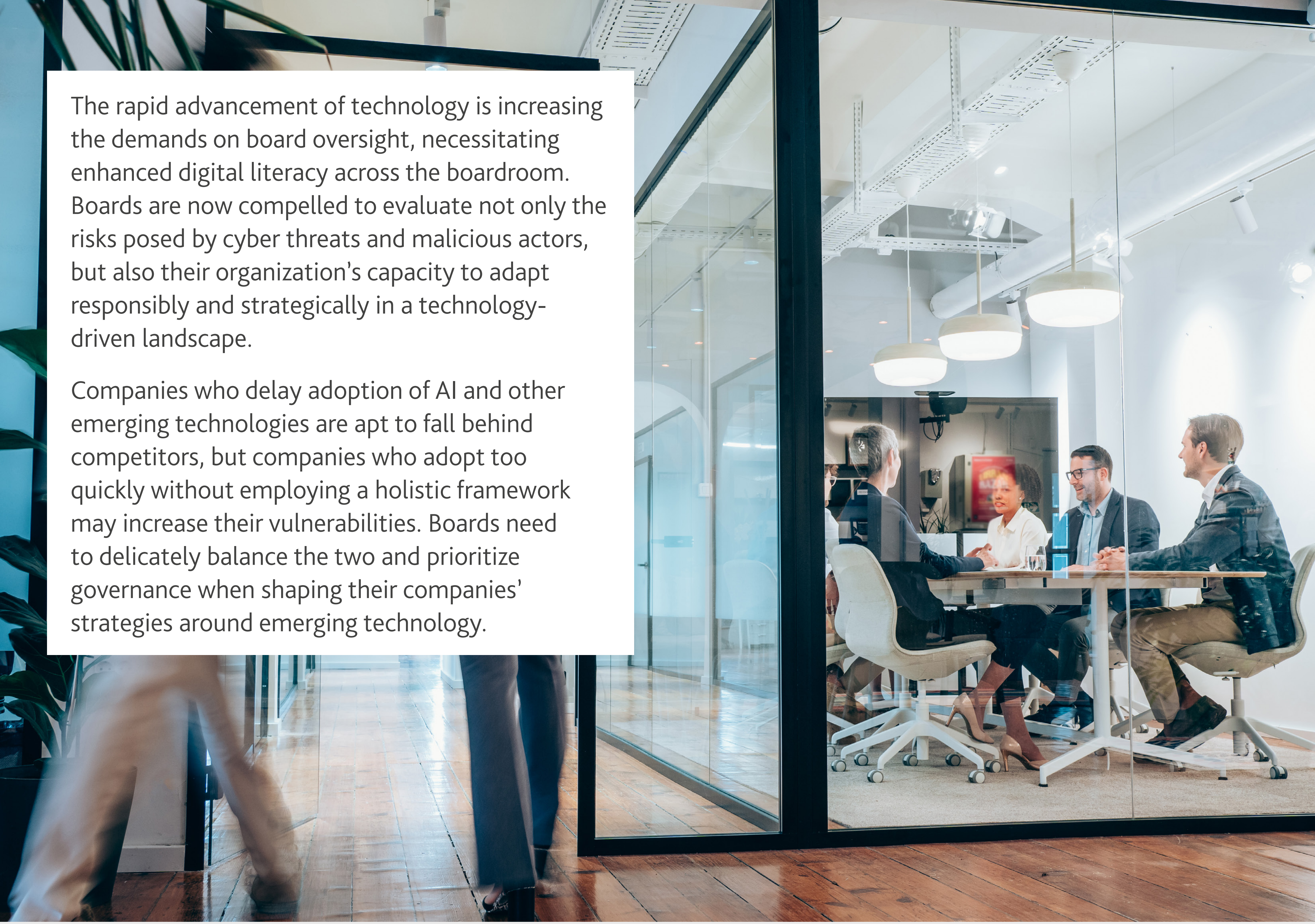
NAVIGATING TECHNOLOGICAL ADVANCEMENTS AND RISK:

Strategic Oversight and Governance in the Age of AI



The rapid advancement of technology is increasing the demands on board oversight, necessitating enhanced digital literacy across the boardroom. Boards are now compelled to evaluate not only the risks posed by cyber threats and malicious actors, but also their organization's capacity to adapt responsibly and strategically in a technology-driven landscape.

Companies who delay adoption of AI and other emerging technologies are apt to fall behind competitors, but companies who adopt too quickly without employing a holistic framework may increase their vulnerabilities. Boards need to delicately balance the two and prioritize governance when shaping their companies' strategies around emerging technology.

During a recent Corporate Board Member's Director Peer Exchange: *The Intersection of Technology and Governance*, **Dominique Shelton Leipzig**, Founder & CEO of Global Data Innovation, and **Danny Tobey**, Partner and Global Co-Chair and Chair of DLA Piper Americas AI and Data Analytics Practice, shared their expert knowledge on navigating risks while leveraging AI and other emerging technologies for innovation and resilience. Here are several highlights from the session:

TECHNOLOGY'S PARADOX: DRIVING INNOVATION AND FACILITATING CYBERCRIME

Technology and Generative AI have the power to do immense good in the workplace -improve efficiencies, enhance communication, automate and streamline processes and procedures, and support collaboration across platforms all while freeing up time for more meaningful work and reducing human error. When used thoughtfully and strategically, technology fosters long-term value creation. However, these advancements have created an opportunity for bad actors to infiltrate these systems and use these tools to steal data and other information. While AI holds the promise of enhancing human capabilities across various industries, it also equips cyber criminals with advanced tools to bolster their attacks.

Generative AI is being exploited creatively by malicious actors for malware generation, automated vulnerability discovery, password cracking, phishing, social engineering, command, and control communication, disguising malicious code, and deepfakes. The universal vulnerability to such attacks underscores the necessity for trustworthy AI deployment.

The use of these technologies gives companies a competitive edge, but only with the proper oversight. Oversight is essential to not only mitigate potential data workflow errors, but also to continuously monitor and mitigate security breaches. Investments decisions in technology need to be two-fold: to drive opportunity and defend against risk.

CULTIVATING ETHICAL LEADERSHIP: PREPARING BOARDS FOR AI INTEGRATION AND CYBERSECURITY CHALLENGES

Effective leadership and training on responsible AI use are crucial for managing AI's impact. Companies must not overlook aligning both of these with core values and the company's mission. This approach incorporates applied ethics to identify potential biases, prevent privacy violations, assess risk, and detect anomalies and cyber vulnerabilities associated with rapid technological advancements. This mindset starts at the board level.

It's the board's responsibility to oversee the implementation, use, and monitoring of all technologies. Having knowledge of all these elements enables boards to make the appropriate investment decisions. Boards must assess their current expertise in technology and cybersecurity, identify skill gaps, and create strategies to enhance necessary skills. This might involve recruiting new members, planning for succession, and/or using third-party advisors to influence proper oversight.

- **Cybercrime is now considered the third largest economy in the world**, following the US and China, with a **growth rate of 15%**. It was valued at **$9.2 trillion in 2024 and is rising**.
- According to **Microsoft's Digital Defense Report 2023** and **Microsoft Digital Defense Report 2024**, **password attacks increased** from 4,000 per second in 2023 **to 7,000 per second in 2024**.
- As attacks are getting more sophisticated, **threat actors** tracked by Microsoft **increased from 300 in 2023 to over 1,500** in 2024.

BUILDING DIGITAL TRUST: FRAMEWORK FOR AI GOVERNANCE

Reliance on technology is built on trust. Dominique Shelton Leipzig's TRUST framework is a risk management framework for AI that emphasizes trust as a strategic asset in the digital economy and responsible data stewardship as essential to building long-term value.

What is TRUST and what should boards be asking?

TRIAGE

Classify AI use cases by risk like a traffic light. Red light for prohibited AI, yellow for high risk and green for medium/low applications tied into enterprise goals and ROI.

Ask: How does management prioritize and categorize AI risks to help ensure timely and effective responses?

RIGHT DATA

Verify the training data is precise, ethical, and unbiased. Verify that there are privacy, intellectual property, and business rights to utilize the data. Companies using generative AI models trained on flawed internet data must correct for these issues.

Ask: Do we have the right data to train the model? What measures are in place to support ethical sourcing and handling of data? Are we aligned with legal standards and regulations and have the rights to use the data?

UNINTERRUPTED MONITORING

AI systems must be constantly tested and audited for accuracy. This can be accomplished by embedding checks into the application.

Ask: Do we have continuous oversight mechanisms in place to detect and address system failures and breaches?

SUPERVISION

Human oversight is a necessity. Companies need to embed their values and ethical standards into their AI systems and continue to monitor so that they can act quickly upon notification of deviations.

Ask: Who is responsible for overseeing the system? Did we embed ethical standards into the systems?

TECHNICAL DOCUMENTATION

When AI models drift (e.g., degradation of machine learning model performance over time) or fail, having clear documentation enables teams to identify problems, restore functionality, or deactivate the system, if necessary.

Ask: Is there comprehensive documentation of AI systems in place? Do we have the ability to quickly deactivate the system if it goes awry?

GLOBAL
DATA
INNOVATION

REGULATORY COMPLIANCE: SAFEGUARDING DATA

Data is undoubtedly one of a company's most valuable assets and the ability to safeguard it is critical. Data breaches and cyberattacks have the power to ruin reputation and brand in an instant. It is crucial for a board to expect regulatory compliance with rules and regulations designed to underscore strong trust in a company's data protection practices.

Failure to remain current with evolving laws and regulations — on a local, state, federal, and international level — can be catastrophic to a company's compliance posture as well as the board's ability to demonstrate duty of care to stakeholders.

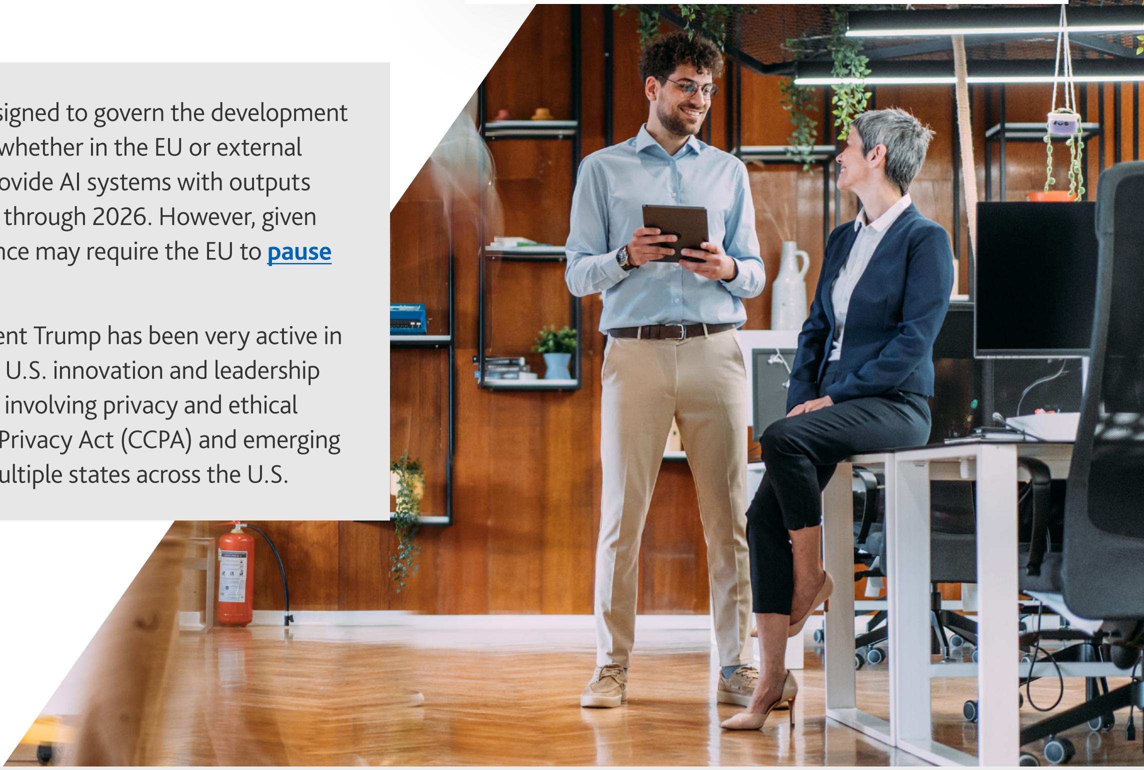
AI legislation is currently being driven by the European Union (EU) in terms of data protection, privacy, and cybersecurity. The EU has become a global leader in setting regulatory frameworks that influence other countries, and their frameworks are often seen as a blueprint for others – e.g., General Data Protection Regulation (GDPR) and the Artificial Intelligence (AI) Act. While the U.S. does not have comprehensive federal AI legislations, existing federal and state laws concerning privacy, intellectual property, and consumer protection are being applied to AI. Certain federal agencies, including the Federal Trade Commission (FTC) and Food and Drug Administration (FDA), are issuing guidance. Furthermore, various U.S. states are developing legislation as well across a variety of concerns, including disclosures pertaining to generative AI and protections against deepfakes. All these moving pieces require careful and specific consideration as to applicability to the company's business.

The EU's AI Act represents a comprehensive global legal and regulatory framework designed to govern the development and use of AI in the EU. This broadly applies to companies within the AI value chain — whether in the EU or external to the EU that develop, distribute, or use AI systems in the EU, as well as those that provide AI systems with outputs used within the EU. Provisions of the EU AI Act have planned staggered effective dates through 2026. However, given increasing demands from industry to provide needed standards and compliance guidance may require the EU to pause application and enforcement of certain provisions of the AI Act.

Meanwhile, the U.S. federal government has been slow to adopt AI regulations. President Trump has been very active in amending elements of Obama- and Biden-era Executive Orders in favor of promoting U.S. innovation and leadership while at the same time safeguarding national security concerns along with public trust involving privacy and ethical use. Companies must further rely on existing regulations like the California Consumer Privacy Act (CCPA) and emerging state-level AI legislation e.g., Colorado's AI Act, and various bills being considered in multiple states across the U.S.

CONCLUSION

The corporate stakeholders are calling for board directors to proactively oversee the development and deployment of AI within their organizations. By understanding and embracing frameworks, like the TRUST framework, directors can effectively enable navigation through the complexities of AI, address associated risks, and enable strategic growth. This proactive approach will not only safeguard the organization against potential threats but also position it to leverage AI for innovation and long-term success. Directors who lead with foresight and responsibility enable technological investments to drive sustainable growth and resilience.



Wherever you are in your AI journey, BDO provides comprehensive AI services and solutions to help you find efficiencies, address business challenges, and foster sustainable growth.

The BDO Center for Corporate Governance endeavors to support directors in engaging in effective governance by providing insights, learning, and networking opportunities in collaboration with BDO subject matter specialists and advisors designed specifically for boards of directors.

Have questions or want to learn more? Contact us!

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.

© 2025 BDO USA, P.C. All rights reserved.