Cyber resilience amid uncertainty

Securing digital frontlines amid regional tension

The current regional situation has turned UAE cyberspace into a frontline, with expected increase in cyber attacks on critical services. Kinetic escalations, such as outages at a cloud data centre, can create digital single points of failure. Cyber resilience has therefore become a core business continuity and national resilience priority. This requires organisations to assume persistent, sophisticated attacks and design for secure, rapid recovery. It is important for organisations to enhance the preparedness and sophistication of cyber resilience through layered controls, zero-trust architecture, robust backup and Disaster Recovery (DR), continuous monitoring and incident response rehearsals.

Top 5 questions

Cyber resilience teams need to ask

01 **What is truly 'critical' and needs to be prioritised?**
Do I have a current, risk-based view of our most critical digital assets and services, and how exposed they are to threats linked to conflict?

02 **Tighten access, identity and remote connectivity**
Are we comfortable with security around access (e.g. multi-factor authentication, privileged access management and zero-trust principles), especially for remote access and third-party connections?

03 **Strengthen backup, DR and technical recovery for cyber scenarios**
Can we detect, contain and recover from a sophisticated attack on our most critical services within an acceptable business impact window?

04 **Identify failure points**
Do our third-party and cloud dependencies introduce single points of failure that could be impacted by this situation, and are we actively managing that risk?

05 **Increase visibility, early warning signals**
Are we giving senior management clear visibility of cyber risks, trade-offs and priorities in this environment?

Emerging trends in cyber resilience that can help organisations become more robust

Extended Defense and Response (XDR) platforms

Modern XDR platforms use AI to correlate signals across endpoints, network, cloud and identity, spotting subtle attacker behavior and automating containment at machine speed. In a fast-moving hybrid conflict, this helps organisations detect coordinated campaigns, credential abuse and lateral movement early, and isolate affected assets before business critical services are hit.

Zero Trust (ZT) architectures to limit blast radius

Zero with identity-centric access, micro-segmentation and continuous verification can contain intrusions and ransomware. For organisations potentially caught in the cyber spillover of the conflict, ZT helps ensure that even if an endpoint, VPN or partner is compromised, attackers cannot easily pivot into core banking, payments, operational technology or other critical systems.

Ransomware-resilient backup and immutable storage

There is a strong global shift towards immutable, isolated backups and tested recovery runbooks specifically designed for destructive attacks and wipers, not just hardware failure. This is crucial in the current crisis, where state-linked and hacktivist groups might use wipers and data-destruction malware against regional targets.

Reach out for any discussions or support regarding cyber resilience.

Anand Balasubramanian
Partner, Head of Risk & Compliance Advisory
anand.b@ae.gt.com

Krishna Manghat
Director, Business Risk Services
krishna.manghat@ae.gt.com

Raj Pittala
Director, Business Risk Services
raj.pittala@ae.gt.com

Follow us on LinkedIn

Grant Thornton

grantthornton.ae

© 2026 Grant Thornton UAE. All rights reserved.
Grant Thornton refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires.