SDA Bocconi
SCHOOL OF MANAGEMENT

Managing Risk and Building Resilience

Key Insights and Summary

Managing Risk and Building Resilience

Digital Strategies Roundtable
An executive roundtable series of the
SDA Bocconi School of Management at the Università Bocconi

The sudden disruption to the global economy from COVID-19 gave new context and new urgency to how enterprises define, identify, and respond to risk. Unexpected re-structuring and re-locating of workforces and customers created new threats in supply chain, cyber, and talent management, to add to an already swiftly growing list of enterprise risks. In parallel, the accelerating pace of business and technology change means that companies increasingly must define what constitutes unacceptable vs. acceptable risks, and how they are going to mitigate each category.

CIOs and their colleagues in risk, strategy and compliance from Airline Reporting Corporation, the American Bureau of Shipping, Angelini Holding, Chevron, Conagra Brands, Huntsman Corporation, Owens Corning, Tenaris, Tetra Pak and US Foods convened by web conference nearly a year into the coronavirus pandemic to discuss the changing nature of risk, what that means for risk management approaches and processes, and how enterprises can build resilience to risk into their cultures and operations.

Key Insights Discussed in this Article:

1. **The scope of business risks continues to accelerate in both breadth and depth.** COVID-19 has accelerated and exacerbated threats in cybersecurity, supply chain, and workforce continuity, among others……..**pages 2-3, 5, 10-11**

2. **The unpredictable risk landscape requires new approaches to identify, prioritize, and mitigate risk.** Traditional annual executive-level reviews need to be supplemented with top-down and bottom-up scenario planning, feedback loops, and interviews inside and outside the corporation — with a focus on continuous, rather than episodic, assessment……..**pages 4-5, 7-8, 11-13**

3. **In this dynamic environment, companies need to come to terms with acceptable risks, and draw clear lines between unacceptable and acceptable risks.** Prevention of all risk is both impossible and undesirable: Growth opportunities come from risk, and clear corporate purpose helps distinguish risks worth taking……**pages 6-7, 10-11, 15-17**

4. **The resilient enterprise balances flexibility with redundancy.** Redundant systems and processes used to be sufficient to mitigate internal risks around products, security, et al. Now that many significant risks are external and uncontrollable — e.g., cybersecurity, climate change, and COVID — business agility in the face of the unexpected is at least as important……..**pages 6, 8-9, 13-15**

5. **Practice makes prepared.** Rehearsing different situations at the executive, department and corporate levels, including table-top exercises, stretches and improves organizational thinking, and defines clear roles and responsibilities in time of real crisis……**pages 8, 11-13, 17**

 This overview was written by Hans Brechbühl, Associate Professor of Practice at SDA Bocconi & Director, Digital Strategies Roundtable, and Stephen Plume, Executive Fellow, Digital Strategies Roundtable. The Digital Strategies Roundtable publication series is edited by Hans Brechbühl.

"A ship in harbor is safe … but that is not what ships are built for."
John A. Shedd, *Salt from My Attic*, 1928

"Shedd reminds us that without risk there is no business," remarked Hans Brechbühl, Associate Professor of Practice at the SDA Bocconi School of Business.

> Resilience, i.e., how to handle risk, is a topic that's been building for a long time, but it's had a different flavor to it for the last two decades or so, particularly for Americans, with everything that happened in the early 2000s. It hit a crescendo in 2020 with the pandemic, but resiliency is a much bigger and broader discussion. It includes strategic, operational, reputational, regulatory and hazard risks, among others, and we have to be able to handle all of them: resilience has to be built into the DNA of the enterprise.
>
> That said, the pandemic has had an undeniable impact on this topic, and we're going to start by looking at the risk landscape and the big buckets of risk that we face.

The Changing Landscape

Robert Clyne, General Counsel and Corporate Secretary for the American Bureau of Shipping (ABS), launched the discussion:

> Given ABS' marine and offshore safety mission, the Shedd quotation hits home. We set standards for building and maintenance of vessels and other offshore craft, and so one of the big-bucket risks for us is geopolitical risk, particularly with China.
>
> Our second big bucket is around innovation and technology: COVID has really ramped up remote inspections and remote surveys. That's all well and good, if it's done right, but you're relying on other people to take video footage, to get the right samples. There's also a regulatory lag here: some governments are not fully confident that remote can adequately replace in-person inspections.
>
> We operate in nearly 60 countries. Particularly with the remote-work environment from COVID, we have to make sure that our isolated employees feel that they are still part of the company. Ethics and compliance become issues in that regard as well. And of course, we have the same cyber risk as everybody else.

"We also categorize risks at a high level," agreed Twila Day, CIO of Huntsman Corporation. "We track finance, strategic, compliance and legal, operational, technology, and human capital. We review each category annually: What needs to be added, what can be deleted, which ones need to be moved on our heat map in terms of their likelihood and financial impact."

"For us, history matters and current events matter, which sounds like it includes everything," offered Steve Zerby, CIO of Owens Corning. "For historical reasons, product liability is at the top of the 24 risks that our eyes are always on. In the current environment, those 24 risk areas also

include international trade barriers and policy and tariffs. We have a long supply chain that has become very important, and then all the same concerns that the rest of you have. Our overall perspective is shaped both by history and by events that are in the news every day."

Bruce Niemeyer, VP Strategy & Sustainability for Chevron, described a similar approach.

> Our risk management process has 13 categories that span all the risks that we could face. It's important that every aspect of what might represent risk to the enterprise appears somewhere in those 13 categories. The Board has made it very clear to us that risk management is one of our top three priorities.
>
> We spend a lot of time identifying the nature of events that could impact us, and we work principally on what we can do to stop those events from occurring. But given the nature of enterprise risks, many are not in our control, and so then we look at what we can do post-event to mitigate their impact. As an example, from prior work we had a pandemic response plan in advance of COVID-19, and it allowed us to be a step or two ahead in our enterprise reactions.

Maria Carla Pastori, Group Risk & Compliance Officer of Angelini Holding, provided a counterpoint:

> For us it's very difficult to speak about one risk model that fits the whole company, because we are a multi-faceted industrial group. We operate in pharmaceuticals, consumer, personal care, machinery, perfumery, cosmetics, and wine. So each company in the group has its own risk model. Strategic, financial, operational, and compliance risks are the first level of our framework, but starting from the second level, each company faces very different kinds of risks.

Leslie Roberts, Head of Risk Committee, listed the major risk categories tracked by Tenaris:

> We have commercial risk from products and services liability. Our pipes run for miles beneath the surface, under extreme physical conditions. So they have to be done correctly. Procurement risk: Our products are made mainly from iron ore. After the Vale dam accident in Brazil, we had to make sure we could source ore from other places. Intellectual property risk: We invest a lot of money in development, and we need to make sure we can protect it. Environmental risk: Climate change is a big topic right now. Financial and tax risk: All governments want to collect more every single day.
>
> Then there's regulatory risk: With the Trump administration, we saw tariffs come on and off. This is an emerging risk. Business conduct: We are a publicly listed company, and we operate with national oil companies, so we need to be extremely careful. Human resources. And of course, cyber and IT risk. All of our systems — industrial, procurement, invoicing — are connected. Working from home has created new challenges for these systems.

“Regulation is certainly a growing area to watch,” emphasized Christopher Lukas, GM Information Risk Strategy & Management at Chevron. “More and more, companies like us are being integrated as part of the critical infrastructure of nation-states, and so there are different expectations of how we operate, both with our data and in partnership.”

“For us, product innovation and digital strategy have moved into the focus of strategic risk discussions, since where and how people eat has changed so much in this last year,” declared Kim Fugiel, VP of Internal Audit at US Foods.

> In the operational bucket, there’s supply chain risk, all the way from producer to consumer. Also pricing and margin pressure, as during this crisis restaurants have become really focused on the best price possible, as they switch to carry-out, or change their menu mix to focus on carry-out. Then we have many of the same compliance and regulatory risks, and of course IT has cyber risks. Finally, the majority of our associates are front-line workers, so we’ve learned a lot in the last year about how to keep them well-trained and safe.

“The pandemic does bring new risks related to the workforce,” agreed Mark Meyer, Global IM for Tetra Pak.

> Our brand promise is to “Protect what’s good,” and that’s always been important in our risk profile. During the pandemic we have extended that promise to, “We will protect our people and we will protect the food chain.” The number one issue was that if we don’t protect our people, we will have no one to deliver our service to protect the food chain. The pandemic made this clear for everyone: Suddenly you can’t treat your front-line workers as simply “capacity,” because if they’re out, you’re gone.”

"I also worry about talent *after* the pandemic,” added Mindy Simon, Chief Global Business and Information Officer for Conagra Brands. “As we go to the workforce of the future, if key talent chooses or demands to work from home, or to migrate to certain areas, then keeping them, or at least managing their transition, is an emerging risk where we can’t predict what is going to happen.”

“Supply-chain risk has been out there for a while, but it became very real this year,” Meyer observed following up on Fugiel’s earlier comment. “With the pandemic, we all suddenly realized that we are dependent on things that we have no control over, or at least not at the level that we want. We need to get good control over how well our suppliers are managing risk as well, because without their inputs, we can’t create output.”

“This year has really changed the process of supplier evaluation,” concurred Anders Hellstrom, VP Legal Affairs and Meyer’s colleague at Tetra Pak. “The IT resilience of suppliers has now popped up on risk assessments in supplier management, along with the normal list of financials, ethics, and so on. This clearly has been a consequence of the pandemic.”

“The cyber attack surface has increased so significantly,” Lukas offered. “The days of protecting ourselves by castle and moat are over. When you look at cloud, IoT, BYOD, and working from

home due to the pandemic, the sheer scope that we're now looking to protect really needs a risk-based approach, because it is just going to continue to expand."

"We've gone from 10 or 15 percent of people connecting to our network from outside to basically 90 percent working externally all the time, from any point on the internet," Meyer agreed. "This acceleration and complexity around cyber risk consumes much more of my time and concern than it did a year ago."

"Cyber in the supply chain is clearly an emerging threat," Simon nodded.

> Our largest cold storage provider got locked down with ransomware one week before Thanksgiving, which is our peak busy season. More recently our largest packaging supplier also got hit with ransomware. We have over 3,000 suppliers, and understanding our real leverage in this environment is critical.

"Like everyone on this call, we spend a ton of time on cyber-related risk in the key elements of our supply chain," Zerby acknowledged.

> But with the enterprise risk committee, I sometimes struggle to get attention onto cyber: We're very focused on who is accountable for it, it's well-managed, and very much in the news, so people are up to speed. It's like a classroom with A students and D students: the A students don't get much attention, and I wish they would. There's no better way to get something that's in a good state to *not* be in a good state than to not spend time on it.

"We've been able to partner with our risk committee to get help on technical obsolescence with the CEO and the Board," countered Alejandro Lammertyn, Chief Digital and Strategy Officer for Tenaris. "It's a topic that's not fancy, and difficult to get money for, but we've found that with the right message at the right moment about cyber risk, it helps a lot in advancing our IT infrastructure."

Triggers of Change

Richard Licato, CISO for Airline Reporting Corporation (ARC) suggested that new approaches to risk management are required as the risk landscape changes:

> We're trying to move away from a somewhat academic view of risk to a more practical view. We think of the same overall pillars that others have already defined: strategic, financial, operational, compliance. Historically we focused on strategic risks, but in the past year in the airline industry, things have shifted drastically to operational and financial risk. We are concentrating on identifying our top risks, and what the indicators are that suggest we might want to address those risks more quickly.
>
> One area that has been evolving is data risk, especially around privacy and GDPR. Another is fourth-party risk. That's really about how intertwined you are with your partners: We interact with Partner A, but it's really Partners B, C, and D who expose us

to more risk. So we're trying to drive these focus areas down into the organization, where the people handling specific risks on a daily basis are the people generating leading indicators of our exposure.

"As far back as the '90s and early '00s, we talked more about key goals and objectives than we did about risks," observed Bob Bagley, Chairman of ARC's Audit Committee.

> The risks were always things that we could control. We had the ability to make things happen whether it was resources or training, or whatever. We could do it. Today, a lot of the risks that ARC faces, and that the rest of you face, come from things that you have no control over, like changes in government policy, or new rules from regulators. So now we have to think about risk not just in terms of what we do on a day-to-day basis, but also what other people could do to us that would make us change.
>
> "To add context, when COVID hit our business dropped 90 percent in 7 days," explained Dickie Oliver, CIO of Airline Reporting Corporation. "That moved our entire risk model to a different place, with financial risks much higher than they were in the past. But we still have to keep an eye on other risk areas, like the third, fourth, and fifth levels of vendor security. That's pushed us to push our risk assessment processes much deeper into the business, so we can get clearer signals when we see moves or changes in each of the specific risk areas."

Andrea Wykman, Associate General Counsel — Compliance for Huntsman Corporation, highlighted the changing landscape:

> We look more now at what we can't control versus what is in our control. It's not that we don't worry about them: it's just that we feel the strength of our policies and our training deal with areas like insider trading, for example. Operational risks like a major EHS incident or process safety get the same treatment, at a different degree of magnitude.
>
> There's definitely been a shift in terms of things that happen and impact us. We're always going to have the traditional categories of risk — supplier issues, outages. Those are constant. But other things have filtered onto the map: cyber security certainly has taken on a different aspect than before, with knowledge management, knowledge transfer, data security. There are more significant regulatory issues around the globe, and the speed with which they come at us feels like a constant barrage. So we look at what we can control versus what we can react to, and then we put procedures in place for what the reaction will look like and how we'll do it.
>
> All of these issues have much greater prevalence than before, and keeping them updated is a challenge. When we did a risk review in late 2019, no one anticipated there was going to be a global pandemic. So this isn't just a one-time-a-year deal to review anymore. As we look at the pandemic and natural disasters, it's clear we can't just operate with that model anymore. And as ARC said, you can't do this only at an office or at a Board level: you also have to take the pulse further down in the organization.

“Risks continually change,” agreed Maria O’Neill, CIO of ABS.

> That’s why we have an annual process for reviewing our big risks to determine if we’re doing all the right things to avoid and mitigate them. But risk management is also a really important part of business operations, because of shifting geopolitics, or things that just come out of the blue. Nobody anticipated COVID. No one anticipated that we were going to have a prolonged, extended, deep freeze in Houston, Texas that would bring our power grid to its knees, but we did. And now we have to look, because if it’s happened once, it can happen again. We have to review continuously so that we know what we have to change and when.

“We operate everywhere on the planet, and so it’s more or less impossible for us to comply with everything on the spot,” Hellstrom explained.

> We’ve had to become better and better at risk management by building more processes, policies, and controls. That’s meant shifting from big annual events — assessments, control audits — to an ongoing, continuous approach. We spend a lot of time identifying triggers of change in the risk landscape, and we’ve been able to reduce our control points from 7,700 to fewer than 2,000. If a process has been stable for a long time, we replace it with a trigger. It’s not automation, but it’s very close to it.

“There’s also a cultural piece of risk that gets to where risk management intersects with digital innovation, and how to get those two to play nicely together,” remarked Bill Braun, CIO of Chevron Corporation.

> Some years ago in one of our global town halls, a 20-something new hire asked our chairman why we were so risk-averse as a company, why we seemed unwilling to take chances. He replied that Chevron is in an incredibly risky business: financial risk, geologic risk, political risk, every risk under the sun. What piece of “risk” was she not understanding?
>
> In hindsight I think she was referencing that in our effort to eliminate risks around *safety*, we’d become a culture where people believed that *every* risk was there to be mitigated and removed. Whereas in a digital world, you actually *want* a higher degree of certain kinds of risk. So in the last few years we’ve been trying to separate acceptable risk from non-acceptable risk, and to be more tolerant of the former.

All Swans Look Black in the Dark

“Are there different approaches to different risk categories?” Brechbühl asked. “There are debates here: the question of redundancy vs. efficiency. Are you better off mitigating certain specific issues, or just building general capabilities? How do you decide which you’re going to do, and where to allocate resources?”

“At Tenaris, risk management is embedded in our culture, all the way to the Board of Directors,” Roberts answered. “We are always thinking of what could go wrong and how we would manage that event.”

> We have a Critical Risk Committee reporting to the Audit Committee of the Board and to the CEO. The committee assigns each of the risk categories that I mentioned before to a risk owner, who typically reports to the CEO: Alejandro for IT and cyber; others for physical assets and commercial and so on. Each owner is in charge of mitigation plans for the risks and their consequences. These roll up into a risk map that we review completely every two years. From the risk map we define which ones are critical based on the probability of occurrence and the financial impact, and those six or seven severe risks are monitored directly by the Critical Risk Committee.

“We are relatively new to risk management,” Pastori admitted. “We are still moving from a siloed approach to a more integrated one, with a homogenous group methodology. From the top-down, we are still fragmented, so we are also taking a bottom-up approach: we are having the risk owners spread across all our companies identify and evaluate main areas of risk to create a single roadmap from an operational point of view. To build the full risk awareness really takes both the top-down and the bottom-up.”

“We update our risk universe a couple of times a year,” Fugiel volunteered.

> We monitor metrics throughout the year, and if we see things start to go sideways, we’ll ask questions. But our formal interviews are really conversational: What is management monitoring, what are they worried about, how do these concerns align with strategic initiatives, what other challenges are out there? We touch 60-70 people. It’s a lot of work, but we learn so much that, with the pace of change, we haven’t switched to a survey approach — we just wouldn’t get the same depth of information. I also spend quite a bit of time with our external auditors, which sounds financial, but is much broader. They always bring good insight into risks that other Boards are asking about, or risk spaces where they’re helping other clients.
>
> We roll up the major themes, ask whether each risk is getting better or worse, and identify any new risks. Then we take it to our Business Risk Committee. They challenge the rollups, help us position risks in the context of management plans, and we create a heatmap first for the ELT, and then for the Audit Committee and the Board. We have also just started to create position papers for our top 10 risks, to make sure we are focused on them and stress-testing our plans.

“The energy and thoughtfulness that each level brings to the process means that it’s all worked out pretty well,” Fugiel finished. “Because it’s an art, not a science, and we need to be fully-aligned.”

“We also use interviews with senior people,” Wykman concurred. “Historically, those have been annual, but with risks changing much more quickly, it warrants a formal look at least semi-annually. Risk is part of the ELT’s fixed monthly agenda, and we do monthly communications

across the organization, to get the conversation flowing. As we move forward we'll see those formal conversations happening much deeper in the organization, as well as more frequently."

"It's really about having these conversations at the appropriate levels," Licato emphasized.

> What gaps do you have? How are you addressing them? Create position papers to document the risk and the response, whether the response adequately addresses the risk, and how you're actively managing it.
>
> Then as Bill said, the last piece is to change the conversation: What is acceptable risk versus focusing on avoiding *all* risk? What is the risk that you *want* to take on at the appropriate level? Instead of focusing on probability and impact, it's a shift to appetite and value, at the level of operations and the executive team and the board. We go top-down and bottom-up, and then we merge those together. What we've found is that everybody agrees on 60 percent of the top risks, and then the remaining 40 percent are similar, but people add a few things. As to timing, the group meets bi-weekly so that we don't lose anything in the conversation.

"It really should be a more or less continuous process," Hellstrom affirmed.

> The number of risks and controls should be reduced to make the process more relevant. Otherwise you just add and add and add everything, and it becomes too much for everyone. There is a tendency that the whole activity turns into a list thrown down from the top, and it just becomes a checkbox exercise. The process needs to be built from the bottom up, then come to the center. We work with it, we challenge it, we allocate resources, and then it goes down again. It's a balancing act.

"Interviews at the top are where you get a lot of great information that you'll never get out of a survey," interjected Scott Solberg, Chief Risk Officer for Conagra Brands. "But we still do the surveys, so we can get a broader swath, and go deeper in the organization. Do the lower levels view risk differently versus the higher levels? Is there a disconnect? And if so, what is the driver? Is it an information gap, or is it because something is starting to bubble, and it just hasn't hit the level of the senior managers? It's a lot of work — which is why we only do it once a year."

"We look at hypothetical, worst-case scenarios, highly unlikely to occur, but the process allows us to think about the types of things that might ultimately challenge us," Niemeyer stated.

> These get rolled into a summary for the Chairman and the ELT. If there are actions to be taken, they're endorsed at that point, and then presented to the Board. We discuss the very highest risk space in the enterprise, and they interrogate us about mitigations, and about how we are approaching emerging risks.
>
> Our greatest challenge is to stretch our thinking. Some of the early analysis about the recent freeze in Texas suggests that the peak energy load was above the worst-case winter scenario that the utility had planned for. We don't normally get the scenario

exactly right, but by being prepared for a certain kind of scenario, it allows us to more readily adapt to the things that actually do emerge.

"Do you do black swan planning events?" Day asked.

"Technically, the answer has to be No, because a black swan is unpredictable," Niemeyer replied. "But all swans look black in the dark: We try to shine as much light as we can on things that could materially impact our business. It's challenging, because when you get into that conversation, you're thinking, '*Really*? Can the whole world shut down because of a pandemic? Can that *really* happen?' It's hard to imagine until you've experienced it."

Competition and Partnering

"COVID has forced us to focus on freight and transportation," Fugiel volunteered. "We're hoping for a great recovery after the pandemic, but we're concerned about how constrained the freight market could be in terms of driver availability, and whether it will be able to handle volume expectations."

"It's not as if more people are saying, 'I'd like to drive a truck for a living,'" Fugiel's colleague Mel Hudson-Nowak, VP Corporate Systems & Strategy for US Foods explained. "The demographics are not supportive of a growing pool, plus there are the infrastructure challenges based on the increased volume that we and others will face. As a society, we expect that goods and services come to us much more quickly. So it's a significant risk, not just for our industry, but for other industries that rely on moving significant volumes of goods."

"We see transportation similarly," Simon agreed. "Amazon's two-hour delivery, with everyone else trying to follow their lead, is changing people's expectations of immediacy. And we've had consumer behavior on our watch list for years — that's not a new thing. But we're the opposite of US Foods, in that Conagra has been the beneficiary of people staying at home. They're hoping people go back to restaurants; we're betting people are going to continue to eat at home. What consumers ultimately do, and how they do it, is a big risk in both directions."

"Tetra Pak isn't in the same business, but Amazon has impacted even us," Meyer remarked. "The delivery of liquid food through their channel creates a different opportunity, and it shifted really fast. We had to shift the way that we provide our products to them, and part of the reason 2020 was a good year was our ability to adapt. That whole supply chain is an opportunity."

Solberg stressed the point: "You do have to flip the risk on its head, and ask how you can take advantage of the opportunity. A lot of supply chains are set up in an older school of thought, whereas our customers are getting more and more just-in-time inventory, and there are repercussions for not delivering on-time and in-full. If you can lead the effort to change, you can become the company that's out in front."

"That addresses the topic of emerging third- and fourth-party risk," Licato observed.

> Who are the critical set of third parties that you're interacting with, and what will happen if there's any disruption? This gets really tough, because now there are laws and regulations saying you have to evaluate not only *your* third parties, but whoever *they* are doing business with. How do you accumulate that information? I doubt anyone has a complete mapping — you might have SOX or ISO certifications for your first tier of third parties, but I doubt anyone has it for the fourth and fifth parties down the road. But if any of them fail, your business can come to a halt in an instant, especially in something like cloud services.

Hudson-Nowak proposed cyber insurance as a partial solution to third-party risk:

> With the growing trend towards ransomware and other attacks that affect people's ability to work, premiums are going up and coverage is being constrained. Another market this is happening to is in property, because of climate change. Climate and cyber are very different things, but they both in the group of big gnarly externalities that make it harder and harder to protect yourself financially.

"It's a Swiss cheese approach to protection," Solberg suggested. "Each layer has its own holes, and you keep layering different pieces until all the holes disappear, or at least get smaller. You get property coverage for physical perils, and cyber coverage for third parties, and a product recall policy for manufacturers. So you can mitigate your financial risk, but in no way should you rely exclusively on this approach. You still have to do all the things you would do if you didn't have the insurance policies."

"Part of the problem is the inability to know who the parties are," Day lamented. "It's hard enough to identify all the third parties from arrangements that were made when shadow IT was bigger. We've been bitten by those a couple of times, not in big ways, but the facts are that we didn't know we had a relationship, and the third party didn't know whom to call when they had a security issue. I have no idea how to even start to build a list of fourth and fifth parties. It would require contractual changes to identify them. It's a big blind spot at this point."

"But what if we all say that the third-, fourth-, fifth-party risk is unmanageable, and therefore unacceptable to carry?" Hudson-Nowak protested. "Will we all go back to building our own systems, within our own moats? There's no way to rally enough dollars and resources to build the standalone applications required to be successful in the marketplace. Most companies have expanded their technology stack because other firms created great solutions. We can't lose access to those solutions, because our businesses won't be as successful."

Too Many Cooks

"We've talked about transportation of goods; ARC is focused on transportation of people," Oliver began.

> What's the airline industry going to look like? What are consumer travel habits going to be? But there's also massive downstream impact when consumers start traveling: They have to stay in hotels. They have to go out to dinner. They have to rent cars, and

> go to events. Is everyone prepared to ramp back up? This is going to put massive pressure on supply chains and the movement of people and products. And there are no forecasting engines out there that will tell us anytime soon what this all looks like.
>
> We're not talking about a bubble that's coming in three or four years. It could be a bubble that pops up instantly, and then could instantly go back down. We can't get any certainty as to when it's going to happen or the pace it's going to happen, but we all have to be ready for it.

"Has anyone in their career gone through a similar massive shift?" Hudson-Nowak asked.

"9/11 would be the event that we all experienced in the United States that had the biggest kind of similar drop," Day offered. "Everything else is regional and smaller — for instance, hurricanes in a certain area."

"You'd have to look at a large-scale war to find anything similar," Meyer suggested. "If you look at industries and leaders before World War II and after, it's a completely different landscape. Total devastation of industries."

"But even to that, you've got to factor in that this 'war' could start back up at any moment," Oliver countered. "There could be another outbreak a month later, two months later, that shuts us all down again. How do you ramp up — hotels, drivers, servers, food — in that situation? We're searching as hard as we can, and we're in contact with every major airline, and they're all over the map in terms of predicting how this is going to play out over the next 6 to 18 to 24 months."

"There are more ingredients in the soup now than there were after the war," Hellstrom pointed out. "There's a plethora of chefs, everyone is cooking their own soup, and it's not helping anyone. Our larger customers establish their own standards, and some of them make I must say outrageous demands on control. There's no unity, and it's not going to help the recovery at all."

"You're hitting on the pace of change and the variability," Solberg commented.

> We've gone from a model of nice slow growth to a society that's bouncing all over the place: really high highs one day, and really low lows the next. That variability is what makes it difficult for all of us to forecast what the trends are going to be. How do we strategize for our businesses, where do we need to deploy resources for future growth, how do we maintain margins? It's always been tough to predict the future, and this variability has made it even more difficult. And it's not like a commodity where you can put some floors and ceilings — there's really no way to hedge your guess.

"There is another big difference between the end of World War II and now," Brechbühl added. "At that time, governments were a lot more in control. Governments have less influence now, the world over. Companies are more in control of certain things, and consumers are — or at least, think they are — in charge of things that no consumer in 1950 dreamt of having control

over, even extending to a company's reputation. Given social media, it's much harder for any entity to fully control its own narrative."

"Outside social media posts are a real concern," Day acknowledged. "Huntsman is moving closer to customers, and we haven't been in that environment before. So have to shift our viewpoint to include posts that could attack our company or our products."

"We've had to hire someone dedicated to social media," Day's colleague Wykman continued. "Previously social was part of our communications strategy group. Now we have an individual who is responsible for proactively putting out positive messages, and also reacting to what is out there. We also have to educate our employee base on the implications for us as a company when they post, even as individuals. They don't have nefarious intent, but in the heat of the moment, they don't always appreciate the consequences of their posts on the corporation.

"In the last four years Chevron has really invested in understanding sentiment around the company and our initiatives," Lukas commented. "We have good control of the outward-facing message. But an emerging threat is the use of deep fakes: organized, purposeful misinformation to discredit or confuse the message of a corporation. We've yet to see this happen at scale against a large company, but it certainly could be."

"There are also groups and movements out there with different purposes, whether it's for animal rights or vegan or whatever, and they produce a lot of messages," Hellstrom noted. "From many perspectives their causes are good and honest, but the ripple effects can be very large. They can spread accusations and rumors, and whether they are deep fakes or just fake or not even fake at all, they grow, and it can easily go out of control."

"It's quite clear that we now need to manage consumers, because they have much more power in a way than governments do," Meyer concluded. "Consumers can decide in a moment that you and everybody like you is out, and it goes very quickly."

The Perfect and The Good

"So how do we build resilience into the DNA of the enterprise?" Brechbühl asked. "How do we create it, and imbue it into our organizations?"

"Planning and testing," Licato declared. "Understanding the scenarios where resiliency is necessary is the biggest thing."

> From a technology perspective, there's already a lot of muscle memory for disaster recovery plans. But are they really built for resiliency, which is not only technology but also business? What these exercises come down to is, who are you going to call for what? Do you have a department for resiliency, and they take care of everything, or is it layered throughout the organization, and everybody is responsible for their own plans?

> Then you can set up the individual business process plans, and know everything from about how you're going to do things, but if you don't test the plans, they're basically useless. The big problem is, what plans do you test? Should they be executive exercises? Or a department? What about a company-wide exercise? You have to run all of these, on different schedules, to make sure that you are covered and resilient as an organization. And if you don't analyze how you did after the fact, then you'll never learn and you'll never mature. Creating corporate-wide resiliency takes a lot of time and effort and commitment from the organization. Those things are hard.

"Conagra has been doing those exercises for years, both at our plants as well as at the corporate level," Solberg remarked.

> We have business continuity plans and disaster recovery plans and instant response plans, and crisis management plans that lie over the top. Over the years we've learned two things. The first is to have proper training on roles and responsibilities. Inevitably there are people who say, "I don't know if this is being done, so I'm going to do it." They're trying to be helpful, but they're actually causing more issues.
>
> The other is to ensure coordination between the strategic piece and the tactical piece. Without that tie-in, the tactical folks worry about day-to-day operations, and they run down that path, but they may not understand the overall strategy of where we are trying to get. So we created a role specifically designed during a crisis to make sure we have coordination between those two groups, and to ensure that people understand their roles and responsibilities.

"A lesson we've learned at Chevron is to be clear on who gets to make what decisions," Braun offered.

> The person whose business is affected? The head of cyber? The head of financial? I'll also give you one example of how we built a culture that's good at identifying risks. In operational risk reduction we deployed something called a hazard wheel, and the majority of our employees carry them in field environments to spot potential hazards. We trained the whole organization to be watchful, and mindful of these risks in order to improve our process safety performance.
>
> And now our senior leaders have been able to change their tone to reflect acceptable outages and acceptable risks. We've learned to distinguish between the risk of a first-aid incident, which always can happen, versus events that could kill people or have a long-lasting impact on the quality of life. Not all risks are bad: we don't always need perfection. Speed and agility is what we're trying to build into the culture.

"Tetra Pak had too many years of a perfectionist mentality, then in the early 2000s we moved to a mantra of 'good enough,'" Meyer shared.

> But "good enough" *doesn't* mean "*not* good enough," or "not tested." In IT, we define a set of go-live criteria up-front, and rank them as critical, high, medium, and low. If the critical count is not zero, then we don't go live, period. So now we have the culture

> to separate the nice-to-haves from the must-haves, and we've taken the drama out of the go-live decision: Criticals are fulfilled, or they're not. That line gets defined early, so that we feel comfortable about the decision when it's time to make it.

Hudson-Nowak illustrated Meyer's point:

> We had recent IT project where the team was working against a deadline, and they didn't want to have any defects leak into production, they didn't want to have anything that didn't work. I told them, we're either going to have nothing, or we're going to have something this is functional but not yet where we need it to be. I can easily tell you which side of that equation I need to be on.
>
> "Expect Excellence" is about challenging ourselves and others to delight customers — which has to start with the foundation of taking orders and moving cases. Everything has to come from that. That's often exactly where we need to go in terms of resiliency.

"You also have to have strong risk management protocols in place to catch what is core to the enterprise," Simon pointed out. "Make sure there are clear lines of demarcation of what is core and what is not core. It requires balance for people to have both those mindsets, and know when to cross between the two to make the right decisions."

"That's exactly right," Hudson-Nowak confirmed. "We can't be slavish to perfection, but we can't close our eyes to things that would cause catastrophic damage, or significant impact to the business. Young leaders ask all the time, 'Do you want me to do X or do you want me to do Y?' And the answer is, 'Both. You need to think through both of those things.'"

We Choose to Go to the Moon

"Redundancy and flexibility both bring some resilience," Brechbühl observed. "Is there a tension between the two?"

"For years, 'resiliency' meant redundancy," responded Marco Lanza, Chief Information & Digitalization Officer for Angelini Holding. "Now redundancy is not the most efficient. The spare wheel is no longer enough, and sometimes the spare wheel propagates the problem every more quickly. You need to be resilient in other ways."

"Flexibility is the other side of the coin in terms of efficiency," Braun agreed. "If you're going to build flexibility into your supply chain, for example, you're going to do so at a cost. How much cost are you willing to bear for that flexibility, and where do you say, 'Here's my balance point? I don't have ultimate flexibility, but I have enough, and more than zero.' The pandemic has caused a reinvigoration of these conversations, but they fit right into the broader topic of digital nimbleness, of agility versus perfection."

"So if we put risks into particular categories, do responses differ by the different kinds of risks, depending on the category and what tools are in the toolbox?" Brechbühl followed up.

“We used to differentiate risk categories in terms of methodology for our mitigation plans, but it became impractical,” Lanza answered. “These are complex ecosystems to manage. To differentiate thinking — financial, budget, whatever — isn’t straightforward, and it isn’t enough.”

“Resiliency is related to the controls that are appropriate for a given risk,” Meyer proposed. “It’s not one thing or another; it depends on which risk you’re trying to control. We map out the risks, put controls in place, and then accept a net risk level that’s left over. Resiliency is everywhere, spread in many small pieces.”

“You do get resilience that way, but you also risk getting used to doing the same things all the time,” Lammertyn warned.

> You have been successful at coping with crises, but you’ve been adapting to different crises using the same tools. The pandemic brought a different context about the future. For Tenaris, a long-term strategic vision of sustainability became an urgent matter. We knew that we had fewer CO2 emissions than our competitors, but that we had to do a conversion across our entire supply chain to take advantage of it. An area where we were lagging behind, and didn't want to even discuss, suddenly became a strategic guideline for change.
>
> I give this as an example of how sometimes risks can become opportunities of differentiation. And on the other side, how you can believe you’re managing all your risks, but the one that can really hurt you might not get the proper attention until it’s too late.

“What about the cultural piece,” Brechbühl inquired. “What cultural characteristics help organizations be resilient? An MIT scholar, Yossi Sheffi, has proposed four main cultural traits of a flexible and resilient organization:

- Continuous communication among informed employees
- Distributed power
- Passion for work
- Conditioning for disruption

“What should be added or subtracted?”

“I would add commitment,” Roberts said.

> You can have a passion for work, but you need to be committed to the company’s project, with its objectives. You need to buy what the top management is proposing for the foreseeable future of the company. The second addition would be training. As an example, we have a “safe hour” program. Top management walks around our facilities to make sure that the entire population knows that we are in a dangerous business, and that everybody needs to take care of themselves. The only way to obtain employee commitment is to show that we are concerned for everyone’s safety.

“Instead of ‘commitment’ I would say ‘purpose,’” Meyer recommended. “If you have an organization aligned around a greater purpose, then you get the commitment and energy needed to handle situations when they happen. ‘Protect what’s good’ is very important to us, to make food safe and available everywhere. Everybody buys into that. It’s like Kennedy’s ‘We are going to the moon.’ It’s amazing how purpose can increase resilience.”

“Add a constant feedback loop,” Wykman proposed. “You have to allow people to ask those ‘stupid’ questions; you have to allow people to fail. And then you have to take their feedback. Because if people feel like they’re not being heard, then they’re not going to give feedback, and eventually their voices become silent, and that’s when you lose the most valuable part of the organization.”

“There’s a level of resiliency in actually taking on some risks,” Solberg reiterated. “There has to be an element of rewarding individuals for taking on educated risks, when you know you’ve managed other risks down. That allows you to drive your business forward and to stay relevant with your customer base, which plays into long-term business resiliency.”

“Our companies are all pretty good at understanding what the typical risks are, but we’re not good at understanding what’s going to hit us out of left field,” Day observed.

> When this pandemic hit, no one was expecting a global issue, it’s truly a global issue that’s lasted a long time, and it’s not over yet. We all need to get better at figuring out what’s the next thing, the next conspiracy theory, that we need to have at least some conversations to prep for. Black swans are not likely to happen, but when you do the scenario planning, the war exercises, the tabletop simulations -- that gives you the ability to pick and choose whatever becomes relevant. The planning and thought processes you go through for those unrealistic scenarios develop into things you can use when something really happens.

“In Houston we’ve had two 100-year flood events and one 500-year flood event in the last 20 years,” Braun mused.

> What does that tell you about our predictions, or our abilities to model the risks we are all facing? There’s a parallel to where cyber was a couple of decades ago: it was an issue, and we had a few people working on it part-time, as part of their jobs. There wasn’t really a profession.
>
> Is risk management going to be similar, an art that becomes more of a science? Is there going to be increasing sophistication, will there be more shareholder expectations around how we manage it? The pace of change is increasing, the disruption levels are increasing, unpredictability is increasing. We need to spend more time on resilience.

“My takeaway from this whole discussion is that the most important thing is not how you’re organized, or what tools you have, but your culture,” Lanza summarized. “Managing risk means thinking about all the things that have to be taken into account, but resilience to risk is what makes money. Every company needs to have a culture that accepts risk.”

PARTICIPANT LIST

Managing Risk and Building Resilience

Bob Bagley	Chairman, Audit Committee *Airline Reporting Corporation (ARC)*
Bill Braun	CIO *Chevron Corporation*
Hans Brechbühl [moderator]	Associate Professor of Practice Director, Digital Strategies Roundtable *SDA Bocconi School of Management*
Robert Clyne	SVP, General Counsel and Corporate Secretary *American Bureau of Shipping (ABS)*
Twila Day	VP and CIO *Huntsman Corporation*
Daniele Del Monaco	Head of Group Internal Audit *Angelini Holding*
Kim Fugiel	VP of Internal Audit *US Foods*
Anders Hellström	VP Legal Affairs GRC *Tetra Pak*
Mel Hudson-Nowak	VP, Corporate Systems & Strategy *US Foods*
Alejandro Lammertyn	Chief Digital and Strategy Officer *Tenaris*
Marco Lanza	Chief Information and Digitalization Officer *Angelini Holding*
Richard Licato	CISO *Airline Reporting Corporation (ARC)*
Christopher Lukas	General Manager, Information Risk Strategy & Management *Chevron Corporation*

Mark Meyer	Global IM *Tetra Pak*
Bruce Niemeyer	VP, Strategy & Sustainability *Chevron Corporation*
Dickie Oliver	SVP and CIO *Airline Reporting Corporation (ARC)*
Maria O'Neill	SVP and CIO *American Bureau of Shipping (ABS)*
Maria Carla Pastori	Group Risk & Compliance Officer *Angelini Holding*
Leslie Roberts	VP, Head of Risk Committee *Tenaris*
Mindy Simon	Chief Global Business and Information Officer *Conagra Brands*
Scott Solberg	Chief Risk Officer *Conagra Brands*
Andrea Wykman	Associate General Counsel – Compliance *Huntsman Corporation*
Steve Zerby	VP and CIO *Owens Corning*