

THE M&A ADVISOR SYMPOSIUM REPORT

Featuring



Mario Rebello
Management Consultant



Carlos Moreira
Founder and CEO
WISeKey



Gregory J. Suhajda
Senior Managing Director
Mackinac Partners



Gregory Bedrosian
CEO
Redwood Capital



Jeffrey Wells
Executive Director of
Cyber Development
Maryland Department of Business
& Economic Development

> STALWARTS ROUNDTABLE: CYBERSECURITY – PROTECTING FINANCIAL PERFORMANCE

At The M&A Advisor's Annual Summit in New York on November 18, 2014, Carlos Moreira, Founder and CEO, WISeKey, chaired a Stalwarts' Roundtable discussion on Cybersecurity.

In this report, we gather the insights and reflections of five high-level Cybersecurity and M&A technology experts, responsible for billions of dollars of investment among them, who participated in this session. The pages to follow highlight the stalwarts' perspective on cybersecurity management and what lies ahead for what is forecast to be one of the fastest growing industries in 2015.

The principle issues addressed in this symposium session included:

- The need for "trusted identity" policies and technology to replace obsolete online password protocol.
- Whether and how the U.S. and other governments will take action on cybersecurity threats in the private sector.
- The opportunities for early stage companies in cybersecurity.
- How CEO's and Boards of Directors should address cybersecurity concerns and requirements.
- The role that consolidation will play in the cybersecurity industry.

The growth of M&A transactions in the cybersecurity industry, over 50% in the first half of 2014, is directly tied to the risk of cyber-attacks on the financial performance of corporations, governments and individuals. Spending on cybersecurity is expected to top \$100 billion in 2015 with a forecasted annual growth rate of over 20 percent over the next five years.

Presented by



I invite you to read this insightful report about an industry whose growth represents a tremendous opportunity for the M&A community and whose service will affect us all.

David Fergusson
President and Co-Chief Executive Officer
The M&A Advisor

Contents

Executive summary	1
Introduction	1
From passwords to "trusted identities"	2
Opportunities for cybersecurity start-ups	3
The threat from inside	4
Not just a technology problem	4
Cybersecurity on the M&A checklist	5
Consolidation and building trust	5
Cyber-warfare and fragmentation	6
Video interviews	8
Symposium session video	9
Contributors' profiles	10
Report sponsor profile	12
Publisher	13

Presented by



Executive summary

Demand is increasing for organizational and individual cybersecurity. Destructive cyber-attacks on high-profile companies (Target, Home Depot) and financial institutions (JP Morgan) in the past year have heightened awareness of risks and vulnerabilities throughout the business world. These data breaches, affecting millions of customers, increase liability on boards and CEOs, who are realizing it is no longer enough to leave cybersecurity to the IT department. More than 50 percent growth in M&A transactions in the cybersecurity industry in the first half of 2014 is directly tied to the risk of cyber-attacks on financial performance. Spending on cybersecurity is expected to top \$100 billion in 2015 with a forecast annual growth rate of over 20 percent over the next five years.

Introduction

At The M&A Advisor's Annual M&A Summit in New York in London, on November 18, 2014, a panel of experts discussed the protection of financial performance with cybersecurity. The panel comprised:

Carlos Moreira | Founder and CEO, WISEKey

Jeffrey Wells | Executive Director of Cyber Development, Maryland Department of Business and Economic Development

Mario Rebello | Management Consultant

Gregory J. Suhajda | Senior Managing Director, Mackinac Partners

Gregory Bedrosian | CEO, Redwood Capital

Moderator Carlos Moreira, founder and CEO of WISEKey, a leading global cybersecurity company, noted that the discussion by Cybersecurity Panel would continue at the World Economic Forum in Davos in January. Moreira led the panel in a wide-ranging discussion on:

- Whether the U.S. government will take action on cybersecurity threats in the private sector.
- The need for “trusted identity” policies and technology to replace obsolete password technology.
- The opportunities for start-ups in cybersecurity.
- Whether consolidation will play an increasing role in the cybersecurity industry.
- Threats by state actors on a global basis.

Moreira opened the discussion with a question to Mario Rebello, Management Consultant, on the outlook for legislation or government action on cybersecurity in the near term.

“The issue is real,” Rebello said, adding that the Obama administration and Congress are discussing the situation “in real time.” But with the political gridlock in Washington, Congress and the administration are having great difficulty in “agreeing on a baseline and on a cybersecurity framework.” Some want to make cybersecurity measures voluntary; some want to make them mandatory. The administration has proposed “an excellent cybersecurity framework,” Rebello said, which is voluntary in nature, but is meeting resistance from Congressional leaders.

Presented by



At the state level things are different, he said; governors have been able to get some things done because both parties were at the table, and they put politics aside on the cybersecurity issue. “At the state level we’ve actually been able to work on it and form a coalition, whereas in Congress it’s more difficult to find that coalition – even within a party,” Rebello said. Nonetheless, Rebello was hopeful that, on the national level, “we will see some action very soon.”

In the private sector, business and industry leaders need to do more to bring “clarity in the legislation,” Rebello said. “For example, the number one issue that would help us collectively is the sharing of information on vulnerabilities and risks,” he said, but stressed that many companies are afraid to come forward and share that information for fear that it will be held against them – thus there is a need for a “safe harbor provision” in any legislation that will allow and encourage the sharing of information on cybersecurity risks and solutions. “Having corporate sectors and leaders and IT come forward and say, ‘These are the threats that we are seeing coming in,’ would help agencies and law enforcement address the issue,” Rebello said. “But there’s just hostility at times at working together right now in Washington.”

“We have been using passwords for more than 30 years now and the password technology is totally obsolete.”

– Carlos Moreira

From passwords to “trusted identities”

Carlos Moreira turned to the topic of password technology. “The password is dead,” he declared. “We have been using passwords for more than 30 years now and the password technology is totally obsolete. You are all using passwords to access your mobile phones, to access your websites – and your passwords are totally unprotected.”

Moreira said that the United States is finally looking at the issue with the administration’s “national strategy for trusted identities in cyberspace... something that we started in Europe years ago.” He believes that “cybersecurity ground zero” is a country “first protecting its citizens.” Corporations have ways to protect themselves but citizens are being hacked every day, Moreira said, adding that in 2013, 18 million Americans lost their personal data, and that these numbers will keep rising. He asked Mario Rebello to explain how the U.S. government is protecting its citizens.

“Today, we’re really not,” Rebello said. “We are, all of us in this room, we’re the low-hanging fruit for the hackers.” Government, and business, he said, is not focused on the consumer – instead, it is trying to protect data and networks: “The hackers are three or four steps ahead of us, but the opportunity is for us to educate the consumers on how to apply a new standard, a new framework, and [to ask], ‘How do we protect privacy and individual identities?’”

Carlos Moreira turned next to Jeffrey Wells, Executive Director of Cyber Development from the Maryland Department of Business & Economic Development. Because of its proximity to Washington, D.C., and myriad government agencies, Maryland is a hub of cybersecurity in the U.S. “Is cybersecurity a major economic growth engine for the states? Can states create jobs [and] startups around cybersecurity? What is the strategy in Maryland?” Moreira asked.

“The State of Maryland is certainly considered the epicenter of cybersecurity with the strong presence of the NSA and Cyber Command and the other agencies that are there,” Wells said,

Presented by



adding that cybersecurity is a “cool word,” but asked, what does it really mean? It’s really not about ones and zeros, Wells said; it’s about the user: “Focusing on the technology is a quick way to make money, but it’s not about solving the problem.”

Wells explained that Maryland benefits from its geography, its base of customers and educational institutions, and its startup business community, and that it has evolved with a very serious focus on providing services to customers – the U.S. government being one of its biggest customers. Wells said the state tries to approach various sectors and ask what kind of problems they are facing. “What can we use from what we know in the past and apply that to developing new companies with products – whether those be software or hardware products – to address very specific customer needs?”

“Focusing on the technology is a quick way to make money, but it’s not about solving the problem.”

– Jeffrey Wells

Opportunities for cybersecurity start-ups

Wells further stated that cybersecurity is a great opportunity for new business models. “It’s never going to go away. Every single person in this room, every piece of data you have, is already corrupted,” he added. From a business perspective, he said, whether trying to maximize an investment or solving internal issues, organizations need to realize they have “already been invaded, and how to handle that properly.”

By the year 2020, Carlos Moreira said, more than 50 billion devices will be connected to the Internet. “Car companies are not car companies any more – they’re software companies making cars,” he said, further stating that these companies are morphing into information technology platforms and must be able to secure their products: “Hacking your phone is fine but imagining hacking your car or hacking your house or hacking your power grid or your nuclear stations?” With this in mind, there’s a huge possibility for the United States to be a leader in cybersecurity, Moreira said to Wells.

“There’s an incredible opportunity for business growth...to increase efficiency, to really grow your business and to address real problems,” Wells said. But on the flip side, he said, “There is an insurmountable number of issues that are out there, and you can’t address every single risk in cybersecurity on a daily basis because the volume is too much.” Companies and investors need to employ hedging strategies – identifying the biggest risks and the way to spread risks across portfolios. They should address cyber threats “from a risk perspective rather than from a defensive perspective,” he said.

Moreira noted that often, when he would meet with CEOs at companies concerned about their cybersecurity, the CEOs would say “talk to the IT guy.” But now, with notorious cyber breaches at companies like Target, Home Depot and, more recently, at JP Morgan, CEOs are realizing that cybersecurity needs to be their concern. “Basically, an entire company’s valuation can be withered by just having a bad issue of cybersecurity,” he said.

Presented by



The threat from inside

Gregory Suhajda, Senior Managing Director of Mackinac Partners (a leading financial advisory and turnaround firm), was asked by Moreira to explain how his firm advises client companies about cybersecurity, and answered: “This is the old corporate espionage – now with cyber threats, you can do it from thousands of miles away, and steal proprietary information or employee information – and there’s so many different ways to infiltrate a company. Does it still involve an insider? Yes!” The likelihood of a cyber break-in occurring is much higher if someone on the inside of a company is involved.

“Today’s CEO must realize that cybersecurity is a team effort and not just the task of the IT department.”

– Gregory Suhajda

Today’s CEO must realize that cybersecurity is a team effort and not just the task of the IT department, said Suhajda, who prior to Mackinac had gained more than 20 years of experience within the investigative and international intelligence community as a former Special Agent with both The United States Secret Service and The Federal Bureau of Investigation (FBI). Company executives, sales people and representatives at all levels—often traveling with laptops and hard drives and mobile devices – are at extreme risk. “Your reputation is on the line,” he said. “You can’t just narrow it down to the C-level, or IT, you’ve got to try to get your arms around everything and narrow it down as best you can.”

Moreira then noted that corporations traditionally viewed themselves as fortresses: “The bad people are outside and inside we are all good people and therefore if we buy a lot of technology to protect at the rear we are safe.” But 99 percent of the latest cybersecurity threats happen inside, Moreira said, because of employees bringing in an unprotected mobile phone, or because a company has not segregated its personal data from its corporate data. “How do you advise companies to protect against those threats?” he asked Gregory Suhajda, who said that the foundation is a very solid set of policies and procedures, but that it carries on from there – in other words, a company must have a layered system. An example, he said, is having an effective policy for dealing with terminated or disgruntled employees. “All these simple things now hold a lot of weight and can cause a lot of damage, so it might not just be a cyberthreat – it might be sabotage that can cause a great amount of damage.”

Not just a technology problem

“You touched on something really important – this is not just a technology problem,” Jeffrey Wells interjected. “Technology is the tool but everything in cybersecurity is a people problem, whether it’s bad design, whether there’s a bad actor somewhere trying to do something internally. It all comes down to people. This is an entire company’s issue, or an entire ecosystem’s issue.”

But, asked Carlos Moreira, cybersecurity technology is available. Why aren’t companies, why aren’t people using it? Why aren’t corporations buying this technology?

“At times it’s just priorities,” said Mario Rebello, adding that, in the past, cybersecurity wasn’t viewed as a big problem or risk. But now, with Target, Home Depot, JP Morgan and other major cases, he said, “it’s a major problem. It’s now reached the board level and the CEO and the board members are liable and are even starting to lose their jobs over this.”

Presented by



Cybersecurity on the M&A checklist

Gregory Bedrosian, CEO of investment banking group Redwood Capital, said he is seeing more and more boards elevate the cybersecurity role to the CEO, or someone at the board level with cybersecurity expertise. This is increasingly important in the M&A processes of a company within any sector, especially large-cap acquirers. Bedrosian said that “cybersecurity diligence is being added to closing checklists in addition to financials, in addition to calling vendors and customers. They don’t want a situation where it’s been ignored or under-invested in for years, and then they acquire the business and inherit a lot of those issues,” he said. “It’s unfortunate for some of those high-profile cases that have been all over the news, it’s unfortunate for those CEOs and those boards. But the silver lining is that it’s created awareness at a much higher level, and there will be more focus on that as it relates to value-building.”

“But are we investing enough in cybersecurity?” asked Carlos Moreira, noting that the revenue-generating ability of the cybersecurity industry has been forecast to be \$180 billion by 2018.

Bedrosian said statistics over past couple of years in investment in cybersecurity businesses show that most are early-stage start-ups. Over 60 percent of the capital deployed into cybersecurity-related companies over the past 12-18 months was in either seed or A-round investments, he said. “What it’s saying is there is a whole younger generation of start-ups that are addressing these emerging needs but they’re at a very early stage,” he added. The positive side is that the types of investors that are focused on cybersecurity start-ups are some of the world’s leading venture and private equity groups – Intel, Kleiner Perkins, Sequoia, Accel Partners, Andreessen Horowitz, Bedrosian said. “So the smart, the high-IQ investors, the cream of the crop of Silicon Valley, are investing but they’re targeting young, smarter players.”

Consolidation and building trust

Over time that could mean a consolidation play, Bedrosian added. “Consolidation is a critical point in cybersecurity,” noted Carlos Moreira. “My experience as a private company – when I’m trying to sell my technology to a top 500 firm – the first question they ask me is, ‘When are you going to be public? Because I don’t trust you being a private company on cybersecurity, because there are critical assets to protect.’”

He added: “So I guess consolidation is a solution, but we also have to educate these C’s that cybersecurity is not like social media – that you can create a fuss about it and just collect money... cybersecurity is a long-term process that requires a company to go through the process of building trust – because it’s all about building trust.”

Jeffrey Wells said that, in Maryland, “...we’ve seen [in] the last 24 months a large number of ex-government – NSA, PhDs, ex-military,” go into new cybersecurity, many of which are getting investments by those organizations mentioned by Bedrosian. “One of the challenges again is educating the customer base as to what the problem is that they have,” Wells added. “There is

“Cybersecurity diligence is being added to closing checklists in addition to financials, in addition to calling vendors and customers.”
– Gregory Bedrosian

Presented by



no silver bullet. That's one of the problems the C-level suites have...they just think, 'I'm going to call my IT department, and they'll put a box in, and that solves all my problems.'" Moreover, Wells added, companies that have invested in legacy systems are loathe to hear that they need to invest even more to protect them: "I heard somebody at a conference two weeks ago saying you should be spending 20 percent of what you have to lose on cybersecurity. That's a big number and that's hard for most people to swallow," Wells said.

Cyber-warfare and fragmentation

Turning to the geopolitical arena, Carlos Moreira noted recent and recurring instances of "cyber warfare" such as attacks on Saudi Aramco in 2012 and the nation of Estonia in 2007. [Editor's note: Since the 2014 Annual M&A Advisor's Summit, Sony Pictures USA incurred a major cyber-attack that some experts claim to have been engineered by North Korea, which has denied the claim.] "This is going to be recurring," Moreira said.

"This is a grave concern," said Gregory Suhajda. "That's why you're seeing government agencies gearing up. It's incredibly challenging, incredibly difficult, and going to take time. Some companies already know they're going to fall victim to this so they build it into their budget." Said Carlos Moreira: "But the world needs leadership and needs the United States to be the leader." He also said Europe is hopelessly fragmented: "We have countries and companies that don't talk to each other. The United States should be the leader because it has the biggest companies, the biggest budget – but you also have a major issue now, which is trust. Snowden has caused damage. How do you rebuild it?"

"Trust is not going to be resolved anytime soon," Mario Rebello offered. "European companies don't want to deal with American companies because of Snowden." He recommended forming joint ventures between cybersecurity start-ups, and collaboration on an individual level with key industry players in the U.S., Europe, Asia and Brazil. "These are hotspots – but nobody's talking to each other, nobody's sharing information. They're all in their little corner doing their own thing. What we need to do as business leaders, as political leaders, as think tanks or influential groups, we need to bring these stakeholders and really address the trust issue by allowing them to work together around innovation that is simple and secure. I think that's how we overcome the trust issue," said Rebello.

Gregory Bedrosian said the large U.S. financial institutions "need to take a leadership role [in rebuilding] that trust –but that's a big leap for them." He said he knew from personal experience with the JP Morgan cyber-attack that the number of employee hours at all levels of the bank dealing with customer outreach and mitigation "was enormous." Yet, "there's a great opportunity for an institution like JP Morgan to turn that into a positive in terms of touching tens of thousands of consumers across the country and across the world."

Wrapping up the discussion with an audience Q&A, the panel agreed that the Internet is changing dramatically, from initially an informational network to a transactional one – and is faced with fracturing issues such as China and Brazil restricting access to data-gathering sites. Panelists also

"Trust is not going to be resolved anytime soon. European companies don't want to deal with American companies because of Snowden."

– Mario Rebello

Presented by



agreed with a questioner who asked if electronic gamers could be an asset to cybersecurity. “Teaching hacking as a positive thing – as a defensive gesture – can teach a generation of students to see that there are other ways to solve problems,” said Mario Rebello. “Companies like Google and Microsoft are actually paying bounties to hackers to help them find flaws in their products.”

Presented by



Video interviews

To watch exclusive M&A Advisor interviews with these industry experts on ‘Cybersecurity – Protecting Financial Performance’, click on the following images:



Carlos Moreira

Founder and CEO
WIS@Key



Jeffrey Wells

Executive Director of Cyber Development
Maryland Department of Business &
Economic Development

Presented by



Symposium session video

To watch Stalwarts Roundtable ‘Cybersecurity – Protecting Financial Performance’ at M&A Advisor’s 2014 Summit in New York, click on the following image:



**Cybersecurity –
Protecting Financial
Performance**

Presented by



Contributors' profiles



Mario Rebello
Management Consultant

Mario Rebello is a management consultant and public affairs advisor with more than 20 years experience working with the Information Communications Technology high-tech and manufacturing sectors, and public sector. Mario worked at Microsoft for over 12 years managing and rebuilding government relations programs and devising new engagement initiatives post Microsoft DOJ & EU anti-trust eras. Most recently, Mario headed Good Technology's effort to secure Common Criteria Evaluation Assurance (EAL4+) to open financial and public sector markets in Europe & Asia; secured FIPS 140-2 certification in the US; and hosted policy makers and ICT media from around the globe. Mario started his career at United Technologies Corporation managing state and local government relations in Hartford, CT; and then went on to serve on the cabinet of Rhode Island Governor Lincoln Almond as Policy & Legislative Counsel, as well as Policy Advisor to US Senator John Chaffee (R-RI). Following these government services roles, Mario served as Government Relations and Telecommunication Policy Counsel at AT&T. Mario has served as President and Board member of the Portuguese American Scholarship Foundation; Advisor to the Brookings Institute Metro Program; and supports the Boys & Girls Clubs of America and NFTE.



Carlos Moreira
Founder and CEO
WiSeKey

Carlos Moreira is the Chairman, Chief Executive Officer and Founder of WiSeKey, Switzerland. Mr. Moreira began his career as a UN expert on IT, e-security and trust models; 1983-98, he worked for ILO, UN, UNCTAD, ITC/WTO, World Bank, UNDP and ESCAP. He was also an early stage pioneer in the field of digital identity. In 1999, Mr. Moreira founded WiSeKey. Mr. Moreira is a member of: UN Global Compact; Global Clinton Initiative. World Economic Forum: Founding Member, Global Growth Companies; 2007-13, New Champion; 2012-13, Vice-Chair, Global Agenda Council on Illicit Trade; Partnering Against Corruption Initiative. Founder: Geneva Security Forum; Geneva Philanthropy Forum. He was named one of the 300 most influential people in Switzerland for 2013.



Gregory J. Suhajda
Senior Managing Director
Mackinac Partners

Gregory J. Suhajda is the President of the Mackinac Partners Business Intelligence Division and manages the Company's service capabilities for corporate due diligence, investigations, cyber security and business intelligence. Greg brings more than 20 years of experience within the investigative and international intelligence community to Mackinac, where he has built a platform to service clients across various industry sectors and business environments. Prior to joining Mackinac Partners, Greg was the President of Rehmann Corporate Investigative Service, a global risk management and intelligence firm based in Troy, MI. In his role as President, Greg led a team of seasoned professionals including former agents of the Secret Service, the FBI and local law enforcement agencies to provide a comprehensive array of global intelligence and security advisory services. Greg established a widespread client base ranging from high net worth individuals, Fortune 500 businesses to small size local clients. Greg's leadership and experience solidified both the expansion of the Corporate Investigative Services capabilities and its consistent year over year revenue growth. Greg is a graduate of Grand Valley State University where he earned a Bachelor's of Science Degree in Business Law. He is a Certified Fraud Examiner and a graduate of The Stanford University Executive Management Program.



Gregory Bedrosian

CEO
Redwood Capital

Gregory Bedrosian is the Co-Founder, CEO & Managing Partner of Redwood Capital Group. He is responsible for the overall strategic direction and management of the firm and takes an active role in Redwood's relationships across the corporate and investment communities. Mr. Bedrosian is an award-winning and seasoned Investment Banker and Private Equity Investor, who lived and worked in Europe for over half of his 20-plus year career, and whose experience spans both domestic and cross-border M&A and private equity transactions across the US, Europe and emerging markets. Prior to the formation of Redwood Capital, Mr. Bedrosian was a Co-Founder of Renaissance Capital, a leading investment bank focused on the emerging markets of Russia, Eastern Europe and Africa and Co-Founder and General Partner of The Sputnik Funds, a \$1 billion private equity firm investing in the media, communications and other growth sectors. He has served on numerous corporate and non-profit boards across the US and Europe and he currently sits on the Harvard Business School Alumni Board of Directors (Emeritus), the Editorial Advisory Board of a Financial Times unit (ExecSense), Chairs the Investment Committee of a \$100 million New York-based foundation and serves on the Board of an emerging markets-focused special situation hedge fund. Mr. Bedrosian holds an M.B.A. from Harvard Business School and a B.S. in Economics from the Wharton School of the University of Pennsylvania.



Jeffrey Wells

Executive Director of
Cyber Development
Maryland Department
of Business & Economic
Development

Jeffrey Wells is Executive Director of Cyber Development in the Maryland Department of Business & Economic Development (DBED). Jeffrey Wells was appointed Executive Director of Cyber Development in September of 2013. In that role, his responsibilities include utilizing his knowledge of the commercial and federal/military aspects of Maryland's rapidly evolving Cyber Security industry to support growth, as well as driving the business development and strategic marketing of Maryland's many cyber assets. In addition to providing guidance to emerging cyber companies within Maryland or contemplating moves to the state, Wells directs general cyber outreach and education, particularly to the business community. He advises individual companies in incubators, universities, federal labs and other start-up environments, connecting them with potential investors, buyers and contractors. Wells has over 25 years of experience in providing analysis, strategy, insight, and leadership to companies in international markets. He has devised and facilitated profitable and sustainable business initiatives—with a focus on contributing social value—across diverse cultures and organizations throughout North America, Europe, Africa, Middle East and Asia. In 2007, Wells established the social business and anti-poverty enterprise Khalakom. Khalakom used access to mobile technology as a conduit for community, empowerment, and social change. Prior to Khalakom, Wells was Chief of Operations and Lead Analyst for the innovation arm of Nokia, Innovent.

Report sponsor profile



Mackinac Partners

Mackinac Partners is a leading financial, turnaround and business intelligence advisory and management firm that helps clients resolve financial and operational crises and provides solutions for business intelligence, investigations and security needs. Our team is focused on helping our clients, both corporate and private equity, meet emerging challenges and threats. We develop and implement strategic, financial and operational plans that result in enhanced competitiveness, increased profitability and reduced risk. Our professionals have deep-rooted expertise in managing financial distress and restructurings, implementing financial and operational plans, and spearheading the purchase or sale of assets. We are a leading firm providing C-level interim management to companies experiencing financial distress, loss of credibility and management turmoil. While we are generally industry agnostic, we have particularly deep industry expertise in manufacturing, real estate, hospitality, consumer products, financial services and insurance. Our senior executives have significant experience in international operations including Europe, Mexico and Asia.

Publisher



The M&A Advisor

The M&A Advisor was founded in 1998 to offer insights and intelligence on mergers and acquisitions through the industry's leading publication. Over the past seventeen years, we have established the world's premier leadership organization of M&A, Turnaround and Financing professionals. Today, we have the privilege of presenting, publishing, recognizing the achievements of, and facilitating connections among the industry's top performers throughout the world with a comprehensive range of services including:

M&A Advisor Forums and Summits. Exclusive gatherings of global "thought leaders"

M&A Market Intel. Comprehensive research, analysis, and reporting on the industry.

M&A.TV. Reporting on the key industry events and interviewing the newsmakers.

M&A Advisor Awards. Recognizing excellence of the leading firms and professionals.

M&A Connects. Direct connection service for dealmakers, influencers and service providers.

M&A Links. The largest global network of M&A, Financing and Turnaround professionals.

For additional information about The M&A Advisor's leadership services, contact lpisareva@maadvisor.com.