Tech bias among the top risks faced by U.S. companies as technology continues to fuel growth strategies

A large majority of U.S. businesses (68%) report that technology is a core part of their growth strategy, yet most companies are not adequately prepared for the risk of lawsuits and reputational damage arising from technology-related issues such as tech bias, technology failure, and cyberattacks and data leaks, according to a report released today by global law firm Hogan Lovells.

The report, "Litigation Landscape: How to prevail when technology fails," is based on a survey of 550 business leaders.*

Tech bias was one area of particular concern, according to the report, which found that 45% of businesses globally do not check their technology – such as wearables, "smart" home products, voice or facial recognition – for racial and gender bias.

Most improvements in AI systems are made because of advances in machine learning. However, algorithms often adopt unwanted biases found within the data on which they are trained, which can lead to failures by facial recognition sensors to accurately identify people with dark skin; the application of AI that results in women receiving lower credit card limits than men; and medical devices that give higher priority to white patients for the treatment of complex medical conditions.

The report also found that:

- Only 35% of U.S. businesses are confident that their senior executives understand the risks associate with technology.
- Just 6% of U.S. businesses' boards deem technology risk to be as important as financial risk and other traditional risks.
- 56% of U.S. business leaders are not actively considering how to prevent and mitigate technology failure, including failures that would render critical systems or products unusable or unprotected.
- Half of businesses do not have an up-to-date response plan in case of a cyberattack, despite hacking concerns over areas such as cloud technology, autonomous vehicles or wearables.
- Most companies don't involve their legal teams in cyber response planning.
- 70% of U.S. businesses do not involve privacy specialists in product development.

The report also noted that major businesses may not be prepared for the legal risks associated with technology partnerships:

- 58% of U.S. businesses plan to outsource a key business function to a technology company.
- Yet 74% of U.S. businesses do not check if all their suppliers have the adequate cybersecurity credentials.
- U.S. businesses are particularly eager to engage technology businesses: 57% of U.S. companies plan to enter into a joint venture in the next two years; a significant increase from the 34% who did so in the last two years.
- More than half of businesses find it difficult to assess the legal risks associated with M&A and JVs with technology companies.

In addition, the report found that while 52% of businesses plan to accelerate their hiring of tech experts over the next

two years, many are not aware of the risks.

Given the breadth of technology-related litigation risks, businesses should engage in contingency planning based on four key principles, according to Hogan Lovells:

1. Boards and the C-Suite should be involved in identifying risks.
2. Collaboration with legal teams and privacy specialists is key.
3. Risks should be monitored through the entire tech lifecycle.
4. Businesses are only as strong as their weakest third party.

METHODOLOGY

*The companies surveyed have a turnover of between US$200m – over US$1bn. They operated in seven sectors: technology & telecoms (82), financial services and insurance (82), life sciences (82), automotive (83), consumer (83), diversified industrials (83), energy and natural resources (55).

The survey is based on 550 interviews with GCs, data privacy officers or equivalent at 550 companies, among them some of the largest multinational companies, in late 2020. The respondents were based in the U.S. (100), UK (100), Germany (100), France (100), China (45), Japan (45), Hong Kong (20), Singapore (20), Italy (10) and Spain (10).