Risk Management Summit

Redefining Resiliency: New Approaches for New Risks

Hosted By:

SULLIVAN & CROMWELL LLP

In Partnership With:

KNOWLEDGE@WHARTON

Presented By;

RANE
Risk Assistance Network + Exchange

DOW JONES
RISK & COMPLIANCE

Redefining Resiliency: New Approaches for New Risks

The speed at which enterprise-level threats have evolved in today's climate means that corporate leaders increasingly understand that it is necessary to prepare for "when," not "if," such risks materialize. Now, anticipating a myriad of new, interconnected risks is the norm — one that will require rethinking current approaches, as well as redefining how risk is understood and managed. One critical component of an organization's planning is an integrated front that incorporates boards, officers, legal, and compliance, among others. The 2019 RANE Risk Management Summit brought together some of the world's most respected business leaders, legal, and risk experts to discuss the critical issues corporations can expect to face in the future, and how enterprises can leverage resources and information to "peer around the corner," expand their peripheral vision, and take a more proactive approach to risk mitigation. Highlights of the day's keynote addresses and panels follow. In keeping with the Chatham House rule that was in effect, specific speakers are not identified by name, unless otherwise noted with the speakers' approval.

TABLE OF CONTENTS

Keynote Fireside Chat

Jules Kroll, K2 Intelligence

David Lawrence, Founder & Chief Collaborative Officer, RANE

Jules Kroll spoke about watching his father run "a small, struggling business" within "a corrupt industry" — the New York printing industry in the late 1960s — and realizing as a young person that he did not want to follow in his footsteps. Instead, he ran for public office in Queens "on an anticorruption campaign," albeit unsuccessfully.

It was an era when industry contracts were being fixed, noted Lawrence, and kickbacks were a common practice. That's when **Kroll** created an investigative product that became synonymous with his name. "Everyone refers to this as a 'Kroll report,'" **Lawrence** said. "Before information was digitized, he saw the need for people to have access to information," and in the process "revolutionizing the process of due diligence."

Asked to speak about the evolution of his thinking, **Kroll** recalls an early client. Working without a fixed rate, his arrangement earned him "25 percent of everything I saved." (**Kroll** also leveled a critique against time-based compensation: "Why is selling it by the hour relevant for anything?") Yet his success also ran into a snag when in the first quarter he stood to make more money than the chairman.

THE EARLY DAYS

Kroll recalled that his first investigation — now commonly known as "due diligence" — didn't occur until the late 1970s. His work began first advising on best practices, consulting on what kind of performance could be generated, and eventually evolving into the areas of white-collar crime and corruption — a phenomenon that evolved on a global scale, as seen in the 1970s' Lockheed Martin scandal. "We were a reflection of the events that were happening around us," Kroll said.

The 1970s were "a tough time," he added. "There were a lot of failures. The economy was not good." Professional services were a fraction of what they are today, **Kroll** noted. For example, in 1972, the net worth of Goldman Sachs was $21 million, and Lehman was $13 million. "The scale was radically different than it is today."

In the 1980s, initial public offerings began to proliferate, and the trend "gave us the ability to say there are much better ways to do things," **Kroll** said. The investigative process, as he developed it, began to involve an increasingly diverse set of roles, including accountants and investigative journalists, "bringing together people who haven't been brought together before."

The shift led to an evolution of business-related investigations, as well, with a balance . "I need to put on an equal basis information and judgment," **Kroll** added.

COMPETITORS EMERGE

Kroll said that his firm's success drew attention — and competitors. "Wonderful, first-class institutions saw what we were doing," he said. "The world of competition took over, which made it hard for me but made it better for the world."

Yet **Kroll** also recognized the ongoing need for expert perspectives, noting that one of the struggles for financial institutions, governmental agencies and regulatory bodies is they are being flooded with information. "We're short on judgment," he said, adding that more people are needed "to separate the wheat from the chaff" and away from "checking boxes because that doesn't work."

The ultimate goal, **Kroll** said, was to create "a smarter room" — a room of people who are more highly qualified. "That's my hope for the next generation."

CONFLICTS OF INTEREST

Lawrence said that after Marsh & McLennan bought Kroll Inc. in 2004, **Kroll** saw the need for a better system for bond ratings that was not "corrupted by conflicts of interest." **Kroll** said that **Lawrence** was one of the first people he went to with the idea of a ratings business — Kroll Bond Rating Agency — that was "really nothing more than what the truth was. Some people would call it 'due diligence.'"

Kroll described the existing system as one in which credit-rating agencies, law firms and investment banks worked in tandem. "The only people who got screwed were the investors," he said. "The idea was to move away from an inherent conflict of interest." But the challenges are formidable when bond sellers face the choice of a thorough and robust examination of their product vs. a process that results in the highest possible credit rating. Beyond that, there was the issue of charging for a review that investors were already receiving for free. "We were stuck with the existing model, which was inherently conflicted," **Kroll** said. Yet one of the credit agencies, Fitch, "has copied everything we've done," he added.

NEXT STEPS

Lawrence noted that in building their firm, K2 Intelligence, **Jules Kroll** and **Jeremy Kroll**, "saw cyber in terms of what institutions needed: access to technology," recognizing that it was "not just about information but about judgment." **Lawrence** added, "The resiliency issue of constantly trying to get actionable information is a constant effort."

Kroll said that it was critical to "put ourselves in the mind of someone who has a risk role — whatever kind of institution. We tend to be more in financial spaces, but it could be in any field." He noted that there was a tendency to approach those responsibilities with what came before, what is expected. "We're all a product of these experiences and these different roles."

Kroll praised the government's response to the 2008 financial crisis and the tone set by regulators since then. "If not for the leadership, I'm not sure how bad the calamity could have become," he said. "Armies of people are now working on things that relate to the financial crisis."

Yet while **Kroll** praised the work that took place in the aftermath, he sees room for improvement going forward. "I'd like to see fewer people focused on these issues, but they ought to be better trained,

better compensated, more analytical — in a sense, smarter. This ticking-the-box stuff is not useful."

These days, **Lawrence** said, the public is looking at private enterprise to address a range of problems, whether it's financial risk, cybersecurity risk or school shootings. "People are constantly looking at leadership of corporations to solve these issues," he said. "Overall, the system has a long way to go," he said, adding that everyone can think about how to work more collaboratively, how to scale solutions to meet the challenges.

MAKING A DIFFERENCE

Kroll emphasized the role of individuals in effecting change. "There's going to be a greater concentration of effort on people that can make a difference in institutions," he said. "That will take in-depth training, support for difference-makers. That will take board-level participation instead of the rubber-stamp nonsense which takes place." **Kroll** said that such focus was increasingly important in an era with inequality in terms of income, gender and race. "This is not going to be solved by 3,000 people checking the boxes. There's going to be a need to educate them." For **Kroll**, there is a three-pronged approach: "Status, compensation and promotion.

"There'll be organizations that will figure out how to take 400 hours of training down to the 10 hours that really count," he said. "I think it starts with those individuals. It's not about changing regulations."

Kroll also lamented the "criminalization" of financial wrongdoing. "I don't think that's working," he said. "If you look at what life was like in the mid to late '80s, things that had relatively modest penalties have been replaced by sentences of 20 years, 35 years, 50 years. Is that really having an impact? I don't think so."

While he called insider trading "insidious," **Kroll** said that it is critical to look "at the 20 ways people use report (corporate) earnings. … It's gotten out of control." More focus is needed on the area of genuine financial performance, "and the investors have got to stop being so passive and start insisting on it. Because they're the ones who are going to get hurt."

Crisis in the Boardroom: Managing Misinformation at Digital Speed

PANELISTS:

Gordon Crovitz, Co-Founder, NewsGuard

Sharon L. Nelles, Partner, Sullivan & Cromwell LLP

Arielle Patrick, Senior Vice President, Financial Communications & Capital Markets, Edelman

MODERATOR:

Troy A. Paredes, Founder, Paredes Strategies

What should be done when companies and boards are confronted with the spread of false information and rumors? Today's technology gives individuals the ability to information-share at the click of a button. This panel focused on how companies can best confront the influence of misinformation and how boards can respond — quickly separating fact from fiction and managing reputational risk before it spirals out of control.

THE KEY QUESTIONS TO ASK IN A CRISIS

Moderator **Troy Parades** kicked off the panel discussion with a series of fundamental questions that organizations in a crisis should consider: "Do we respond?" "How do we respond?" "To whom?" "Why are we doing any of this?" "Where does the board sit in all of this?" **Paredes** identified these as "key questions that don't have an off-the-shelf answer," noting that people are going to render different judgements in any given situation. "A lot of tough judgment calls are going to have to be made," he added.

"Gone are the days when your biggest fear as a CEO or board member was something leaking to the Wall Street Journal," Arielle Patrick said.

Sharon Nelles offered, **"**From my perspective, what I see, companies and boards tend to be extremely ready. Good management and good boards know how to deal with crises." A problem tends to arise, she added, when there is an unexpected crisis — legal, cultural, as in MeToo — or geopolitical.

Arielle Patrick noted the evolution of reputational risk. "Gone are the days when your biggest fear as a CEO or board member was something leaking to the *Wall Street Journal*. Now, employees have Slack, which are seen as safe places to communicate openly. A business partner can speak off the cuff in a setting that is on-the-record. Everyone is a journalist and can self-publish. One of the other things we've noticed is how media agenda has changed. Online media has created pressure for faster, sloppier reporting. Journalists are also judged more on the impact of their stories, rather than how many clicks their article is getting. For example, did an article lead to a social movement like MeToo? Did it prompt a legal or regulatory investigation? On top of this, there is a global, systemic lack of trust in the establishment today." **Patrick** cited an annual Edelman study, The Trust Barometer, which polled more than 30,000 respondents this year and found that 1 in 5 respondents think that the system is

working for them. Over 70 percent of employees think it is important for a CEO to speak out on social issues. Over 60 percent of consumers say a reputational ding impacts their choices about what products they will buy.

Gordon Crovitz responded, "As former publisher of *The Wall Street Journal*, I take Arielle's point about the Journal personally, but she is right: The biggest change in communications in our lifetimes is the internet. I start by borrowing a question from the earlier session featuring Jules Kroll and David Lawrence and ask: Is the internet working? The answer is that it is not working well for news consumers and presents new challenges for boards and managers. Most of the people in this room can remember the era when we got our news from newsstands and could ask for the *Philadelphia Inquirer,* not the *National Enquirer,* knowing the difference very well. On the internet, it's hard to know generally trustworthy sources from generally not trustworthy sources. Along with Steve Brill, I founded NewsGuard last year, which tries to address this problem by giving consumers more information about the sources they encounter online. Our team of analysts rate and create 'Nutrition Label' write ups of all the news and information websites that account for 96 percent of engagement online. Each news website gets a green or red rating, based on nine apolitical, fully disclosed criteria of journalistic practice. Our business model is for the digital platforms to integrate these ratings and write ups into their social media feeds and search results. Microsoft is the first to make NewsGuard available to its users. About 20 percent of online news sources get rated red. This includes hundreds of anti-vaccine websites. The Russian government is highly skilled at disinformation. One of the top news sources on YouTube, for example, is RT, which most people don't know is Russia Today, funded by the Russian government."

"One of the top news sources on YouTube, for example, is RT, which most people don't know is Russia Today, funded by the Russian government," Gordon Crovitz said.

WHEN TO BRING IN THE BOARD OF DIRECTORS

When judging when to involve the board, **Nelles** said it was important to "think about culture of a company and the nature of the problem." She added, "If you're an airline and all of a sudden Twitter is blowing up because someone took a video of someone being dragged off an airplane or a dog died in an overhead compartment, that's a different scenario than a car company that was found to have been submitting false information to government agencies. Having a quick response to a story that has been going on could create additional trouble. That's not a face of quick response. That's a situation when there's a case for coordination between legal, management, and the board."

Who participates in a conversation is critical, **Patrick** said. "An important part of crisis preparedness is diversifying what a 'smart' board room looks like. Since these rumors can come from anywhere and are being disseminated in unexpected places, the core team needs include decision makers who understand all stakeholders that impact the company. For example, the head of HR should be in the room so that the management team and board fully understand employee sentiment. Same goes for a CRM to educate on client or customer impact. It really depends on the scope and nature of the issue."

Crovitz noted the difficulty board members can face in obtaining accurate information. "It's not easy to be a smart board member. On the way here, I noted the websites that were sources today of news articles delivered by Google News alerts about the three publicly traded companies on whose boards I serve," he said. "These sources have names that make it hard to know how reliable these are as

news sources—and I can guarantee none of these is as trustworthy as *The Wall Street Journal*. These have names such as the *Fairfield Current, Augusta Review* and *Lakeland Observer,* which make them sound like traditional newspapers. They are not. But these kinds of sites are now sources of information for many board members. As a result, directors may mistakenly believe they are getting the important information about the company, and management can't be sure what news directors may be seeing. This puts more pressure on management to ensure that directors are kept well informed about real news affecting the company, including its reputation (By they way, it's much better to rely on a professionally curated source of news such as Dow Jones's Factiva or Nexis than on services that simply scour the open internet for anything calling itself a news site."

WHO IS THE CLIENT?

Nelles said, "Often we are retained by the board. Obviously, if you're management, the client is the board. Thinking about it, let's say you have a slightly rogue CEO, the real control client is almost necessarily going to be the board. In a situation. It would seem to me, in such a situation, likely I would be advocating for the board to show confidence in the CEO as well stability in its own oversight role. Excellent example when the board participation is in public — extremely important. In most situations, you likely have the control room being run by management, by the company, ideally with board oversight, whether from the full board or a liaison, or someone with hands in the conversation. The trick becomes that the board and the comms teams have coordination, and is there every step of the way. If you have someone going out there from senior management, in effort to calm things down, goes off script or says something that is not vetted, you've just pushed yourself into an amplified crisis. Ultimately, I think the client is whoever is the control mechanism."

Crovitz offered his perspective. "Maybe the answer is: 'Who is credible?' There's less trust nowadays in anyone, whether it's the CEO, the board, the government, or the media. There's a high level of skepticism," he said.

WHO IS THE AUDIENCE?

Patrick said, "Any good communications counselor will coordinate closely with legal. Situations where that doesn't happen often fail." She added that it was important "from Day 1 that you introduce the legal and communications teams immediately so they are aligned on the message, and understand what litigation risk exists before putting pen to paper. It's best to have that discussion beforehand."

Nelles framed the question in terms of the scope of the crisis. "The bigger the problem, the more audience you have. You've got customers, regulators, a judge, maybe criminal authorities, etc. I firmly believe to avoid the bloody red line is to have a coordinated response team on Day 1," she said. "The worst words to use during a crisis are 'my job,' 'siloed,' and 'swim lane." Putting any part of the crisis response team into a swim lane will not allow them to effectively manage the crisis, **Nelles** added. "What there's got to be is a single coordinated message. Everyone has to stay disciplined. Pick somebody from each of your silos to make a smart room. General counsel, outside counsel, outside PR person because in-house comms can have trouble juggling a response with a long-term strategy, a board liaison — to make sure you're on message at every step of the way."

"The worst words to use during a crisis are 'my job,' 'siloed,' and 'swim lane." Putting any part of the crisis response team into a swim lane will not allow them to effectively manage the crisis, Sharon Nelles said.

PUTTING CRISIS PLANS IN PLACE

While no one can plan for every possible contingency, preparation does make a difference — and also there is almost always room for improvement, the experts said.
"My experience is: If you have the crisis plan, you don't have the crisis," **Nelles** said. "It is the unexpected, off-brand crisis where everybody has shortcomings."
Patrick identified room for improvement in developing crisis plans. "Where they exist, they're not comprehensive enough," she said. "Many of the crisis plans that I've seen haven't addressed every stakeholder channel. Where is the employee approach? What about other stakeholders beyond media or an external-facing strategy?"

Nelles added, "The reason that you need to have an on-point, consistent message over and over again is you can easily turn a crisis that is about a product into a crisis that is about management. That's where you need to watch out. Whatever you're selling, there's a framework there. If all of a sudden the CEO is talking off the cuff, there's a question about the CEO. If it's about the people than products, it's more interesting."

THE GROWING USE OF TABLETOP EXERCISES

"Companies should know their crisis comms teams in advance and engage them on preparedness so that trust is established early," Arielle Patrick said.

Patrick said she has seen an increase the trend toward real-time simulations. "We have seen some of the most powerful CEOs sweating buckets in a social media simulation exercise where comments attack the company or its people," she said. "It's definitely something companies are investing in more because they realize they need it now more than ever.

"Often we're brought in when things are in full swing. Companies should know their crisis comms teams in advance and engage them on preparedness so that trust is established early," **Patrick** continued. "There's turnover, people change, but at least there's familiarity with the firm and its people. When stakes are high, there's less friction to get the job done because the team has experience working well together."

Nelles said, "There's a lot of news out there. Now it's just everybody's just reporting on everything. … Some of what we're seeing boards do is, 'Walk me through the response, how to manage that situation. What would you suggest?' Taking an hour with a board and sort of explaining some of the basics of an actual situation helps, and boards respond positively."

Paredes said there was a clear benefit in holding tabletop exercises. "Even if you don't have time for a full-blown meeting, I'm a big fan of hypotheticals. 'What about this scenario? What about that scenario?' Going from concept can be illuminating. Low-cost, high-impact — those are the kinds of things we should be looking at — not just preparedness, but thinking long and hard about who you need around the table, that people know each other," he said. "My experience is that these require tough judgment calls. Knowing how people approach risk helps understand how that informs my response. I'm going to have a much better time understanding, and that only comes from trust, rapport, relationship, which means you've got to put in some support."

The Insider Threat: How to Detect, Prevent, and Defend Against Rogue Employees

As insider threats become more prominent, companies are increasing their focus on the risk of bad actors inside their businesses. Our panel discussed how a one-size-fits-all approach is unsuitable for the risk, as each threat poses different risks and complications for different businesses.

PANELISTS:

Nicholas Bourtin, Partner, Sullivan & Cromwell LLP

Alphonzo Grant, Managing Director and Head of the Global Litigation Group's Special Investigation Unit for Institutional Securities and Investment Management, Morgan Stanley

Molly Levinson, President, The Levinson Group

Timothy P. Murphy, President, Thomson Reuters Special Services

Troy A. Paredes, Founder, Paredes Strategies

MODERATOR:

Jeremy M. Kroll, CEO and Co-Founder, K2 Intelligence

- Before any threat reveals itself, management should be asking itself four important questions. First, what is happening inside the company on a day-to-day business that may present a threat avenue? Second, how do employees perceive what is happening inside the company and their role in it? Third, how does company leadership respond to crises of any kind? Finally, how can the company prepare to protect its reputation through challenges?

- Even having the answers to these questions, though, is not enough. Companies often make the mistake of believing that people respond to rational incentives, and if the company just gathers enough information, it will be able to prevent any incentive that leads to an insider threat. This thinking is outdated, says the panel. "Different people act different ways at different times under different circumstances." It will be impossible to gather all the information necessary to totally prevent insider threats.

- Before any crisis, a "smart room" needs to have been established. This should consist of everyone who will be needed to respond to the crisis, from CEO and other management team, to board members, to outside counsel and communications. Clear leadership should also be delineated long before a crisis.

Different people act different ways at different times under different circumstances." It will be impossible to gather all the information necessary to totally prevent insider threats.

- The "smart room" needs to be aware of what it says and how it acts. The initial instinct is to always defend the company and say too much. This risks making the crisis worse if the company's public posture and statements lead to the perception that it is more interested in covering up a problem than investigating it. People see through corporate spin easily, and during a time of crisis, there is precious little goodwill or trust to spare.

The initial instinct is to always defend the company and say too much. This risks making the crisis worse.

•The "smart room" should be cognizant that the communications and the legal teams will have different approaches to a crisis, but these approaches need to be unified under legal's lead. Any public statements should be reflective of the company's corporate values, but especially reflective of integrity, safety, and transparency.

- Finally, companies should never let a crisis go to waste. Corporate leadership should enable themselves to get to the root cause of a crisis, and avoid thinking narrowly about just getting through the current one. What wider issues/questions does the crisis raise? What were the root causes of the crisis? Has the company been lucky or good in resolving and avoiding crises? How can the company get better? How did the company's strong leadership and decisive and proactive actions throughout a crisis underscore core values and a positive ongoing narrative?

Companies should never let a crisis go to waste.

What Will It Take to Become Cyber Resilient?

PANELISTS:

Geoff Brown, Chief Information Security Officer, City of New York

Nicole Friedlander, Partner, Sullivan & Cromwell LLP

John Riggi, Senior Advisor for Cybersecurity and Risk, American Hospital Association

Kevin Zerrusen, Managing Director and Head of Technology Division Risk Governance, Goldman Sachs

MODERATOR:

David Lawrence, Founder and Chief Collaborative Officer, RANE

Cyber breaches are still dominating the threat environment given another year of significant data breaches. The current approaches do not seem to be working especially with hackers always a step ahead of corporate defenses. Although data breaches might be inevitable, the failure to sufficiently minimize and lessen cybersecurity threats could lead to considerable operational, legal, financial, reputational as well as other enforcement problems. The panel examined and discussed the best practices and new models for identifying breaches and remediating cyber issues while companies try to stay operational.

CYBERSECURITY: NOT JUST ABOUT TECH

The panel began with the premise that cybersecurity resiliency is not just a technology problem. As **Kevin Zerrusen** stated, "Nothing happens just by itself, there's always someone behind the keyboard. The wonderful thing about cyber is it has changed the way we live our lives, communicate, and navigate at work," he said. Cyberattacks span the gamut — service attacks, ransomware attacks, and threats to the financial sector and operations. "The threats are going to continue to grow in volume and sophistication. We are going to have to deal with this for a long time. Cybersecurity and the way you think about the threats has evolved as well," **Zerrusen** said.

Initially, cybersecurity was just a technology problem, with the focus on what could be done to prevent an attack. Then it became about detecting bad actors getting into the network, followed by how quickly are companies able to respond.

Nicole Friedlander said that the headline message is that resiliency in cybersecurity is not just a technological issue, but a legal and full-function governance matter for organizations. There has been a paradigm shift in thinking by regulators and enforcement authorities in this area. "Ten years ago, the question was how can you have been breached, and how could that happen? Now there is a broad recognition by the authorities and the public that breaches will happen. Currently, the questions being asked are, 'Did you take reasonable steps to mitigate the risk? Did your company respond quickly enough and were you as resilient as you should have been?'" **Friedlander** said.

Zerrusen said that in the past year, regulators have focused on how resilient firms are. It is an interconnected world: If an organization goes down because of a cyberattack, this is going to impact other markets and sectors of the country. So companies should ask themselves: What are the dependencies and can those be improved? How can you have a resilient organization?

PRIME TARGET: HOSPITALS

John Riggi said that hospitals are particularly heavily targeted by various cyberattacks, and as a consequence, they need to be resilient against three general types of cyberattacks.

John Riggi said that hospitals are particularly heavily targeted by various cyberattacks, and as a consequence, they need to be resilient against three general types of cyberattacks.

- The first type of cyber threat involves the **theft of data**. Hospitals do not just have medical information, but payment and personal account file information. Many hospitals are also involved in medical research and innovation. All these data sets are highly valued by adversaries individually. But, combine them and these data sets become exponentially valuable because they provide a complete picture of the patient, the medical research and also provide a more complete intelligence picture for nation-state adversaries who may want to steal health records for intelligence value.

- There have also been many instances of **theft of funds through business email compromises**. Sometimes, it is easier to penetrate or impersonate organizational emails, than hack a database. Especially targeted are the emails of individuals with payment authority. Cyber criminals may penetrate legitimate organizational emails by compromising easy passwords or through social engineering techniques. Once inside the email account, they will monitor the email traffic for an opportunity to divert legitimate funding. At the appropriate time in an email string concerning payments, they will insert their own email from the compromised account and change the wiring instructions to a bank account under their control. This has become very common and often much easier to execute than trying to penetrate the network with malware. Email traffic between hospitals and vendors regarding payment instructions are often targeted for this type of scheme.

- The third category is **ransomware attacks**, in which an adversary **encrypts or destroys data that impacts or interrupts patient care delivery operations**. Hospitals have been heavily targeted by ransomware since the 2017 Wannacry incident. Hospitals were the hardest hit in the Wannacry outbreak, with medical devices providing the greatest vulnerability through which the ransomware penetrated hospitals. If data is encrypted, it may impact the function of medical devices or make it inoperable. There have been numerous documented instances of hospitals which were subject to a ransomware attack having to issue ambulance diversion orders and cancel surgeries, negatively impacting care delivery to patients, especially in the UK during the Wannacry ransomware attack. There was also a variant of ransomware known as NotPetya in which the encrypted data could not be de-encrypted resulting in data destruction.

Hospitals may be unprepared to handle sophisticated cyber threats, especially those originating from nation states. However, in terms of incident response, hospitals may have somewhat of an advantage because they are required to continue operations and have “down-time” procedures during all types of hazardous conditions impacting operations such as natural disasters. But in those events, they generally have the benefit of time to prepare for the disaster. When Hurricane Sandy was approaching, the forecast provided days for hospitals to prepare for its impact. However, with a cyber-

attack there is no "forecast." Often the solution to a cyber-attack is to restore systems from backup, although it is not always clear how long it will take to perform a full system restore from a backup for mission critical and life support functions. With hospital operating 24/7/365, it is difficult to interrupt hospital operations to run these type of backup restoration tests or real world simulations.

RESPONDING TO CYBERATTACKS FROM A REGULATORY PERSPECTIVE

According to **Friedlander**, the Securities and Exchange Commission (SEC) is focused on cyber resilience as a legal and governance matter. In short, the SEC has been increasingly focused on what senior executives and control functions are doing to address cyber risk, and what the board is doing to fulfill its oversight responsibility in terms of cybersecurity and to ensure cyber resiliency?

According to Nicole Friedlander, the Securities and Exchange Commission is focused on cyber resilience as a legal and governance matter.

For instance, the SEC recently issued a report about cyber fraud, specifically business email compromises and their relationship to internal accounting controls requirements that companies have. Similar to hospitals, these email schemes have become a plague for public companies. It is an enormous challenge for law enforcement to respond to the number of incidents that they are notified of despite the fact that these incidents can cause serious losses. There was a recent case that involved two major U.S. corporations wiring $100 million to a cybercriminal in Lithuania in response to one of these phishing schemes.

The SEC examined the internal accounting controls of nine victims of this type of scheme to see whether the companies were appropriately risk managing in light of what is now a well-known scheme. The SEC did not bring any enforcement action, but cautioned that public companies must consider cyber threats when implementing internal accounting controls, underscored that this type of cyber fraud may pose accounting controls issues for the company. "You can expect that the SEC will be looking at companies that are victims of cyber fraud schemes to see whether their internal accounting controls were appropriate."

The SEC also recently issued cybersecurity disclosure guidance for companies where it emphasized the need for disclosure controls and procedures across the company — obviously not limited to information security — designed to ensure that cyber risk incidents are disseminated appropriately within a company and escalated internally in a timely manner so that the company can make any disclosure related to that cyber incident. The SEC also emphasized the importance of the SOX certification, where the CEO and CFO have to take into account cyber security risk, the disclosure control and procedure within cybersecurity risk and oversight.

CYBERSECURITY AS A SHARED RISK

Geoff Brown focused on cybersecurity as a shared risk, and asked the audience to consider two key things.

- The first is how risk professionals should **evaluate the municipal space in their risk calculations**. **Brown** argued that how cybersecurity is executed within the municipal space, especially considering critical services that a municipality delivers, can impact a company's employees. New York City itself thinks about this reality in defending the City operated technologies that deliver

services to New Yorkers, but also by acknowledging cybersecurity as a public-facing mission.

- The second thing **Brown** advocated is the concept of **community resiliency**. The key to community resiliency is evaluating the inter-connected, often critical services, that must be resilient to all kinds of risks, and delivered reliably and consistently for a City to be successful overall. Approaching cybersecurity from silos only ignores the reality of the domino effect seen by various realized attacks in the global cybersecurity landscape, where an impact at one organization rapidly spreads across corporate verticals and beyond borders. "Something I don't do well may land on your doorstep. It is good to talk to each other and take a community approach to the resiliency of our system as we adopt more and more technologies. I am advocating for community resiliency in cybersecurity," **Brown** said.

Brown stated that it is important to make sure that companies have the capacity to test what they consider to be their production service. It is not just about preparing a drill where everyone knows it's going to be drill. When it comes to cybersecurity, there's a very real element of surprise. Firms that are mature in their business functions and technology resiliency and reliability testing exercise this unpredictable element, and some firms are even testing the resiliency of their production level environment.

Geoff Brown stated that it is important to make sure that companies have the capacity to test what they consider to be their production service.

Brown added, "When I describe my organization's enterprise mission, it is to make sure that the technology that deliver services to New Yorkers is safe. But we also have a public-facing charge. It is that public-facing charge that highlights the interdependencies of the risk we all face by being interconnected. Our public-facing charge is to let New Yorkers know that their cybersecurity problem is our problem too."

INCIDENCE RESPONSE: DIFFERENT RISKS TO BE CONSIDERED

Friedlander points to a common problem, particularly for large companies, in terms of cyber response — that is, different areas of the company **lack communication** with each other in advance of and during a cyber incident, which can contribute to delays in companies disclosing a cyber breach. For example, even at companies whose information security personnel have strong relationships with law enforcement and regulators, the legal department should be involved in any communications with these parties about cyber incidents. In addition, it is not uncommon for companies to have an incident response firm lined up in advance to investigate an incident once it occurs. However, companies do not always arrange in advance for legal counsel to be involved in retaining the incident response firm, which creates challenges during incident response, where the company will want the firm to be retained and supervised by outside counsel for purposes of maintaining attorney-client privilege. Another example of why coordination is important is that financial institutions have to file Suspicious Activity Reports or SARs, including regarding suspicious cyber-related activity. The compliance department needs to be aware of these incidents timely so that they can file SARs within the required amount of time.

Riggi said hospitals should to view cyber risk as an **enterprise risk** issue, identify embedded or hidden cyber risk through vendor relationships for mission critical services and understand how that risk impacts their resiliency. For example, following the Wannacry ransomware incident, Russia launched a cyberattack against Ukraine, known as NotPetya. There was a major corporation in the U.S. called

Nuance Communications, which had a business relationship in Ukraine, and was infected by Non-Petya. Why is this important for hospitals? Nuance was the main medical transcription services for thousands of providers. A hospital trying to calculate what its cyber risk is, must also understand the cyber risk of the vendors it relies on for mission critical and life support services because, ultimately the vendor's cyber risk becomes the hospital's cyber risk. For example, the lack of medical transcription services due to a cyberattack l could delay care, impact revenue cycles and delay billing, which may be an unforeseen consequence of a cyberattack.

Zerrussen said that the real question there is what is the weakest link. Companies would need to find that out, which might include the organization's critical systems and applications. He cited a study conducted by possibly IBM that said that only 2 percent of the data that organizations have is critical, but it represents 70 percent of the value of the organization. "If 2 percent equals 70 percent, a company should probably know what that 2 percent is. It's not enough to know what the critical systems are, but knowing what the underlying technologies and platforms that are necessary to keep those going is key," he said.

Kevin Zerrussen said that companies would need to find what their weakest link is, which might include the organization's critical systems and applications.

CYBERSECURITY: WHAT NEEDS TO BE DONE

Brown said that it is critical to **get technology right via principled approaches**. This means acknowledging the organization's principles. "We've done this in New York. For us, cybersecurity is a public safety issue in the city and it's an essential service and everything we do is about respecting New Yorkers' privacy," he said.

"Having the experience and perspective of working in both government and in the private sector, I realize that cybersecurity is a problem that neither the government nor the private sector can solve on its own. We used to say in the FBI that certain threats such as drug trafficking or terrorism required a "whole of government" approach. But, countering cybersecurity threats requires the combined efforts and expertise of the government and the private sector, working together in a truly "**whole of nation" approach.**" **Riggi** said. Imposing more regulations on the victims of cybercrime is not the preferred solution to mitigate cyber threats. The ultimate deterrent for cyber adversaries is to increase the consequences of conducting a cyberattack — however that's done, whether through offensive cyber actions, law enforcement or economic sanctions — "but there has to be an increase in consequences, because that is the only way to change behavior," he said.

John Riggi said the ultimate deterrent for cyber adversaries is to increase the consequences of conducting a cyberattack.

Zerrusen said that a better response from international response, laws, treaties, or regulation is not going to happen anytime soon. To have a more resilient system, companies should think about doing the work themselves and working with others to to attain cyber resiliency. "Cyber security, with a few exceptions, is not a competitive advantage, it's something that we can all benefit from having more of. So I encourage companies to **look at it from a team perspective**," he said.

Cryptocurrency, Blockchain, and the Implications for Financial Crime Compliance

PANELISTS:

Andrew Gerlach, Partner, Sullivan & Cromwell LLP

Gabriel Hidalgo, Managing Direcyor, K2 Intelligence

MODERATOR:

Thomas C. Baxter, Of Counsel, Sullivan & Cromwell LLP

The rising utilization of blockchain technology is a significant legal, operational and compliance challenge that many companies have to overcome. Cryptocurrency transactions are known to be anonymous and untraceable, increasing the risks of their use in money laundering, terrorist financing and other illicit transactions. And as the panel discusses, identifying the entities and locations of blockchain participants requires sophisticated analytics and transaction monitoring approaches and processes.

RECENT CASES OF INSIDER THREATS

The panel's moderator **Thomas C. Baxter** started with the problem of insider threats with respect to cryptocurrency and blockchain by citing some examples from recent headlines.

- One of the threats was a newspaper story about a South Korean cryptocurrency exchange that filed for bankruptcy after it learned that it owed $30 million in bitcoin. The loss that led to the bankruptcy was caused by an employee who appropriated the private keys of several hundred bitcoin wallets.
- Another example is the major Canadian cryptocurrency exchange that filed for creditor protection when, after the death of its co-founder, it lost access to its wallets and the corresponding keys that held the assets owed to the firm's clients.

To understand how these cases of insider threat happened, **Gabriel Hidalgo** started with an explanation of how cryptocurrency works. He explained that the basic cryptocurrency, which is bitcoin, gives the control of the asset from inception and a digital code is created that is equal to the amount of bitcoin. The exchanges are basically custodians of that asset's digital code.

- In the case of the South Korean currency exchange, the firm did not do enough to secure access to that transactional wallet or, in this case, several wallets that held customer assets.
- In the case of the Canadian exchange, the CEO was the only one who knew where the funds were going, and that person passed away while not leaving anyone behind to manage how to move those funds out of the wallet. The key concept in this case is the "key man risk" because the deceased co-founder was the only person who knew whether or not those funds were moved to different wallets.

BIGGEST HURDLES IN CRYPTOCURRENCY

According to **Hidalgo**, the **biggest hurdles in cryptocurrency boil down to two things**.

- The first is **fear**. Whenever there's a new technology and people are unaware of how it works, they are more likely to back away from it.
- The second thing that hampers cryptocurrency's broad introduction is **the lack of communication** including the lack of understanding on how to mitigate the risk from a financial crimes perspective. People often talk about what blockchain does. However, they never get to the heart of the matter of how compliance mitigants are supposed to be used on these transactions. Neither do they communicate an understanding of how these principles can be applied for anti-money laundering (AML) or present a workflow that makes sense to regulators.

"When you look at the underlying tech, there isn't anything that people should be scared about. It's a workfow that all started with the concept of a digital wallet."

"When you look at the underlying tech, there isn't anything that people should be scared about. It's a workflow that all started with the concept of a digital wallet," the panelist said. To send funds, all that is needed is a wallet address, and the assets can be shipped in a few minutes in whatever bitcoin amount, costing less in fees than what is paid in a wire. "The beauty of the system itself is having a low-fee structure and the fact that it's all done digitally," **Hidalgo** said.

However, tracking transactions remains an issue. When a wallet is created, it does not have a name, address or anything that would identify an entity or person. However, there are tools like CipherTrace that help track wallets. These tools also have a proprietary list of bad wallets. "Similar with sanctions where we can't really know every single player that we would want to sanction, when we identified those sanctionable officials or entities, we rely on these proprietary lists in addition to information we receive from law enforcement to try to ban or track wallets," **Hidalgo** said. "We know when, for example, there's terrorist financing that's occurring in the crypto space because we've identified wallets tied to ISIS, Al Qaeda or any other terrorist financing."

KYC IN CRYPTOCURRENCY

Unlike other parts of the financial services industry, there is one thing that is distinct with respect to cryptocurrency and blockchain, which is so new that there is not the kind of history that the financial industry has, illustrating the challenge of the burgeoning sector.

Cryptocurrencies also have unique capabilities because of the open-ledger nature of digital currencies. The basic compliance framework for a cryptocurrency company is no different from other financial institutions, as the things that they have to do well are the same — Know Your Customer (KYC). This means knowing customers' identities and knowing who is behind them.

FORENSIC INVESTIGATIONS IN BLOCKCHAIN

Typically, the computer is going to have software that would either generate wallets, or they have the reserve key for the wallet. In forensic work, getting access to this computer is the most crucial step. From a forensic standpoint, if access is gained to that key and to the wallet, a link analysis is done using the tools to trace back where this money came from. Usually other pieces of information are available including the owner of other wallets. These tools are used as link analysis to trace

where these transactions have been, what wallets are associated with them and what is known about the people who either control or hold the wallet.

"Part of what we're trying to do in a lot of the cases is to get a circle around the due diligence to where all these funds come from. We have investors and companies who wanted to invest in companies that these were founded on such as ICOs. The investors want to understand where these funds are coming from," **Hidalgo** said. Many ICO funds are in digital format. So the investors didn't come with a bag of cash, but what they did was send Ethereum or bitcoin, and investigators or compliance officials want to know what the source of funds are and that comes from through a link or wallet analysis.

C. Andrew Gerlach said that mixer companies are advertised on the Internet through ranking services that allow for customer reviews.

Fraud can arise in cryptocurrency activities where the intended purpose can be either good or bad. One such practice is called mixing. **C. Andrew Gerlach** said that mixer companies are advertised on the Internet through ranking services that allow for customer reviews. These services can run coins through their mixers and deliver them to multiple anonymized addresses to hide where they came from and where they are going. In some cases these services destroy all transaction records shortly after transactions occur (just long enough for customer service inquiries). "You can literally Google these services. They may be legitimate services with legitimate uses, including shielding the identities of people who have been deliberately targeted because of their cryptocurrency holdings. However, there are obviously many nefarious use cases as well. It must be very challenging to figure out when they are at play, who is using them, and to determine the circumstances where they are legitimately set up," **Gerlach** said.

SANCTIONS AND SOVEREIGN CURRENCIES

One use of bitcoin is as an alternative to a nation's currency. However, in cases like Venezuela and Iran, where they can be used to avoid sanctions, caution should be exercised in these transactions. Venezuela's government recently launched the petro, which is the country's own cryptocurrency backed by oil. Iran has also launched a gold-backed cryptocurrency called PayMon. Participants shared their observations on the trend of sovereigns issuing cryptocurrency.

- "It's pretty transparent what Venezuela and Iran are trying to do. They are subject to a very heavy sanctions regime and it's weighing down on their ability to move funds outside of Iran and Venezuela," **Hidalgo** said. "The petro is clearly designed to open the market for oil sales to certain countries like Russia who are looking for cheap oil and for Venezuela to generate sanction-proof revenue."

However, there are legitimate uses for these sovereign currencies., either digital or not. In Ecuador, their sovereign currency was the Sucre but they have formally replaced that with the U.S. Dollar, which allowed them to move away from the Sucre to fight inflationary pressures. Other countries might use digital currencies to reset the value of their sovereign currencies to fight similar inflationary pressures.

- In Greece, for example, there has been talk of moving back to a sovereign currency and away from the euro. "So I would caution against throwing all the sovereign coins in the same bucket," **Hidalgo** said.

ABOUT THE PANELISTS

Thomas Baxter, Of Counsel, Sullivan & Cromwell LLP
As a member of the Firm's Financial Services Group, Thomas C. Baxter, Jr. focuses his practice on advising clients in the financial services, insurance, securities and FinTech spaces. Mr. Baxter's advice relates to complex issues arising from supervision and regulation, investigations and enforcement actions, governance, compliance and risk management, crisis management and organizational culture. He also brings extensive experience dealing with central banks from around the world, and with sovereigns and their instrumentalities, as they address sovereign debt and dollar-liquidity issues. Mr. Baxter's deep knowledge in these areas comes from more than 35 years at the Federal Reserve Bank of New York, most in senior leadership roles.

Prior to joining Sullivan & Cromwell, Mr. Baxter was General Counsel and Executive Vice President of the Federal Reserve Bank of New York. While serving for more than 20 years in that senior official position, Mr. Baxter led the New York Fed's Legal Group. In addition to nearly 50 lawyers providing legal services, the Legal Group has significant non-legal functions, including the law enforcement unit, the corporate secretary's office, the compliance and ethics function and the banking applications function. Mr. Baxter also served on the Management Committee, the bank's highest-level executive committee.

Nicolas Bourtin, Partner, Sullivan & Cromwell LLP
Nicolas Bourtin is a litigation partner and the Managing Partner of Sullivan & Cromwell's Criminal Defense and Investigations Group. His practice focuses on white collar criminal defense and internal investigations, regulatory enforcement matters, and securities and complex civil litigation. He is one of the coordinators of S&C's FCPA and Anti-Corruption practice group.

Mr. Bourtin has represented individuals, corporations and financial institutions in numerous high-profile matters involving accounting fraud, antitrust, FIRREA, the FCPA, insider trading, money laundering, mortgage origination and servicing, OFAC sanctions, securities fraud, tax fraud, and trading. He has extensive experience representing financial institutions in parallel regulatory and criminal investigations and representing non-U.S. companies and individuals in connection with U.S. investigations.

Mr. Bourtin has conducted numerous jury trials and has argued frequently before the U.S. Court of Appeals for the Second Circuit.

Geoff Brown, CISO, City of New York
Geoff Brown was appointed Chief Information Security Officer for the City of New York in 2016, a position focused on cybersecurity and aggregate information risk across all 100+ NYC departments and agencies. In July 2017, Mayor de Blasio established New York City Cyber Command, led by Geoff and charged with setting Citywide cybersecurity policies; directing response to cyber incidents; and advising City Hall, agencies and departments on the City's overall cyber defense. Prior to joining City government, Geoff worked in financial services, developing and operating threat management disciplines including threat intelligence, detection, response and countermeasures. Geoff also served in the federal government, including work with the National Commission for Terrorist Attacks Upon the United States (the 9/11 Commission), supporting the investigation's work with the first responder community in NYC. Geoff is a graduate of Middlebury College.

Gordon Crovitz, Co-Founder, NewsGuard
Gordon Crovitz is the co-founder and co-CEO of NewsGuard, which is countering false information, misinformation and disinformation online. He is former publisher of The Wall Street Journal, where he also served as an editorial board member and opinion columnist. Along with his NewsGuard co-founder Steven Brill, Crovitz co-founded Press+, a digital subscriptions technology company acquired by RR Donnelley in 2011.

Crovitz was the founding editorial page editor of The Wall Street Journal Europe, based in Brussels. He was editor and publisher of the Far Eastern Economic Review, based in Hong Kong. He served as CEO of Houghton Mifflin Harcourt, the largest learning company serving kindergarten through high school in the U.S. He serves on the board of directors of Houghton Mifflin Harcourt, Marin Software, Business Insider, Blurb, Spirited Media and the American Association of Rhodes Scholars. He previously served on the board of directors of Dun & Bradstreet, ProQuest and Factiva. He graduated from the University of Chicago and has law degrees from Wadham College of Oxford University and from Yale Law School.

Nicole Friedlander, Partner, Sullivan & Cromwell LLP
Nicole Friedlander is a member of the Firm's Criminal Defense and Investigations Group and co-head of the Firm's Cybersecurity Practice. Ms. Friedlander's practice focuses on white-collar criminal defense, regulatory enforcement proceedings and internal investigations. She has particular expertise in fraud, anti-money laundering, tax and cybercrime matters.

Ms. Friedlander joined the Firm in 2016 from the United States Attorney's Office for the Southern District of New York, where she was Chief of the Complex Frauds and Cybercrime Unit. During over eight years of service, she prosecuted sophisticated financial frauds, cybercrimes, money laundering and Bank Secrecy Act offenses, FCPA violations, and criminal tax cases. Ms. Friedlander's white collar work includes leading major prosecutions of offshore banks for facilitating tax evasion, securing one of the largest-ever FCPA resolutions and bringing a groundbreaking, successful racketeering case against the owner of multibillion-dollar payday lending companies. Her cybersecurity experience includes leading the successful investigation of the largest-ever cyber theft of customer data from a U.S. financial institution; overseeing the indictment of Iranian state-sponsored hackers for coordinating cyberattacks on 46 financial institutions; leading cutting edge virtual currency-related cases; and prosecuting a Russian national for hacking U.S. banks in a case the FBI named one of its top ten of the year. For its consumer protection work during her tenure, the FTC awarded the Complex Frauds and Cybercrime Unit its Criminal Liaison Unit Award in 2016.

Andrew Gerlach, Partner, Sullivan & Cromwell LLP
Andrew Gerlach is a partner in the Firm's Financial Services and Mergers and Acquisitions Groups and co-head of the North America insurance practice. Mr. Gerlach's practice is primarily focused on mergers and acquisitions, divestitures, joint ventures, securities offerings and similar transactions involving financial institutions. He also advises clients on a variety of regulatory, takeover defense and corporate control, general corporate, strategic and corporate governance matters. Mr. Gerlach represents both U.S. and non-U.S. public and private financial institutions, including banks, insurance companies, private equity funds, hedge funds, investment advisers and broker-dealers.

Mr. Gerlach has worked on a variety of regulatory matters with federal and state banking, insurance and securities regulatory agencies and other governmental agencies on behalf of a number of U.S. and international financial institutions.

Alphonzo Grant, Managing Director, Head of Special Investigations for ISG and IM at Morgan Stanley, Legal & Compliance Division

Alphonzo Grant, Jr. is a Managing Director of Morgan Stanley and currently serves as the Head of the Global Litigation Group's Special Investigation Unit for Institutional Securities and Investment Management ("SIU"). SIU is responsible for conducting internal investigations of employee business conduct violations across the Firm's several business units. Mr. Grant also oversees investigations of institutional customer complaints in the Americas and represents the Firm in various regulatory and criminal matters. Mr. Grant joined Morgan Stanley in 2011. Since 2012, Mr. Grant has served as an Adjunct Professor at Benjamin N. Cardozo School of Law, where he teaches trial advocacy.

From May 2011 to October 2014, Mr. Grant served as a Commissioner on the New York City Civilian Complaint Review Board ("CCRB") following his appointment by Mayor Michael R. Bloomberg. The CCRB investigates, makes findings and recommends disciplinary action regarding civilian complaints of excessive or unnecessary force, abuse of authority, discourtesy and offensive language by NYPD officers.

Gabriel Hidalgo, Managing Director, K2 Intelligence

Gabriel "Gabe" Hidalgo, a managing director at K2 Intelligence, has 20 years of legal, regulatory compliance, and Anti-Money Laundering (AML) experience working with wholesale and retail banks, FinTech companies, broker/dealers, and money services business entities. Gabe is a recognized subject-matter expert in the cryptocurrency and digital assets market and is able to help clients navigate and mitigate Bank Secrecy Act and Anti-Money Laundering (BSA/AML) compliance risks as they strive to keep up with the latest developments occurring within the new value-transfer digital asset marketplace, establish new banking relationships, and satisfy regulatory requirements domestically and internationally. Gabe also works with FinTech companies to establish dynamic and comprehensive compliance programs that incorporate the essential elements for sound oversight—effective governance and management controls, clear and practical policies and procedures, efficient transaction monitoring and sanction screening systems, comprehensive training, and sound quality assurance controls.

Prior to joining K2 Intelligence, Gabe served as chief compliance officer for Noble Bank International, a new innovative bank providing transactional settlements for various asset classes including cryptocurrency, FX, energy, and precious metals.

Jeremy Kroll, President, CEO, Co-Founder, K2 Intelligence

As president, CEO, and co-founder of K2 Intelligence, Jeremy M. Kroll is responsible for charting the firm's growth strategy, including market development, strategic partnerships, and acquisitions. With more than two decades of investigative and leadership experience, Jeremy has led K2 Intelligence since its inception in 2009 through its growth into an internationally recognized firm with six offices across the United States and Europe.

Using the strategic acquisition of intelligence to inform risk mitigation strategies, Jeremy helps executives and business owners to further their business objectives. He serves as a trusted advisor and complex problem solver to business owners, boards of directors, and C-suite executives, working with them to mitigate risk across the corporate and family office spheres. He advises clients on risk management as they pursue strategic investments, including cross-border acquisitions and multinational investments, and helps them to navigate the changing physical and cybersecurity landscape in a way that embraces technological change while minimizing strategic risk.

In his capacity as CEO, Jeremy is also responsible for managing the company's global business lines. He spearheads K2 Intelligence's technology initiatives, with an emphasis on cyber defense, information security, and data analytics, helping the firm marry professional excellence with cutting-edge technology.

Jules Kroll, Chairman & Co-Founder, K2 Intelligence
Jules B. Kroll is chairman and co-founder of K2 Intelligence. He also serves as chairman of Kroll Bond Rating Agency, Inc., and as a member of the board of directors of BlueVoyant.

Jules is the founder of Kroll, Inc., and the acknowledged pioneer of the modern investigations, intelligence, and corporate security industry. In 1972, he established Kroll Associates Inc. the prototype for a new breed of professional services firms dedicated to mitigating risk. By employing former prosecutors, law enforcement officials, journalists, and academics who used sophisticated fact-finding techniques to address decision-makers' need for accurate information, Jules established investigations and risk consulting as indispensable corporate services.

David Lawrence, Founder and Chief Collaborative Officer, RANE
David Lawrence is the Founder and Chief Collaborative Officer of RANE. He previously served for approximately 20 years as Associate General Counsel and Managing Director at Goldman Sachs. During his tenure, David formed and was the global head of the Business Intelligence Group. His role covered a wide range of legal, regulatory, diligence and transactional responsibilities for the firm, as well as advising Goldman's clients directly. David served on a number of the firm's global risk-management and investment committees, including its Commitments and Capital Committees. In 2014, David received the FBI Director's Award for his efforts in combating international terrorism.

Over the years, David and Goldman Sachs were jointly awarded over 20 risk management patents. While at Goldman Sachs, he helped create and lead the firm's formation of Regulatory Data Corp (RDC), in which 20 of the leading global banks invested. Prior to working at Goldman Sachs, David served for 10 years as an Assistant US Attorney, in the Southern District of New York. During this tenure, he served as the Deputy Chief of the Criminal Division and Chief of the Public Corruption and General Crimes Units. David serves as a member of the Board of Trustees for the John Jay College of Criminal Justice Foundation (City University of New York). David received a B.A. from Brandeis University in Urban Studies, Magna Cum Laude with Highest Honors. He attended the University of Texas School of Law and received his J.D. from New York University School of Law.

Molly Levinson, President, The Levinson Group
Molly Levinson, President of the Levinson Group, is a seasoned communications and public affairs specialist, providing strategic advice, crisis and issues management, media relations, and reputation management for CEOs, corporations, non-profits, and other organizations. She has worked with law firms across the country on some of their most critical matters. Her deep knowledge of media, including global landscape, relationships, and competitive positioning, has contributed to a track record of leveraging brand strengths in dynamic and complex environments. Her two decades of practice in the center of media and public affairs includes experience on both sides of high-profile, high-stakes news: developing comprehensive communications campaigns to connect targeted audiences to compelling stories, and conversely, leading political coverage at major media outlets.

Timothy Murphy, President, Thomson Reuters Special Services
With 30 years of public and private sector experience—primarily in the Federal Bureau of Investigation—Timothy P. Murphy is a recognized leader in the global law enforcement, intelligence, and business communities.

A Michigan native, Mr. Murphy became a police officer after graduating from college in 1983. In 1988, he joined the FBI as a special agent. He held a number of operational positions in a variety of field offices

nationwide, investigating matters as diverse as counterterrorism, intelligence, cyber and organized crime, and even serving as an FBI pilot. Mr. Murphy served in various management roles, to include serving as a Special Assistant to the FBI Director—a position that gave him a unique, high altitude view of the Global FBI from both operational and administrative perspectives. He steadily climbed the Bureau's management ladder, eventually serving as the Special Agent in Charge of the Cincinnati field office, the Bureau's Chief Financial Officer, and then it's Chief Operating Officer. He eventually rose to become the Deputy Director of the FBI, a position he held until retiring in 2011. Prior to joining TRSS, Mr. Murphy was a Vice President at MacAndrews and Forbes, Inc.

Sharon Nelles, Partner, Sullivan & Cromwell LLP
Sharon Nelles, a partner in the Firm's Litigation Group and member of the Firm's Executive Committee, represents financial institutions and global companies in high-profile, critical company matters that implicate not only civil litigation but also related regulatory, congressional and criminal investigations and enforcement actions. She is currently active in matters arising from the Volkswagen diesel crisis and the #MeToo movement, among others.

Ms. Nelles has represented such clients as Airbnb, Moody's, JPMorgan Chase, Standard Chartered Bank, Microsoft and Diageo, in high-profile investigations and litigation, including matters arising from the subprime mortgage crisis, such as JPMorgan Chase's groundbreaking $13 billion global settlement. She has tried cases in the state and federal courts on behalf of such clients as Microsoft, Eastman Kodak Company and General Bank, and has represented prominent firms and individuals in proceedings before the Department of Justice, the United States Congress, the Securities and Ex
change Commission, the Federal Trade Commission, the Federal Reserve Bank of New York and virtually every state attorneys general.

Troy Paredes, Founder, Paredes Strategies
From 2008-2013, Paredes was a Commissioner of the U.S. Securities and Exchange Commission, having been appointed by President George W. Bush and confirmed by the U.S. Senate. Paredes served as an SEC Commissioner during an especially historic time at the SEC and for our economy – namely, throughout the financial crisis and its aftermath, including the implementation of the Dodd-Frank Act. He played a key role in rulemakings and other regulatory matters concerning all aspects of the SEC's mission and securities regulation, including, among other things, antifraud and anticorruption, public company disclosures, capital formation, corporate governance, executive compensation, investment management, investment advisors, broker-dealers, exchanges, credit rating agencies, equity market structure, fixed income markets, derivatives, auditing and accounting, and cybersecurity. At the SEC, Paredes was a strong advocate for small business and the JOBS Act, for solving the information overload problem of securities law disclosure, and for rigorous cost-benefit analysis. He also consistently expressed concerns about the overregulation and overreach of the Dodd-Frank Act.

Arielle Patrick, Senior Vice President, Financial Communications & Capital Markets, Edelman
Arielle Patrick is Senior Vice President & Transaction Director at Edelman, the world's largest communications consulting firm. Arielle is an advisor to C-suite executives and boards of directors of public and private companies. She specializes in all-stakeholder communications strategies for financial special situations and crisis management. Areas of focus include: mergers & acquisitions, bankruptcy, restructuring, and other sensitive transactions.

In her spare time, she sits on the Board of Trustees of The Harbor Sciences & Arts Charter School; the National Advisory Board of the foundation for Yellowstone National Park; the Leadership Council for the

SpecialOlympicsof New York; and is Fundraising Chair of the Alumni Board for the Princeton Tigerlilies acapella group. Arielle graduated Princeton University, where she studied in the Department of Classics with a concentration on Ancient Greek and Latin language, literature and history. Arielle has been featured in Forbes, the Financial Times, and other publications. She has also been a speaker at various conferences at institutions, including Bloomberg, Columbia University, Princeton University and The Wing.

John Riggi, Senior Advisor for Cybersecurity and Risk, American Hospital Association
John Riggi, having spent nearly 30 years as a highly decorated veteran of the FBI, serves as the first Senior Advisor for Cybersecurity and Risk for the AHA and their 5,000+ members. In this role John serves as a resource to assist AHA members identify and mitigate cyber and other sources of risk to their organizations. John will also support the AHA's policy, advocacy and government relations efforts on cyber and risk issues. Previously, John led BDO's Cyber and Financial Crimes Practice. At the FBI Cyber Division, he led the national program to develop mission critical partnerships with the healthcare sector, other critical infrastructure sectors and across government for the investigation and exchange of information related to national security and criminal cyber threats. John held a national strategic role in the investigation of the largest cyber-attacks targeting healthcare, energy, entertainment, technology, financial services, government and other sectors. John also served as a representative to White House Cyber Response Group. In addition, he serves as an official private sector validator for the White House's Presidential Policy Directive on U.S. Cyber Incident Coordination (PPD-41)

Kevin Zerrusen, Managing Director and Head of Technology Division Risk Governance, Goldman Sachs
Kevin Zerrusen was previously Global Co-Head of the Security Incident Response Team, Goldman Sachs. Prior to joining Goldman Sachs in 2013, he had a career in the Central Intelligence Agency (CIA), where he served in multiple roles at the agency's headquarters in Langley, Virginia and overseas. He most recently directed a cyber center at the CIA. Zerrusen earned a BA in Political Science from the University of Dayton and an MBA from Syracuse University.

Call-out text