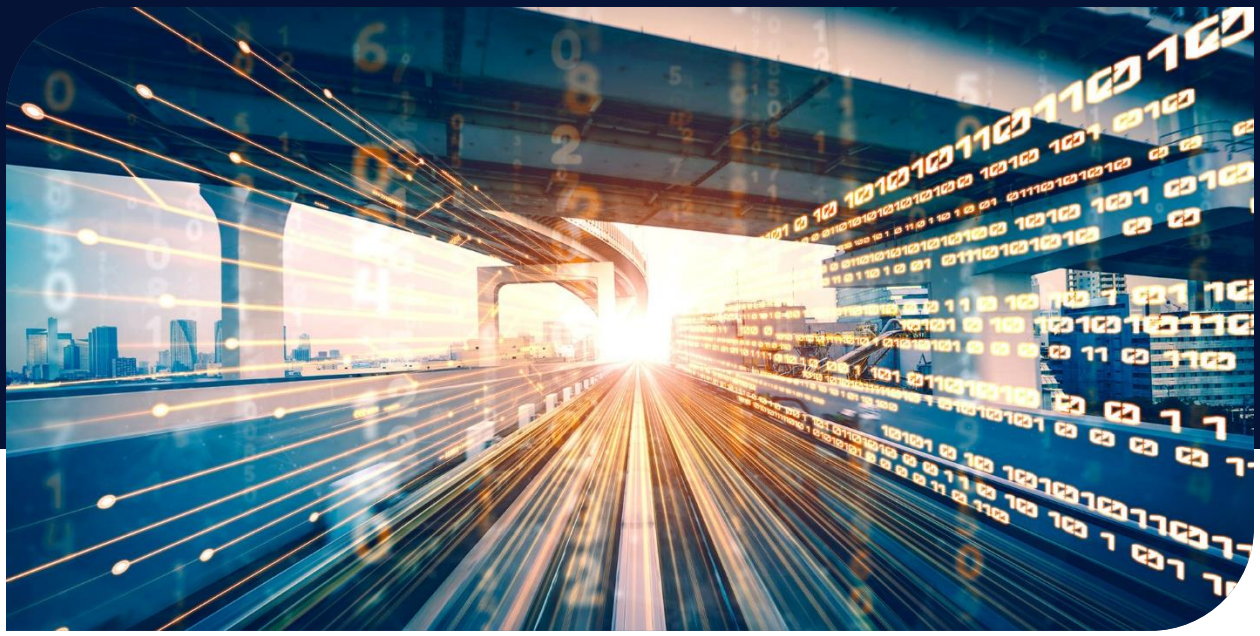
Teneo

2025 Cyber Outlook: New Year, More Risk

Teneo Insights | December 2024



The past year highlighted an undeniable reality for global businesses: the digital threat landscape is more volatile and unpredictable than ever. As businesses enter 2025, the challenge is clear—embrace the transformative potential of technologies like artificial intelligence (AI) while defending against an increasingly sophisticated and diverse array of cyber threats.

An unprecedented global election year, including in the U.S., brings the potential for regulatory shifts that could impact cybersecurity priorities. Geopolitical tensions, third-party vulnerabilities and the ever-evolving tactics of cybercriminals add layers of complexity. For C-suite executives, balancing innovation with risk mitigation has become a high-stakes exercise in strategic discipline.

To ensure a resilient cybersecurity posture, global businesses must elevate their capabilities to anticipate and mitigate the myriad of cybersecurity risks posed to their operations in the new year. In the following pages, Teneo's Risk Advisory team provides perspectives on the 10 key trends, threats and developments facing corporate leaders in 2025.

1. AI: Transforming Business, Escalating Cyber Threats

The rapid adoption of AI in 2025 will transform corporate operations, but it will also significantly increase cybersecurity risks, creating a much more complex threat environment. *While advanced generative AI models will be key to automating tasks and improving data analysis, they will also provide cybercriminals with powerful new tools to design sophisticated phishing schemes, social engineering tactics and automated hacking scripts. These risks will be intensified by the rise of AI-driven malware that can adapt in real-time, bypassing traditional security measures. As AI becomes more integrated into corporate decision-making and infrastructure, new vulnerabilities will emerge, such as adversarial attacks in which malicious actors manipulate AI algorithms to generate false predictions or outcomes. Securing the vast amounts of data used to train these AI systems will also become a notable challenge, as compromised data could expose sensitive business information or allow attackers to alter AI behavior.*

As illustrated by the above italicized text produced by OpenAI's ChatGPT, generative AI is a highly sophisticated technology capable of reasonably assessing the key risks, topics and trends that the technology itself will face and generate in the coming year, while clearly communicating that information. Teneo's Risk Advisory team assesses that 2025 will be the year in which AI fully integrates into corporate operations as AI use cases, tools and capabilities evolve and mature into more apparent implementations alongside the employees who operate them. Compounding these challenges, Teneo's Risk Advisory team identifies further drivers of cybersecurity risk involving AI in 2025, such as deepfakes, disinformation and AI misbehavior. Deepfakes – altered videos, images or audio recordings made with advanced AI – will become more widespread in 2025, and fears are rising that they will be used for nefarious purposes, such as spreading misinformation, committing fraud or posing as someone else, further undermining trust in online communications. Cybercriminals and nation states are increasingly leveraging generative AI's capabilities to disseminate mis- and disinformation at scale across online communication platforms. Another concern is the potential for AI systems to "misbehave," making mistakes or exhibiting biases in decision-making. Poorly trained AI models could incorrectly flag harmless activities as threatening or fail to detect more-advanced threats.

To address these risks, organizations will need to implement strong frameworks for governing AI, ensuring transparency, fairness and accountability. Advanced detection methods must also be developed to identify and combat malicious uses of AI, such as deepfake creation and adversarial manipulation. As the landscape continues to evolve in 2025, constant vigilance and innovation will be necessary as both defenders and attackers push the boundaries of AI capabilities.

2. International Business in the Crossfire of Cyberpolitical Risk

With a continued rise in geopolitical tensions heading into 2025, the threat to international businesses and trade from politically motivated cyberattacks is increasing. As noted in our September 2024 Teneo Insights article, "From NotPetya to Today's Global Conflict Landscape," international corporations now find themselves in the crosshairs of financially motivated criminals, hacktivists and sophisticated nation-state cyberwarfare.

The costs associated with "cyberpolitical risk," the interplay between geopolitics and cybersecurity, can be devastating. Cyberattacks by nation-states have generated billions of dollars in damages, with annual averages increasing year-over-year. The most destructive politically-motivated cyberattack in history, NotPetya, crippled Ukraine's public and private infrastructure and paralyzed the global operations of

international firms doing business there, generating over $10 billion in total damages. Attributed to the Russian military, NotPetya demonstrated the emerging reality of cyberspace as a direct means for nation-states to punish adversaries and their corporate partners. Similar attacks, including the 2020 SolarWinds supply chain attack impacting U.S. government agencies and private firms, and the 2021 Colonial Pipeline ransomware attack, further highlight the vulnerabilities in national critical infrastructure that cyber threat actors target amid geopolitical tensions.

These cyberattack methods continue to grow in sophistication, with nation-states now also sponsoring hacktivist groups or providing them with more sophisticated tools to carry out politically motivated cyberattacks on their behalf, thus complicating attribution efforts. Even when not state-sponsored, hacktivist groups will likely continue engaging in geopolitical conflicts via online means, launching Distributed Denial-of-Service (DDoS) attacks to render company systems or websites inaccessible and actively seeking to exfiltrate data. The resulting threat landscape is complex and will require organizations to increase both their geopolitical awareness and cybersecurity preparedness in the coming year.

3. International Progress to Regulate Cybercrime and AI Despite Enforcement and Scope Concerns

Although the EU, U.S. and UK have signed the first legally binding international AI treaty and the United Nations (UN) is expected to adopt a global cybercrime treaty by 2025, organizations will need to navigate complex international and domestic regulatory environments, particularly with anticipated policy changes as President-elect Donald Trump takes office.

The international AI treaty provides a legal framework for AI systems and their usage, with the objective of protecting human rights and safeguarding against risks to democracy. While the treaty marks substantial progress in international AI regulation, there are concerns over its broadness and ultimate enforceability. Additionally, though President-elect Trump has disclosed little about his plans for AI, we assess that his administration will likely adopt a more hands-off approach toward AI regulation and repeal a Biden administration executive order on AI. Given President-elect Trump's significant deregulation efforts during his first term, we assess that similar measures will be applied to AI policy, particularly concerning the adoption of AI within the federal government for defense and national security purposes. More broadly, we anticipate that President-elect Trump will likely aim to limit federal government regulation of cybersecurity, with deregulation efforts attempting to balance national security concerns. We also expect his administration to implement changes to the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the regulations they develop, which will likely impact businesses' regulatory and reporting requirements.

The UN's global cybercrime treaty is a pivotal moment in the global fight against cybercrime but carries potential risks of government repression if the UN does not implement necessary safeguards. Human rights organizations, such as Human Rights Watch, have raised concerns that the treaty's scope is too broad, extending to any crime committed using information and communications technology systems, rather than being limited to cybercrimes targeting computer networks, systems, technology and data. The treaty also presents significant risks to corporate IT systems, as it empowers law enforcement to compel citizens to disclose their access credentials, unlock secure systems or otherwise compromise corporate or governmental networks.

While the creation and implementation of these international agreements fall under the responsibility of national governments and institutions, Teneo's Risk Advisory team advises organizations to review existing legal obligations to ensure compliance, ensure proper cyber protocols are in place to address cyber risks and vulnerabilities, and continuously engage in partnerships with other organizations and governmental agencies to support information-sharing and collective efforts to combat cybercrime.

4. Cyber Threat Actors Will Increasingly Leverage Lucrative Ransomware Attacks

As in recent years, 2024 saw a surge in increasingly sophisticated and lucrative ransomware attacks, with no signs of abatement as we enter the new year. Cybercriminals have developed more advanced infiltration methods to deploy ransomware, including automating ransomware campaigns, drafting more convincing phishing emails with AI assistance, exploiting vulnerabilities at scale and carrying out brute force methods to deliver malware and gain access to organizations' systems. As of July 2024, ransomware demands per attack averaged $5.2 million, with anonymous cryptocurrency exchanges as the primary form of payment, complicating law enforcement efforts. Ransomware attacks also undermine customer trust in organizations, resulting in long-lasting reputational and financial consequences.

In 2025, we anticipate that cybercriminals will increasingly focus on stealing companies' data – rather than just encrypting it – for extortion payments, known as "double extortion ransomware." This method makes ransomware increasingly lucrative, further incentivizing this form of attack. We also assess that the proliferation of "Ransomware as a Service" (RaaS), in which sophisticated cyber criminals sell malware to those with limited technical skills, will continue to drive the increase in ransomware attacks.

Organizations, particularly those in high-risk sectors such as finance and healthcare, should employ endpoint protection and regular patching, as well as provide continuous cybersecurity awareness training for employees. Maintaining offline copies of sensitive data, installing security software and updating systems frequently can aid in mitigating or preventing breaches.

Organizations, particularly those in high-risk sectors such as finance and healthcare, should employ endpoint protection and regular patching, as well as provide continuous cybersecurity awareness training for employees. Maintaining offline copies of sensitive data, installing security software and updating systems frequently can aid in mitigating or preventing breaches.

5. Attacks on Third-Party Vendors May Rival Direct Cyberattacks

Amid vast information, data and communication ecosystems, 2025 will likely see cybercriminals continue to escalate attacks on corporations by targeting their third-party partners, rivaling the capabilities of direct cyberattacks. In recent years, threat actors have shown growing abilities to exploit interdependence between organizations by compromising trusted third parties and then pivoting to intended targets. Commonly referred to as supply chain attacks, third-party disruptions have had far-reaching impacts. For instance, in February, Change Healthcare, one of the largest health payment processing companies in the world, suffered a ransomware attack that left it unable to provide critical services for weeks, disrupting more than 90% of pharmacies across the U.S., potentially compromising the data of 100 million people and causing at least $2.5 billion in financial impact.

Vulnerabilities stemming from attacks on third parties are amplified by a growing reliance on cloud service providers (CSPs) and other vendors with their own security standards, which manage an ever-growing volume of sensitive data and have access to organizations' systems and infrastructure. Organizations must prepare for significant impact when their vendors or partners suffer an incident. A proactive approach to cybersecurity in 2025 will require comprehensive vetting of potential third-party contractors and ongoing coordination with existing partners and vendors to plan for cyber incidents, as well as continuous monitoring and audits of these providers. We also recommend that organizations ensure contractual clauses related to managing cyber incidents by partners are continuously reviewed to account for emerging cyber threats.

6. Security Leaders Will Diversify Cybersecurity Providers to Mitigate Single Point of Failure Risk

The July 2024 incident involving CrowdStrike's software update, which led to widespread system crashes and disrupted critical services globally, underscored the vulnerabilities inherent of relying on a single cybersecurity provider. This event affected approximately 8.5 million Windows devices, causing significant operational disruptions across various sectors. In response, organizations are reevaluating their cybersecurity strategies, recognizing the risks associated with single points of failure. The trend is shifting toward diversifying suppliers to enhance resilience against such disruptions.

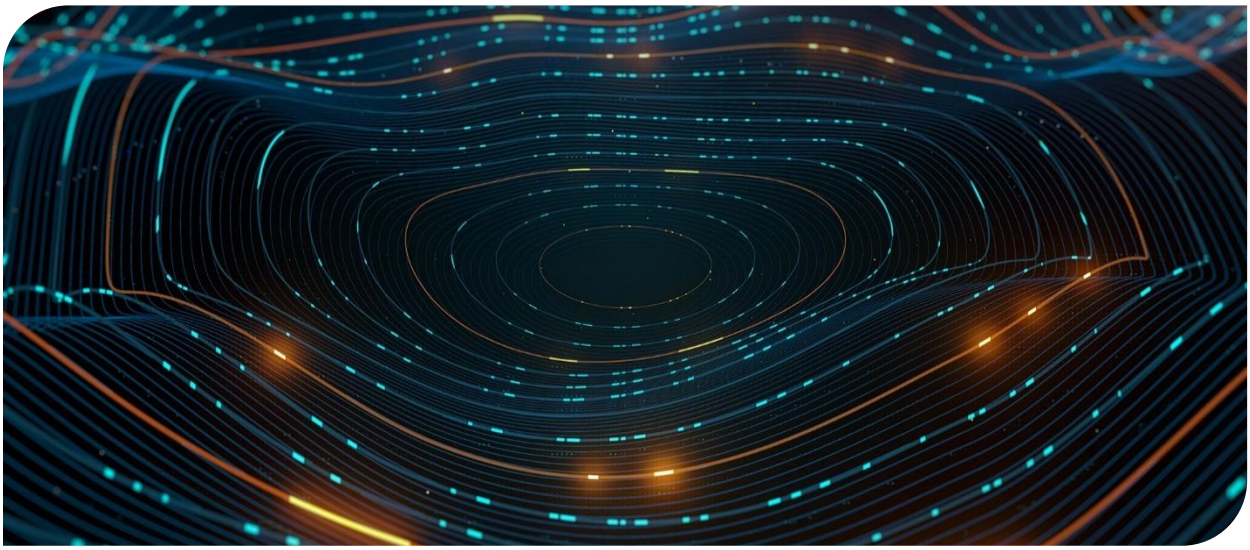
By integrating multiple cybersecurity solutions, companies have an opportunity to mitigate the impact of potential failures from any single provider. Emerging technologies, particularly AI, are playing a pivotal role in this diversification. AI-driven platforms can analyze vast amounts of data to detect anomalies and potential threats, offering a proactive approach to cybersecurity across network and application infrastructure and corporate endpoints such as laptops and mobile devices. Implementing AI solutions from different vendors can provide layered security, reducing dependence on a single system and enhancing overall protection.

Diversification does introduce complexities, such as increased costs and the challenge of managing multiple systems and vendors with varying environments and service levels. Organizations must weigh these factors against the potential risks of supplier dependency. The CrowdStrike incident serves as a critical reminder of the importance of a robust, multi-faceted cybersecurity strategy in an increasingly digital and interconnected world.

7. Threat Actors Will Target Growing Reliance on Cloud

Among the myriad of third-party risks, vulnerabilities stemming from the cloud will proliferate in the coming year as cloud computing increasingly becomes an indispensable resource for companies conducting business operations and providing essential services to clients. As the cloud expands an organization's attack surface and hosts a growing repository of sensitive data, these environments will become increasingly attractive targets for cyberattacks. With threat actors eager for financial gain or access to valuable data for other nefarious purposes, 2025 will likely see the exploitation of outdated authentication mechanisms, insecure application programming interfaces (APIs), misconfigurations and inadequate access controls, among other vulnerabilities, to access organizations' sensitive data. These risks are further amplified by the growing use of AI to identify exploitable vulnerabilities in cloud environments, as well as the increased reliance on the cloud for additional data storage due to organizational AI use.

Finally, the oligopoly of operating systems and productive suites renders a select few tools as the default choice for businesses of various sizes. As such, although integrating cloud computing and relying on a single provider to manage productivity tools, data, digital infrastructure, user authentication, and security is convenient, such reliance may create a single point of failure. In turn, managing data, encryption keys, devices and user access and behavior analysis through the same platform poses significant risk if a single service provider is compromised. To mitigate against these risks and associated impacts, such as data breaches, reputational challenges and even regulatory penalties, organizations both small and large must take a proactive approach to protecting cloud environments. This includes implementing robust authentication and encryption measures (including for APIs), securely and continuously backing up sensitive data, monitoring the cloud environment and assessing reliance on major technology providers while being mindful of the need to diversify digital infrastructure.



8. Critical Infrastructure Will Continue to be Both a Vulnerability for Global Economies and a Target for Threat Actors

The security of critical infrastructure, from power grids to water treatment facilities, faces mounting risks from increasingly sophisticated cyber threats. The evolution of operational technology (OT) into internet-connected devices has amplified vulnerabilities, leaving outdated systems exposed to exploitation. Many of these legacy systems were never designed to operate in a connected environment, creating serious gaps in defenses.

Reporting on cyberattacks targeting critical infrastructure between January 2023 and January 2024 highlighted that global critical infrastructure faced over 420 million cyberattacks. Although the report notes that the U.S. was the primary target, at least 163 other countries experienced attacks, often linked to state-sponsored threat actors from China, Russia and Iran. As part of the ongoing conflict between Russia and Ukraine, the Russian-affiliated group Sandworm disrupted Ukraine's power grid, demonstrating the potential for catastrophic outcomes. In 2024, nation-state actors, including groups linked to Iran and Russia, targeted key infrastructure in the U.S., manipulating systems in sectors such as water, agriculture and healthcare. In November of this year, the Environmental Protection Agency (EPA) issued a comprehensive report stating that "inspectors have identified alarming cybersecurity vulnerabilities at drinking water systems across the country and taken actions to address them." The report noted that water systems had inadequate risk and resilience assessments and emergency response plans. Similarly, the energy sector remains a focal point for attackers, but risks extend across sectors and global organizations. In 2022, The Government Accountability Office (GAO) highlighted that many critical infrastructure operators have not adequately evaluated growing threats, leaving them vulnerable to sophisticated intrusions. As Internet of Things (IoT) devices become more prevalent, the attack surface expands, exacerbating the challenges faced by organizations relying on outdated technology. While some progress has been made, the urgency expressed by agencies like the EPA, GAO and CISA suggests that significant opportunities for improvement remain.

To counter these risks, collaboration between public agencies and private operators is crucial. In the U.S., with roughly 85% of critical infrastructure operated by the private sector, CISA advocates for information sharing and coordinated defense measures to bolster national resilience. Strengthening these partnerships and investing in modernized systems will be vital to securing critical services against escalating cyberattacks.

9. Cryptocurrency Awaits Additional Tailwinds

Following the U.S. presidential election, bitcoin has surged to all-time highs. Since President-elect Donald Trump was announced as the victor, the value of the cryptocurrency poster child rose by nearly 40% over the month of November and surpassed a $100,000 price threshold on December 4 for the first time since its debut in 2009. Now, all eyes are focused on the incoming administration of President-elect Trump, who pledged during his campaign to create a national bitcoin stockpile and make the U.S. "the crypto capital of the planet." Recent developments are accentuating that vision, pointing to potential risks related to the use of cryptocurrency for cybercrime and other illicit activity.

On November 22, U.S. Securities and Exchange Commission (SEC) Chairman Gary Gensler announced he would resign from his role when President-elect Trump assumes office, concluding a term marked by aggressive regulation of what he called the "wild west" crypto industry. Last week, President-elect Trump officially nominated former SEC Chairman and cryptocurrency advocate Paul Atkins as Gensler's replacement, indicating an incoming departure from the prevailing regulatory policy towards crypto. Atkins' nomination, along with the November 24 nomination of pro-crypto hedge fund manager Scott Bessent for Treasury Secretary and the December 5 appointment of former PayPal Chief Operating Officer David Sacks to White House A.I. & Crypto Czar, have provided cryptocurrency and its supporters with significant momentum heading into the new year.

While the second Trump administration's formal approach to crypto policy remains to be unveiled, recent developments signal an industry-friendly stance and the possibility of legislation being passed in the Republican-controlled House and Senate that would unify the government's approach to crypto and provide the regulatory clarity the industry currently lacks.

In doing so, lawmakers will need to address serious concerns surrounding the use of cryptocurrency to finance illegal activity, as previously advocated by departing Treasury Secretary Janet Yellen. Although cryptocurrency offers increased global accessibility, lower transaction costs and a decentralized method for financial transactions, it also provides anonymity that cyber criminals can leverage to obfuscate transactions and launder money. The ability to move funds across different blockchains almost instantaneously provides criminals and illicit groups with the ability to rapidly launder money while circumventing law enforcement detection. The anonymity provided by cryptocurrency has made it the preferred method of payment by hackers conducting ransomware operations like the 2021 Colonial Pipeline attack. DarkSide, the hacker group responsible for the attack, extorted over $90 million in bitcoin payments in a series of ransomware operations conducted from October 2020 to May 2021.

To mitigate the risks associated with the illicit uses of cryptocurrency, executives should strengthen their organization's cybersecurity incident response plans, prioritize cooperation with law enforcement and emphasize the need for private-public partnerships to disrupt payment in the event of a ransomware attack.

10. The Human Factor Will Continue to Challenge Global Organizations

Human behavior remains a formidable challenge in safeguarding organizations, their data and other critical assets. Whether unwitting (error-prone) or malicious (targeted malfeasance), insiders can compromise security measures, leading to significant breaches. In 2024 in the U.S, the Department of Justice reported a case where an Army civilian employee orchestrated a $100 million fraud

scheme, exploiting her position to divert funds for personal luxuries. Separately, a former Disney employee was accused of unauthorized access to internal systems, causing disruptions by altering menu displays – some of which had potentially lethal consequences. Statistics underscore the prevalence of such threats. A 2024 report revealed that 76% of organizations experienced an insider attack, up from 66% in 2019, while 90% of companies found these incidents as challenging to detect, if not more so, compared to external attacks.

To counter these risks, emerging technologies offer promising solutions. AI and machine learning can analyze user behavior patterns to identify anomalies that may indicate insider threats. Implementing zero-trust architectures ensures that access to sensitive information is continuously verified, regardless of an individual's position within the organization.

However, technology alone is insufficient. Cultivating a culture of security awareness and providing regular training are essential to mitigating human errors and deterring malicious activities. By integrating advanced technological tools with comprehensive employee education, organizations can strengthen their defenses against the multifaceted challenges posed by insider threats.

Conclusion

From AI and blockchain technologies to ransomware, critical infrastructure vulnerabilities and the impact of human behavior, the year ahead points to both significant opportunities and the likelihood of new business, operational and reputational risks related to cyber threat. While Teneo's Risk Advisory team has outlined our perspective on cybersecurity-related risks for 2025, we are also confident that organizations that create and promote a culture of cyber-mindedness – prioritizing intelligence,

awareness, training and mitigation strategies – will be well-positioned to embrace and benefit from the promise of innovation while managing the challenges ahead.

Authors

Courtney Adante
President, Security Risk Advisory

Gareth Woods
Vice President

Rachel Cole
Senior Associate

Liad Mansky
Associate

Lauren Menzie
Associate

Eric Ryan
Associate

For more information, email TeneoRiskAdvisory@Teneo.com.

Teneo
The Global CEO Advisory Firm

Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance, ESG and DE&I.

The firm has more than 1,600 employees located in 40+ offices around the world.

teneo.com