma vez que os confinamentos obrigaram as organizações a fechar as portas. Quando os tanques russos entraram na Ucrânia em 2022, as restrições ao abastecimento mundial de alimentos e combustíveis fizeram disparar os preços e perturbaram as cadeias de abastecimento.

O aumento de formas de tecnologia cada vez mais avançadas e facilmente acessíveis, combinado com o fato do trabalho remoto estar cada vez mais generalizado e enraizado, introduziu um novo nível de risco. As fronteiras geográficas das organizações se expandiram dos escritórios construídos para o efeito e centralizados para os sótãos, escritórios e jardins de residências privadas, muitas vezes a muitos quilômetros da sede e frequentemente num país diferente. A segurança dos processos e dos dados confidenciais num ambiente tão disperso é duplamente difícil, transformando cada colaborador num potencial ponto de fuga ou de sabotagem.

A *Economist Impact*, patrocinada pela Iron Mountain, efetuou uma pesquisa primária para determinar como os executivos percebem os principais fatores internos e externos que moldam a abordagem das organizações em relação ao risco e o papel que os executivos, a tecnologia e a estrutura institucional desempenham na gestão de riscos. Ela também alavancou dados de entrevistas a especialistas e uma enquete personalizada a 656 executivos de setores principais na Austrália, Brasil, Canadá, França, Alemanha, Hong Kong, Índia, México, Nova Zelândia, Singapura, Reino Unido e EUA.

Gestão de riscos — tendências e percepções

A gestão de riscos evoluiu como uma disciplina para confrontar à transformação das ameaças. Passou a estar cada vez mais enraizada e elevada na estrutura das organizações, envolvendo mais pessoas e recursos (embora, segundo consta, nunca suficientes) a um patamar mais alto. A responsabilidade pelo risco é frequentemente assumida ao nível do conselho de administração, com os gestores de riscos (CROs) a reportarem diretamente ao Diretor Financeiro (CFO) ou ao Presidente Executivo (CEO). Simultaneamente, os gestores de risco são vistos não tanto como chefes de uma divisão distinta, e sim mais como coordenadores de atividades espalhadas por toda a organização. A assunção do risco e a responsabilidade de comunicá-lo ao topo da cadeia pertencem frequentemente aos chefes de divisão, cabendo à função de riscos fornecer orientações, recolher dados e recomendar medidas corretivas ao gerenciamento sênior.

O caminho desde o risco, como um elemento pouco reconhecido, até a atual arquitetura de risco de toda a empresa tem sido longo. A conscientização do risco como preocupação organizacional existencial surgiu na segunda metade do século passado, mas os primeiros CROs só foram nomeados na década de 1980. Esta função não foi considerada uma resposta generalizada ao risco até os primeiros anos deste século. Atualmente, a gestão de riscos é reconhecida como uma competência essencial do gerenciamento sênior. Quatro em cada

cinco organizações representadas na enquete mencionam ter investido em equipes de gestão de riscos à escala da empresa como parte da sua abordagem tática à disciplina.

A pesquisa sugere que a jornada continua incompleta, embora os gestores de risco seniores estejam sendo cada vez mais sofisticados na compreensão da disciplina. Por exemplo, a atenção está passando da reação aos riscos à medida que estes surgem para a sua antecipação e para a criação de resiliência na organização, previamente à ocorrência de danos. A identificação do risco aumentou em importância desde 2020 para mais de 90% dos entrevistados, tal como a modelação preditiva do risco, que apresenta uma porcentagem aproximadamente igual. O foco na antecipação estende-se à reformulação da organização para esse efeito. Agora, 28% afirmam procurar uma melhor capacidade de identificar e antecipar ameaças, enquanto 41% dizem que antecipam os riscos através do monitoramento de ameaças emergentes e da identificação de anomalias nos processos. Esta mudança de foco não é surpreendente, dada a sucessão de choques nas últimas décadas que surpreenderam os gestores das organizações.

Ademais, as organizações se debatendo com a interconetividade do risco. Um acontecimento adverso numa parte da organização, ou no mundo, pode repercutir na operação de inúmeras



formas. Se um fornecedor crucial interromper o fornecimento devido a uma catástrofe natural, este poderá provocar atrasos na produção e um aumento dos custos devido à procura de fornecimentos alternativos. Além disso, pode também levar à perda de receitas devido a atrasos nas encomendas ou a estas não serem satisfeitas, e um golpe na marca e na reputação da organização à medida que a notícia da perturbação circula. Basta um risco de um terceiro para que toda a organização se veja envolvida numa gestão de crise. Antecipar estas ameaças contingentes é um elemento fundamental da gestão moderna de riscos.

Novamente, as organizações estão progredindo, mas há margem para melhorias. Sophie Heading, responsável pelos riscos globais no Fórum Económico Mundial, explica que “há uma melhor apreciação da conectividade entre os riscos, mas continua em evolução. Com um pouco de imaginação, a implicação de acontecimentos num canto do mundo pode ser utilizada para prever um risco potencial no outro lado. A falta dessa visão pode tornar a organização suscetível aos riscos que surgem destes acontecimentos”.

Simeon Fishman, vice-presidente executivo e gestor de riscos da *The Clearing House*, acredita haver cada vez mais um foco nos riscos emergentes, isto é, os riscos que são menos definidos e aparentes. “Agora é mais crítico para as organizações obterem maior visibilidade no horizonte e tentarem compreender melhor estes riscos” — explica. “Uma área crucial dos riscos emergentes diz respeito ao papel dos riscos tecnológicos, que estão em evolução contínua. Por exemplo, apenas alguns fornecedores prestam serviços de nuvem, o que potencialmente leva a uma concentração da computação nela. Um negócio centrado na tecnologia, por meio do software que utiliza ou desenvolve, colocará inadvertidamente todos os seus esforços numa só possibilidade”.

Os gestores são ajudados nesta transição de uma gestão de risco reativa para uma gestão de riscos proativa por um conjunto emergente de ferramentas digitais, tal como refletido nas respostas à enquete, na qual 43% dos executivos destacaram que utilizam tecnologias cognitivas e IA para gerir o risco. No entanto, apesar da mudança ser a base do negócio dos gestores de risco, a mudança ao ritmo que estamos observando na IA traz os seus próprios desafios. É claro que o *machine learning* oferece uma nova forma de interrogar os dados que entram e saem de uma grande empresa, auxiliando os analistas humanos a detetar padrões que estes podem falhar. Porém, também pode ser um vetor de ciberataques, uma vez que os *hackers* e os golpistas utilizam a tecnologia para reforçar a sua programação. O simples fato é que ainda é muito cedo para dizer como esta tecnologia se desenvolverá e qual o seu impacto líquido na gestão de riscos.

A necessidade de antecipar os riscos e os suas repercussões no negócio todo, num patamar de rápida evolução tecnológica, realça a importância de adotar uma abordagem holística da gestão de riscos. Confiar na reação às ameaças assim que estas se materializam deixa as organizações sem

A tecnologia só pode levar você até determinado ponto se não tiver o design, a arquitetura de riscos ou os dados corretos nos seus sistemas. É também fundamental compreender em que medida os processos do negócio e os dados estão conectados.

Assim que o design e os dados estiverem implementados, será possível tirar partido das ferramentas de análise e interrogação de dados para obter um entendimento mais abrangente dos riscos numa organização.

Simeon Fishman, vice-presidente executivo e responsável de riscos da *The Clearing House*.

rumo e com dificuldades em recuperar o atraso. Concentrar-se separadamente em cada área das operações expõe a organização a riscos contingentes. A resposta não é simplesmente confiar em tecnologias inovadoras. A adoção cega da inovação deixa as empresas expostas a ameaças novas e imprevistas. Heading adverte que “a tecnologia permite a gestão de riscos, mas precisa ser combinada com o elemento humano”.

A abordagem holística da gestão de riscos exige uma liderança a partir do topo e uma coordenação em toda a estrutura organizacional para levar toda a informação disponível à atenção das pessoas mais bem colocadas para a interpretar e agir. O Dr. Witold J Henisz, vice-reitor e diretor da faculdade *Environment, Social and Governance Initiative* (Iniciativa para o Ambiente, o Social e a Governança) da Wharton School, concorda com esta afirmação. Ele acrescenta que “tornar os dados compreensíveis, transparentes e fáceis de entender é extremamente importante quando se juntam pessoas com diferentes competências em matéria de dados e antecedentes funcionais”.

Tal como o rótulo “holístico” sugere, a gestão de riscos está virando a responsabilidade de toda a empresa (e dos seus fornecedores, parceiros e distribuidores). Os gestores de risco implementam e coordenam o sistema, mas, ao contrário do diretor de marketing ou do diretor de operações, esta não é uma competência reservada apenas para eles. Evoluindo de um cargo inserido em algum lugar no organograma, a gestão de riscos se transformou em um elemento integrante da cultura organizacional, a par da sua marca, declaração de missão ou abordagem ao desenvolvimento e retenção do capital humano. Inclui compromissos ao nível de toda a organização, como a afirmação de apetência pelo risco, uma característica cada vez mais comum das organizações modernas que definem o nível de risco aceitável e a sua atitude geral de assunção de riscos.

No centro desta abordagem, está a coordenação entre as várias unidades da organização, a sua cadeia de fornecimento estendida e os seus principais *stakeholders*. Muitos gestores de risco seniores são defensores desta abordagem nos seus negócios, como mostra a nossa enquete.

Redefinição de riscos: passar da reação à antecipação

Entre os entrevistados, 77% concordam que a gestão do risco deve considerar todas as partes da organização, enquanto 46% referem ter investido em equipes de gestão de riscos à escala da empresa. Outros 36% afirmam que a integração da gestão de riscos na estratégia organizacional geral e na tomada de decisões é uma prioridade.

Isto exige “mudanças estruturais que variam conforme o tipo e a dimensão da organização,” segundo Fishman. “A comunicação desde a liderança sênior e o CEO até todos se torna mais crítica para garantir que a gestão de riscos faça parte do DNA do negócio todo e não apenas de uma função criada para o efeito que assume a responsabilidade especial de orientar a gestão de riscos.”

Entretanto, os executivos ainda estão longe de alcançar a situação ideal. 57% destacaram que a sua organização precisa de melhorar a colaboração interfuncional. Apenas 4% dos executivos entrevistados afirmaram ter uma comissão de gestão de riscos diretamente responsável pela condução de tal gestão, enquanto 27% mencionaram que o seu CEO/presidente/parceiro é diretamente responsável. Mais de 60% dos entrevistados consideram que a sua organização precisa de melhorar o envolvimento dos colaboradores e a partilha de informações entre funções, equipes e parceiros externos.

A gestão do risco em quatro pilares



Pela sua natureza, o risco é difuso. Mesmo quando as fontes são claras (o que é raro), o percurso do risco — onde entra na organização e como a atravessa — é difícil de prever. Nesta seção, analisaremos quatro manifestações distintas dos riscos organizacionais, faremos o monitoramento dos seus efeitos e exploraremos como os gestores os abordam. Os quatro pilares são:

- Evolução do local de trabalho
- Cibersegurança e governança de dados
- Sustentabilidade
- Eficiência operacional

Evolução do local de trabalho

Uma organização é mais do que um grupo de pessoas reunidas para cumprir a sua missão. Os seus diferentes talentos se combinam para transformar os *inputs* em *outputs* de maior valor. É com razão que muitas empresas dão grande valor aos seus recursos humanos e investem dinheiro e esforços no seu recrutamento, formação e retenção. No entanto, a par das suas capacidades e energia, os seres humanos são imprevisíveis e têm tendência para cometer erros. Os riscos relacionados com as pessoas são dos mais difíceis de gerir por três razões. Primeiramente, todos os processos que um negócio executa, com ou sem tecnologia, são mediados por pessoas, pelo que os riscos que estas representam se manifestam em todo lugar. Segundo, estão sujeitas a impulsos humanos, o que resulta num desempenho imprevisível em comparação com o de uma máquina. Por último, a relação entre as organizações e o seu pessoal está evoluindo, com o trabalho remoto e está se tornando mais comum, já que o que prevalece hoje pode diferir do que prevalecerá amanhã.

As pessoas sempre foram a maior força e a maior vulnerabilidade das organizações, mas os desenvolvimentos recentes vieram aumentar os riscos. A transformação digital nas últimas décadas aumentou a produtividade em geral. Porém, também aproximou os funcionários de processos de missão crítica e dados valiosos. Devido a esta proximidade, os colaboradores descuidados ou mal-intencionados podem causar mais danos e mais rapidamente do que nunca. Recentemente, a pandemia da covid-19 forçou uma transformação profunda e repentina de muitos ambientes de trabalho, deixando as organizações com falta de colaboradores

numa altura crítica e apressando-se a criar sistemas de trabalho em casa. Esta realidade também colocou as organizações perante um novo desafio de gestão, como explica Fishman. “Podemos não ter a mesma compreensão das funções e responsabilidades de cada um — obter visibilidade dos comportamentos de cada um e de algumas vulnerabilidades de risco se torna mais difícil com o trabalho remoto”, afirma.

À medida que a pandemia diminui, as organizações descobrem que as atitudes dos seus colaboradores em relação ao trabalho mudaram, talvez permanentemente. Os atuais colaboradores não estão, na maioria das vezes, entusiasmados com o retorno ao escritório, ao passo que os potenciais e novos recrutados esperam, por norma, trabalhar em casa. Os negócios também sofreram uma escassez de mão de obra, em parte devido aos impactos a longo prazo na saúde provocados pela pandemia, mas também devido a uma tendência apelidada de “a grande demissão”, que foi provocada por uma confluência de fatores, como o protesto contra locais de trabalho tóxicos.

No futuro, as mudanças geracionais nas atitudes e expectativas dos colaboradores, incluindo uma prioridade crescente de valores como a diversidade, a sustentabilidade e a justiça social, dificultarão a atração e retenção de pessoas. Só o salário não será suficiente. Este fato ameaça criar um desfasamento entre as competências necessárias num ambiente tecnológico em rápida mutação e a disponibilidade e vontade dos recrutados no mercado. As organizações podem operar em si com um déficit de competências, prejudicando a produtividade e aumentando o risco de erros e atos maliciosos.

Redefinição de riscos: passar da reação à antecipação

Tal como em outras áreas de risco, nem todas as organizações estão acompanhando a evolução, embora muitas o façam. As mais inovadoras estão deslocalizando os escritórios para se adaptarem à nova realidade, mais descentralizada. Os resultados da enquete mostram que 94% das organizações diversificaram a sua abordagem sobre o escritório físico e ao local de trabalho, tendo a pandemia levado 45% delas a fazê-lo nos últimos três anos. Em conformidade, 96% dos entrevistados indicaram que a sua organização desenvolveu novas políticas e procedimentos de gestão da mão de obra, incluindo o trabalho híbrido. As empresas estão também avaliando as necessidades de talentos para um mundo do trabalho em transformação, incluindo a função de riscos. As principais organizações estão

“analisando modelos de gestão de pessoal do seu negócio para garantir que têm gestores de risco tecnologicamente competentes”, diz Fishman. “O papel dos especialistas em tecnologia em matéria de riscos e recuperação é fundamental, assim como especialistas em computação na nuvem e IA”.

As empresas também estão coletando mais dados sobre questões relacionadas com a força de trabalho e a desenvolver processos mais sistemáticos para gerir o recrutamento e a retenção. A enquete corrobora este fato, com metade dos entrevistados destacando que utilizam mais dados para fazer isso, com um número minimamente superior declarando que desenvolveram uma reserva de talentos.



Cibersegurança e governança de dados

A adoção entusiástica da tecnologia de informação por parte das empresas transformou as suas operações. Longe vão os velhos tempos das instalações centralizadas com exércitos de colaboradores supervisionados por gestores austeros em hierarquias rígidas, pois as organizações se tornaram mais flexíveis, mais ágeis e muito mais produtivas, na maioria, graças à digitalização. Os computadores, a automação e a Internet alteraram profundamente os modelos de trabalho, e desenvolvimentos futuros como a computação quântica, a Internet das Coisas onipresente e o metaverso prometem mudanças igualmente fundamentais.

De modo geral, o impacto da revolução digital na gestão dos riscos organizacionais tem sido triplo: os riscos surgem mais repentinamente e se propagam muito mais rapidamente; os dados, o seu armazenamento, transmissão e interpretação se tornaram um ingrediente fundamental nas operações; e, embora a digitalização tenha criado novas áreas de risco, também deu origem a novas ferramentas para enfrentá-las.

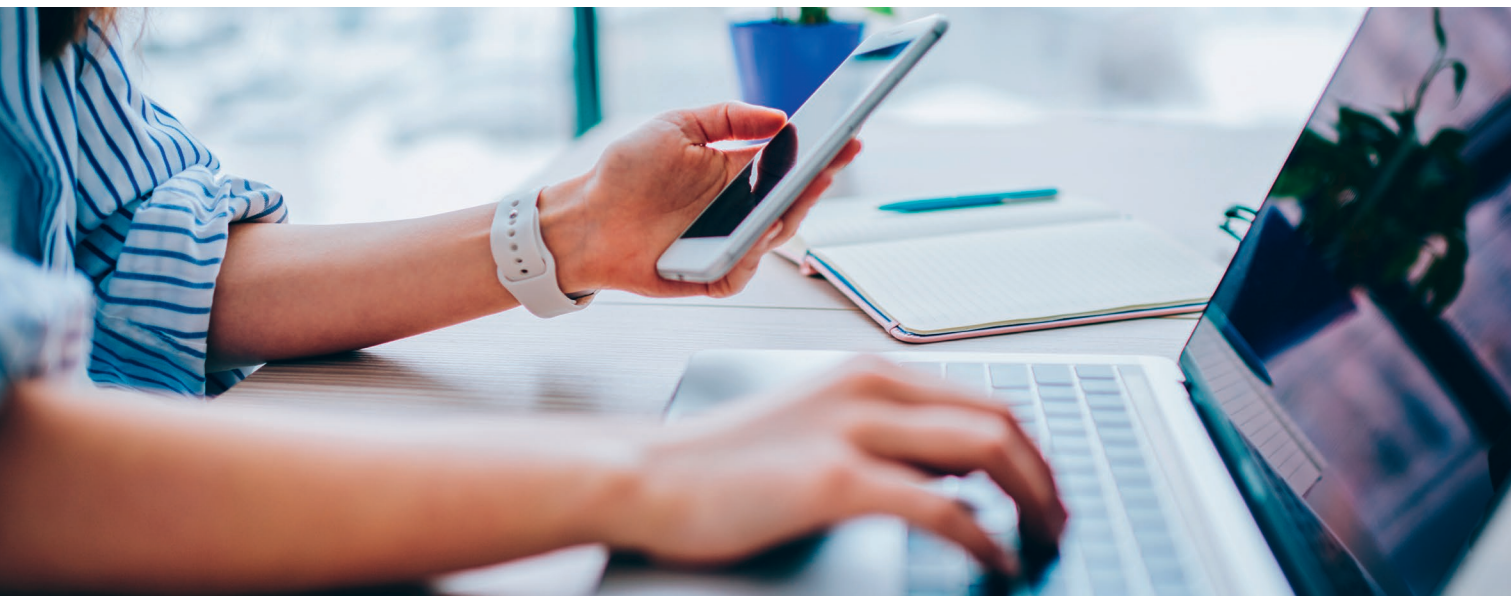
Quando as informações viajam à velocidade da luz por uma rede digital global, as coisas mudam mais rápido do que a possível reação de um ser humano. Com os computadores tomando a cada vez mais decisões em nome dos humanos, os processos podem avançar mediante inúmeras iterações antes de ser detetado um erro ou um resultado não intencional. Com clientes, parceiros e consumidores ligados à mídia ao nível mundial, a reputação de uma marca pode ir parar ao tribunal da opinião pública antes dos executivos da organização terem totalmente percebido o que está acontecendo.

Referente à IA generativa, assistimos ao surgimento de um novo e potencial risco cibernético. O ritmo da sua adoção deixou a sociedade em seu rastro, com os decisores políticos e os reguladores — e os criadores pioneiros da tecnologia — a se esforçarem por acompanhar o ritmo. Os gestores de risco não sabem a quem recorrer para obter os melhores conselhos nesta fase inicial do que poderá se revelar tão perturbador para os modelos de negócio como a própria Internet. “Quem tem conhecimentos especializados em matéria de risco sobre o rumo que a IA generativa está tomando?” — pergunta Fishman. “Que formas sofisticadas podemos adotar para monitorar melhor a concentração de dados na nuvem? Dado que a evolução do panorama cibernético pode mudar, como podemos continuar a integrar a resiliência nas nossas infraestruturas e processos?”

Este domínio coloca questões urgentes e desafios complexos aos gestores de riscos e às organizações. Atualmente, é bom começar pela abordagem dos aspetos básicos. Ainda é fundamental que as organizações se concentrem em três grandes áreas de riscos quando se trata de gerir os seus ativos digitais:

- Governança de dados: garantir a exatidão, a coerência e a acessibilidade dos dados.
- Segurança de dados: proteger os dados contra acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados.
- Privacidade de dados: proteger a privacidade das pessoas, controlando como os seus dados pessoais são coletados, utilizados e partilhados.

Redefinição de riscos: passar da reação à antecipação



Os mesmos princípios de proatividade e de análise do horizonte continuam a ser válidos, mas com mais urgência do que antes. Do mesmo modo, garantir a conformidade é um desafio maior num panorama regulamentar tão incerto e em rápida transformação, mas não menos vital.

Os resultados da enquete indicam que as organizações têm demonstrado dedicação e consistência nos seus esforços para mitigar os riscos dos dados e da cibersegurança por meio de diferentes medidas. Nos últimos três anos, 49% das organizações investiram em planos de recuperação de desastres/continuidade de negócios para sistemas digitais e 48% investiram em serviços/armazenamento em nuvem e no monitoramento e prevenção contínuas de riscos e ameaças cibernéticas. Durante o mesmo período, 46% dos executivos entrevistados referiram também investimentos em talentos de TI e de cibersegurança e formação em educação técnica/dados.

Enquanto isso, os gestores de risco devem ter um grande interesse na evolução da IA, não só como fonte de risco, mas também como meio de o mitigar. 43% dos nossos entrevistados destacam utilizar tecnologias cognitivas e IA nos processos de gestão de riscos. Devidamente treinada e orientada, a IA pode identificar padrões estranhos, identificar tendências, traçar cenários

e detetar áreas de risco que os analistas humanos arriscam falhar.

Poucas organizações estão isentas de riscos cibernéticos, mas alguns sectores são mais propensos do que outros. Por exemplo, os sectores da saúde e das finanças captam enormes quantidades de dados sensíveis dos clientes. Conseguir tirar o melhor partido deste tesouro de dados, como forma de calcular o risco para o cliente ou para a organização, mantendo-os seguros, é uma tarefa gigantesca. Os custos do fracasso podem ser devastadores. Não é de surpreender que, entre todas as indústrias, o setor de saúde tenha tido a percentagem mais elevada de entrevistados, com 83%. Isto indica a importância crescente dos indicadores tecnológicos nos últimos três anos. Estes incluíam o tempo de atividade da rede, incidentes de cibersegurança e erros de software.

O setor da energia depende igualmente dos dados para racionalizar as suas operações, enquanto o Estado moderno se apoia fortemente nos dados dos cidadãos para prestar serviços públicos com a máxima eficiência. No caso dos governos, os custos de reputação de um fracasso podem ser particularmente prejudiciais, colocando os políticos e os seus partidos em conflito direto com aqueles que votam neles.

Sustentabilidade

A industrialização trouxe à humanidade benefícios inimagináveis para os nossos antepassados pré-industriais. No entanto, ao queimarmos combustíveis fósseis para alimentá-la, colocamos em risco a sustentabilidade do nosso estilo de vida — e das nossas vidas. Os gases de efeito estufa (GEE) liberados para a atmosfera, na maioria devido à nossa atividade econômica, estão aumentando as temperaturas médias globais. Os efeitos serão potencialmente catastróficos nas próximas décadas, mas não temos de esperar tanto tempo. Fenômenos meteorológicos extremos estão crescendo, o nível do mar está subindo e a biodiversidade está sob ameaça.

Esta situação afeta as organizações de duas formas. Em primeiro lugar, as operações e as cadeias de abastecimento são vulneráveis a perturbações causadas por fenômenos meteorológicos extremos e outros efeitos ambientais difíceis de antecipar. Os acontecimentos dos últimos três anos levaram 47% das organizações entrevistadas a se concentrarem na manutenção de redes de cadeias de abastecimento diversificadas e flexíveis. Em segundo lugar, as partes interessadas das organizações, desde os clientes aos investidores e aos trabalhadores, esperam, com razão, que as entidades façam a sua parte no combate ao esgotamento dos recursos, à degradação ambiental e às emissões de GEE.

Por enquanto, a segunda é mais urgente para os gestores de risco (embora a primeira seja uma ameaça crescente). Os grupos de ativistas destacam rapidamente os que consideram infratores flagrantes das práticas sustentáveis, com um arsenal crescente de meios criativos para chamar a atenção do público. As empresas

petrolíferas e energéticas, e os investidores e bancos que as financiam têm sido alvo de ataques persistentes. Estas campanhas podem perturbar diretamente as operações comerciais, mas podem ter um impacto mais grave ao minar a reputação de uma organização e a sua “licença social” para operar.

A importância dos indicadores de risco de reputação entre os executivos tem crescido nos últimos anos devido à crescente complexidade dos ambientes operacionais e à necessidade das organizações serem mais transparentes, responsáveis e socialmente competentes. Um número significativo de 80% dos entrevistados identificou os indicadores de risco de reputação como os mais cruciais em termos de importância crescente para o seu monitoramento de risco.

Tal como acontece com a cibersegurança, a sustentabilidade e as áreas associadas de política social e governança (ESG – Política Ambiental, Social e de Governança) constituem um cenário de risco em rápida transformação. As preocupações ambientais ganharam proeminência na agenda pública, com as organizações respondendo com afirmações em que anunciam as suas credenciais “verdes”. Todavia, essas afirmações são frequentemente consideradas como “*greenwashing*” ou “lavagem verde” e insuficientes para proteger as organizações da ira do público. As afirmações relativas à missão ecológica têm sido cada vez mais substituídas por promessas de atingir “net zero líquido” de GEE, acompanhadas de roteiros que demonstram como isso será conseguido.

Para as grandes empresas, isto já não é suficiente. Os cidadãos exigem uma atitude “positiva em relação à natureza” por parte dos sectores público

Redefinição de riscos: passar da reação à antecipação

e empresarial, pressionando as organizações. Isto com o propósito delas apresentarem planos para restaurar o ambiente ao seu estado pré-industrial ou, pelo menos, para fazer com que os indicadores climáticos voltem a estar dentro dos limites compatíveis com uma economia sustentável. Heading aponta para “uma mudança na gestão de riscos, que deixa de se limitar à verificação pura e simples da regulamentação/conformidade, para ter uma função muito mais estratégica, que se incorporem valores sociais como a ESG”.

Nossa enquete reflete o fato da ESG aparecer agora nos registros de risco das organizações. Quase metade das empresas entrevistadas dedicou mais recursos a iniciativas ESG, enquanto um número semelhante se concentra na comunicação do desempenho de ESG — exigida pelos reguladores em algumas jurisdições.

Eficiência operacional

O mais próximo de casa para as organizações e os seus gestores de risco são as suas operações internas. A maioria pode fazer pouco para influenciar as circunstâncias para além das suas paredes, físicas ou virtuais, mas o que acontece no seu interior está, principalmente, sob o seu controle direto. Independentemente se é sobre pessoas, processos ou requisitos regulamentares, a eficiência do funcionamento interno de um negócio é a diferença entre o sucesso e o fracasso. E está repleta de riscos: os colaboradores podem não ter o desempenho esperado, podem ficar desiludidos com o equipamento do qual dependem ou serem vítimas de vulnerabilidades nos processos concebidos para os tornar coletivamente produtivos.

A proteção contra esses riscos tem sido uma característica central da gestão de riscos desde os primeiros dias da disciplina. Como tal, os gestores de risco podem facilmente cair na velha percepção de serem pouco mais do que um policial interno que coloca obstáculos no caminho de outros departamentos. A função de riscos passa, assim, a ser vista como um centro de custos e um fardo para o impulso empreendedor das verticais “lucrativas”. Esta percepção era (e por vezes ainda é) uma pedra de moinho à volta do pescoço dos gestores de risco, mas as coisas estão mudando. Os gestores de risco tem melhorado a medição dos custos das falhas operacionais e a compará-los com o custo de manter uma função de riscos adequada à sua finalidade. Em comparação com a suspensão das operações para restaurar um processo falhado,

uma sanção regulamentar pesada por mau tratamento dos dados dos clientes ou a perda de negócios devido a uma falha ética bem divulgada, o custo de uma função de gestão de riscos ágil é menos trabalhoso.

Não há duas organizações iguais, pelo que não existe um modelo para alcançar a eficiência operacional. Na realidade, o que se entende por “operações” pode variar muito nas empresas e entre elas. O setor da energia se centra no equipamento e nos processos, uma vez que a perfuração de petróleo ou a extração de minérios é altamente intensiva em termos de capital e uma falha pode provocar desastres humanos e ambientais. O setor financeiro é um setor com muitos dados e vulnerável a falhas do seu pessoal devido a violações ilegais de políticas e funções, má execução, falta de formação e comportamentos pouco éticos. Estes podem resultar em perdas diretas, bem como em custos regulamentares, legais e de reestruturação. A conformidade legal e regulatória é particularmente importante, complicada pelo fato de muitos bancos e instituições financeiras operarem em várias jurisdições legais. Outros setores variam no foco de seu gerenciamento de risco operacional — um dos muitos fatores que complicam o trabalho dos gestores de risco.

A enquete reflete a importância dos riscos operacionais para as organizações, com uma clara sensação de que o investimento nesta área melhora o desempenho e os resultados financeiros. Em especial, 42% dos entrevistados referem uma melhoria do desempenho

Redefinição de riscos: passar da reação à antecipação

resultante da aplicação de boas práticas de gestão no planejamento das instalações e do espaço físico de trabalho. Uma percentagem semelhante relata uma melhoria significativa da eficiência operacional da sua empresa. Entretanto, dois terços dos inquiridos reconhecem que se trata de uma aposta a longo prazo e que o investimento na gestão de riscos perturba as operações a curto prazo.

Henisz afirma que o reconhecimento da relação entre investimento e retorno é fundamental. “Podemos rentabilizar o impacto do risco, calculando os dias de paragem e a produção perdida” — ele diz. “Traduzir os dados para a linguagem das finanças ou das operações é fundamental. Caso contrário, a função de gestão de riscos será vista apenas como um custo, enquanto todos os outros geram receitas”.

Desafios para a gestão de riscos



Ao longo do tempo, a profissão de gestão de riscos se tornou mais influente e sofisticada e está atualmente integrada na cultura e na estrutura da maioria das grandes organizações. Contudo, o seu papel e as suas metodologias estão sob pressão contínua para acompanhar um ambiente de risco em constante transformação. Teve uma tendência para considerar suficiente uma estratégia de risco capaz de enfrentar todas as ameaças registradas no passado, mas o passado é frequentemente um mau indicador da forma como o risco se manifestará no futuro. Em resposta, a gestão de riscos deve estar em constante evolução, à medida que surgem novas ameaças e fatores de perturbação. Particularmente, a profissão tem de continuar a percorrer o caminho da reação para a antecipação, criando resiliência contra as ameaças futuras, em vez de se limitar a responder às já conhecidas.

A este respeito, a enquete revela alguns progressos, mas sugere que há ainda muito a ser feito. A esmagadora maioria dos executivos entrevistados está confiante de que as iniciativas de gestão de riscos implementadas pelas suas empresas são suficientes para mitigar ou prevenir os danos causados pelo risco. Isto indicia um grau de excesso de confiança por parte das organizações que pode deixá-las mais expostas do que elas pensam. A resolução deste potencial déficit envolve três grandes áreas de atenção: medição, recursos e coordenação.

Medição

O monitoramento do desempenho da gestão de riscos é intrinsecamente complicado. Se houver uma falha nela, os custos incorridos poderão ser atribuídos ao programa de riscos. Isto parece claro, mas determinar a porcentagem dos custos que deve ser atribuída à função está longe de ser simples. É ainda mais difícil atribuir o crédito à gestão de riscos quando as coisas correm bem. Há uma tendência para considerar que isso não passa da “atividade normal” e para negar completamente a contribuição dos gestores de risco. Mesmo ao fazer algum esforço para dar crédito à função, é difícil quantificar o que deve ser registrado na coluna do “positivo”.

A função de riscos deverá ser responsável pelos investimentos efetuados na antecipação de riscos que nunca se concretizaram? Deverá ser responsável por acontecimentos do tipo “cisne negro” (difíceis de prever, mas que, em retrospectiva, pareciam inevitáveis) que não ultrapassaram o limite de atenção? No rescaldo da crise financeira mundial de 2008-2009, amplamente considerada como um acontecimento do tipo cisne negro, a disciplina do risco (incluindo as agências de classificação de crédito), foi abalada até os alicerces. Sem dúvida, a crise do crédito foi uma indicação do fracasso na compreensão e gestão de risco, mas os erros políticos e a imprudência do público foram igualmente responsáveis. Nestas circunstâncias, é difícil efetuar uma contabilidade forense do desempenho da gestão de riscos, mesmo com uma pretensão de precisão.

A gestão de riscos também partilha a dificuldade sentida em muitas áreas operacionais de justificar o investimento a curto prazo para a obtenção de benefícios a longo prazo. “Investe-se em algo hoje e pode não se ver o retorno daqui a cinco ou dez anos, ou podemos vê-lo dentro de três meses” — refere Heading. “Dependendo do que está se tentando controlar, pode ser muito difícil articular esse tipo de custo-benefício de uma forma que seja facilmente compreendida pelos executivos”.

Os executivos reconhecem os desafios da medição do desempenho da gestão de riscos. Cerca de três quartos dos entrevistados concordam que a falta de métricas de avaliação normalizadas para medir o risco dificulta a demonstração de progressos.

“É essencial criar métricas que relacionem os riscos aos objetivos organizacionais e garantir que sejam claros, desde o trabalho de base até o conselho e a liderança executiva” — afirma Fishman. “As ferramentas podem ajudar, mas a estrutura de medição dos riscos diretamente ligados às atividades e ao seu impacto é fundamental. É necessário observar este impacto, mas também entender os fatores causais. Por exemplo, embora a medição dos ciberacontecimentos seja importante, é igualmente crucial medir a eficácia com que processos e sistemas corrigem vulnerabilidades e garantem a continuidade dos negócios”.

Recursos

Poucos departamentos se consideram adequadamente financiados, mas o argumento dos gerentes de risco é particularmente forte. Isto devido a que as organizações tendem a financiar a função de modo a refletir o panorama de risco do passado, em vez de equipá-la para se preparar para o futuro. A amplitude e a complexidade dos riscos enfrentados pelas organizações têm aumentado constantemente à medida que as cadeias de suprimentos se estendem e se tornam mais enxutas, e à medida que a tecnologia acelera o ritmo da mudança. Do mesmo modo, as organizações podem recorrer a um conjunto crescente de ferramentas para monitorar o risco e criar resiliência, mas estas exigem grandes despesas iniciais e, como já foi mencionado, o momento e a dimensão do retorno do investimento são difíceis de quantificar.

Os entrevistados refletem sobre a percepção de que os departamentos de risco não dispõem de recursos suficientes. Os executivos acreditam que os recursos financeiros, tecnológicos e humanos da sua organização dedicados à gestão de riscos são insuficientes, com quase dois terços a afirmarem que a sua organização precisa de melhorar neste domínio.

Parte do desafio reside no fato de que, à medida que as organizações se tornam cada vez mais digitais, os gestores de risco têm de possuir um âmbito de especialização mais amplo. Isto significa que, mesmo para manter um nível consistente de proteção, as empresas têm de gastar mais para atrair os conjuntos de competências necessários para a função de gestão de riscos. “Os gestores de risco são um produto de primeira necessidade” — afirma Fishman. “Mesmo com as demissões em massa nos setores financeiro e tecnológico, é difícil encontrar bons gestores de riscos”.

Com desenvolvimentos como a IA, a automação e a robótica a exigirem atenção, é provável que este gargalo se agrave. Juntamente com a abordagem de tecnologias como a computação quântica e a tecnologia de registo distribuído à escala, não haverá espaço para complacência no setor da gestão de riscos num futuro previsível.

Coordenação

Como já abordamos, um requerimento essencial da gestão de riscos nos próximos anos será a capacidade de levar a mentalidade de risco a todos os cantos da empresa. Os fluxos de informação ascendentes devem ser coordenados em toda a organização, com os gestores de risco estabelecendo as regras e ferramentas que todos os departamentos e funcionários devem utilizar. A liderança geral (*Top-down leadership*) precisa dar o tom para que a função central de criar resiliência contra ameaças conhecidas e desconhecidas permeie a cultura organizacional. Os parceiros, fornecedores e clientes devem ser incluídos na rede, ampliando o radar de risco da

organização para além das suas paredes. Todo o aparelho de gestão de riscos deve centrar-se no que está acontecendo no dia a dia na empresa, mas também, e de forma crítica, no que poderá acontecer no futuro, dadas as tendências emergentes. Os negócios mais bem sucedidos serão aqueles em que este esforço é concebido e coordenado por gestores de risco de topo, munidos das competências e dos recursos exigidos por um ambiente em rápida transformação e com o apoio dos executivos sêniores.

O percurso da gestão de riscos ainda não está completo, mas a direção a seguir é promissora.



Conclusão

A gestão de riscos percorreu um longo caminho desde a sua primeira manifestação como uma função organizacional distinta. Evoluiu de uma disciplina limitada principalmente ao setor bancário, em que a solução consistia em criar almofadas financeiras mais generosas para garantir a liquidez durante uma evolução adversa do mercado, para um elemento central da gestão moderna. Os gestores de risco ocupam um lugar de destaque nas organizações de todos os setores, tanto no setor privado como no público. Apreendem e quantificam as ameaças mediante uma vasta gama de fatores, que surgem tanto dentro como fora da organização, onde existe menos visibilidade e controle. A gestão de risco se adotou a níveis cada vez mais elevados do negócio, com muitos gestores de risco trabalhando atualmente na direção executiva (*C-suite*), com acesso ao CEO ou ao conselho de administração. Esta tem sido a direção seguida durante algumas décadas, e a função continua a ser cada vez mais integrada.

Contudo, estão surgindo novos desafios e os antigos estão se transformando à medida que a tecnologia, a geopolítica e as mudanças sociais afetam o ambiente operacional. A gestão de riscos sempre foi uma disciplina dinâmica, mas a necessidade de mudança é cada vez mais urgente. Este novo século está marcado por uma série de perturbações ao nível mundial. Desde a crise financeira global de 2008-2009 e a subsequente crise de confiança na democracia liberal, até à pandemia da COVID-19 e à invasão da Ucrânia pela Rússia, os movimentos tectônicos nos assuntos mundiais multiplicaram a incerteza. Isto aconteceu no contexto de uma transição há muito estabelecida, mas em aceleração, para um cenário digital, bem como de preocupações ambientais que estão afetando as empresas, a sociedade, a política e a economia global.

A aceleração da adoção do digital, exemplificada pelo surgimento de modelos linguísticos generativos pré-treinados de grande dimensão, é simultaneamente promissora e ameaçadora. Ao mesmo tempo que promete criar uma nova geração de ferramentas para auxiliar as organizações a monitorar e a responder aos riscos, comporta a ameaça de preparar agentes maliciosos com armas igualmente inovadoras para roubar ou corromper dados preciosos. Os novos padrões de trabalho, em particular o crescimento do trabalho remoto, expandem e dissolvem a linha da frente digital da organização, abrindo novas rotas para as ciberameaças.

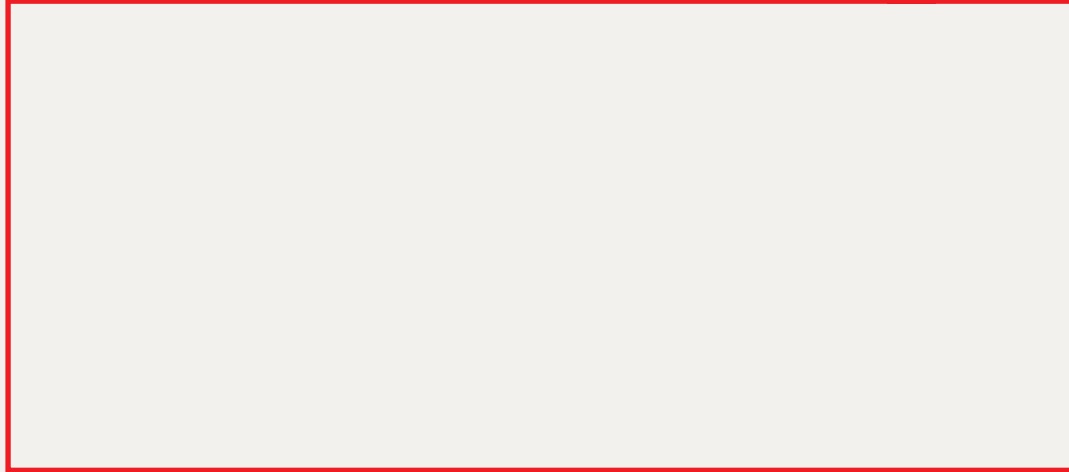
Os gestores de risco estão prosseguindo a viagem iniciada há décadas, incorporando uma abordagem “orientada para o risco” até as operações na empresa toda. Estão lidando com a natureza cada vez mais contingente do risco, na qual um evento num canto remoto da cadeia de abastecimento pode produzir ramificações imprevistas em outros locais.

De forma crítica, estão também fazendo a transição de uma postura reativa para uma postura proativa. A primeira abordagem se centra na criação de resiliência contra ameaças esperadas e na resposta a elas quando se materializam. No segundo caso, os gestores de risco gastam recursos e esforços na análise do horizonte para detetar ameaças não refletidas no registo de riscos, preparando-se para cenários que podem parecer improváveis e que comportam um elevado potencial de danos.

No atual cenário de riscos em constante mudança, mais amplo, mais rápido e mais complexo do que nunca, adotar a abordagem proativa pode ser a ação mais eficaz que a disciplina de gerenciamento de riscos pode adotar para se preparar para o futuro.

Redefinição de riscos: passar da reação à antecipação

Embora tenham sido empreendidos todos os esforços para verificar a exatidão destas informações, a Economist Impact não pode assumir qualquer responsabilidade ou compromisso pela confiança que qualquer pessoa deposite neste relatório ou em qualquer das informações, opiniões ou conclusões apresentadas no presente relatório. As conclusões e opiniões expressas no relatório não refletem necessariamente as opiniões do patrocinador.



LONDON

The Adelphi
1-11 John Adam Street
London WC2N 6HT
United Kingdom
Tel: (44) 20 7830 7000
Email: london@economist.com

GENEVA

Rue de l'Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
Email: geneva@economist.com

SÃO PAULO

Rua Joaquim Floriano,
1052, Conjunto 81
Itaim Bibi, São Paulo,
SP, 04534-004
Brasil
Tel: +5511 3073-1186
Email: americas@economist.com

NEW YORK

900 Third Avenue
New York, NY 10022
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
Email: americas@economist.com

DUBAI

Office 1301a
Aurora Tower
Dubai Media City
Dubai
Tel: (971) 4 433 4202
Fax: (971) 4 438 0224
Email: dubai@economist.com

HONG KONG

1301
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
Email: asia@economist.com

SINGAPORE

8 Cross Street
#23-01 Manulife Tower
Singapore
048424
Tel: (65) 6534 5177
Fax: (65) 6534 5077
Email: asia@economist.com