Managing Enterprise Risk

A Roundtable Overview

European Chapter Discussion
Managing Enterprise Risk

A Thought Leadership Roundtable on Digital Strategies
An executive series presented by the
Center for Digital Strategies at the Tuck School of Business

The European chapter of the Roundtable on Digital Strategies convened in London at Misys in April 2013, to discuss the many aspects of risk in a modern enterprise. In our post-9/11 world, real and imagined attacks consume the media, but far less spectacular events have more frequent and more profound impact on an enterprise’s operations, finances, and reputation. The Roundtable topics included top risks faced by each entity; frameworks and processes for predicting, evaluating, managing, and responding to risk; and how IT specifically contributes to preventing and mitigating risk situations. Participants in the session included executives from ABB, Deloitte Consulting, DSK Bank, the Hilti Group, the International Federation of the Red Cross and Red Crescent Societies, Nestlé, and Tetra Pak, as well as academics from the Center for Digital Strategies at the Tuck School of Business at Dartmouth. The roundtable was moderated by Mark Lange of Anthro|Capital.

Key Insights Discussed in this Overview:

• **Enterprise risk is ubiquitous and unavoidable, but often foreseeable.** Well-managed companies gather and simulate risk scenarios from all over, with the intent to mitigate, but not to eliminate. Pages 3–4, 6–8, 12–13

• **Exogenous risks can have direct and profound impact on an enterprise’s reputation.** Supply chain breakdowns, false information in social media, and even failures by competitors can significantly damage an enterprise’s standing in the market. Pages 4–6, 8–9

• **Managing risk is critical.** Enterprises that ignore risk will fail, as will enterprises that try to eliminate risk. The trick is in preparing and anticipating to keep risks within tolerable limits. Pages 2–4, 6–7, 9, 12–13

• **Risk management should not be stove-piped in an enterprise.** An effective risk-management approach involves participation from and escalation within multiple departments, especially including IT and Operations. Pages 3, 6, 10, 12–13

• **In the specific context of IT risk, it is no longer possible to protect the IT perimeter.** Successful IT security risk mitigation will move to a new paradigm. BYOD, the Cloud, and very smart bad guys means the security focus needs to move to data and context, not devices. Pages 8–11

• **Not all risk-mitigation is high-tech.** Extremely effective responses to risk span the gamut from advanced cloud computing to human ingenuity plus old-fashioned handheld radios. Pages 8, 10, 12–13

• **People are the key security asset.** Creating and fostering a culture of innovation, flexibility, and risk awareness is both the best risk prevention and the best risk response. Pages 3–4, 9, 11–14
Introduction

The word “risk” has two distinct, though related, meanings: one is the probability that something bad will happen — a fire, a terrorist attack, a successful hacker, a key supplier that goes out of business. The other meaning is defined in Peter Bernstein’s classic history of risk, “Against the Gods: The Remarkable Story of Risk.”

The word “risk” derives from the early Italian *risicare*, which means “to dare.” In this sense, risk is a choice rather than a fate. The actions we dare to take, which depend on how free we are to make choices, are what the story of risk is all about. And that story helps define what it means to be a human being.

Bernstein might equally have said “…what it means to be a modern enterprise.” Without understanding, management, and — crucially — acceptance of risk, the modern economy would be very much different, and very much smaller. To quote Bernstein again,

Without a command of …risk management, engineers could never have designed the bridges that span our widest rivers, … electric power utilities would not exist, … no airplanes would fly. … The great innovative enterprises that define our age…might never have come into being. The capacity to manage risk, and with it the appetite to take risk and make forward-looking choices, are key elements of the energy that drives the economic system forward.

CIOs and their business partners from elsewhere in the corporation have to deal every day with both types of risk, from the predictable to the unforeseen “black swan” event; from the operational to the existential; from the controllable parameters of supply-chain contracts to the wildly uncontrollable conditions of extreme weather. Certainly one way to approach risk is to try to eliminate as many dangerous factors as possible — but that approach also eliminates progress, and it ignores the real world. As a rocket designer on the Saturn 5 rocket said, “You want a valve that doesn’t leak and you try everything possible to develop one. But the real world provides you with a leaky valve. You have to determine how much leaking you can tolerate.”

Tricky Subjects

M. Eric Johnson, Director of the Center for Digital Studies at the Tuck School, led off the Roundtable discussion by highlighting the ubiquity of risk:

The topic of risk speaks to everyone. It doesn’t matter what area of business you’re in, or the nature of your business, or what role you play in it, we’re all risk managers. It’s a uniquely human experience. Already this morning you’ve made many risk decisions: You got out of bed. That’s a big risk — bad things can happen getting out of bed. You climbed into the

2 Ibid, p. 3.
Managing Enterprise Risk

shower. People die in the shower every day. You ate some breakfast. That’s a big risk-taking initiative.

Of course, that’s just everyday life. What makes this topic really fascinating is that organizations and individuals spend lifetimes managing risk, and yet things can go wildly wrong for even the very best risk managers. Look at the Enron meltdown and Arthur Andersen, a company that built a long and successful business by helping its clients manage risk, but within a few weeks, 50,000 people are out of work. It’s completely over. Just unbelievable, when you think about the consequences of a risk decision and how badly it can go wrong. But that is the nature of even well-managed risk. Things can go wildly wrong.

“Risk is not inherently something bad,” offered Johnson’s colleague Hans Brechbühl, Executive Director of the Center for Digital Strategies. “It is sometimes a choice one makes, and it’s a part of doing business. There are strategic risks and bets that one takes, and those are actually quite positive.”

“Risk management is not just part of business,” added Markus Koch, Partner at Deloitte Consulting, “It’s a requirement for doing business.”

You could stay in bed the whole day, and then you’ll have the least risk. Risk management has two purposes. One is obviously to avoid risks where you could lose your license to operate because of some compliance issue where the SEC pulls the plug. And the other is to enable you to take the right risks, risks you know about that you can make decisions on, risks that if they materialize will not put you out of business.

Peter Knutsson, Vice President of Corporate Governance at Tetra Pak, built on Koch’s theme:

When we look at risk management, we start with Why we exist as a company, we start with our vision: Making food safe and available. Then we get to How — what do we need to do to achieve those goals? Because if you mis-align the How, then you could actually risk your whole reason for being, you could lose your way on the ethical side or compliance side, or you could miss something really big on the strategic side. Our risk governance model does have a bottom-up approach where we group risk portfolios, but they are always within the context of what we’re trying to do as a company.

“It’s part of being a principle-based company, rather than a systems-based company,” agreed John Peterson, Group IS/IT Security Manager for Nestle. “And that makes all the difference when you get to these tricky risk subjects.”

“It may sound dramatic,” finished Koch, “But the main risk is the risk of going out of business. The first element to understand is that it can happen to any company — there’s no eternal life. Companies take too many risks, and take risks that they don’t fully understand.”

“Risk management is part of your leadership and management responsibility,” agreed Knutsson. “It should be on your agenda all the time, not just on the occasional time when you talk strategy. It should be integrated in the way you run a good business.”
Managing Enterprise Risk

Risk, from A to Z

The variety and sources of enterprise risk seem as if they could be infinite: hostile attacks on both physical and virtual assets, lost or stolen devices, unreliable suppliers...the list goes on. Moderator Mark Lange of Anthro Capital asked the group to speak only to the top risks faced by each company. Terence Stacey, Group CIO & GLOBE Director for Nestlé, focused on geopolitical risk:

There is nowhere in the world that we don’t market Nestlé products in one form or another, and that means we trade in some really difficult parts of the world. We have operations in Syria, quite substantial business in Egypt, in Iran. Israel, Palestine, India, Pakistan, North Korea, Ivory Coast. In some instances our facilities have been damaged. But Nestlé won’t be threatened or frightened away. Danger means there’s a time you have to pull people out, but then we’ve managed to do things through local agencies. It’s part of the risk that we have to manage, and we’ve never pulled out of a country, in 150 years.

Stacey concluded with a theme that resonated throughout the day: “This approach requires a resiliency in the way we accommodate to pursue doing business.”

“There are some risks that have to be managed in minute detail,” observed Tetra Pak’s Knutsson, building on Stacey’s political point. “We need to understand what equipment we’re sending to, for example, the Middle East; we need to not break competition rules in markets where we could be deemed ‘dominant’ within our category. We do not want to have an authority on our back because someone took a risk in a local market for some small win.”

“The top risk we had last year, number one, is competition from lower-cost countries,” said Massimo Muzzi, Head of the Enterprise Risk Management Unit for ABB. Per-Åke Tobiasson, Tetra Pak’s Head of Global Process Office and Knutsson’s colleague, extended Muzzi’s comment: “Competition from Asia is trying to copy us and to do it cheaper, yes. And the problem is, consumers believe that all packages are the same, whether they’re competitors’ or they’re Tetra Pak.”

“Absolutely,” agreed Knutsson. “If something goes wrong and our competitor compromises the safety of the food, we could all be put in the same category. We would have a massive food safety issue on our hands, and we would have to defend the packaging even though it’s not us, it’s them. That’s bad, bad, bad news. So food safety is one of our top risks not only because we are responsible for it, but because there are other players in the category with products that look similar to ours.”

Martin Petry, CIO of the Hilti Group, raised another aspect beyond the company’s control:

Product liability is the highest risk for the company, because obviously our products are used in critical areas. Every country has institutions to review that buildings meet specifications, but no company can monitor the applications. So mistakes are made every day. We do not assume that boreholes are cleaned after they are drilled, or that they are
perfectly cleaned, or that the anchor setting is monitored perfectly. The question is, ‘How big are the mistakes, and what can we do to help the customers recover?’

Our number two risk is data: knowing whether we have the availability of products. Our customers rely on a maximum 24-hour delivery from us; if we are not able to keep that promise, work simply stops on a project that could have 2,000 people. It’s as bad as an insufficient anchor, it’s over-proportional damage to our customer, but that is simply the nature of our business.

Moderator Lange brought up supply-chain risk, and referenced a news story from some years ago: A toy company “where one of the suppliers in China of these little wooden toys ran out of a certain paint, went out and got some other paint, and that paint had lead in it. So a supplier several steps downstream from the company presented huge risk.”

Nestlé’s Stacey acknowledged supply chain risk, but suggested that issue can also be a source of significant competitive advantage:

Consumers have confidence in large food companies to produce products first of all that are safe; secondly, that the ingredients are what they say on the pack; and third, to have end-to-end responsibility for sustainability, ecological friendliness, no child labor… The whole big picture. It’s a really big risk to the global operators in the food industry, especially when you’re sourcing products from and selling them across multiple countries.

If you understand that supply chain, though, from sourcing of raw materials all the way to delivery, and you’re able to manage it, then you’re in a much stronger position than those who can’t: “Do you know what you’re getting in ABC Supermarket’s no-name brand? You’re paying less for it, but do you know what’s in it?”

“That seems like it would have pretty big upside,” commented Tuck’s Johnson. “If part of the Nestlé brand promise is food integrity, and food integrity is questionable for Brand X, you can really build that promise in consumers’ minds, so that they know if they buy a Nestlé product, it’s been properly gathered, harvested, treated, all those kinds of things.”

“Provided you can demonstrate that and don’t get caught out,” responded Stacey.

There are 700 microbiological tests that can be done on a product, and another 400 to make sure it doesn’t have contaminants from fertilizers and such. But the test for horsemeat is a DNA test, and just because that test comes out negative, it doesn’t preclude donkey meat. But if you want to do all of these tests, you can put yourself out of business. How do you get to the balance?

“Customers need to trust that we are doing the job for food safety,” concluded Knutsson. “I always make the analogy with airlines: Airlines don’t compete on flight safety. It’s a given.”

“It’s interesting how many of these risks ultimately rise to the level of reputational risk,” observed Lange, “Which in turn affects the opportunity curve in any number of ways,
Managing Enterprise Risk

anticipatable or not. I love the question of what we should be mitigating that we can’t anticipate.”

“One aspect that’s unique about risk,” concluded Johnson, “Is that we suffer from what psychologists call ‘the limits of imagination.’ There are things we just could have never imagined would happen. Something seems too crazy or unbelievable, and then, Oh! It happens. Had we known it, we might have managed it. Talking about this subject is so vexing because of the unknown unknowns.”

Wild Cards and Black Swans

Enterprises that think systematically about risk employ different approaches to identify and prioritize them. Brechbühl described how the vice president of risk management at Sysco used every Friday the 13th to conduct a ‘black swan’ risk exercise for senior management: “She wasn’t responsible for a single risk in the end, but she was responsible for inculcating this behavior into the culture and making sure it was part of the thinking.”

Muzzi described a similar process for how ABB institutionalizes risk identification:

We ask all countries and all business units to have a risk roundtable at least once per year, with people from different functions. They select the top 5 risks. Once we have collected all the input from the countries, then we prioritize the top 20 risks of the group. On top of this top 20, we also add ‘wild cards’ or ‘black swans.’ And this list is what goes to the Board, with a description, assessment, and mitigation plan.

Lange turned to Edward Happ, the Global CIO and Head of ISD for the International Federation of Red Cross and Red Crescent Societies (“IFRC”). “In the case of the Red Cross and Red Crescent I would imagine that you have a lot of exogenous risk that’s relatively unpredictable. I’m wondering about risk intrinsic to your operations and how you think about those?”

“We’ve identified a list of 9 enterprise risk areas,” responded Happ. “But interestingly, you won’t see on that list ‘A disaster occurs.’ That’s our core, that’s what we do. Implied in many of these risks is basic brand reputational risk. Being a trusted organization to respond in disasters and being trusted by populations around the world is critical to how we work.”

Happ explained the IFRC’s model for IT connection points to enterprise risks (reproduced in redacted form below):
The blue line through the center is our ‘risk frontier.’ We don’t have the capacity to deal with all of items on our IT risk register, so we want to make sure that we deal with the ones that have the highest impact and the highest likelihood. We pay attention to the items ‘north’ of this frontier. We don’t ignore the items below the line, but we take longer to address them.

“It’s an insurance approach,” Happ continued:

If we were to spend all the money and time to address all the risks, that would be buying the maximum insurance. But if we did that, we’d be spending far too much of our donor dollars in administering and mitigating risks. So we’re constantly making tradeoffs between what’s a good use of our donor dollars versus what’s a good risk profile for us to achieve. We’re accepting known risks.

“That’s very similar to our approach,” Hilti’s Petry commented.

It’s not very different between non-profit and for-profit. We have the stakeholder instead of the donor, and in the end they both expect that we make reasonable and good decisions. The question I ask myself is, ‘How do you actually deal with things on the isobars of risk impact vs. probability? Is there more focus on things that are more likely but have a lower impact, or is there more focus on higher impact but lower likelihood?’ You cannot eliminate all the risks, because then you would spend tons of money, which is probably also a reputational risk in the end.
“In our case the priority is on impact,” commented Miroslav Vichev, CIO of DSK Bank (Bulgaria). “The bank goes through regular business impact analysis, taking into account all the different areas and systems and processes. The likelihood is a different story. Something might happen very often, but if it is managed, it’s not such a problem.”

Happ gave a hypothetical example: “Imagine if the IFRC campus burned down, and our website, which is hosted on that campus, goes down, and the story is that ‘World’s oldest, largest disaster-response organization can’t respond to its own disasters?’ Well, having more cloud-based features means more world-class resiliency for data centers, better than we can build. So that’s the path we’re taking, to mitigate by outsourcing our risks to the cloud vendors.”

“The point is valid,” rebutted Peterson, “But there are two other things:

As a cloud provider, how do you show me as the enterprise that you are more secure than we would be? It has to go beyond the classical SSAE 16. That’s very generic, it doesn’t tell me what is in place to give me insurance for my data.

Secondly, you have concentration risk. Everything is in one place. The bad guy is out there as well. I’m not saying that the cloud service is more or less secure. I’m just saying it’s difficult to get the assurance that we need.

“I would go one step further,” added Peter Kalt, Strategic IT Project Manager and Petry’s colleague at Hilti, “Because one real difference is, if I have a problem and I decide to do something, I can do it in an internal data center. With external cloud, how do you influence the cloud provider?”

Tobiasson provided one approach: “At Tetra Pak, if we have a system that must be up 24x7, then we say that it is not a core business for us, and we outsource it. But we put in an agreement that there should be a data center, and a backup data center, and so on.”

**Return of the Mega-Trends**

Social Media and BYOD are IT mega-trends (in addition to Cloud Computing, Big Data, and the Consumerization of IT) that have been recurring themes at the Roundtable on Digital Strategies. This roundtable on Enterprise Risk was no exception.

“You constantly have things today with social media,” Stacey began, “When people get onto Facebook or Twitter and express their opinions, accurate or not. It doesn’t really seem to matter. And all of a sudden, you can have an explosive situation on your hands. There was an event eight years ago, and it’s still the number one item in our daily scanning. It’s not accurate, it’s not current, but this is the kind of thing we have to deal with.”

“The key is responding on time,” suggested Vichev. “We have whole teams watching, trying to react quickly to things, because otherwise, it costs a lot.”
“One rule we’ve found,” Happ added,

Is that if you try to argue or defend any social media, you absolutely make it worse. The only approach you can take is to increase the number of positive things that are said. You can’t defend the negatives. You can try correcting them, but you probably will find even that backfires. Participating in those conversations becomes an important strategy for managing risk. You can’t ignore them. You can’t defend, but you can participate.

“And then you can turn a bad thing into something good,” Stacey concluded.

If something crops up like bad packaging, you can go back and listen to the consumer. Then you can bring a re-packaged product to the market, and there’s a positive spin to it over time. Quite a lot of product renovation and innovation comes as a result of listening. The best you can do with the bad is a “We’ll fix it” sort of thing, but over time, with the right level of interaction, you can gradually get more wins than losses.

While the primary risk from social media is reputational, the primary risk from BYOD is ‘data leakage’ — risk of enterprise data falling into the wrong hands through loss or theft of the device. One mitigation approach is simply to maintain corporate control over the device, as described by Tetra Pak’s Tobiasson:

We have not prohibited bringing your own device, but you have to accept the company rules, and that we can wipe all the information on the device, even if it’s your own private information. If you have private information and you access our network, you have to follow our rules. We haven’t had to wipe any of them; people are cautious about their own devices, but at least we can now monitor and control.

The IFRC’s Happ described a completely different approach that turns BYOD policy “on its head:”

Instead of asking, ‘How can we control this?’ We asked, ‘What if we took a laissez-faire approach, how much risk exposure is there?’ Because the other thing we’ve noticed is, now that 40 percent of our users bring their own devices, calls to the help desk are down 15 percent. The generation that brings their own devices expects to support themselves.

“Support is one thing, but what about data leakage prevention and personal data?” asked Petry. “That is a risk that extends to any device, the approved ones or not,” replied Happ. “An executive of a colleague organization left his laptop at an airport, and got a call the next day because they were able to open it and find out whose it was. Would you like to bet that the project and financial files and everything else were on that laptop?”

“In itself BYOD poses no additional risk,” added Vichev. “If someone loses a device, if it’s well-managed by a meaningful and effective corporate policy, it will not bring any risk. There are many ways to guard the data if you want to encrypt or use other methods to guard against potential loss or theft. And if the data are synchronized elsewhere, remote wiping does not solve the data leakage problem at all.”
Managing Enterprise Risk

“I’ll agree with that!” exclaimed Peterson.

Wiping a device will never protect your data. A guy going after your data is smart enough not to connect the stolen device to the Internet. He knows that if he connects the device, it’s going to be remote-wiped. The risk is very different now from some years ago, in terms of how you protect data outside of the enterprise. Cloud solutions mean it’s very easy to get data out there, and to access it through smartphones and tablets and laptops. Trying to secure it is a game you can’t win, because every time you secure one thing, up pops another channel to get data out of the enterprise. There’s no easy solution to data loss prevention that’s both solid and practical for usability.

Vichev described one way to improve information security by integrating it with physical security: “If you don’t enter the building with your ID card, you are not able to access your PC at all. As simple as that. It immediately shows a number of exceptions, and most of them appeared quite suspicious, and rightly so.”

Hilti’s Kalt objected: “In the past we always protected the boundary, and this approach is again boundary protection. If I can’t protect the boundary, I can close it completely. And then I’m safe. And then, I can just stop doing business. The reality is that we are now absolutely mobile, and we can’t continue with the same approaches to just protect boundaries. That’s not working anymore.”

The New Face of Security

If perimeter protection is necessary but no longer sufficient, and closing the boundary is self-defeating, then what are new approaches to information security? Happ bridged the topics of mobility and overall information security: “The traditional response is to continue to improve the perimeter. But one of the things we’re saying around the table is, we’re realizing each month that perimeter security is less and less real. We can’t not do it, but if you ask where to invest money and time, it has to be at the data level.”

“Exactly,” affirmed Peterson. “If you don’t follow the data, if you just run around and patch holes and do all of this advanced security on your mobile devices, then the data is still open.”

Brechbühl referred to a past experience of an Americas Chapter roundtable member:

The paradigm is really shifting, and the question is, ‘Do you have a response in place for the new paradigm, or are you still wrestling with the old one?’ The new paradigm is, assume you’re going to be penetrated. You can’t put zero focus on prevention, but what do you do after that? Bechtel’s model has four steps: “Deter-Detect-Respond-Remediate,” and they’ve created a combined network operations and security center to manage it. The key question is, ‘What do you have that the bad guys want?’ Because there are at least three variants: There’s IP theft; there’s stealing funds; and there’s the whole hacktivist side of things. Taking real steps towards dealing with these scenarios
is becoming an imperative, and if you had told me so six months ago even, I would have said you were crazy.

“Information classification is a key element to managing that,” Kalt pointed out. “Who here is monitoring data traffic, not just quantity, but content?” added his colleague Petry. “Do we know what is moving in and out? Does anyone profile users to say, ‘John has a certain usage pattern; now he is suddenly looking at other information; what should we do?’”

“We define scenarios that look suspicious,” Peterson replied. “If an administrator is recycling two passwords in the treasury system and those accounts are used to do transactions — that gets blocked. We’re looking for excessive access on certain things, and they pop up as alerts that then need to be investigated.”

“There’s one more security aspect,” added Vichev from DSK Bank, based on the stringent security requirements imposed on the financial industry:

We as IT guys have exactly the wrong mindset for this purpose. You need to get the professional cops on the task, not IT professionals. They start from a completely different angle. They don’t compromise based on the technology deficiencies at all. They just know what should be done, and how to do it is entirely up to the IT guys.

This contradicts IT’s concepts of connecting from everywhere, of technically enabling business in one or another way. We are creative, trying to solve, trying to deploy, trying to enable the business. They think in exactly the opposite way. They know what shouldn’t be done, and they don’t take “No” for an answer.

This level of security existed before computers, and these guys know how to deal with paper, and certifying different levels of security of documentation. They start applying this old paper principle to think about how to delegate rights, how to request delegation of rights, how to classify information, the levels of classification and following from there all the processes. They have been training for this all of their careers. If you want to tackle these matters properly, then you need to take the right guys with you.

The Resilient Enterprise

With the participants in agreement that not all risks can — or should — be eliminated, a frequent topic during the day was how to recover from an event in a particular risk area. Examples ranged from a burned-out warehouse to social media ‘attacks’ to the severing of one of the main transoceanic internet fiber lines. Global business is now such that it’s not possible for an enterprise to cease operations for any length of time, even if disaster strikes. There’s been much discussion about self-healing networks, and the group turned its attention to describing characteristics of the self-healing enterprise.

DSK’s Vichev described the transition that enterprises have made over time in their approach to risk scenarios:
If you look back years ago, disaster recovery centers were mandatory. But if we did a disaster recovery exercise, it was just a complicated IT task. It wasn’t till we moved to business continuity planning that the real dialogue with Operations began and the whole bank was involved. That simple exercise created differences in mindset, process, and culture. When you go through business continuity testing, you start to see at what level is the right decision-taking body — it’s the level at which you experience the risk and the opportunity. The process is relevant for every operational risk.

“That’s the big thing in this,” Brechbühl commented. “No plan survives the first shot, as they say in the military. It’s not about the plan that you come up with in the scenario, it’s about the communications pattern and the getting together, it’s the building of the ‘neural pathways’ of the organization that allow you to handle actual situations.”

Martin Petry from Hilti suggested that innovation in itself can contribute to enterprise resilience:

If you innovate at the speed that copying doesn’t pay off anymore, then you are in a good position. Even IP is not a huge issue, because you simply move faster. In an industry with long cycles, product innovation isn’t enough, but the business model itself has a certain resilience: If you combine innovation in the sales force, the service centers, the supply chain and so on, then someone has to copy all of that, too, in order to make use of the data taken from the data center.

“It’s a matter of how can you systemically create an organizational culture that is equipped to anticipate and mitigate risk,” suggested Lange, “Rather than a stimulus-response regime of identify-remediate.”

“Even if you identify the risks,” Peterson continued, “there are a hundred different ways that things can go wrong, and many different ways to deal with it. It’s a matter of getting the right people together, and based on that collective experience, figuring out how best to approach it. A lot of risk decisions are made on a day-to-day basis, and you have to rely on people.”

Happ from the IFRC illustrated Peterson’s point about reliance on people for resiliency:

In disaster response it’s a disconnected world for the first 24 to 48 hours. The experienced field people, the first responders, know how to operate, they can get things done manually. After the Haiti earthquake, the cell phone network was out, the IP network was out, what do you do? We have people in the Red Cross who are just passionate about older technology, about radio. Radio still gets through, and it’s easy to deploy the tower and cover an area. It’s a low-tech backup network. Then, communications came back on within 24 hours, but you couldn’t get through to anyone because all the voice lines were jammed. But text messages queued up, and maybe they took seven hours, but they got through. Plain old dumb text messages suddenly seemed pretty smart in that situation.
Managing Enterprise Risk

Stacey described similar lessons learned at Nestlé:

We talk to a lot of countries about business continuity, and their answer is, “We need a backup system.” That’s disaster recovery, not business continuity. Places like Indonesia, India, and Pakistan have regular outages; they just do, because of the telecommunications infrastructure. In those places we have a proper business continuity plan. So what we’ve done is bring those people to more first-world environments to help build plans that are workable in the event of an absolute outage. It’s hard, because people who live in a world that is always switched on can’t believe it’s possible to work any other way. But we’ve taken people from these other environments and shown how it is possible to put something together that actually does work when you have a real outage, a real crisis.

Johnson summarized: “With any risk it’s all about reducing the impact. If risk is the probability of some event happening, then resilience is really about reducing that impact, so that even if it happens, it doesn’t matter.”

Returning to his earlier theme about core values, Tetra Pak’s Knutsson addressed the difficult topic of how to create such a resilient and secure culture and how to get people inculcated to it:

We work a lot to minimize any impact. There’s the technical side to resilience, but then there is the people side to resilience. We have a mandatory program on information security to create awareness, to move into understanding and, therefore, to move into compliance. 19,000 people have taken this program, and it’s been highly appreciated because it’s also very useful for you personally. We’re all afraid of being hacked or being compromised on our Facebook accounts and so on, so we made it quite personal. It has had a big effect on people’s awareness and therefore with compliance on how you use Tetra Pak devices or your own devices when you’re connecting to our network.

Happ emphasized the point: “The best security we have at the Red Cross is the goodwill of the employees, and the number one intrusion risk, the number one risk of a malicious action, is a disgruntled employee.”

“That is core to the difficulties,” responded Stacey. “How do you get people up to speed around the individual internalizing of risk, and the importance of compliance and security? People always tend to think it’s somebody else’s problem.”

Previous roundtables, the media, daily life all deliver the messages that risk is everywhere, security is permeable, and that the bad guys figure out how to compromise new technology as fast as the good guys can create and deploy it. Knutsson concluded his comments with the only practical way that an enterprise can stay resilient for the long term, even in the face of all these threats:

If you can hit people’s hearts with the core value that you are part of protecting the good business we have together, the good company, and our good name and reputation, then everyone becomes a security officer in a way.
<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
</tr>
</thead>
</table>
| **Hans Brechbühl**          | Executive Director
                            | Center for Digital Strategies
                            | Tuck School of Business, Dartmouth College |
| **Edward G. Happ**          | Global CIO and Head of ISD
                            | International Federation of Red Cross and
                            | Red Crescent Societies |
| **M. Eric Johnson**         | Associate Dean for the MBA Program
                            | Benjamin Ames Kimball Professor of the
                            | Science of Administration
                            | Director, Center for Digital Strategies
                            | Tuck School of Business, Dartmouth College |
| **Peter Kalt**              | Strategic IT Project Manager
                            | Hilti Group |
| **Peter H. Knutsson**       | Vice President, Corporate Governance
                            | Tetra Pak Group |
| **Markus Koch**             | Partner
                            | Deloitte Consulting |
| **Mark Lange**              | IT and Enterprise Venture Advisor
                            | Anthro|Capital LLC |
| (Moderator)                 |                                                                          |
| **Massimo Muzzi**           | Head of Enterprise Risk Management Unit
                            | ABB |
| **John Petersen**           | Group IS/IT Security Manager
                            | Nestlé |
| **Martin Petry**            | CIO
                            | Hilti Group |
| **Terence Stacey**          | Group CIO & GLOBE Director
                            | Nestlé |
| **Per-Åke Tobiasson**       | Head of Global Process Office
                            | Tetra Pak Group |
| **Miroslav Vichev**         | CIO
                            | DSK Bank (Bulgaria) |