Make cyber resilience the strongest link in your supply chain

By **Anand Balasubramanian**,
Partner and Head of Risk & Compliance Advisory, Grant Thornton UAE

Emerging technologies, and specifically Artificial intelligence, have become a core component of modern cyber conflict enabling cyberattacks to be conducted at a higher volume, tempo and level of sophistication than ever before. The region has seen a steady increase in cyber activity, reflecting the evolving global and geopolitical landscape.

This is not merely an issue of volume, but a reflection of how modern cyber risk manifests. As organisations expand their digital footprint and become more reliant on interconnected partners, cyber exposure is no longer confined within organisational boundaries. Risk now moves fluidly across suppliers, platforms and third-party providers, often exploiting the least visible point in the supply chain.

In practical terms, this means cyber risk is now a leadership issue, rather than a purely technological one. Boards and executive teams must take ownership of how cyber risk is governed, understood and managed across their organisation's entire network of partners and suppliers.

Regardless of industry, organisations should operate under the assumption that disruption is inevitable, constantly pushing to embed resilience across every part of their networks through rigorous oversight, scenario planning and cross-entity coordination. Since every sector is now a potential target, these proactive measures can mean the difference between mitigating a successful intrusion and being overwhelmed by one.

A rising rate of risk spillover

Across multiple industries we are seeing these multi-front supply chain cyberattacks deliver increasing disruption and damage. This brings to light how structural gaps can easily appear within large organisations that rely on a widespread network of suppliers, vendors and other third parties. Access points have increased to enable smoother supply chain management, but identity governance and intrusion detection efforts simply haven't kept pace.

It's this systemic exposure that creates space for supply-chain-level cyberattacks. A single vulnerability opens the door to significant disruption that extends well beyond the initial point of entry.

Defend at the ecosystem level

In 2026, the prospect of stopping every single attempted breach is becoming increasingly slim. Ecosystem-level defence requires three crucial components:

Containment: Strong identity controls, multi-factor authentication and zero trust principles are essential to limit how far an attacker can "move" across the digital infrastructure of your entire supply chain.

Visibility: Decision-makers need a clear, risk-based view of critical assets, dependencies and potential points of failure, including those introduced by third parties and cloud environments.

Responsiveness: Incident response must be treated as an ecosystem capability. Plans need to extend beyond your organisation, with clearly defined roles, escalation paths and tested recovery strategies developed by internal teams coordinating with external partners.

The priority businesses should focus on is aligning controls, governance and incident response across the full ecosystem, rather than managing them in isolation. We're seeing a clear shift – organisations that treat cyber risk as an ecosystem issue are responding faster and limiting disruption more effectively.

The UAE's current threat environment is a real-time test of organisational resilience. The scale and persistence of attacks underline that this is not a hypothetical risk, but an operational reality.

For business leaders, the question is no longer whether their organisation is secure in isolation, but whether their entire ecosystem can withstand disruption. That requires stronger collaboration with partners, clearer accountability at board level, and a willingness to invest in resilience beyond organisational boundaries.

Organisations that act now will strengthen their ability to contain and recover from inevitable incidents. Those that fail to do so risk learning that their most critical vulnerabilities sit not internally, but across the interconnected networks that support their business.