The 2016 Risk Management Summit: The Management of Enterprise Risk & the Evolving Role of the Chief Risk Officer

In partnership with

DOW JONES RISK AND COMPLIANCE

The spectrum of risks that modern companies must be prepared to manage continues to broaden – financial, cyber, security, and geopolitical, just to name a few. Driven by higher expectations from regulators, investors, and employees, the increasingly complex and interrelated nature of these exposures has wide-ranging financial, operational, legal, and reputational implications. As organizations struggle to assess their vulnerabilities and allocate responsibility for identifying risks and for taking appropriate measures to avoid and mitigate the consequences of these risks, the Chief Risk Officer (CRO) has emerged as an interdisciplinary executive role that is critical to integrating the management of risks.

Following last year's Cyber Risks in the Boardroom program, which was attended by more than 200 practitioners and leading experts in risk management, the 2016 Sullivan & Cromwell / RANE Risk Management Summit recently brought together a broad group of leading thinkers from the public, private, non-profit and educational sectors to discuss pragmatic ways to handle risk management and the challenges that boards face, as well as to examine the crucial evolving role of the CRO. Highlights of the day's special address, panel and roundtable discussions follow. In keeping with the Chatham House rule that was in effect, specific speakers are not identified by name, unless otherwise noted.

Understanding Existential Risks

In a special address, H. Rodgin Cohen, senior chairman of Sullivan & Cromwell, brought his unique perspective and years of experience to the day's wide-ranging discussions.

- "When you look at financial institutions, the topic of risk management used to be primarily about credit risk," Cohen said. "Today, the risk for those institutions is much more widespread – for the first time in history, operational risk is greater than credit risk."
- The most challenging and arguably crucial aspect of that operational risk is enforcement risk, Cohen argued. "I believe that the principal risk management issue for any financial institution is dealing with the regulatory environment. For many institutions, actually limiting risk means convincing regulators that you have sound enterprise risk management."
- "AML/BSA risk is almost equal to cyber in being an existential risk – particularly for financial institutions," Cohen stated. "Financial institutions and boards need to remember that they cannot rely on regular AML/BSA exams as a good

housekeeping seal of approval. Many banks have a clean examination prior to AML/BSA enforcement actions."

- An essential component of risk management, and one that regulators now demand, is the oversight performed by a company's board of directors. Boards should be directly involved with the CRO, Cohen advised; in turn, the CRO or whomever is formally and directly responsible for risk management should be appearing regularly before the board. "It is not just about the number of people you have in risk management, but the quality of people you have. Companies should be devoting some of its top people to risk management."
- Mitigating risk is a function, in part, of solving cultural problems. There is no single "best" culture, Cohen said, but rather a culture should reflect the mission, goals and ideals of an organization, and be based on principles, not rules. The principal problem has been subcultures. "When major financial losses happen," he posited, "there has frequently been a small group within the company that has veered off from the cultural norms, decided to take risks that exceed the risk appetite of the company as a whole, and believe that the company's code of conduct does not apply to *them*."
- When a breakdown does occur, the key is to respond to it as promptly and thoroughly as possible. Cohen cautioned that the most serious enforcement penalties are often reserved not for the company's underlying misbehavior, but when the conduct in question was not properly investigated.
- "Cyber-risk is an existential risk not only for financial institutions, but for the entire world economy," Cohen warned. Today's massive cybersecurity challenge is too complex and systemic to rely on individuals to solve, and what is needed is "a new paradigm for combatting cyber warfare," he proposed. "This new approach requires more centralization within the government, more collaboration between the public and private sectors, and more cooperation within the private sector."

"We're in the process right now of looking at new facilities in a bunch of cities around the world, and as we look at those, we get the question of: 'What should we do to protect the facility's physical security?' But the first question we need to ask is: What is the threat we are trying to protect against? Is it against us, it is against the city, or a neighbor?"

Identifying the Threats

Throughout the day, most panelists agreed that identifying and defining the threats is one of the toughest parts of effective risk management. On a macro level, it may seem simple enough to point the finger at cyber-breaches, geopolitical turmoil or regulatory creep, but pinpointing what more specifically poses the biggest risks to any single organization is much more complicated. As one speaker put it, "before you prepare, you have to predict."

- "In risk management, you're only as good as your ability to imagine the next threat, to know what is not knowable," one speaker noted. That is especially true in an era of limited resources, where a variety of risks compete for priority in attention and for scarce funding, another participant said.
- Human nature doesn't help matters. After claiming that whatever terrible event has occurred is a wake-up call, we invariably end up treating it more like a snooze

alarm and drift back into complacency, according to one panelist. "Lessons are learned, but rarely applied," he lamented.

- Another speaker summed up the dilemma; "We're in the process right now of looking at new facilities in a bunch of cities around the world, and as we look at those, we get the question of: 'What should we do to protect the facility's physical security?' But the first question we need to ask is: What is the threat we are trying to protect against? Is it against us, it is against the city, or a neighbor?"
- The current populist political wave around the globe, from Brexit to the U.S. election, is an example of the inherent unpredictability that we face in today's threat environment. "The notion that globalization would continue, with an unfettered, seamless information flow around the world, and that governments would continue to pursue the Western political order, that is now all up in the air," one participant noted. Perhaps it's not surprising then that surveys have shown that geopolitical risk is a category that risk professionals feel least prepared for, another speaker pointed out.

"This new approach requires more centralization within the government, more collaboration between the public and private sectors, and more cooperation within the private sector."

What Makes a Successful CRO

Initially focused on financial and operational risks, the Chief Risk Officer is poised to take on broader responsibilities, including managing areas such as compliance and reputational risk. The risk manager of the future will have to move beyond a static protective wall of controls and procedures to ensure that risk management becomes part of the an organization's culture and fundamental business decision process, what one panelist called "collective risk management."

- In many organizations, the role of the Chief Risk Officer is still relatively new, assuming they have a formal CRO at all. Companies are still grappling with what precisely are the responsibilities of this executive, and also how those responsibilities relate to and overlap with those of people who traditionally handled a good share of enterprise risk issues, lawyers for example. The conflict this could pose was highlighted by one participant who asked, "Do you really want legal and compliance risk to be part of your enterprise risk management, or do you want that [enterprise risk management] to be handled by your lawyers?"
- Another panelist argued that a major failing of stand-alone CROs has been that they are too far removed from day-to-day operations. "The independence of the CRO was a root cause of the financial crisis. It led to their inability to understand the evolving risks." By the same token, however, a general counsel or chief legal officer may likewise not be sufficiently involved in daily commercial to appreciate fully emerging risks. Either way, collaboration and breaking down barriers within organizations are increasingly important conditions for effective risk management. By way of example, one speaker remarked, "What I'm finding is to deal with almost any type of risk you have to have IT people at the table."
- To be successful at his or her job, a participant noted, a CRO has to know as many people at a company as possible and encourage an open culture of conversation.

The CRO needs to understand various business units and their subcultures and how they all work together. Equally critical for a CRO is to have a firm understanding (and buy-in from all stakeholders) of an enterprise's risk appetite; knowing how much uncertainty and potential damage you can live with is essential to figuring out how to best manage various risks.

- Not every company, however, needs a dedicated CRO, one speaker argued. Depending on their business and size, many firms may be fine with risk functions being shared by a General Counsel, CFO, CSO, CCO and head of human resources, for instance. "To the extent that the nature of the business is such that a couple of routine high frequency actions have the potential to blow up the company or a market, then you will have a CRO," the panelist said.

Keeping Pace with Changing Risks

At a time of shifting regulations and evolving technology, it can be hard for a CRO to ever feel adequately prepared. And though panelists had no easy solutions for this problem, they did offer some valuable insight on how to approach that daily dilemma.

- While there is no doubt that thorough preparation makes a big difference for dealing with a sudden challenge or threat, one panelist suggested that any successful risk manager has to be careful not to let such preparation lead to paralysis. Documentation that lays out how to respond to a hack, for example, can't be too specific or drag on for 50 pages; no one will ever read the plan, let alone follow it. "Anyone who has ever done an internal investigation knows that when you get the first call and someone describes what they think the violation is, it is almost guaranteed that the facts will be different within a week," the speaker stated.

- At the same time, there is a danger of adapting too much to changing circumstances. For instance, though many observers expect the regulatory environment to change dramatically under the incoming Trump Administration, one participant cautioned against letting an organization's collective guard down. If it turns out that the shift is more about enforcement than actually rolling back the regulations themselves, it could be "a CRO's worst nightmare. Four or eight years from now, the rules are still on the books, and the next creative regulator may be enforcing something your people were not enforcing." The speaker further counseled, "CROs should be looking at best practices grounded in ethics irrespective of what is absolutely required of regulation."

- All too often, people mistakenly think tools to improve risk management are some kind of silver bullet. Such may be the case with Big Data, for example, which many executives believe incorrectly can be harnessed easily to find bad actors inside an organization. The reality, unsurprisingly, is much more complicated. Unless you have a clear, specific idea of what you are looking for, Big Data isn't likely to be all that helpful, and can in fact be just the opposite by generating false positives. Big Data can also create other, unrelated risk management issues, given the potential

If it turns out that the shift is more about enforcement than actually rolling back the regulations themselves, it could be "a CRO's worst nightmare. Four or eight years from now, the rules are still on the books, and the next creative regulator may be enforcing something your people were not enforcing."

legal ramifications of all the personal information companies are now routinely collecting and storing.

Ransomware Case Study: Cybersecurity and Crisis Management

To cap the summit, an esteemed roundtable of cybersecurity and legal experts used a hypothetical scenario to tease out the best practices for how organizations should respond to a cyber breach. In the case study they discussed, a healthcare company has been hacked by a group threatening to permanently disable access to thousands of patients' medical records unless they are paid $500,000 in Bitcoin within two hours. Already, there are reports of patients' confidential data appearing for sale on the Dark Web. With the media, regulators and hospital officials calling for answers, the firm's stock already taking a drastic hit and the CEO unreachable during a business trip to remote part of Brazil, the company must decide quickly how to act.

To avoid finding themselves in such a vulnerable position, there is basic hygiene all companies should be taking — anything that helps reduce the chance of letting in malware.

- Long before any kind of cyber incident occurs, enterprises need to have a cooperative working relationship well established with the FBI and other law enforcement agencies. Companies also need to really understand what their crown jewels are that may be most at risk, and how much of that information they are willing to share with authorities. Reaching out to officials ahead of any such attack will also curry favor with regulators investigating the response after the fact.
- If hackers have proved that they have the data, an organization must prepare to inform regulators. It's possible that the Treasury Department, Department of Homeland Security, the National Security Agency or the U.S. Secret Service, may come in to investigate, or may be interested in the malicious actors. But everything starts with notifying the FBI, one panelist said. Depending on the scope of the breach and the investigation, companies might be able to obtain a "safe harbor" letter, which protects the company from having to publicize aspects of the breach. While notification laws vary by state, enterprises might want to reach out to state attorneys general that don't require notification anyway, one panelist said. "To think that the AGs don't talk to each other is kind of naïve."
- Within a company, all the people tasked with responding to a cybersecurity crisis "have to know who one another are ahead of time," a participant stated. Tabletop exercises should have already clearly established the crisis chain of command, and the CEO may not necessarily be leading the response. As part of this, organizations have to understand "who's calling the shots on external communications"; inaccurate messaging — such as one company's announcement that it thought a nation-state was responsible, without concrete evidence — can complicate matters, said one panelist. Equally important is having a plan for internal communications. Companies would do well to have backup internal communications methods set up, whether it's via phone calls or non-company email, in order to hold discussions away from a network that hackers could be monitoring, one panelist suggested.
- Making the decision whether or not to pay a hacker's ransom is no easy task. "Part of it is an ethical question," one panelist pointed out, given the ongoing debate

that paying a ransom just encourages more ransomware breaches. Of course, if it's hospital data that can't be accessed and lives are at stake, that's going to be an important consideration.

- Organizations that have been attacked must complete an analysis of the alternatives. "You have to be very careful. You have to start planning how quickly you start doing things so you don't tip your hands to the hackers," one panelist said, offering an example of a company that refused to pay the ransom, attempted to recover the data itself and had all its data permanently deleted, later going out of business.
- Most ransomware organizations are well-run businesses, sometimes complete with a help desk that is ready and willing to negotiate, another participant noted. Organizations that consider paying should also verify how quickly they could secure their systems after their data has been recovered because they remain a target.
- To avoid finding themselves in such a vulnerable position, there is basic hygiene all companies should be taking — anything that helps reduce the chance of letting in malware, one panelist said. This includes cyber-awareness training, so employees know to be on the lookout for spearphishing emails and understand the growing risk of the Internet of Things (IoT) – connected devices that one participant dubbed the Internet of Insecure Things.