FOLLOWING FIRTH
NOVEMBER 2025

BIG DOESN'T MEAN SAFE:

Why companies should rethink putting all their eggs in one tech basket

MIP
A SOCIAL SOLUTION IN A DIGITAL DIMENSION

The recent wave of Microsoft SharePoint breaches, allegedly carried out by Chinese state-sponsored hackers, has brought a stark reality into sharp focus: Being “all-in” with one big tech vendor doesn’t guarantee safety or resilience. In fact, it can make you a bigger target.

The breaches, which have already impacted more than 60 organisations worldwide, including the US National Nuclear Security Administration, highlight the vulnerability of widely adopted platforms. While Microsoft has issued patches, cybersecurity researchers have warned that these exploits have been active since early July and are likely to continue, adding that SharePoint’s deep integration with the Microsoft ecosystem magnifies the risk, potentially creating cascading vulnerabilities across the entire digital environment.

This underscores the fact that companies that rely too heavily on a single vendor, particularly one as omnipresent as Microsoft, are centralising risk. A single security flaw can expose vast amounts of sensitive data, disrupt operations, and lead to significant financial and reputational damage.

Think outside the box

The mantra "nobody gets fired for buying Microsoft" echoes the old IBM playbook to stick with the biggest, most established name to avoid risk. Yet, as these breaches demonstrate, size and dominance can make a vendor a prime target for hackers. The same widespread adoption that ensures market trust also provides a single, highly attractive entry point for cybercriminals. It's not that Microsoft is inherently unsafe – no tech company is immune from vulnerabilities – but its ubiquity means that when something goes wrong, it goes wrong for everyone.

Even ignoring the potential security risks, the "Microsoft-everything" approach has created operating environments that prioritise predictability over innovation. While this full-stack model offers convenience, it also limits flexibility and adaptability.

To truly manage risk and foster innovation, companies need to rethink their over-dependence on single-vendor ecosystems. Custom-developed solutions and multi-vendor strategies can spread risk across multiple platforms, reducing the impact of any single vulnerability. They can provide the flexibility needed to adapt systems to unique business models and workflows, encouraging innovation, since teams are not constrained by off-the-shelf templates. Most importantly, custom solutions can offer better cost control, especially compared to dollarizing your expense base.

The perception that custom solutions are expensive or hard to maintain is outdated. Today's tools and technologies make it more cost-effective than ever to build and maintain bespoke systems that serve strategic needs.

A wake-up call

The SharePoint incident should serve as a wake-up call for IT and business leaders alike. Big doesn't mean safe. It doesn't mean innovative, cost-effective, or tailored to your business, either. It often means predictable, targetable, and difficult to escape once you're locked in.

Businesses must adopt a proactive strategy that combines cybersecurity vigilance with architectural diversity. This means challenging the "bigger is better" mentality and thinking beyond what everyone else uses. In a digital landscape where threats are becoming more sophisticated, resilience is not about picking the biggest vendor, it's about choosing the right tools, balancing risk, and enabling innovation.

RICHARD FIRTH
CHAIRMAN & CEO, MIP HOLDINGS