TUCK SCHOOL OF BUSINESS AT DARTMOUTH
Glassmeyer/McNamee
Center for
Digital Strategies

The Agile and Resilient Enterprise

A Thought Leadership Roundtable on Digital Strategies

The Agile and Resilient Enterprise

Thought Leadership Roundtable on Digital Strategies

An executive roundtable series of the
Center for Digital Strategies at the Tuck School of Business

The Thought Leadership Roundtable on Digital Strategies recently convened for a discussion on building agility and resilience in anticipation of unexpected business disruptions. How are companies approaching risk assessment, planning, preparedness and disaster response? What can be done to build resilience into enterprises' DNA? The sessions included academics and business leaders from Bechtel., Canadian Pacific Railway, Eaton, The Georgia Institute of Technology, Hasbro, IBM, ING, Massachusetts Institute of Technology, SYSCO, and the Tuck School of Business at Dartmouth.

Key Insights Discussed in this Article:

- **Unexpected disruptive events are increasing in frequency at the same time global business is becoming leaner and more interconnected, heightening the importance of investing in resilience and agility................................ 2, 4, 5**
  Companies face a constant tradeoff between preparedness and efficiency.

- **It's the planning—not the plan—that matters most: building general capabilities is far more effective than trying to anticipate and protect against specific threats................................ 5, 6**
  Companies should focus on establishing communications systems, building experienced response teams, and empowering local decision making and initiative.

- **Building flexibility is preferable to redundancy as a strategy for preparedness..................... 7, 8**
  The ability to quickly redeploy assets, resources, and people, is more powerful than specific, costly "redundancy" preparations like safety stocks, especially for low-likelihood, high impact scenarios.

- **Companies should use high profile events as catalysts to drive awareness, given the challenge of justifying time and resource investments in continuity planning................................ 3, 4**
  SARS, avian flu, Hurricane Katrina, 9/11 and port strikes all spurred companies to focus on resilience and agility.

- **People and relationships are key success factors in crisis response, and companies should focus their preparation energies accordingly 6**
  Pay particular attention to the well-being of employees' families and to the personal relationships with key suppliers.

- **Treat well-understood risks and completely unknown threats differently, both in preparation and response 5, 11, 12**
  Don't underestimate the "fear factor," confusion and potential effects of compounding issues and timing factors in an unknown scenario.

- **Resilience and risk management should be embedded in DNA as a core cultural value, like safety and quality 12, 13**
  There are competitive, brand, and operational advantages to a consistent, continuous, and well-integrated focus on risk management.

The Thought Leadership Roundtable on Digital Strategies (www.tuck.dartmouth.edu/roundtable) publication series is edited by Hans Brechbühl, Executive Director of the Center for Digital Strategies**.**

Introduction

As large-scale, unexpected business disruptions increase in frequency, and global businesses get leaner and become more interconnected, building agility and resilience into the enterprise takes on greater importance. How should executives think about preparing for abrupt change and business disruptions? What are best practices in risk assessment, planning, and response? And most significantly, how can companies build agility and resilience into their corporate DNA?

Approaches to Vulnerability and Risk Assessment

Many companies' current approaches to vulnerability and risk assessment have been galvanized or given new urgency by a variety of recent large-scale disruptions or threats.

Eaton's Rick Jacobs said that risk assessment, catalyzed by concerns about pandemic risk, is now a strong board-level focus for his company. "We convinced our COO it's really not about pandemic, but enterprise risk management," explained Jacobs. "We looked at it from a reputational, financial, and operational risk standpoint and even loss of key facilities." Though the company has identified and prioritized key threats within IT and supply chain, Jacobs said, it hasn't yet finished prioritizing threats company-wide.

SYSCO's John Holzem said his company's legal group took ownership of the risk assessment process following difficulties getting buy-in from the business side. His colleague Twila Day added: "It's really our executive council driving; legal was picked to coordinate because it wasn't going to be driven effectively from an operational standpoint." SYSCO ranks potential threats on both likelihood and impact, Day noted. But the company could do a better job drilling deeper into potential threat impacts, she said, as it had done with avian flu. "We have baseline plans related to weather or power outages, but we've had a difficult time getting buy-in."

IBM's Nancy DeLapp said that although her company previously had a broad-based corporate risk assessment team in place, the recent avian flu threat brought new life and structure to the effort. "The pandemic effort revitalized this process," concurred IBM's Michael Bradshaw, noting that traditionally risk management had been done at the divisional level, and mainly focused on IT and physical security. "It's gotten it out of the corporate ivory towers, where it was before, and down into the operations team."

IBM is now trying to determine which of its far-flung facilities it should prioritize under a risk management plan, DeLapp explained. The challenge, she said, is "to take all the diversity and decisions that have come through the years down to a tighter number you can actually manage, the key things we're doing right now." Everybody initially thinks their team and mission is the most important to protect, she added, "until you start going through the business scenarios—we're trying to make it an operational discussion."

Bechtel's Ed Richardson said his company routinely conducts detailed risk analysis, both by project and with a global geopolitical view, given its personnel exposure in many volatile areas. "We had folks held hostage by Saddam in Iraq in '91, we do pipeline work in Algeria and there's a civil war going on there," Richardson noted. "What happens if there's a war between India and Pakistan, and we can't take advantage of our engineering centers there … how do you pull the work back?"

His colleague Geir Ramleth added that the company's risk assessment process is a highly guarded piece of IP: "We think its one of our competitive advantages." He noted that Bechtel often must take on responsibility for large local civilian populations near its projects, in addition to the project employees. "There are huge ramifications of simple things like not getting food in there on a day-to-day basis, or if an epidemic starts," he explained. "A core value for us is the safety and health of our employees."

Hasbro's Doug Schwinn recalled that the SARS epidemic in Hong Kong helped jumpstart a reassessment of the company's enterprise risk management processes, after local authorities started shutting down and cordoning off entire floors of buildings. "So much of our business risk is in that area," he explained. "It was a very real wakeup call because the majority of our sourcing business flows through Hong Kong and Shenzhen."

SARS triggered a review by the board's finance and audit committees, Schwinn said, prioritized by revenue tiers, which determined that the company was "in pretty good shape" from a disaster recovery standpoint (e.g., IT and infrastructure), but not in terms of business continuity (distribution, sales, and marketing). The board charged the CFO with leading a senior management team to do a deeper dive on that piece, including global sourcing. "We're trying to take it up a notch," concurred Hasbro's Jackie Daya, "looking across the whole supply chain, including the quality piece, and asking a series of questions. Not just what happens if there's instability in China, but throughout the organization, is there inherent risk?"

ING's Steve Van Wyk suggested that leveraging independent assessment expertise is valuable in risk analysis, and said his company had worked with outsiders to develop an assessment process and do a geographic vulnerability analysis. "It helped us think about things we would have never thought of, like how transportation goes in and out of certain areas, and getting people to airports. It was interesting to get a sense of the vulnerability we had."

Canadian Pacific's Allen Borak said that when his company went public in 2001 as a spin out, the newly formed board engaged consultants to do a formal enterprise-wide risk management assessment. "We already understood a lot of the physical and operational risks and how we would deal with those," Borak said. "There isn't really a day goes by that a train doesn't fall of the track some place." But the outside assessment "helped us really understand some of the reputational risks and financial risks," he added. The new formal process is "reassessed annually at the corporate level with board oversight in terms of 'what are the 20 risks in the matrix, have we got them ranked properly in terms of the most damage if they occur.'"

What Risks Do You Care Most About?

Prioritizing risks is one of the most difficult pieces of vulnerability assessment, participants agreed. IBM's DeLapp pointed out that not everybody sees risk in the same light, for example “teams that live with the risk everyday.” If you ask a South Korean employee about what’s happening in North Korea, for example, they may not be as concerned “because they’ve just lived with it forever.”

Bechtel’s Ramleth agreed it’s hard to evaluate risk if you’re not close enough to know all the local details. But he also pointed out that if you are, you may not be able to evaluate the risk objectively. “We’ve got this multi-billion dollar project on the Pakistani border, and we think we’re putting it in the middle of a war zone,” he said. “But if you ask the local people they’ll say ‘There’s no conflict here. That’s my cousin!’” “You need both pieces,” DeLapp indicated. “They know what’s going on there, but they don’t necessarily understand the business risk associated with what you’re putting there.”

Tuck’s Hans Brechbühl noted that bringing groups with different perspectives together might be an opportunity to improve the risk assessment process. “Things could emerge that are maybe unanticipatable from one point of view, but not so if you put yourself in somebody else’s shoes.”

IBM’s Michael Bradshaw said getting people to be realistic about the severity of different threat scenarios is important, noting that during an internal pandemic assessment many employees felt electronic order taking capability would mitigate any physical disruption. “It’s not always as simple as people think,” he said. “While that may pertain to 27% of our revenue it doesn’t cover the whole business, not to mention that just because we can accept an electronic order, is anybody going to be placing one?”

Participants agreed that just the act of going through the risk identification process, especially on a continuous basis, can improve an enterprise’s ability to anticipate risk, and that its important to involve all levels of the organization, from the CEO and the board on down.

In terms of specific risks, participants assembled and categorized a list of threats. The final list (see Table) necessarily involved considerable overlap between categories. Tuck’s Eric Johnson noted that the risks put forward tended to fall into two buckets: shared risks that would affect all firms to some extent (e.g., natural disasters, terrorism), and those that would primarily affect individuals firms (e.g., ethics risks).

Table: Possible Threats

Terrorism
Data/privacy risk
Vendor/supplier risk
Technology risk (e.g., widespread virus)
Critical infrastructure (e.g., ports, utilities)
Natural disasters
Medical risk (e.g., avian flue, pandemic)
Product risk (e.g., safety)
Political risk
Human capital risk
Market risk (e.g., sudden currency fluctuations)
Ethical or reputational risk (e.g., child labor)
Regulatory risk

Eaton’s Rick Jacobs emphasized that although threats like nuclear war or pandemic or hurricanes are more dramatic, he personally worries more about things like the Suez Canal or the port of LA running out of capacity. “Are you really focused on the right risk?” he asked. “There have been hurricanes and natural disasters forever, but there are a lot of manmade things that you can see coming and most companies aren’t prepared for.”

Cargill’s Richardson said the distinction between a sudden out-of-the-blue event like 9/11 and a slower roll like Hurricane Katrina or the Gulf War is a big one. In the latter cases, he noted, “you could see something significant was going to happen, open up a command center and start keeping track of people.”

Different risk scenarios also come with different types of dependencies and compounding effects, all significant in the risk assessment process. “The avian flu is very geographic,” pointed out IBM’s DeLapp, “so we can make all the corporate decisions we want, but if the government in India decides to do nothing, or if the president of the U.S. decides to take resources and facilities, you have to deal with that.”

Eaton’s Jacobs also advised participants to look at supplier dependencies in each threat scenario, saying his company had recently surveyed 2,000 key suppliers; and most exhibited a “shocking” level of unpreparedness. Canadian Pacific’s Borak added that dependence on suppliers doesn’t just stop at your vendor, but goes to their own suppliers. “How far upstream do you go? It’s like unraveling a ball of string.”

And IBM’s DeLapp advocated using conservative rather than best-case scenarios in evaluating threats. “We’ve always assumed that if something happens within a day or two everybody’s kind of recovered,” she said. “But one of the things we’ve learned, from events like Katrina and the big hurricanes, is they can go on a long time and the employees needed to be home with their families and taking care of their families.”

Building Organizational Preparedness

Although most corporations have formal planning processes, participants agreed that planning for specific disruptions is less useful than building generic organizational capabilities.

ING’s Steve Van Wyk, who was with Morgan Stanley at the World Trade Towers on 9/11, related his key learning from that day: that capabilities matter more than plans. “We had 3,700 people in tower two, and my office was on the 67th floor,” he recalled. “You never plan for the one that’s going to happen. It really comes down to risk management, how you’re going to manage the crisis through. When it happened to us, never once did the plan come off the shelf.”

Eaton’s Rick Jacobs said his company is putting communications and control structures in place as a centerpiece of its preparedness process. “We broke out first-, second-, and third-level responses based on impact and time to recover,” explained Jacobs. “We also hired an external firm to help us put a communication tree and very rough playbooks together, so that you can reach out to the right person and they know what to do. Every quarter we expand it more, moving to the next level or area of risk.”

Hasbro’s Doug Schwinn suggested focusing on the decision-making process as a key to agility. “On the business continuity side, we’ve said we need to identify the decision makers and how structurally they would make the decisions.” MIT’s Yossi Sheffi agreed, pointing at flawed decision making as the critical failure point in FEMA's performance during Katrina. "This is something that you actually can exercise, drilling to hone the decision-making ability."

Tuck's Hans Brechbühl noted that the ability to make quick local decisions has often been decisive in disruptions, for example for the U.S. Army in military conflicts. And Sheffi recalled that the most effective government agency during Katrina was the Coast Guard, which includes "local initiative" as one of its top three guiding principles. "They're drilled in the fact that it's the boat captain and the local base commander who take action without asking Washington, and they ask for forgiveness later," explained Sheffi. "The one thing that will kill you in a disaster is the decision making," agreed Van Wyk. "It has to be extremely clear who's making the decision."

Geir Ramleth described Bechtel's formal mechanism for decentralized execution called DOR, or "division of responsibility," which breaks down what decisions can be made at what levels. "It's in the company's DNA, how you treat people when they make independent decisions," added his colleague Ed Richardson. "We have guys who, if we need something, they just take out their personal credit card, and they know they're going to get paid for it."

And Hasbro's Schwinn noted that his senior IT managers have put together a global team structure, which he thinks would function well in a crisis even if communication was cut off. "As part of the basis of our disaster plans, we identified the key points where expertise was around the world and everyday they get together," he explained. "That team, or whatever portion of it is left, knows that they are the decision makers." Schwinn also added that this team has already helped the company get out ahead of potentially disruptive events, such as a computer virus that came out of Asia. "By the time it hit the U.S. it was a non-event for us, even as it was crashing other companies," he recalled.

Canadian Pacific's Borak proposed that building strong relationships, especially with vendors, is another key organizational preparedness element. "A couple years ago one of our major fuel suppliers had a big refinery fire in a very tight supply situation," he recalled. "We had general plans about what we'd do, but the fact that our supply people had excellent relationships with the other major suppliers was what really made it work."

Several participants highlighted the importance of resource mapping during planning, with the Georgia Institute of Technology's Saby Mitra advocating a business process-oriented review of disaster preparedness, "mapping out what resources you'll really need to get your mission critical areas up and running." "We look at resource availability in the event of crisis," agreed Van Wyk, "and do a lot of testing to make sure our systems and people are going to be available."

Employees are the most valuable resource in a crisis, emphasized MIT's Sheffi, who offered British Petroleum (BP) as an example of best-of-breed planning to ensure the welfare of employees' families, enabling employees to stay on the job in a disruption. BP has built an information technology system for their oil platforms in the Gulf of Mexico, explained Sheffi, which tracks each employee's family, where they work or go to school, including elderly parents that the workers must take care of. "They have a team that will take care of them, so the worker can stay on the platform," he said. "Worrying about the family is something advanced companies understand and do very well."

Finally, exercising the "crisis management muscle" is an important part of organizational preparedness, participants agreed. "We did a war-gaming scenario the other day where a terrorist came into the facility," recalled Van Wyk. "When you work the memory muscle and you keep it going, people get good at it."

But the group also acknowledged that while being adept at such drills and tests in areas like IT disaster recovery are important, the real issue is that most organizations have lagged behind in doing so for business continuity preparedness. "In Katrina, the IT systems were all up and running," said SYSCO's Twila Day. "But it had nothing to do with IT, the employees had all left. That's the harder thing to test."

Getting to Resiliency: Redundancy vs. Flexibility

Making financial investments in resiliency, like bulking up on inventory, can be challenging as it's difficult to determine an ROI in advance for those investments. Instead, participants agreed that today's business environment requires a mix of strategies to build agility and resilience.

IBM's Michael Bradshaw noted that the business environment increasingly demands greater efficiency and takes slack from the system, often competing with the business continuity agenda. "In some of the competitive decisions we're trying to make, like single sourcing," he said, "we wrestle with the economics versus the risk."

Although a few participants said they'd bulked up on product inventories or key supply stocks like fuel in the wake of 9/11, the majority said that they were trying instead to make their supply chains and other key processes more flexible to achieve protection without the added cost.

"Redundancy is not just about adding inventory," explained SYSCO's Day, noting that her company has experience quickly reshuffling its supply chain to serve priority customers such as hospitals, schools, and relief agencies in a crisis. "You have to look at that specific scenario and your obligations—can you pull inventory from another location?"

Eaton's Rick Jacobs said his company tries to substitute vigilance for redundancy by watching for early warning signals of disruptions, and making supply chain adjustments in real time. "When we saw Katrina coming into New Orleans, we worked with our logistic carriers and pulled our inventory out of the warehouses there—not everybody did that," he recalled. But he also noted that such vigilance does not necessarily help avoid key supply problems in a crisis. "We had difficulty getting gasoline during Katrina so our employees could get back and forth to work," he said. "The bigger part for us was what you *couldn't* get."

Georgia Tech's Mitra said resource flexibility is crucial to preparedness as specific needs are impossible to anticipate in advance. He had talked to Greyhound's CEO who said the company was pretty effective during 9/11, "because buses can basically go from any place to any other place, so they were able to redirect and respond to something they really had never planned for."

"Flexibility is interchangeability," echoed MITs Yossi Sheffi. "It's being able to switch, to change supplies, to change routes, move parts between products, and cross-train people. Redundancy and safety stock are too expensive."

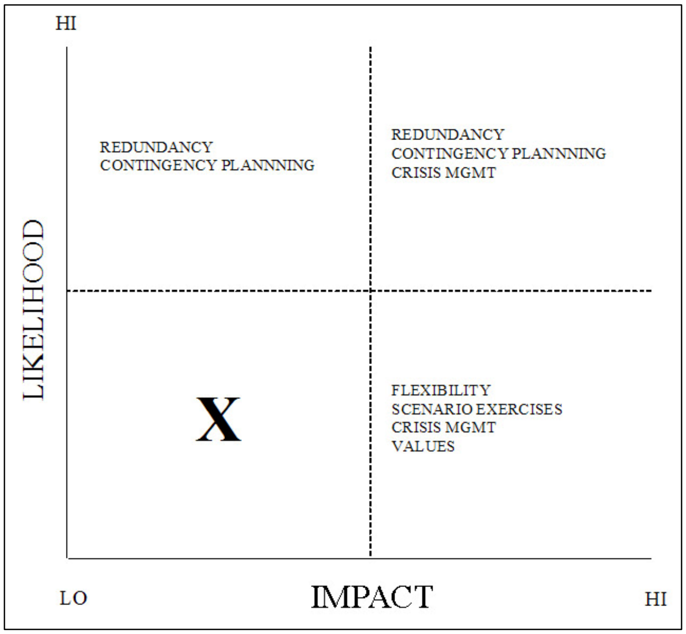
IBM's DeLapp cautioned that this mentality must be constantly enforced from the senior leadership team. "It's the decisions you make day in and day out that contribute to that," she said. "If that senior group isn't engaged in it, they can undo all the flexibility in the world in a set of five decisions at a board meeting."

Hasbro's Daya is optimistic that discussions about building flexibility into supply chain operations can also have synergistic business benefits. In one case, she recalled, having a well-tuned supply chain "early warning system" enabled the company to foresee the loss of revenue from a major retailer's store closings in time to proactively build out new channels to replace it. "One of the values we're going to get out of this deep dive into risk is, we may find, that we're investing in the wrong places. Are we putting too much effort into an area that actually doesn't really matter? Can we redeploy funding to an area where we get a higher return?"

Yet MIT's Sheffi cautioned the group not to confuse day-to-day business optimization with protection against large, infrequent disruptive events. "If you want to cover them with inventory," he said, "you need a lot of inventory for a long time."

Participants agreed that the relative importance of flexibility versus specific preparations depends on the nature of the event, and discussed a four-quadrant matrix categorizing potential preparation and response strategies based on the likelihood and impact of the disruption (see Chart—lower left quadrant not discussed).

Chart: Preparation/Response Strategies



* This framework is based on concepts and charts in Yossi Sheffi's book titled *The Resilient Enterprise* (MIT, 2005)

Tuck's Hans Brechbuhl summarized the discussion: "For high likelihood, but low impact events, redundancy is worth looking at and certainly contingency planning is. But where likelihood is low, but impact is high, it's much more about flexibility and general capabilities—exercising the memory muscle—and crisis management."

Do the Financial Markets Reward Resilience?

An ongoing debate throughout the day was whether companies get financially rewarded for effective risk management and resilience.

"How much time and money can you invest in running business continuity scenarios, on getting people up to speed on how to behave in a crisis, in an organization that is basically run around efficiency?" asked Eaton's Bill Blausey. "We generally don't think of it as the first thing."

Several participants said they believed that the market would increasingly place a financial value on risk management and preparedness. "Shareholders see a value to having a critical enterprise risk management assessment of the business, but it's not very sophisticated yet," said Hasbro's Daya. "Companies that have really taken the dive will get financial rewards in the longer term."

And ING's Van Wyk noted that risk reduction is often directly rewarded in the financial services industry, both through regulatory and market mechanisms. "As we prove our ability to manage our risk through Basel and Sarbanes-Oxley (SOX), it eliminates and reduces the economic capital we need to have within our fund." He noted that the financial cost of outages for the bank is known, in terms of potential exposure to customers transactional losses.

Bechtel's Ed Richardson added that financing terms for his company's projects often hinge on the ability to demonstrate risk management, thereby translating into hard dollar ROI. "We have to provide financial guarantees to bond the project. When we go into a job, we price something called risk, which takes into account the more extreme things that can hurt you depending on the part of the world you are living in."

Others disputed whether markets would reward companies for preparing for the unknown—although all agreed that markets would mete out punishment to unprepared companies who suffered a disruption. "Wall Street cannot measure unprecedented risks, like SARs or 9/11 or Chernobyl," said MIT's Sheffi. "You can say, I am resilient, but are you 7.3 or 6.5? There is no clear way for the markets to come up with the equivalent of ROI."

"I don't think Wall Street is asking the right questions," countered Eaton's Rick Jacobs. "Maybe you can't afford redundancy, but what are the reasonable things you can do to protect the viability of that product line against the most likely events?"

Jacobs said his company looks at risk from a cash flow and profit perspective. "We're looking at which products, which factories, which lanes have good cash flow and EBIT," he explained. "It just doesn't cost you more when you take a longer-term view. If you can't back up natural gas but you can back up electric, you don't throw out your furnace today, but the next time you buy a furnace you buy something you can protect. Over a 30-year time horizon I become a little more resilient every year as I protect my profit and cash flow streams."

Tuck's Eric Johnson proposed that as with quality improvement, the availability of data on risk impacts in a business shapes the perception of the ROI of managing that risk. "In ING's environment they have a lot of data on what happens when things go wrong, so they can put a number on it," noted Johnson. "It's the after-action reports you really learn from."

Johnson related some research he'd done with DHS about the potential vulnerability of oil refineries' SCADA systems to cyber attacks. "It's hard for them to imagine that occurring, until they actually get attacked," he noted. "They're saying to themselves, how is this investment going to make better oil for us?"

Does Resilience Translate to Competitive Advantage?

Does investing in resilience pay market share or profit margin dividends? ING's Van Wyk recalled that Morgan Stanley's ability to restore business quickly after 9/11 became a strong competitive advantage for the firm. "The amount of brand loyalty as a result of being up when trading started, was incredible … many clients won't leave Morgan Stanley because of it."

Ed Richardson noted that Bechtel's customers' entire value as an enterprise often hinges on his company's ability to deliver a large project to them successfully. "You're dealing with highly capital intensive things," he explained. "Protecting their financial position is very significant determinant of who they choose, and they'll pay a premium to do that."

SYSCO's Twila Day conjectured that the answer may depend on the type of business and market. Her company views disruptions as an opportunity to gain market share, she said, but many customers will buy strictly on price until the moment a crisis occurs. "New Orleans is a perfect example," she said. "We had customers begging us to service them, but we had to service the primary customers first."

Her colleague John Holzem added that avian flu had provided opportunities for competitive positioning in the food industry. "Tyson Chicken, they used it as a competitive advantage," he recalled. "They had documentation, presentations; they were telling the distributors, 'Here's what we are doing. Here is how we are making it safe.' And so we built off of that."

Bechtel's Ramleth and Richardson proposed that resilience, like quality or safety, is one important selling point among many. "You don't win on that alone," said Ramleth, who noted that some clients will balk at paying a premium for safety, even though they say they want it.

Hasbro's Jackie Daya pointed to the company's participation in CT-PAT, a security program for container shipping, as an example of an investment in risk management that paid business dividends, enabling Hasbro to move containers speedily through the ports. "Customers know we will do everything we can to continue to flow product, whereas smaller suppliers may not be so reliable." When challenged on whether customers were willing to pay for that reliability, in terms of better margins, Hasbro's Schwinn said he believed it translated into greater shelf space for the company. "Because the retailers know that it means a consistent flow of goods."

On the downside, participants debated the impact a lack of resilience might have on a company. Ed Richardson cited JetBlue's recent snafu that left passengers stranded for hours in a storm. "Up until then they were on top of the heap," he said. "But they didn't have the redundancy the other fellows had, they were tested and failed and now there will be an impact."

Yet MIT's Sheffi disagreed that a big negative impact has to follow, noting that other airlines have survived similar situations without major consequences. "U.S. Air had a complete meltdown over Christmas two years ago, a lot of people missed Christmas because of them. And U.S Air now is doing very well, they came out smelling like roses even without the reservoir of goodwill JetBlue has."

Whatever the specific impact in an individual case, participants agreed that the rate of learning from disruptions can become a key competitive advantage. "JetBlue should be thankful they had this meltdown because now they've got a data point," said Tuck's Eric Johnson. "As our friend Edward Deming would say, 'The process spoke to them and they should listen carefully.'"

Crisis Management and Recovery: Two Scenarios

Two disruption scenarios were presented to participants in small group break-out sessions (see Appendices A and B). In one, the internet and all IP-based private networks suddenly fail globally, and the outage continues for several days. In the second, a health pandemic starts in Asia and spreads globally.

Each break-out group was presented with both scenarios. Afterward the groups discussed the scenarios, and it was clear they'd had a strong emotional, not just intellectual, reactions. "The first pandemic group imagined a world where the productivity would rapidly devolve, people would stay home just from the news alone," recalled Tuck's Eric Johnson.

"We felt that fear would immediately start spreading," added MIT's Sheffi. "We started thinking about law and order." By contrast, the group saw the network outage scenario as more manageable, less of a big deal. "We didn't feel there would be as much threat to family, children, to one's own life," he said.

Yet the group that heard about the network outage first had similar concerns about keeping order in the streets if people couldn't use ATMs to get cash to buy groceries, or if planes weren't flying. "We felt it was more massive, because it happened without any kind of warning and people don't understand what's going on," said SYSCO's Twila Day. "The pandemic scenario was a slow progression: you have more time to be able to prepare for it."

"I was distraught," recalled ING's Van Wyk of the network outage scenario. "Maybe we overestimated the impact; but we went all the way to the medical. What would the hospitals be doing? If it's that pervasive, something serious has happened."

Hasbro's Schwinn highlighted the psychological aspect of his group's reaction. "The network outage had the immediacy; but the fear of pandemic was out of our control. We felt like we were jumping in to solve the second (internet outage) situation, because it was eminently solvable versus spinning out of control. It's a very different when you're personally threatened."

For both scenarios, the groups settled on similar courses of action. "Establishing a crisis team was number one," said Schwinn, "and then communicating to the appropriate constituents, internal or external." In both scenarios the groups also conducted quick situation assessments, locating employees, taking inventory of facilities, supplies, and infrastructure, and figuring out what if any business was still moving.

Communication is a crucial area to be proactive, participants agreed, given the likely level of confusion, competing messages from mass media and the government, and basic employee questions about coming to work and how they will get paid.

"How do we get out ahead of that, get some credibility established as an alternate voice?" asked IBM's DeLapp. "We need to communicate in advance what we're doing on topics like pandemic, so employees have more of a comfort factor about what's going on," concluded SYSCO's Day.

And IBM's Bradshaw pointed to timing of information flow as a critical issue, especially in the pandemic scenario. "By the time (President) Bush is out in front, things have already been happening," he said. "Also in the countries where this is coming from, it may have been squelched by the governments there. So people may see this as the tip of the iceberg."

Participants conjectured that in the pandemic scenario coordinating government bodies like WHO and CDC would be crucial whereas in the IT scenario government would be largely ignored in favor of industry and vendor collaboration. "There isn't somebody we would immediately run to in the IT scenario," said Bechtel's Ramleth. "I think everybody would run for whoever answers the phone. It's a very scary scenario." And his colleague Ed Richardson added he thought there should be collaborative planning in advance for such a critical outage, that it didn't make sense to have every company trying to solve the problem independently. "This is something that ought to be thought out ahead of time, if we have a serious problem with the backbone, here's our response."

The group also noted that the network outage threat will continue to get more serious over time. "Ten or twelve years ago, we had absolutely no dependencies on the internet at all," pointed out Ramleth. "And in 20 years, there will be no one in our companies with experience doing business prior to the internet."

Building Resilience into Enterprise DNA

Infusing business risk management and resilience into the enterprise DNA and mental models to make it an ongoing, high priority, continuous process was the logical outcome to strive for, agreed the group.

Participants pointed to existing cultural strengths in areas like safety, disaster recovery, regulatory compliance, operational problem solving, and financial risk management, and wondered how to get business continuity planning and resilience on the same footing. “I think we’re very resilient in many ways,” said Hasbro’s Daya, “we’re just trying to make it more formal as a process.”

Bechtel’s Ramleth proposed a new mental model for collaboration on resilience: attempting to leverage the power of informal, decentralized networks similar to the open source software movement, for both intelligence gathering and for response. “We all do this planning in islands,” he said, “but should it be federated so we can do more sharing across-company boundaries? I’m fascinated how quickly stuff can happen if you take some of the constraints away. The average resolution for a Linux bug is about 20 minutes, compared to four days for a Microsoft bug.”

Eaton’s Bill Blausey agreed that there needs to be a mindset shift so firms can work more collaboratively on building resilience: “You have to get over the competitive part and change it to more social responsibility.” But MIT’s Sheffi expressed skepticism this could happen, arguing that “building in resilience is building in flexibility. If you build in the ability through special relationships, contracts, IT, and processes for your entire supply chain to react quickly … that’s a huge competitive advantage.”

SYSCO’s John Holzem noted the cultural tension between empowering local decision making and controlling employee behavior, noting that currently he couldn’t imagine local SYSCO employees pulling out their personal credit cards in an emergency. “It’s a question of how far down the line do we want to push that?”

Several participants stressed the importance of educating employees so they can relate to resilience and risk management personally and take it more seriously. “It’s like SOX, you had to do SOX.” said Habro’s Daya. “So with SARS or the avian flu, you’ve got to use that as an opportunity to educate.”

“People understand controls, and the importance of them,” agreed ING’s Van Wyk. “I don’t think we have that sense of empowerment and ownership for BCP [business continuity planning] and managing risks.” Eaton’s Bill Blausey also liked the SOX analogy because what’s important are the day-to-day processes and mindset. “You’re looking to have a culture that says, ‘it’s not about a specific event, I’m trying to build in flexibility with every decision I make on the fly,’” he emphasized.

Bechtel’s Ramleth noted that one potent weapon, in his company’s push for zero accidents, is that any manager whose employee is injured on the job must go and personally apologize to that person’s family. “And I tell you, you really don’t want to do that,” he said.

MIT’s Sheffi reiterated the importance of recognizing existing cultural value systems, recalling the example of the Coast Guard C130 Hercules pilot who independently changed her team’s mission in the early hours of Katrina from an aerial survey mission to providing badly needed communications support to first responders on the ground. “It’s amazing, a military culture where a second lieutenant pilot would, on her own, take action like this.”

And Tuck's Eric Johnson highlighted the importance and effectiveness of informal communications patterns, and noted that during recent DHS disaster simulations, participants made their first calls to trusted friends or allies. "They called up their buddy," he said. "Understanding and leveraging that is in some ways capturing the natural DNA of the organization, if that's the way things spread."

Looking Forward

At the conclusion of the roundtable, the group summarized some of key issues and insights from the discussion.

"The key learning for me is how you're communicating to employees and having them build in decision-making to eliminate risk in everything they're doing," said Eaton's Bill Blausey. "Building in that flexibility as you're making day-to-day decisions—it's just like a quality decision. Originally, I was thinking about this in terms of the response, rather than an ingrained piece of the way we operate."

"My eyes are more open on vulnerabilities, to the things that I take for granted like the internet and private networks," said Bechtel's Ed Richardson.

Tuck's Eric Johnson said he was struck by how difficult it is to get attention focused on low probability events, to get organizations to seriously consider them. "Two months ago, if you'd walked into JetBlue and said, 'You guys are a walking time bomb,' there might have been some who agreed, but probably a lot of them would have said ,'We're too busy.'" "It's like pushing water uphill, you need to have a crisis to rally the troops," agreed Hasbro's Daya. "We've done a lot already, but how do we create the same burning platform like we had with SOX?"

SYSCO's Day focused on the importance of communication about risk through all organization levels, noting that as businesses continue to centralize and consolidate, their vulnerabilities increase. "We'll definitely be behind the eight ball if we don't communicate," she said.

Bechtel's Ramleth was struck by the challenge of quantifying and benchmarking resilience. "I think there are ways you can get there," he said. "And then you'd be able to say 'Where do we have the delta to where we want to be?'"

ING's Van Wyk reiterated the people aspect of crisis management. "The lesson we got from 9/11, maybe more so than communication, was that it is your people who are going to pull you through anything you face," he said. "People are probably understated and underrepresented in all of our plans."

How to bridge the gap from the known to the unknown was top of mind for Canadian Pacific's Allen Borak. "We've got a company that's used to dealing with unplanned events—derailments or avalanches," he explained. "But that leads to a culture that says, 'I can handle a pandemic the same way,' and I worry about that." Borak recalled the framework participants had discussed with "likelihood" on one axis and "impact" on the other, and the group's conclusion that for high likelihood events you need planning whereas for low likelihood events you want flexibility. “That’s a model that I could get some traction with back home, that’s a big deal,” he said.

SYSCO’s Holzem said the discussion heightened his interest in moving from planning to more active preparation. “We brought in a company to help us create the manual for avian flu— it’s up on the shelf, we haven’t pushed that down and we need to” he said. “Same with the internet piece the likelihood of some of this stuff happening is probably higher than we all realize.”

And Eaton’s Jacobs said that viewing resilience as an ongoing process as opposed to “a flavor of the month” was important for him. “A year and a half ago we didn’t know what enterprise risk management was and it wasn’t even top of the conversation in the company, so we’ve come along way. I look at it as a journey: you’re building this into the fabric of your company.”

However this journey unfolds and whatever unanticipated disruptions may come, participants agreed that the keys to resilience and agility lie in building them into the corporate DNA through a continuous focus on planning, preparation and flexibility, rather than in any specific plans themselves. ‘Exercising this muscle,’ as well as focusing on people, relationships, and communication, will both build strength for the future and help give the business a competitive edge today.

Appendix A: Internet Scenario[*]

NewsFAX – Breaking stories delivered by FAX

Internet Outage Spreads

Tue Feb 27, 2007 9:30AM EST

SAN FRANCISCO (Reuters) – An internet outage that was initially reported shortly after midnight in Palo Alto, CA (3AM EST) seems to be spreading at an alarming rate. Initial reports from Hewlett-Packard and Cisco Systems stated that traffic slowed throughout the San Francisco Bay Area, but that it seemed to be a local problem. However, by 5AM (EST) technologists at Morgan Stanley reported that traffic was also slowing in New York, interrupting communications with global offices as they prepared for the opening of U.S. stock markets. Reports from throughout the U.S. seem to suggest that very little traffic is moving on the public internet and private networks. Additional reports from Hong Kong, Tokyo and Singapore indicated that they are experiencing similar problems, but apparently Europe is largely unaffected.

A representative from Cisco Systems noted that "any normal processes dependent on moving large amounts of data on the Internet and private networks have stopped working. Telephone systems based on VoIP systems have been crippled while some of the public and private telecom/phone systems that depend on older analog technology continue to function."
At 9:15 EST representatives from Verisign, U.S. CERT, Cisco Systems, various telecommunications providers and U.S. Department of Defense emerged from an emergency meeting here in San Francisco and declared that the U.S. internet was under some sort of major attack. Because the source of the problem was not yet clear, they speculated that the situation could last for days or longer. A joint press conference for the Department of Homeland Security, the Department of Commerce, and the Federal Reserve has been scheduled for later this afternoon.

© Reuters 2007. All rights reserved. Republication or redistribution of Reuters content, including by caching, framing or similar means, is expressly prohibited without the prior written consent of Reuters. Reuters and the Reuters sphere logo are registered trademarks and trademarks of the Reuters group of companies around the world.

[*] This fictional press release was scripted for the purposes of the break-out sessions for this roundtable only.

Appendix B: Pandemic Scenario*

Bush Declares Pandemic Is Certain

WASHINGTON, Feb. 27 — President Bush said today that he was certain a global pandemic would have a major impact on the U.S. and the government was taking steps to contain it. The discovery of three cases of a deadly strain of avian influenza in South Korea last week quickly led to a growing number of instances throughout Southeast Asia. Both Hong Kong and Shanghai have initiated local quarantines of affected hospitals and travel throughout the region has been restricted to certified passengers. However, yesterday's announcement by the Center for Disease Control of an individual case in San Francisco immediately followed by a similar Canadian announcement of a Vancouver case brought widespread panic among officials in the U.S.. This morning, two sailors from an ocean vessel unloading in Oakland were said to be showing symptoms of the virus, prompting officials to extend air restrictions already in place to U.S. shipping ports. The boat operator, Chinese Cosco, confirmed the vessel departed from Hong Kong on February 6th with no animals aboard. There is an unconfirmed report of a similar incident in Los Angeles.

Mr. Bush’s morning remarks appeared to be part of a concerted effort by the White House to get ahead of this rapidly unfolding crisis. Speaking at a news conference in the East Room of the White House, Mr. Bush assured Americans that the health care system was ready to deal with a flu outbreak and that agencies at the federal, state, and local levels were fully engaged in stemming the spread of the disease. He warned, however, that more travel restrictions were inevitable. Already, flights between the U.S. and Southeast Asia have nearly stopped and it appears that shipping lanes will see major disruptions. Many fear that travel within the U.S. will also be restricted—a possibility that Bush did not address. Bush called on U.S. business leaders to help fill immediate import shortfalls of items from apparel to computers to toys and to advise the White House on ways to mitigate the economic impact. Mr. Bush is expected to address the nation this evening.

Sheryl Gay Stolberg reported from Washington, and Marc Santora from San Francisco.

*This fictional press story was scripted for the purposes of the break-out sessions for this roundtable only.

Participants in
Thought Leadership Roundtable on Digital Strategies
February 27, 2007

Bill Blausey	VP & CIO Eaton Corporation
Allen Borak	VP, Business Information and Technology Services Canadian Pacific Railway
Michael Bradshaw	Director, Supply Chain Transformation IBM Corporation
Hans Brechbühl	Executive Director Center for Digital Strategies Tuck School of Business, Dartmouth College
Twila Day	VP & CIO SYSCO Corporation
Jackie Daya	Group Executive, Global Operations Hasbro, Inc.
Nancy DeLapp	VP, Global I/T Infrastructure Center of Excellence IBM Corporation
John Holzem	Assistant VP, Information Technology SYSCO Corporation
Rick Jacobs	VP, Supply Chain Management Eaton Corporation
M. Eric Johnson	Professor of Operations Management Director, Center for Digital Strategies Tuck School of Business, Dartmouth College
Dave Margulius (moderator)	Analyst Enterprise Insight
Saby Mitra	Associate Professor Information Technology Management College of Management, Georgia Institute of Technology

Geir Ramleth	Senior VP & CIO Bechtel Group, Inc.
Ed Richardson	Senior VP and Corporate Manager of Engineering Bechtel Group, Inc.
Douglas Schwinn	Senior VP & CIO Hasbro, Inc.
Yossi Sheffi	Professor of Civil and Environmental Engineering Professor of Engineering Systems Director, MIT Center for Transportation and Logistics Massachusetts Institute of Technology (MIT)
Steven C. Van Wyk	CIO, U.S. Financial Services ING