IMAGEM: KIPPER

ESPECIAL LOGÍSTICA

Vulnerabilidade na rede

As empresas estão sujeitas a um amplo espectro de riscos e perturbações que podem interferir drasticamente em seu desempenho, o qual pode se irradiar por toda a sua cadeia de parceiros. Entretanto, nem sempre elas estão preparadas para enfrentar, e superar, tais perturbações. Na prática, muitas empresas reagem aos eventos só depois que eles acontecem. O artigo mostra como contornar essa situação mediante o fomento de uma cultura de gestão de riscos na cadeia de suprimentos.

por **Henrique Luiz Corrêa** CRUMMER SCHOOL OF BUSINESS

Em uma pesquisa mundial recente, conduzida em setembro de 2006 pela empresa de consultoria McKinsey, constatou-se que 55% dos 3.172 executivos de empresas públicas e privadas entrevistados consideram que os riscos relacionados à gestão de redes de suprimentos que suas

empresas enfrentam aumentaram nos últimos 5 anos.

Ao mesmo tempo, 39% dos entrevistados consideram que suas empresas são, na melhor das hipóteses, “muito pouco capazes” de lidar com seus riscos atuais. Em que pese o caráter não científico da pesquisa,

esses dados são ilustrativos da ainda relativa insuficiência dos mecanismos de gestão de riscos em logística e redes de suprimentos usados atualmente, na visão dos seus próprios executivos.

Efeito em cascata. Essa insuficiência ganha cores mais fortes

quando consideramos que o crescente movimento de terceirização (*outsourcing*) e terceirização em escala mundial (*global sourcing*) dispersaram as redes de suprimentos, as quais freqüentemente cruzam fronteiras nacionais e continentais. Se, por um lado, o movimento de *global sourcing* tem trazido vantagens do ponto de vista dos custos, por outro tem trazido também um aumento significativo nos riscos envolvidos.

Uma rede de suprimentos global interconectada e interdependente atua como “vasos comunicantes” em que ocorrências e interrupções em qualquer lugar, potencialmente, causam efeitos em todo lugar. Considere um incêndio de pequenas proporções ocorrido em uma fábrica da Philips nos Estados Unidos em março de 2000, causado por um raio durante uma tempestade. Em menos de 10 minutos o fogo estava extinto pela ação automática dos *sprinklers* e pela ação rápida da brigada interna de incêndio. Ninguém se feriu e os danos materiais aparentemente foram superficiais.

Entretanto, assim como a perturbação de uma pedra que cai em um lago causa ondas concêntricas que se propagam, os efeitos do pequeno incêndio propagaram-se, causando consequências sérias não apenas para a Philips, mas para seus clientes, fornecedores e até mesmo para seus concorrentes. Ocorre que o pequeno incêndio aconteceu em uma das “salas limpas” da fábrica da Philips, responsável por etapas importantes na fabricação dos chamados *chips* de semicondutores que a empresa fornece, por exemplo, para clientes produtores

A gestão da resiliência organizacional, considerando seus potenciais impactos, deveria ser matéria de preocupação estratégica nas organizações, tanto quanto a gestão do próprio desempenho organizacional

de telefones celulares, como a finlandesa Nokia e a sueca Ericsson.

Salas limpas exigem um grau de limpeza do ar e de todas as suas superfícies muito maior que aquele exigido em um centro cirúrgico de um hospital. O simples fato de que a brigada de incêndio entrou com seus equipamentos para extinguir o incêndio tornou imediatamente o setor afetado inutilizável para operação. Outros setores ficaram igualmente afetados pela fumaça que se espalhou. O efeito imediato foi a inutilização de milhões de *chips* em diversos estágios de fabricação, comprometendo a produção de milhões de telefones celulares.

Ainda pior, a recuperação das salas limpas, necessárias para a retomada da produção, levaria semanas – e levaria meses para recuperar o conseqüente atraso no programa de produção. A Nokia, por exemplo, que contava com os *chips* para o lançamento de uma nova geração de telefones celulares, concluiu que algo como 5% da sua produção anual poderia ser perdida, dado o *boom* de demanda que o mercado estava vivendo. Isso complicou ainda mais a questão pela dificuldade de encontrar capacidade produtiva em outras fábricas (todas trabalhando próximas de seu limite de

capacidade) da Philips para transferir a produção afetada.

Com a realocação da produção, e com a necessidade de a Philips atender a Nokia (um dos principais clientes), outros clientes das outras fábricas da Philips acabaram também afetados. Também foram prejudicados os fornecedores, que tiveram de redirecionar suas entregas para os novos locais de produção e re-escalonar suas compras (afetando seus fornecedores), sua produção, suas entregas e seus recebíveis, devido à redução das taxas de produção da Philips.

O impacto do pequeno incêndio levou mais de 9 meses para se resolver. Os prejuízos diretos da Philips foram de algo em torno de US\$ 40 milhões (não muito para a gigante holandesa), mas isso não foi nada em comparação com o prejuízo de alguns de seus clientes. A Ericsson, por exemplo, estima seus prejuízos imediatos como próximos de US\$ 500 milhões – pela falta dos componentes fornecidos pela Philips, seus produtos não puderam ser produzidos e, portanto, não puderam ser vendidos. Como resultado, a participação de mercado da Ericsson caiu de 12% para 9% naquele ano. Interessantemente, entretanto, no mesmo período e sujeita à mesma perturbação, a Nokia teve sua par-

ticipação de mercado aumentada de 27% para 30% (Sheffi, 2005). Nesse ponto poderíamos nos indagar sobre o porquê dessa diferença.

Resiliência organizacional. A diferença pode ser rastreada pela maneira como as duas empresas lidaram com a interrupção. Essas diferentes formas de lidar explicam os diferentes níveis de resiliência apresentados pelas duas empresas nesse episódio. Resiliência, no caso, significa a capacidade de uma rede de suprimentos

manter seu funcionamento eficaz ou recuperar seu funcionamento eficaz depois de uma perturbação como a ilustrada pelo exemplo que demos anteriormente.

A gestão da resiliência organizacional, considerando seus potenciais impactos, deveria ser matéria de preocupação estratégica nas organizações, tanto quanto a gestão do próprio desempenho organizacional. Esforços para o aumento da resiliência organizacional, por si só, não fazem com que o nível de desempenho

organizacional aumente (pela redução de seus custos ou pelo aumento de suas receitas), mas visam garantir que os níveis de desempenho não caiam com eventuais perturbações, evitando custos adicionais ou quedas na receita.

Ambos, gestão de resiliência e gestão de desempenho, afetam os níveis de resultado organizacional, mas justificar esforços para aumento de desempenho é, em geral, muito mais fácil do que justificar esforços para evitar queda em desempenho, sobretudo pela dificuldade de quantificar a magnitude e a probabilidade da queda a ser evitada. Isso talvez nos ajude a interpretar o sombrio diagnóstico da McKinsey. O primeiro passo para contornar essa realidade é entender melhor quais as perturbações a que uma empresa está sujeita e formas de preveni-las.

Mapeando e lidando com as perturbações. Há três tipos de perturbações a que uma rede de suprimentos pode estar sujeita e que, potencialmente, prejudicariam seu desempenho: perturbações aleatórias, perturbações acidentais e perturbações intencionais. Perturbações aleatórias ocorrem usualmente por fenômenos da natureza, como enchentes, terremotos, maremotos, furacões, tornados, raios e outros. As perturbações acidentais são as causadas por imprudência, imperícia, negligência ou outras, em geral não intencionais, na operação. Outros casos seriam a falência de fornecedores, a falta de mão-de-obra, os atrasos em entregas de insumos, os problemas de quali-

dade e os problemas no transporte de recursos. Finalmente, as perturbações intencionais são causadas por ações intencionais, tais como greves, ataques de terroristas, assaltos, roubo de carga, sabotagem e outros.

Como lidar com cada uma dessas perturbações? O primeiro passo é diagnosticar a probabilidade de ocorrência de cada perturbação e seu grau de severidade ou impacto para a operação. A Tabela 1 traz algumas sugestões de técnicas para avaliação de probabilidade e severidade por tipo de perturbação.

Depois de uma avaliação dos níveis de probabilidade de ocorrência e severidade (impacto) das perturbações, é necessário analisar o grau de vulnerabilidade da rede de suprimentos às potenciais perturbações. Isso é feito analisando-se a probabilidade e a severidade das perturbações simultaneamente. É possível utilizar, para isso, uma matriz de vulnerabilidade, conforme ilustrado na Figura 1.

É importante que a empresa atinja um estágio em que o processo de gestão de riscos em logística e redes de suprimentos esteja integrado aos processos gerenciais estratégicos e operacionais da organização.

A partir da matriz de vulnerabilidade representada na Figura 1, quatro quadrantes podem ser identificados. No primeiro quadrante, alta vulnerabilidade indica potenciais perturbações que devem merecer o maior nível de atenção gerencial e esforço, requerendo planos especiais, que enfatizem controle para reduzir probabilidades e impactos, e flexibilidade. Exemplos são a falência de um fornecedor exclusivo, uma greve geral de portos ou de autoridades alfandegárias ou funcionários do transporte.

O quadrante Média vulnerabilidade I indica perturbações que podem ser tratadas por medidas gerenciais

operacionais normais, não requerendo em geral planos especiais com ênfase em ações de controle (para reduzir probabilidades). Exemplos são atrasos na entrega de materiais, quebras menores de máquina, absenteísmo em níveis normais e acidentes rodoviários menores na distribuição de produtos.

O terceiro quadrante identificado, Média vulnerabilidade II, indica perturbações que também demandam ações especiais e atenção gerencial com ênfase maior na redução do impacto da ocorrência quando já se houver reduzido a probabilidade de ocorrência ao mínimo viável. Exem-

Tabela 1 – Avaliação dos níveis de probabilidade de ocorrência e severidade (impacto) de diferentes tipos de perturbações que potencialmente podem afetar redes de suprimentos

PERTURBAÇÕES	PROBABILIDADE DE OCORRÊNCIA	SEVERIDADE DA OCORRÊNCIA
Aleatórias	Estimadas a partir de dados históricos. Exemplo: mapas de atividade eólica para detecção de regiões e correspondentes probabilidades de ocorrência de furacões e tornados.	“O que aconteceria se...?” • Uma enchente fechasse a fábrica por uma semana? • Uma nevasca na região de um fornecedor impedisse o fornecimento do item por 1 mês?
Acidentais	Estimadas a partir de dados históricos do setor industrial. Exemplo: histórico de nível de pontualidade de entregas pelos fornecedores para avaliação de probabilidade de atrasos.	“O que aconteceria se...?” • Determinado fornecedor não pudesse entregar peças por um mês? • Nosso website ficasse fora do ar por um dia devido a uma pane no fornecedor de serviços
Intencionais	Estimadas a partir de dados históricos. Exemplo: distribuição de assaltos por região.	“O que aconteceria se...?” • Sabotadores alterassem o conteúdo de um dos produtos dentro dos frascos? • Uma partida inteira de produtos fosse roubada no processo de distribuição?

É importante que a empresa atinja um estágio em que o processo de gestão de riscos em logística e redes de suprimentos esteja integrado aos processos gerenciais estratégicos e operacionais da organização.

plos são as perturbações causadas por fenômenos naturais raros, como furacões e enchentes.

Finalmente, o quadrante Baixa vulnerabilidade indica perturbações que, em geral, são tratadas pelo gerenciamento normal da organização, não requerendo igualmente planos especiais nem prioridade de ações. A análise de vulnerabilidades deve ser constantemente revista e atualizada, pois mudanças nos ambientes internos e externos das redes de suprimentos podem fazer com que o panorama de vulnerabilidades mude substancialmente em um período relativamente curto de tempo.

Combatendo os riscos. As ferramentas e conceitos discutidos anteriormente são essenciais para que uma empresa defina suas ações referentes à gestão de riscos em logística e redes de suprimentos. Entretanto, seu uso não deveria ser esporádico ou eventual. É importante que a empresa atinja um estágio em que o processo de gestão de riscos em logística e redes de suprimentos esteja integrado aos processos gerenciais estratégicos e operacionais da organização. A seguir, propomos um programa em passos que pode auxiliar a empresa a atingir esse estágio.

O primeiro passo é a identificação dos estágios críticos da rede de supri-

mentos (tanto do ponto de vista interno quanto externo da organização), considerando fornecedores, clientes, colaboradores e unidades operativas. Para isso, inicialmente, o gestor deve analisar o portfólio de produtos e serviços da empresa para identificar os mais críticos (estrategicamente mais importantes), utilizando o princípio de Pareto.

Em seguida, é necessário analisar as listas de materiais dos produtos e serviços estrategicamente mais importantes a fim de identificar seus itens críticos. O gestor pode, então, identificar os recursos internos críticos, bem como aqueles dependentes de parceiros da rede de parceiros ou fornecedores, usados na produção destes itens. Esses recursos representam os estágios críticos da rede de suprimentos.

O segundo passo é a identificação das possíveis perturbações que poderiam afetar os estágios críticos da rede de suprimentos. Essa iden-

Figura 1 – Matriz para análise de vulnerabilidade de aspectos de uma rede de suprimentos.

tificação pode beneficiar-se do uso de **brainstorming** com membros da organização (geração exaustiva de idéias sem avaliação crítica prévia) a fim de gerar a lista de possíveis perturbações que poderiam afetar os estágios críticos identificados no passo anterior. Com base na lista de potenciais perturbações, o gestor deve fazer uma pré-avaliação, eliminando as totalmente implausíveis.

O terceiro passo consiste em o gestor analisar a vulnerabilidade de sua rede de suprimentos. Aqui ele deve estimar a probabilidade de ocorrência e severidade (impacto) de cada uma das perturbações identificadas no passo anterior (confira a Tabela 1). Então, o gestor deve utilizar a matriz de severidade para classificar essas perturbações mais prováveis (confira a Figura 1).

No quarto passo o gestor deve

então desenhar as estratégias de gestão de risco para sua rede de suprimentos. Para os diferentes níveis e tipos de vulnerabilidade, ele deve estimar as possibilidades de uso de estratégias de “controle” (redução da probabilidade de se ter de lidar com a perturbação) e de “reação” (redução da severidade ou impacto da perturbação), ambas ilustradas na Tabela 2. Por fim, o gestor deve planejar, cuidadosamente, a implantação das estratégias, considerando aspectos usuais na gestão de mudanças organizacionais.

Por fim, o quinto passo desse programa de implantação de uma cultura de gestão de riscos é a criação de uma sistemática de avaliação periódica e de aperfeiçoamento contínuo das estratégias de gestão de risco em logística e redes das redes de suprimentos implantadas.

Naturalmente, os passos aqui

apresentados são apenas um roteiro sugerido. O mais importante é as organizações tomarem consciência de que podem antecipar-se a possíveis problemas de desempenho ocasionados por perturbações a que estão fatalmente sujeitas. A literatura sobre gestão de riscos em logística e redes de suprimentos está, infelizmente, repleta de exemplos de casos de empresas desastrosamente afetadas por essas perturbações, demonstrando que a cultura de gestão de riscos ainda não está disseminada. Esperamos que, no futuro próximo, esse cenário aponte no sentido inverso do que temos hoje.

Henrique Luiz Corrêa
Ph.D pela Warwick Business School
Prof. na Crummer Graduate School of Business, Rollins College, EUA.
E-mail: hcorrea@rollins.edu

Tabela 2 – **Exemplos de controle e reação aos vários tipos de perturbação que potencialmente afetam as redes de suprimentos**

PERTURBAÇÕES	CONTROLE	REAÇÃO
Aleatórias	• Troca de fornecedor para outros localizados fora de zona sujeita a interrupções por nevasca • Proteção estrutural de fábricas e armazéns para suportar níveis mais altos de perturbações	• Sistemas de informação redundantes e atualizados para facilitar continuidade ou restauração depois de incêndio • Comunicação rápida e eficiente internamente e com instituições externas
Acidentais	• Uso de parceiros na rede com saúde financeira mais robusta • Coordenação com parceiros da rede para sofrer menos perturbações como as causadas pelo “efeito chicote”	• Padronização de partes para facilitar realocação de produção e de materiais em caso de perturbação • Uso de estoques e capacidade extra para mais rápida reação a perturbações
Intencionais	• Troca de localização de subsidiária para região considerada menos “alvo” ou mais segura • Investimento em segurança, políticas de passwords, firewalls e programas antivírus atualizados	• Linhas de comunicação direta e rápida com autoridades, instituições e parceiros • Uso de tecnologia para facilitar rastreabilidade de bens, recursos e pessoas