AI, TECHNOLOGY & DIGITAL ASSETS · 8 JULY 2026 · 10 MIN READ

UAE Cyber Resilience: A Board Operating Model for Third-Party and Ransomware Risk

Boards can strengthen cyber resilience by governing critical services, identity, suppliers, recovery and incident decisions as one operating system.

Akash Chetwani, CFA
SENIOR PARTNER · ADVISORY

IRAA Global Advisory

EDITORIAL GUIDE

Contents

AI, TECHNOLOGY & DIGITAL ASSETS · 10 MINUTE READ · JULY 2026

Boards can strengthen cyber resilience by governing critical services, identity, suppliers, recovery and incident decisions as one operating system.

> Cyber resilience is the ability to keep critical operations safe, make informed decisions during an attack and recover to a trusted state. It requires board ownership of business risk, not only a technology team’s list of security tools.

The UAE Information Assurance Regulation provides a risk-based control reference for implementing entities, while the National Cloud Security Policy addresses governance, data lifecycle, location, identity, incident handling, supply chain and resilience for cloud consumers and providers. Other sector and contractual requirements may also apply.

Board-level cyber questions

CRITICAL SERVICES	Which processes must continue and what systems, people and suppliers support them?
ACCESS	Who has privileged authority and how is it approved, monitored and recovered?
DATA	Where is sensitive information stored, processed, backed up and shared?
RESPONSE	Who can isolate systems, communicate, notify, pay and restore?
EVIDENCE	When were recovery, vendor failure and executive decisions last tested?

Begin with business services

Identify revenue, payment, customer, production, payroll and regulatory processes that cannot tolerate prolonged disruption. Map their applications, infrastructure, data, identities, facilities and third parties. Set recovery time and recovery point objectives approved by business owners.

An asset inventory should include cloud resources, software-as-a-service, endpoints, network devices, code repositories, domains, certificates and operational technology. Unknown assets cannot be patched, monitored or recovered.

Classify data by sensitivity and operational importance. Apply protection through its lifecycle, including creation, use, sharing, archive and deletion.

Reduce identity and access risk

Require multifactor authentication for remote and privileged access. Use named accounts, least privilege and periodic access recertification. Remove access promptly when roles change or employment ends.

Separate administrator and ordinary accounts. Protect emergency accounts, service identities, API keys and secrets. Monitor unusual privilege, impossible travel, repeated authentication failure and changes to security controls.

Payment and supplier-master changes should require independent verification and dual approval. Cybercrime frequently becomes financial loss through manipulated email or identity rather than technical intrusion alone.

Govern cloud and third parties

The UAE National Cloud Security Policy emphasises governance, contractual protection, data location, supply-chain security, identity, incidents and portability. Before onboarding a provider, understand processing locations, sub-processors, encryption, access, logs, backup, recovery and exit.

Contract for incident notification, evidence, support, audit information, service continuity, deletion and return of data. A certification is useful evidence but does not establish that the service configuration is secure for the company’s use.

Concentrations deserve board visibility. Several critical systems may rely on one cloud region, identity provider or managed-service company. Test failure of the shared dependency.

> *“A backup is not a resilience control until the business has restored it within the required time.”*

Prepare for ransomware decisions

Maintain protected, tested backups separated from normal administrative credentials. Define isolation procedures, clean recovery environments, forensic preservation and the order in which services return.

The incident plan should name executive, technical, legal, privacy, communications, finance and insurer roles. Maintain offline contacts. Decisions about law enforcement, customers, authorities and any demand require coordinated legal and risk assessment.

Federal Decree-Law No. 34 of 2021 criminalises unauthorised access and interference with systems and data, among other cybercrimes. Preserve evidence and use official reporting channels. Do not engage attackers through improvised individual action.

Connect cyber and personal-data response

An incident can trigger personal-data obligations depending on the facts and applicable regime. The response team should determine data types, individuals, locations, confidentiality, availability, likely consequences and containment.

Keep a decision log and protect legal privilege where applicable. Communications should be accurate and consistent; premature certainty can compound operational damage.

After recovery, investigate root cause, persistence, control failure and lessons. Track remediation to verified closure rather than declaring success when systems restart.

Measure control operation

Useful metrics include critical assets covered, privileged access reviewed, vulnerability remediation by risk, phishing reports, backup restore success, incident containment time, vendor findings and overdue actions. Avoid a single score that hides control failure.

Run technical tests and executive simulations. A tabletop exercise should force decisions about shutdown, manual operation, customer communication, regulator engagement and recovery priority. Record actions and repeat the scenario after remediation.

01	**Map:** Identify critical services, assets, data and dependencies.
02	**Protect:** Strengthen identity, endpoints, networks and data.
03	**Govern:** Control cloud, suppliers, contracts and concentration.
04	**Recover:** Test isolated backups and clean restoration.
05	**Exercise:** Rehearse executive, legal and communications decisions.
06	**Improve:** Verify remediation and retest material controls.

Cyber resilience is demonstrated in operation: access is controlled, suppliers are understood, recovery works and leaders can make difficult decisions from reliable information. That capability protects customers and enterprise value more effectively than any one security product.

Set decision rights before an incident

A response plan should specify who may isolate systems, suspend customer services, activate manual procedures, engage external specialists and approve public or regulatory communications. It should also identify deputies and secure communication channels in case corporate email or identity services are unavailable. These choices become slower and more contentious when they are first debated during an attack.

Ransomware planning should address the business consequences of encryption, theft and extortion separately. Restoring systems does not resolve stolen information, and a ransom demand does not prove that data will be deleted. Legal, privacy, insurance, law-enforcement and sanctions considerations may affect the available options. The executive team should know which advisers to

contact and what evidence must be preserved without allowing an untested playbook to dictate a decision automatically.

Demand evidence from critical suppliers

Third-party assurance should be proportionate to the service. For a provider supporting identity, payments, customer data or core operations, ask how privileged access is controlled, how incidents are detected and notified, how backups are isolated, where data and administrators are located, which sub-processors are material and how service can be exited. Certifications can support the review, but they should not replace analysis of the actual service and contract.

Concentration deserves board attention. Several apparently separate applications may depend on one cloud region, identity provider, managed service or telecommunications route. Map those common dependencies and test whether the documented recovery strategy survives their loss. Contractual recovery objectives should be compared with the time the business can tolerate, and gaps should have a named owner and funded treatment.

After exercises and incidents, verify closure rather than accepting a list of recommendations. Evidence might include restored data, revised access, corrected monitoring, updated contracts and repeated simulation. A small set of tested controls and clear decision rights gives the board a more reliable view of resilience than a large dashboard of unverified security activity.

Official sources

1. **UAE Information Assurance Regulation**
2. **UAE National Cloud Security Policy**
3. **Federal Decree-Law No. 34 of 2021 on Cybercrimes**

Online edition: **https://iraaglobal.com/insights/uae-cyber-resilience-board-third-party-ransomware/**

ABOUT THE CONTRIBUTOR

Akash Chetwani, CFA

SENIOR PARTNER · ADVISORY

Cross-border advisory for professionals, founders, investors, and globally connected families.

PHONE	+971 56 921 0222
EMAIL	info@iraaglobal.com
PROFILES	**LinkedIn** · **Contributor page and articles**

IRAA GLOBAL
AUDIT · TAX · ADVISORY

A connected advisory firm for businesses operating across borders.

OUR EXPERTISE

Audit & Assurance	Corporate Tax & VAT
Accounting & Bookkeeping	Finance & CFO Advisory
AML, Risk & Compliance	Business Advisory & Setup
Human Resources Advisory	AI, Technology & Digital Assets
India-UAE Cross-Border Advisory	Private & Family Advisory

IRAA GLOBAL

AUDIT · TAX · ADVISORY

Insight beyond numbers.

IRAA Global Advisory

503 Mustafawi Carpet Building, Sharaf DG Metro Exit 1

Dubai, United Arab Emirates

+971 56 921 0222 · +971 50 677 9455

info@iraaglobal.com · www.iraaglobal.com

LAYOUT & DESIGN BY SURESH TAMANG