January 2017 | Feature Stories

Expect the Best, Plan for the Worst & Prepare to Be Surprised

By Sandra Beckwith

It's not if your supply chain will be disrupted, it's when. Risk assessment and advance planning will help minimize the impact on business.

In late August 2016, Gap Inc. experienced the type of supply chain disruption that's hard to predict or prevent—a massive fire in its 990,000-square-foot Fishkill, N.Y., distribution center. The facility represents about 10 percent of the retailer's U.S. warehouse capacity. In its September sales report, Gap noted that the suspected arson "negatively impacted Gap Inc.'s September 2016 comparable sales by approximately 3 percentage points."

One year earlier, Costco was sued by a California woman for selling shrimp raised with feed—fish— collected by slave labor in Thailand's waters. She cited California's Transparency in Supply Chains Act of 2010, which is designed to fight slavery and human trafficking. It bars companies from making false claims about illegal conduct in their supply chains.

Costco had been alerted to the potential for slave labor one year earlier, and was investigating the situation, so the potential impact on its shrimp supply chain had already been triggered. But the negative impact on its reputational supply chain after the slave labor suit made national news? It has to be significant.

While fire is nearly always a risk at any storage facility, the possibility of slave labor involvement in a supply chain might seem remote to companies without global supply chains. Still, both show up in the supply chain disruption risk list in the Supply Chain Resiliency Report 2016 recently released by The Business Continuity Institute (BCI). They rank 14th and 21st, respectively.

The BCI list, compiled from surveys of 526 people in 64 countries and 15 industries, includes the following top 10 supply chain disruption risks:

- Unplanned IT or telecommunications outage
- Loss of talent/skills
- Cyber attack and data breach
- Transport network disruption
- Outsourcer failure
- Adverse weather
- Currency exchange rate volatility
- New laws or regulations
- Act of terrorism
- Insolvency in the supply chain

The report also details the economic impact of the disruptions. Of those surveyed, 70 percent experienced at least one supply chain disruption, while one-third reported cumulative losses of at least $1.2 million as a result. A single incident generated that loss level for 9 percent of respondents.

GETTING LEADERSHIP BUY-IN

How prepared are companies for that level of disruption? Not as prepared as you'd think, considering what's at stake. While nearly three-quarters report having business continuity arrangements in place for their supply chains, only about one-quarter say top management is committed to supply chain resilience. That's down from one-third in 2015.

That lack of leadership buy-in is a problem, says Nick Wildgoose, global supply chain product leader at Zurich Insurance Group, which provided financial support for the study.

"If you haven't got your C-suite on board with what you're doing, then it's very difficult for bottom-up initiatives to improve supply chain risk management," he says. "To make progress, you need resources. The only way to open up a sensible amount is to get senior management approval, and that's one of the biggest challenges."

Chicago consulting firm Crowe Horwath LLP is exploring the impact leadership risk has on supply chain issues. The firm takes clients through an exercise that explore risks by acknowledging that events in the supply chain are interrelated.

"If you mitigate leadership risk, does that significantly impact lead time risk? Maybe the company needs to allocate resources to leadership risk," says Mike Varney, a partner in the risk consulting practice.

Wildgoose recommends identifying what's important in the supply chain— "critical nodes"—and studying the impact that node has on the most profitable product or service. What happens if there's a failure with that node?

"Calculate to the nearest $10 million, because the exposure is at that magnitude," he says. "The reaction we get from senior management when we do this is, 'What do we have to do to fix this?'"

He also recommends presenting case studies from the company's industry.

There's a third option, too. "The most painful way to get support is to have a crisis that forces management to say, 'We have to do something about this,'" Wildgoose adds.

The BCI report also reveals that two-thirds of companies don't have full supply chain visibility, defined as firm-wide reporting of disruptions.

"There's clearly a gap in terms of awareness in managing their supply chain risks," says Patrick Alcantara, a senior research associate at BCI and the study's author. "When you know that 70 percent of the companies will experience supply chain disruption in the next 12 months, one of the best ways to be prepared is to have full supply chain visibility. Yet a similar percentage of organizations don't. It's like they're flying blind."

RISK AT ALL LEVELS

According to the report, most disruptions—41 percent—occur with Tier 1 suppliers, but a growing proportion of incidents are occurring with Tier 2 and Tier 3 suppliers, as well. Those disruptions increased by 2 points to 31 percent in 2016. This reinforces the need to not only identify key suppliers, but to understand what's happening with them at all levels.

"Companies are asking how they can become more integrated from end to end in the supply chain so that their logistics are more visible and collaborative," says Yatish Desai, managing director and U.S. lead on distribution and logistics at KPMG LLP. He notes that they're sharing more information with third-party service providers and carriers, integrating them into business processes.

"This is where the innovation is taking place," he says.

As wise as that approach is, it isn't without risk, considering that hackers often break into a system through weaknesses in a supplier's connected network. Just one example from many in the headlines: The Target attack in 2013 that affected 70 million customers happened because hackers could take advantage of—"exploit"—a weakness in an HVAC vendor's network. Cyber attacks and data breaches rank third on BCI's list of risks, down from second the year before.

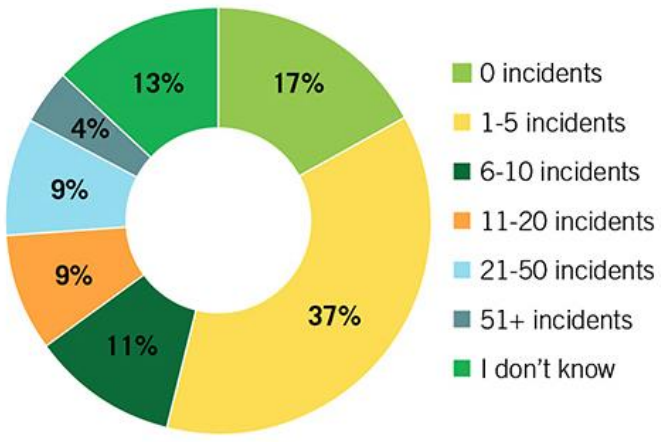
Protection from exploit attacks and other cyber risks is a priority at Yaskawa Motoman, an industrial robotics company, for exactly that reason.

"When you work with the government and auto manufacturers, security becomes a real focus," says Jeff Magnuson, IT architect at the Dayton, Ohio-based manufacturer.

Motoman uses Morphisec's Advanced Threat Protection solution to protect the company's IT systems from cyber risk and exploit software. Its protection is "the tiniest piece of software ever written in cyber security," says Omri Dotan, Morphisec's chief business officer, based in Israel.

Once installed, it continuously changes the system's memory in real time, creating new memories. Exploit software can't react quickly enough so when it attacks an "old" system memory, it's trapped.

SUPPLY CHAIN DISRUPTION IS COMMON



Source: BCI Supply Chain Resilience Report

CONFUSING THE HACKERS

"We change the predictability function so we're unpredictable, which confuses hackers," says Dotan. "When we move the target around, we leave behind a little decoy that looks like the original thing to make sure the attacker gets lured in. As soon as he opens that 'door,' we know he's a hacker because he shouldn't be there."

"We recently caught a few big ones," says Magnuson. "These exploits can pull information off the machine, and we're held liable for that confidential information. If anything's stolen from a customer or vendor, and people in the field find out about it, you may not be able to get the parts or supplies you need for your business anymore."

WEATHER WATCH

Just as cyber threats make global headlines, so do natural disasters that include hurricanes, tornadoes, and earthquakes. In fact, half (51 percent) of businesses surveyed for the 2016 Travelers Business Risk Index believe that severe, damaging weather events have become more frequent in the United States.

One of the more recent was Hurricane Matthew in fall 2016. The impact was felt beyond businesses in the storm's path. The anticipated disruption in the Caribbean and southeastern United States also affected businesses elsewhere that depended on companies in the region for supplies and transportation.

Forklift manufacturer Hyster Company, itself affected at its Greenville, N.C., headquarters, knew that 32 of its Tier 1 suppliers were at risk, too. How? The company learned from its experience with the 2011 tsunami in Japan that it needed to be able to assess the risk to its supply chain more quickly.

The result is a software-based risk impact tool it created that lets the company identify Tier 1 suppliers by location, what products are connected to each supplier, and which customers buy products manufactured with parts from each of those suppliers.

"We build to order, so every truck that comes off the line has a unique customer purchase order attached to it," says Mark Champagne, director of supply chain for the Americas. "If the supply of a part is disrupted, I need to know which customer is affected."

Taking action on Hyster's tsunami lessons paid off during Hurricane Matthew, when the company was able to not only identify suppliers in the hurricane's path, but also contact them plus customers. And they did this while working remotely because much of the headquarter's region was flooded.

"Planners and procurement took their laptops home on Friday. When we couldn't get to work on Monday, we were on a conference call by 8:15 a.m., going through the list of suppliers that were probably affected," Champagne says. "Without this tool, we would have spent all of Monday and Tuesday just going through supplier databases and tracking down addresses."

On the other side of the country, Portland, Ore., operations and supply chain consultant Rick Pay has had to plan for supply chain disruptions caused by bad weather of a different kind—snow. When Pay, principal of The R. Pay Company, LLC, was vice president of operations at a technology manufacturer, the company bought a large quantity of parts from Los Angeles suppliers. Trucks carrying the parts were often delayed as much as one week when the highways were impassible because of mountain pass avalanches.

"We learned to bolster our parts inventory during the four months of avalanche season because one week can make a big difference in just-in-time systems," Pay says.

CYBER RISKS AND CONCERNS

Respondents who say they worry a great deal or some about each cyber risk concerning their company, according to the 2016 Travelers Risk Index.

	All businesses	Small businesses	Midsized businesses	Large businesses
Security breach: Someone hacking into computer system	49%	36%	56%	53%
Computers becoming damaged, going down	48%	45%	48%	51%
Someone gaining access to banking accounts or financial control systems	46%	42%	48%	48%
Employees putting information/systems at risk through unsafe computing practices or by using personal devices for business	45%	30%	48%	54%
Having the resources and know-how to recover from data-related breaches	42%	35%	53%	46%
Potential for theft or loss of control of customers or client records	41%	28%	45%	52%
Remote access or hacking into supervisory control systems or other business operational software systems	40%	27%	45%	49%
Shortage of skilled cyber security talent that can keep ahead of cyber threats	36%	24%	44%	49%
Using online cloud storage for data or information	34%	26%	39%	38%
Company being a victim of cyber extortion	31%	23%	31%	43%
Someone using email or other social engineeering techniques to fool employees into transferring company funds erroneously	31%	19%	33%	44%

RISK ASSESSMENT IS KEY

These kinds of risks—whether they're related to cyber security, extreme weather, or dock strikes-can be identified and planned for in advance with a risk assessment that starts at the corporate level with business continuity planning and drills down to the supply chain specifically.

"Many companies tend to think of risk in terms of insurance, but there are many other mitigations for supply chain risk, so the perspective needs to be more holistic," Pay says.

Wildgoose at Zurich, which looks at 23 risk areas with clients, agrees. "Many do financial due diligence on their logistics providers, especially after the Hanjin bankruptcy, and think that's risk management," he adds. "What about production, key ports, and suppliers' intellectual property situations?"

Ken Katz, property risk control director at Connecticut insurer The Travelers Companies Inc., helps companies reduce exposure to loss. That starts, he says, with a four-step planning process:

1. Risk assessment
2. Business impact analysis
3. Prevention mitigation and recovery
4. Implementing, testing, and improving the plan

"The goal is to identify what can be done better before it's necessary," Katz says.

"One of the best ways to plan for supply chain risk is through scenarios," adds Varney at Crowe Horwath. "It's the 'what if' approach. If you've got stronger supplier transparency as part of scenario planning, your preparedness is even stronger."

Incorporating suppliers in scenario planning also helps organizations anticipate and address supplier weaknesses they might not otherwise uncover, according to Brad Steger, senior vice president for supply chain management and vertical solutions at Atlanta software company Aptean.

"If you know you're going to ask a supplier for another 20 percent of inventory in a certain situation, and the vendor reassures you that it keeps 40 percent extra in inventory, what happens if another company needs an additional 20 percent, too?" he asks.

RISK IN THE TRANSPORTATION SECTOR

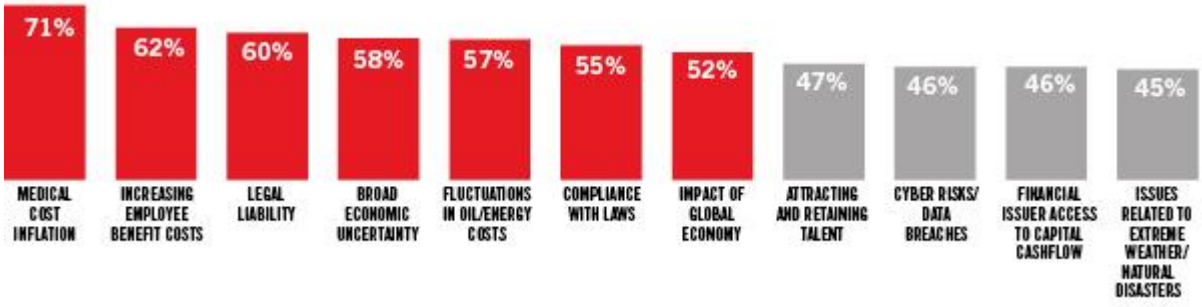
In terms of general risks, medical cost inflation, rising employee benefit costs, and legal liability (including the risk of the business being sued) are the top concerns for the transportation industry (71%, 62%, and 60% respectively), according to respondents to the 2016 Travelers Risk Index. Other concerns specific to the transportation industry are:

- Rising workers compensation claim costs (52%)
- Company computers being damaged or going down (52%)
- Distracted driving as a cause of accidents (under employee safety risk) (52%)
- Ability to retain skilled/experienced employees in a competitive labor market (45%)

Emerging risks:
When asked about emerging trends, respondents list a changing workforce (52%) and the uncertain dynamics of the energy industry (51%) as main causes for concern.

BIGGEST GENERAL RISKS IN THE TRANSPORTATION INDUSTRY

Respondents to the 2016 Travelers Risk Index worry a great deal or some about these threats to their business.



ADDRESSING COMMON RISKS

Risk assessment is only part of the planning, though. Companies need solutions for the supply chain disruption risks they identify. In addition to those already discussed, here are other ways organizations address common risks.

Diversify suppliers geographically so one region doesn't dominate the supply chain. When asked to choose supply chain risks with the greatest disruptive potential, the top choice—32 percent—for businesses of all sizes responding to the Travelers risk survey was the ability to get materials from suppliers.

Most of Pennsylvania-based Apprise Software Inc.'s customers import from China, where there are political risks to trade, so CEO Jeff Broadhurst encourages clients to diversify their supply sources as much as possible.

"If they can get some of their supplies from South America, they can mitigate multiple risks," he says, referring to natural or political disasters as well as dock strikes.

"The only thing that has shut down our business in the past decade is dock strikes in Los Angeles," Broadhurst adds.

Keep your supply chain short. The less transportation that's involved, the less risky it is, advises Pay. Ideally, he says, suppliers, designers, and production teams will be in neighboring time zones, too.

"When people can talk to each other because it's not morning for one and evening for the other, you shorten the communications supply chain as well," Pay says.

Use dual sourcing. Pay also encourages what he calls "dual-sourcing the technology and single-sourcing the part."

In other words, find more than one supplier for several related parts, and buy a single part from all of them, even though one might be able to provide all the parts needed. When one has a problem that interrupts the supply chain, order the part that's affected from another vendor the company is buying something else from already.

Hyster does this, dual-sourcing any large components it buys overseas.

Advocate for supply chain transparency. This is at the core of the Costco shrimp slavery issue.

"Transparency can be a big problem and given the current environment, organizations are working to drive that intimacy across the supply chain," says Varney. "It's important to identify how you work with and engage with suppliers, as well as knowing what you can do to understand where potential issues can arise."

Start by prioritizing suppliers, Wildgoose advises. "You might have 10,000 suppliers, but you probably need to understand only the top 100," he says.

Look to the cloud. Cloud computing adds a level of risk mitigation to information and operations, says Broadhurst. He recommends working with a cloud specialist.

"If you're hosted on Amazon or Microsoft, you're working with a company that invests significantly to make sure your data is secure and that the infrastructure is constantly upgraded," he says.

Connecting with the cloud also makes it possible for businesses to continue when they are literally underwater, as Hyster was during Hurricane Matthew. Cloud computing allowed headquarters employees to work from home when the region was flooded.

Eliminate functional silos. Make sure that purchasing and logistics groups understand risk management and work with the risk management team to prevent problems and identify solutions before they're needed.

Wildgoose cites an example at one organization where the new chief financial officer extended supplier payments to 60 days. Less than two weeks later, a key supplier went out of business because the new policy created cash flow problems.

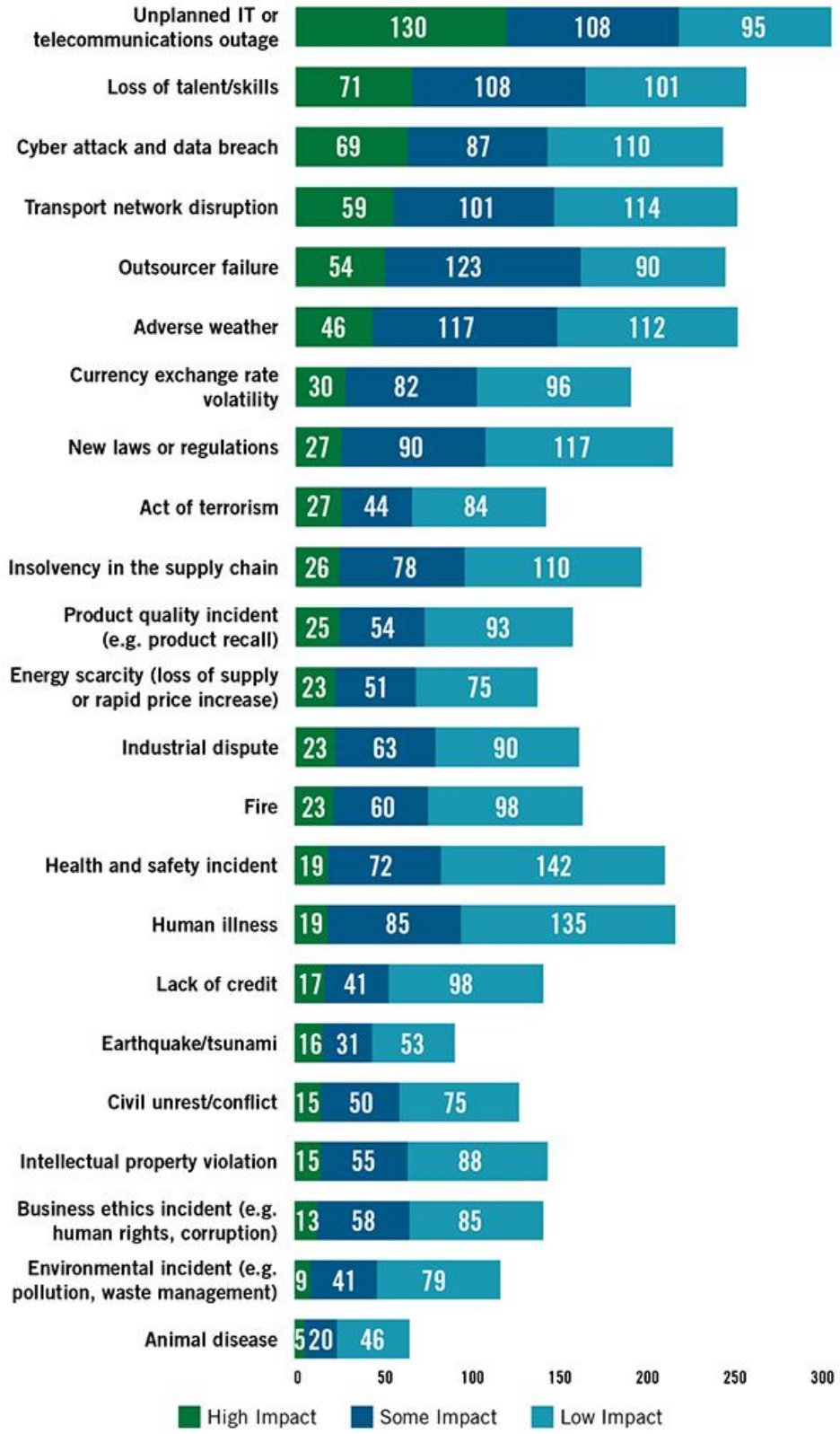
"They weren't thinking through the whole supply chain and talking to different teams," he says.

No matter what type of risk is keeping managers awake at night, vigilance is important. "You need to constantly evaluate and refresh your current knowledge of your supply chain," says Steger. "Your ability to react to these major events as they occur makes a big difference.

"If you can't serve a customer, somebody else can, and they will take that business and loyalty away from you quickly in today's world."

CAUSES OF SUPPLY CHAIN DISRUPTION

In its report, BCI consistently tracks the impact of various disruptions to an organization’s supply chains. Unplanned IT and telecommunications outages remain the top cause of supply chain disruption for the fifth consecutive year. The loss of talent and skills jumps three places from fifth in 2015 to second in 2016. Cyber attacks and data breach, meanwhile, drop one place from second in 2015 to third this year. Nonetheless, the percentage of respondents who say that cyber attacks and data breach had a “high impact” on their supply chains increased from 14% to 17%.



Note: responses to this question were voluntary, which explains the variance in the results.

Source: BCI Supply Chain Resilience Report