Nardello & Co.

‘In the Know’

2024/25 Trends & Insights Report

Table of Contents

A foreword from Dan Nardello 3

Trends in:

- Activist Defense 4-5
- Artifical Intelligence & Cybersecurity 6-7
- Physical Security Risk 8-9
- Bankruptcy 10-11
- The United States 12-13
- Europe, Middle East & Africa 14-15
- Asia-Pacific 16-17

The Market in 2025 18-19

Foreword

No matter is an island, to paraphrase John Donne.

And 2024 proved there are no exceptions. As the novel circumstances of the year unfolded, we saw the work of our clients become increasingly complex.

Together we navigated changing regimes in the United States, United Kingdom, and the Middle East, a rapidly evolving regulatory landscape that tried to keep step with advancements in Artificial Intelligence ("AI") and sanctions, and the economic swings caused by political unrest and war.

2025 promises to be even more tumultuous. And yet, with challenges come opportunities.

In this insights report, our team looks back at 2024 and deconstructs last year's trends in order to identify the opportunities of 2025 to which we think our clients should be alive.

We hope it will prove useful.

Please do not hesitate to contact us with questions.

All best,

Dan Nardello

Author

Dan Nardello
Chairman & Chief Executive Officer
dnardello@nardelloandco.com

Trends in Activist Defense

As if company boards do not already have enough to think about - cyber threats, febrile geopolitics, and the perennial challenge of sustainable growth – along comes more activism.

Yes, that's right. While shareholder activism has long been a feature of corporate life, 2024 was particularly busy on the activism front.

According to Barclays, through Q3 2024, there were 184 activist campaigns globally, 26% above the four-year average. Activist activity is up 22% in the United States and, driven by activity in Japan, up 100% in APAC.

Financial performance, coupled with the prospect of cutting costs, tops the activists' target lists. For example, in May, activist investor Ancora won three Norfolk Southern board seats by promising to force the railroad company to streamline its business. More recently, JCP Investment Management, which had built a 2% stake in The Cheesecake Factory, Inc., pressured the restaurant chain to spin off some of its brands into a growth-focused company, believing that separate management teams would drive better financial performance. And, in a sign of how US activism has an increasingly global reach, in June 2024, Nelson Peltz's Trian Partners focused on improving shareholder value and disclosed a stake in the UK's Rentokil, the worlds' largest pest control company. By September, Trian had won a board seat.

With this increased activity, some interesting trends have become apparent.

First, activists have focused on seating new directors rather than demanding strategic acquisitions or divestitures. As noted by the Harvard Law School Forum on Corporate Governance, activists publicly sought one or more board seats 147 times through Q3 2024, up 24% from 112 in the analogous period in 2023. Also, activists are proposing better candidates, increasingly choosing professionals with extensive industry knowledge.

Second, corporations face an environment in which matters that have long been uncontroversial may now be problematic. We've seen activists target policies that were never at issue in previous campaigns. One example is "national security" concerns. Activists are questioning links directors or senior managers may have, or may have had, with states that have become increasingly unfriendly to the west, such as China or Russia.

Third, we have seen the rise of what the law firm Morrison & Foerster has described as the "occasional activist," investors who are not dedicated solely to activist strategies. Instead, they may be institutional investors who use their leverage to push for changes that will benefit shareholders, themselves included. Others falling into the occasional activist category include company founders, other insiders, and organized groups such as unions.

Contributing to the rise of this activism is the spread of social media, which provides a convenient and inexpensive way for organized parties to air grievances before large audiences, thereby exerting pressure on companies to make desired changes. Accordingly, occasional activism has taken all the forms of traditional activism – public voicing of concerns, engagement with company management, and the launch of proxy contests. Recent examples include company founders who have maintained large shareholdings but are no longer involved in management. For example, founders of the software company SoftwareONE and the telecommunications company Crown Castle launched proxy contests to replace board members with directors of their choosing.

Finally, we have seen that both companies and activists now appear more willing to negotiate, and to do so on seemingly less hostile terms. In other words, there now appears to be a behind-the-scenes dialogue, one in which an investor names several director candidates and solicits a private response from the company as opposed to naming a slate of candidates and inviting a very public response.

Facing such trends, how might the savvy CEO react?

Going into 2025, it remains crucial to know one's opponent. Even when activists appear friendly and foster good relations, it is still important to gather information about them. What is their *modus operandi*? Do they focus on short-term turnaround or long-term viability? How have they behaved in previous proxy battles? Does the entity have a record of operating improperly or unethically?

It is always important to vet any nominee proposed by activists, even one well known to the company, such as a founding shareholder or other executive. Director candidates may appear impressive, but you still want to know as much as possible about them and understand their vulnerabilities as well as their advertised strengths. A substantial amount of this knowledge will come from a comprehensive examination of the public record – looking at litigation or criminal records, judgements, liens, bankruptcies – and social media activity, since even one intemperate remark can reflect on the candidate. On several occasions, we have seen candidates who were not adequately vetted by activists forced to withdraw their candidacy when thorough investigations commissioned by the company identified problems.

An understanding of the nominees' professional history will also remain important. What is the candidate's experience in the relevant sector? Is the nominee a "professional director" or "hired gun," someone who has been proffered perennially by the investor group, no matter their target? Does the candidate have previous ties to the activists? As many such individuals have a history of board service or have held senior executive positions, it is crucial to examine the companies with which they have been affiliated. What happened at those companies when the candidates were in charge? Is there any pattern of problems occurring at companies during their tenure? How did they handle adversity? Talking to people who have worked with the candidate or to fellow board members – or even to former adversaries – can be useful.

All of this information will inform a company's strategy during negotiations and, should negotiations break down, during the proxy battle. Even when activists appear willing to seek a peaceful resolution, management needs to protect shareholders' interests through targeted and thoughtful investigation.

As we progress through 2025, we do not expect the landscape of activism to look vastly different from that of 2024. The tested tactics are timeless.

Authors

Sabina Menschel
Partner, President & Chief Operating Officer
smenschel@nardelloandco.com

Nicholas Peck
Partner
npeck@nardelloandco.com

Artificial Intelligence & Cybersecurity

If two broad trends defined 2024, it was the emergence of multiple vectors of cyber threats and the roller-coaster ride offered by crypto assets.

Cyber Threats

To be sure, digital infrastructure vulnerability is nothing new, but it has been striking to see the sheer range and intensity of threat activity, as well as its evolution. The adoption of automation, cloud computing, and cutting-edge technology like AI has transformed the nature and scale of insider risks. In addition to these rapid technological advancements, we have seen high-profile nation-state attacks alter the insider threat landscape.

In its latest "Global Threat Report," cyber security company CrowdStrike identified two big trends of which clients should be cognizant: the "tactics and techniques that adversaries use to exploit gaps in cloud protection" and "exploitation of stolen identity credentials and increasingly sophisticated methods adversaries use to gain initial access."

Late last year, metadata from a large number of Americans was reportedly stolen in a cyber-attack on multiple telecommunications infrastructure companies by a Chinese hacking group called "Salt Typhoon." The exposed data included text messages, voicemails, call metadata, and wiretap data from US law enforcement investigations, and the finger of suspicion pointed at the Chinese government.

Per the Financial Times, a new form of malware attack has emerged. Called "quishing," it involves data theft via Quick Response or QR codes, the two-dimensional barcodes that can store data such as URLs.

This "continued heightened threat environment" explains why, according to Gartner, worldwide spending on information security is projected to hit $212 billion in 2025 – a rise of 15% from 2024.

As we look at 2025, it is worth keeping in mind that cyber incidents are complex events that impact many areas of an organization. In fact, a cyber incident is an organizational crisis – one that may expose the organization to liability claims, regulatory scrutiny, reputational loss or brand damage, and a reduction in share price. So an organization must respond with a crisis management approach and implement a strong and tested internal controls system.

Crypto Revival

The start of a second Trump presidency has injected fresh life into crypto currencies and the platforms on which they trade. We may now see a renewed push to bring blockchain assets to mainstream financial markets. There is no doubt that we have entered a new era, one in which regulatory enforcement faces a proliferation of use cases that may pose unprecedented compliance challenges.

The collapse of cryptocurrency exchange FTX may seem a distant memory now in 2025, given that bitcoin breached the $100,000 mark in December, buoyed by political and regulatory support. President Trump's nominee for chairman of the Securities and Exchange Commission, Paul Atkins, is a

crypto advocate who established a record as a market-friendly regulator when he served on the commission between 2002 and 2008.

The sector remains a rapidly moving target for anti-money laundering and risk management professionals because the pace of innovation has accelerated, particularly in regard to technology that is focused on realizing cryptocurrency's earliest goal – becoming a medium for the private and borderless peer-to-peer transfer of value. The ongoing tension between the technology's appeal to legitimate and illegitimate clients will define the market in 2025. It cannot be overlooked by risk professionals in their mitigation strategies – or indeed by those seeking to trace the activities, or assets, of illicit actors.

Ephemeral Apps

This year, regulatory attention will likely be directed to another emerging area of interest: ephemeral apps that allow messages or videos to disappear after a short period of time.

Given the obvious need to preserve data for the purposes of regulatory oversight and compliance, how can the use of such apps be reconciled with record-keeping obligations?

At the start of 2024, the Federal Trade Commission and Department of Justice issued joint guidance to clarify the preservation obligations of companies that use third-party and ephemeral messaging applications. Their diktat: There is a need to preserve "any and all responsive messages."

Corporations ought to keep in mind as they assess, in the context of discovery, whether to use platforms like *Signal* where, regardless of the desirability of using ephemeral apps, data is almost always preserved on servers and therefore could be subject to government subpoenas.

Conclusion

In what will likely not come as a surprise, we anticipate that in 2025 technological advances will drive the simultaneous evolution of and response to threats. AI will facilitate deepfake scams and phishing attempts just as quickly as it strengthens defenses to the same attacks. Given the roll out of biometric authentication, such as voice recognition by call centers, we expect to see an uptick in biometric spoofing, which will allow bad actors to circumvent those safeguards. We anticipate malefactors will use the power of large language models to facilitate social engineering attacks. We also expect that, concomitant with the increased adoption of cryptocurrency and blockchain technology, more sophisticated attacks will be directed at those platforms.

Cyber professionals will need to adapt to a dynamic environment as they respond to emerging threats that occasion novel workflows.

Authors

Wendy Wu
Managing Director, Head of Digital Investigations & Cyber Risk
wwu@nardelloandco.com

Joseph Pochron
Managing Director, Digital Investigations & Cyber Risk
jpochron@nardelloandco.com

Physical Security Risk

Far and away, the most important trend in physical security risk in 2024 was the need to re-evaluate the security provided to chief executive officers and high-profile or high-net-worth individuals.

The need to tighten security for senior managers has been brought to the forefront in a shocking manner: the public murder of UnitedHealthcare CEO Brian Thompson on the streets of midtown Manhattan. While the assassination seems to be an isolated event, social reaction to it signals that there is likely a more profound and lasting set of concerns regarding executive security.

The first significant increase in spending for executive security, according to Equilar, occurred when spending spiked 20% in 2020, a year of significant social unrest and riots in major cities occasioned by the death of George Floyd while in police custody. CEOs who took positions on divisive topics became potential targets of those seeking to visit their grievances upon individuals. Since then, we have seen a steady increase in the demand for executive protection. The New York Times reported that between 2021 and 2023, S&P 500 companies doubled their spending on executive security.

What Does This Mean?

Over the past several years, clients ask us the same question: Are we doing enough to protect our executives? This question is impossible to answer without first knowing the mitigation steps they have implemented, as well as the threats against which they are protecting their employees. Ensuring that physical security measures are in place is only half the conversation. The other half is an assessment of the threat environment, an identification of the risks faced by individuals, by companies, and by industry. In 2024, the title of CEO was added to the factors that increase the threat level.

Identifying Threats and Vulnerabilities

Over the past several years, the cyber threats that grabbed headlines were ransomware and fraud schemes. In 2024, cyber-facilitated violence emerged as a top story and kept our teams busiest. In all scenarios, the correct strategy starts with the understanding of one's vulnerabilities. In the current age, that means knowing what can be discovered online about the executive and who is posting inflammatory information. Intentionally and otherwise, individuals routinely reveal to the world a great deal about themselves: executives build online profiles, revealing their professional associations, places of work, and travel plans; the family members of executives place innocent-seeming information on social media without realizing the value it may have to someone less innocent. Additionally, the internet – and more specifically social media – has intensified the threat environment by providing individuals who account themselves as victims with a forum – a place to air their grievances and recruit like-minded individuals to drive up the heat against certain CEOs and companies. This became painfully evident with the assassination of Brian Thompson.

Knowing one's physical vulnerabilities is the second key to protecting executives. During the past year, we have seen an increased need to test physical security programs as rigorously as cyber defenses. Clients must identify vulnerabilities and produce comprehensive assessments to mitigate the threats that their executives face.

Moving Into 2025

In 2025, CEOs will continue to operate in a heightened threat environment, the sad result of the normalization of outrageous entitlement: People feel justified in threatening bodily harm – or worse – to those whom they believe to be responsible for certain conditions in their lives. Corporations need to continue to re-evaluate the security they provide their executives, but just as importantly, need to know from what they seek protection. Aggressive threat monitoring, mapping the groups that pose threats, and actively managing online exposure of information – all will continue to be important in managing physical security risks in 2025.

Author

Timothy Gallagher
Managing Director & Chief Security Officer
tgallagher@nardelloandco.com

Bankruptcy

In 2024, no bankruptcy case was more prominent—or more complex—than the landmark proceedings stemming from the collapse of cryptocurrency exchange FTX, a case that dominated headlines throughout the year, leading to the successful confirmation of its plan of organization.

As one of the largest financial frauds in history, the FTX bankruptcy centered on the recovery of billions of dollars in company assets to make creditors whole. The company's November 11, 2022 bankruptcy filing spurred a global investigative effort, one that Nardello & Co. was privileged to support. Leveraging our global reach and the expertise of our team, we conducted asset tracing, performed background investigations on key individuals, gathered facts to support recovery claims, analyzed financial data, and undertook computer forensics and cryptocurrency investigations. FTX's professionals worked together to support a high-profile plan that provided for full recovery to FTX depositors in record time.

While FTX was unique in its scope and outcome, it provides valuable guidance as we progress through 2025.

First, as ground-breaking as the FTX case was, we do not expect it to usher in any widespread shift in corporate practices that will enable avoidance of bankruptcies.

In 2024, bankruptcy filings increased 14% year-over-year. We expect the trend to continue in 2025. Notwithstanding the strength of the US economy, the world has continued to experience economic uncertainty accompanied by high interest rates and inflation. In the United States, the Trump administration's promise of tariffs and a more confrontational approach to world trade may result in increased business failures as companies adjust to the new environment. In addition, the new administration's deregulatory approach may lead to an increase in private litigation and insolvency proceedings to address matters previously addressed through government oversight or enforcement actions.

This year, as investor interest grows in the shadow of decreased regulatory oversight, some crypto and fintech businesses will be exposed as fraudulent. Many of these firms, which often have business dealings that cross borders, are headquartered or have significant operations in high privacy jurisdictions or territories in which officials have a limited ability to detect and prevent fraud. Furthermore, while these industries are maturing and drawing sound and experienced leaders and investors, some industry participants continue to have limited records of success or questionable backgrounds. This combination has, in part, driven several high-profile prosecutions and bankruptcies. There is thus a strong likelihood that some of the companies in this market segment will prove to be less than what they represent themselves to be, ill-considered, or unprofitable, resulting in insolvency claims and disputes.

Second, FTX's successful exit from bankruptcy shows the value of investing in bankruptcy investigations. FTX's Independent Examiner Robert Cleary, Esq., was appointed after some of the victims of the FTX fraud claimed the company was operating under a conflict of interest and insufficiently dedicated to recovering assets for the benefit of creditors. As a result, the independent examiner was made to evaluate "whether existing and ongoing investigations adequately addressed fraud by the former and current employees of" the company, as well as other claims of inadequate diligence by the company's retained professionals.

After conducting a comprehensive, months-long review of the quality of the company's investigation, the independent examiner concluded that the company's efforts, supported by Nardello & Co. and other professionals, were sufficient to establish all relevant facts concerning the frauds

targeting the company, and that no further investigation was necessary. Because new leadership had invested so thoroughly in investigating who and what led to the company's collapse, FTX was able to continue managing its own affairs, ultimately enacting a plan to liquidate its remaining assets and distribute them to creditors in an orderly manner.

Third, FTX shows that bankruptcy investigations can benefit from the inclusion of professionals with specialized skills in asset tracing; investigations of financial crimes such as fraud, corruption, and money laundering; digital investigations; cryptocurrency analysis; and public records research, source inquiries, and field investigations in a variety of jurisdictions.

Traditional financial advisors will continue to be an essential part of insolvency proceedings. However, in some instances – particularly where a company is a suspected victim of fraud – the best course of action is to hire skilled investigative firms to run the suspicions to the ground and, when misconduct is identified, pinpoint the perpetrators and track the proceeds.

Bankruptcies are particularly suited to the retention of investigators. In many engagements, investigators are limited to what is known to the client, what can be found in the public domain, and what can be learned from speaking with cooperative witnesses. Bankruptcy proceedings, however, feature wide-ranging discovery tools and broad disclosure requirements, which investigators can harness effectively in collaboration with counsel. Investigators with white collar litigation experience, for example, know how to take advantage of these devices, among them the production of schedules and statements of financial affairs; Rule 2004 examinations that some courts have likened to "fishing expedition[s]"; and the compelled production of relevant records from third parties.

Nardello & Co.'s retention by FTX, the creditors of Infowars creator Alex Jones, and the Unsecured Creditors Committee of Purdue Pharma, are a matter of public record, but there are other examples in which specialized asset tracers and investigators were effectively employed, and there will no doubt be many more instances in the coming months where investigators' involvement in bankruptcy proceedings will be necessary.

With the knowledge that fraud and other misconduct will surface in 2025, as it does every year, and that some matters will lead to bankruptcy or insolvency proceedings, bankruptcy professionals should use the lessons of FTX and similar cases to consider early engagement of skilled investigators. FTX shows that diligent investigation can answer important questions asked by creditors, courts, and others; reduce the time and cost of complex proceedings; and improve outcomes for creditors and the bankruptcy estate.

Authors

Howard Master
Partner & Counsel to the CEO
hmaster@nardelloandco.com

Liam Hanlon
Managing Director
lhanlon@nardelloandco.com

The United States

While the 2024 presidential election brought many surprises, one development that felt arresting at the moment but, upon reflection, should have been expected, was the rise of the importance of online communities. The 2024 race saw candidates from both parties reach out to these communities in radically new ways, resulting in the first Influencer Election, as it was commonly called in the media.

President Donald Trump leveraged influencer outreach to solidify his hold on the so-called MAGA manosphere via a three-hour session with podcaster Joe Rogan, multiple appearances with YouTube content creators and pranksters the Nelk Boys and others, and collaboration with Ultimate Fighting Championship CEO Dana White and billionaire X owner Elon Musk. Vice President Kamala Harris targeted her online supporters by inviting influencers, including TikTok creator and North Carolina mom Vidya Gopalan, to the Democratic National Convention, sitting for an interview by Alex Cooper on *Call Her Daddy*, one of the podcasts most listened to by women, and leaning into the endorsement "Kamala IS brat" – meaning confidently rebellious and playfully defiant – by British pop star Charli XCX that ricocheted around social media.

Underpinning this outreach is the reality that the online communities reached by these artists, influencers, and content creators have become significant movers not only in the political realm, but in news, culture, finance, corporate activism, and security. Their importance has risen at the same time that poll after poll shows confidence in traditional influence centers, be they mass media, government, or big business, continues to trend downwards. Musk's influence on Trump administration transition policies and White joining the Meta board of directors are just two examples of how such actors' influence is being solidified and mainstreamed.

These circumstances can lead to significant unpredictability not only for those seeking office, but also those entrusted with the stewardship of private organizations or public companies. All types of demands, even threats, can emerge from these communities, especially when activated by hostile influencers.

Company valuations have experienced wild swings based on coordinated "meme stock" trading by retail investors connecting on online platforms like Reddit. Political activist and online commentator Robby Starbuck has weaponized his million-plus online followers on X, Instagram, YouTube, and Facebook to publicly pressure a wide range of brand name companies to walk away from diversity, equity, and inclusion programs. Companies have faced boycotts – sometimes globally – fueled by mobilization on social media platforms in response to their support for Israel or gay rights. And the surge in online commentary hostile to healthcare executives after the murder of UnitedHealthcare CEO Brian Thompson forced companies across the healthcare industry to temporarily close offices, remove information from their websites, and hire security for their senior executives.

In this rapidly evolving landscape, companies need to identify the online communities that take interest in their activities and stay current with these community conversations. Those who are most efficient at gathering intelligence from these emerging and evolving groups may remain a step ahead.

Authors

Allison Everhardt
Managing Director & Head of the Washington, DC Office
aeverhardt@nardelloandco.com

Chris Ribeiro
Managing Director & Head of the New York Office
cribeiro@nardelloandco.com

Europe, Middle East & Africa

By most counts, there are 115 countries in EMEA – Europe, Middle East, Africa – and more than enough to investigate in all of them. The world's problems seem to congregate there. Three of the top five centers for arbitration – Paris, Geneva, and London – are there, while Dubai is now a mature center for all types of dispute resolution, with a mature legal sector to match. London, despite its many challengers, remains the preeminent place to bring complex civil litigation, with the London Commercial Court continuing to receive more referrals for its services than the New York Supreme Court's Commercial Division or the Singapore International Commercial Court. Picking trends from the related investigative activity creates a problem of choice, but the following top our list:

Paris is leading the way on white collar work

The Parquet national financier, France's economic crime agency, which started life in 2013 – now feels like a fixture of the European investigative landscape. In its first 10 years, it secured over 500 convictions, approved 20 deferred prosecution agreements, or Convention Judiciaire d'Intérêt Public, and, between the convictions and agreements, generated fines and recoveries of €16 billion. In the process, it also created in Paris a strikingly extensive white collar legal sector, which was slow to take hold but is now well established, thriving, and highly competitive. Together with 2016's anti-corruption legislation, this means that French companies now have added reason to fear the prosecutor's telephone call more than any of their peers – bar the Americans, of course, whose investigative agencies show no signs of letting up in seriousness or scope. The UK's Serious Fraud Office, meanwhile, could draw many useful lessons from across the Channel.

Arbitration 1: Nation states are prepared to investigate "original sin'" corruption

Corruption has sat in the background of many investor-state arbitrations for as long as they have existed. A government may suspect that the contract in dispute was secured by bribery but is reluctant to shine a light on it – despite the immense potential value to its case – because to do so would be to damage its reputation, or implicate still-serving officials, or both. Changing attitudes to corruption and an increase in genuine commitment to reform by governments across the region are now playing out in the world of arbitration, which has seen some high-profile reported cases of governments investigating possible instances of old corruption. In these circumstances, the original sin of corruption in a contractual award and the record of the perpetrators can become the focus of the whole dispute, with broad implications for lawyers, arbitrators, and investigators alike.

Arbitration 2: Russia continues to drive arbitrations and asset searching

The Russia-Ukraine war has given rise to countless commercial disputes. Two years ago, there was strong demand for asset searches against the Russian state, which is a more-or-less impregnably defended debtor. Last year, there was a marked increase in inquiries by customers of Russian energy companies – not all of them sanctioned – unable to deliver agreed volumes or, in some cases, any product at all. In preparation for the run of arbitrations, clients have been issuing mandates for asset searches with some unusual characteristics. First, as the process of freezing or attaching certain assets can have deep political and geopolitical consequences, investigators must realize that some asset classes are effectively off the menu, among them energy storage facilities in energy-vulnerable jurisdictions and receivables held by Russia-friendly European companies. Second, as many creditors and potential creditors find themselves targeting a small number of already well-protected assets, the competition in each case is unusually high.

Asset searching resists commoditization

In recent years, some intelligence and investigation firms have sought to compete on price in the two areas of the business where that seems possible: due diligence and asset searching. As a more automated due diligence approach can make sense for compliance-oriented clients, the market has for some time been in the process of splitting, producing a more commoditized product at one end, and, at the other, more tailored work that prioritizes thoroughness, human intelligence, and analysis.

This logic does not apply to asset searching as no two assignments are the same – the context and dynamics of any search, no matter its size, are complex and particular. Failing to grasp this, or, perhaps, not caring, some firms have seen an opportunity to take market share by offering cheap, commodity pricing – as low as $7,000 a shot in some jurisdictions. While this might unearth an interesting finding or two, it scrapes the surface at best – and is a paper dart against the thick armor of a well-defended debtor. Thus, the client is underwhelmed, and the reputation of the industry takes a hit.

In London and Dubai, the two liveliest markets for asset searching, 2024 saw a marked reverse of this trend – not on the supplier side but driven by clients who understand the nuanced, iterative work really required. Competition on quality and efficiency is good, but the market seems to be voting against a rush to the bottom.

There's so much else one might watch out for in EMEA in 2025: investigations into hostile reputational campaigns proliferated last year and show no signs of slowing, given how easy, cheap, and effective it is to wreak havoc online, particularly in the context of disputes; executive "behavior" has gone from being a newspaper buzzword to a central plank of every due diligence assignment; and investigative firms at the looser end of the market are having their own behavior scrutinized after some very public missteps. Anything less than a lively year will be a disappointment.

Author

Chris Morgan Jones
Regional Managing Director of EMEA
cmorganjones@nardelloandco.com

Asia-Pacific

Asia will continue to have an over-sized impact not only in relation to the economies that make up the continent but to the rest of the world.

This is clear just by the numbers. With 4.8 billion people, Asia represents almost 60% of the world's population and accounts for roughly 36% of global exports.

After the United States, China, and India rank second and third in billionaires, while financial hub Hong Kong has more billionaires than the United Kingdom. Altogether, Asia is home to 950 billionaires, more than any other region.

Don't Discount China

In 2024, much of the discussion about the region's largest economy, China, was dominated by its flat-lining economy. Foreign direct investment plunged by almost 28% while capital outflows, which have posed policy challenges for some time, reached a record high of $45.7 billion, according to government data.

China's economy – the world's second largest by nominal GDP – is likely to have expanded by 4.8% in 2024, undershooting the government's target and presaging decreased growth of 4.5% predicted for 2025.

Yet the economic heft and structural importance to the global economy of this country of 1.4 billion make it too big to ignore.

- China is likely to remain the top trading partner for most Asian countries and is still expected to grow at 4.5%, even in the face of likely US tariffs.
- In renewables, China is a global leader in innovative sectors like electric vehicles having become the largest EV exporter in the world by delivering high quality at lower prices.
- US tariffs on semiconductors have spurred China to invest billions in the industry with the aim of dominating the market in legacy chips and eventually reaching technological parity with advanced chips.
- Accounting for 70% of global extraction and 90% global ore processing, China dominates the market for rare earth minerals, which are essential for much of the drive to net zero.

That said, there are three items to watch in 2025. First and foremost: tariffs. China is likely to be the prime target of US tariffs given President Trump's recent statements. Even if the proposed rate of 60% does not materialize, any tariff increase will hurt China's export-driven economy. Second, China will continue to focus on trade with the "Global South." And finally, weak Chinese consumer confidence remains an Achilles' heel. Finally, China is making a concerted play to compete with the US in the AI market, most notably with their DeepSeek large language model which launched late January.

India Rising

With annual growth projections averaging 6.7% between 2024 to 2028, which would make it the fastest growing major economy in Asia, India is projected to become the world's third-largest economy by 2030, surpassing Japan and Germany. A major driver is infrastructure construction: India has expanded its national highway network by 60%, increased its power generation capacity by 70%, and electrified 94% of its rail network in the last decade.

However, as with China, there are red flags, including high structural unemployment. India, where

unemployment hit 8.5% in 2024, has a chronic shortage of jobs, with only 10% of its working-age population holding a formal job. Its shortage of 150 million skilled workers could act as a drag on consumption-led growth.

India's growth may also be hampered by an unfriendly regulatory environment, caused by capricious implementation of tax policies, sudden regulatory changes, and courts that move at a glacial pace.

Don't Forget ASEAN

Crediting the economies of the 10 constituent Association of Southeast Asian Nations ("ASEAN") as one, some claim the entity will have the world's fourth largest economy by 2030. Overlooked by investors focused on China and India, this block has proven its economic resilience time and again.

As the "China +1" approach to supply chain re-engineering has seen manufacturing shift from southern China to Vietnam and Malaysia, Penang has revived its 1970s-era reputation as a technology hub by attracting significant semiconductor investment.

Southeast Asia's rising middle class – predicted to more than double from 29% of the population in 2010 to 65% by 2030 – is becoming a lucrative consumer market, the greater spending power of which is expected to drive consumption-led growth. As middle-class growth widens the wealth gap, pressure increases on governments to deliver services that benefit broader segments of society, making industrial policy and job creation central to governmental strategies across the region.

Yet ASEAN's economic prospects are uncertain. Cheap imports from China may cannibalize ASEAN manufacturing, particularly if affected by US tariffs – tariffs from which ASEAN is far from immune as five of its six largest economies run trade surpluses with the United States.

Asia Pacific's global influence is growing. India is positioning itself as an international arbitration hub. Chinese AI firms have shown they can rival the large language models used by US software developers. Southeast Asia's economic dynamism makes it a prize for foreign investors. And yet, the range of skills needed to succeed in this region is vast as no two single countries in the region are the same. Bet-the-company litigation in Singapore will require vastly different expertise than a case in Vietnam. A shareholder dispute in Japan will have very little in common with a similar case in China.

More than anywhere else, investigators can illuminate Asia's risks and opportunities only if they are embedded in the region. A critical edge for disputes can be captured only if an investigator understands the nuance of inconsistent public records and has a diverse network of sources. The ability to separate chatter from actionable intelligence, and the expertise to navigate sometimes hostile investigative environments will determine the success of litigation and strategic acquisitions in Asia in the year ahead.

Authors

Steven Westervelt
Managing Director & Head of the Singapore Office
swestervelt@nardelloandco.com

Nicholas Blank
Managing Director
nblank@nardelloandco.com

The Market in 2025

The global business intelligence and investigations market experienced continued growth in 2024 as companies navigated a year marked by populist political reversals across the globe, geopolitical instability brought by seemingly intractable armed conflicts in Europe and the Middle East, and shifting, sometimes contradictory, economic signals. The business landscape now requires companies to keep pace with developments in, *inter alia*, fiscal policies, sanctions regimes, mass migration, climate change, and disruptive technology like AI and automation. With 2025 comes a need for sophisticated, ethical, and trusted investigative firms that can collect open-source intelligence and glean timely insights from human sources.

In 2024, global regulators and financial crime enforcement agencies remained aggressive, busy expanding sanctions on Russia in response to the 2022 invasion of Ukraine; increasing restrictions on trade with China to both limit Chinese access to sensitive technologies and protect domestic industry; targeting global media and technology companies with privacy and anti-monopoly actions; and focusing on counter-terrorism financing and transnational organized crime. Amid this flurry of regulations, even businesses outside traditionally regulated industries like finance began to develop business intelligence programs to collect facts for risk analyses of partners, investors, and suppliers, especially if they modified their global supply chains or sought to operate in new geographies.

Continued fallout from high-profile corporate leadership debacles and scandals in technology, biotechnology, and cryptocurrency sectors re-emphasized the need to conduct thoughtful due diligence exercises on those entrusted with the stewardship of companies or investments. An increasing number of boards have found themselves facing shareholder activists, wondering how well they know the strengths and weaknesses of their own executive teams, let alone those of the proposed replacements. Client requests for senior executive background investigations were driven this year by concerns about a range of risks, including corruption or illicit activities; exposure to politically exposed persons; environmental, social, and governance matters; and failures to truthfully represent previous experience.

After a year that saw two assassination attempts on now President Donald Trump and the public assassination of UnitedHealthcare CEO Brian Thompson, corporate boards are re-examining their plans for protecting their leaders and assets. Clients are coming to us for help in understanding their leaders' exposure, whether to violence or data theft. We have been asked to design comprehensive physical security programs, safeguard the personal information of executives, and conduct rigorous online threat monitoring of the new threat landscape.

One notable trend emerged in 2024: press emphasis on "malpractice" in the investigative sector, with many individuals being called out for illegal activity in the context of client investigations. In contrast, we have been steadfast in our ethical approach, in doing things "the right way." We continue to deliver our Ethics in Investigations CLE course and commit to pro bono work, including our ongoing support of Carnegie Hall and pursuit of Alex Jones' assets on behalf of the families of victims of the 2012 Sandy Hook mass shooting.

On the digital front, technological advances in AI have enabled extremists, criminals, and fraudsters to abuse social trust and disrupt businesses in novel ways. The ability of generative AI models to produce content that mimics human-produced text and imagery has augmented the notion that what is seen cannot always be believed. The ease with which threat actors – including hostile nation-states, ransomware groups, organized cyber-criminal organizations, hate groups, and even internet

trolls – can operate anonymously online has led to increased demand for time-sensitive, cross-disciplinary investigations that combine cybersecurity expertise, open-source research, and traditional field-based investigative techniques.

Clients facing existential threats – whether due to regulatory, competitive, reputational, legal, or financial challenges – call on us. Notable engagements included litigation support for high-profile white collar criminal defense matters, civil litigation, and arbitration. We assisted FTX's leadership in, *inter alia*, the recovery of some $9 billion in assets, which made creditors whole. In May 2024, court-appointed Independent Examiner Robert Cleary, Esq., issued a report that highlighted our many contributions to FTX's successes in the bankruptcy process.

With tightened monetary policies emerging worldwide and increasing concern regarding a potential wave of defaults across emerging markets in 2025, the need for investigative services in support of bankruptcies and asset searches will continue to rise.

While making any sort of prediction is hazardous, one can assume that 2025 will be as fraught with challenges as 2024. Hopefully, rigorous and intelligent fact finding and our global team of multidisciplinary experts can help give our clients some defense in negotiating whatever 2025 has in store.

Author

Dan Nardello
Chairman & Chief Executive Officer
dnardello@nardelloandco.com

Nardello & Co.

Where to find us.

Contact

www.nardelloandco.com
marketing@nardelloandco.com