Cybersecurity Has Become a Boardroom Priority in the UAE

UAE boards now face direct accountability for cybersecurity oversight and governance failures.

DUBAI, UNITED ARAB EMIRATES, September 16, 2026 /EINPresswire.com/ -- Cybersecurity oversight in the UAE has moved from a technical reporting line to a board-level governance matter. The shift follows a wave of sector-level regulation across finance, telecom and critical infrastructure that now introduces breach notification timelines, mandatory disclosure requirements, and, in some cases, direct accountability for individual directors.

For much of the past decade, cybersecurity was treated internally as an operational cost managed by IT. That began to change once UAE regulators started framing a breach not solely as a technical failure, but as evidence of inadequate board oversight. Once personal accountability enters the picture, security stops being a matter that can simply be delegated downward and forgotten.

UAE boards are now expected to show more than a signed-off annual report. Regulators increasingly look for documented engagement: meeting minutes that discuss security risk, specific questions put to the security function, and decisions that can be traced back to that input. A board that can produce this record is in a materially different position after an incident than one that cannot.

Boards do not need to understand the technical detail of a firewall configuration to provide meaningful oversight, but they do need to ask the right questions of their security function. Useful lines of inquiry include what the organization's attack surface actually looks like today, what the incident response plan specifies for the first 24 hours after a suspected breach, how vendor risk is assessed before a contract is signed, and whether security spending can be tied to measurable risk reduction. Asked consistently, rather than once a year during an audit cycle, these questions are what separate genuine oversight from a formality.

When boards look outside the organization for expertise, whether for a security assessment, penetration testing, or ongoing managed services, regional regulatory familiarity is a meaningful

differentiator. A provider that understands UAE-specific frameworks and reporting obligations tends to deliver more directly useful engagements than one offering only a generic capability list. Dubai-headquartered Microminder Cyber Security is among the providers active in this space, working with boards and security teams across the UAE's regulated sectors on incident response planning, vendor risk evaluation and compliance reporting.

The UAE Government's cyber safety and digital security portal is a resource boards can engage with directly, rather than relying solely on a summary passed down through IT, since the obligations it outlines apply to organizational leadership as a whole.

About Microminder Cyber Security

Microminder Cyber Security is a CREST and ISO 27001-certified cybersecurity consultancy with more than four decades of experience, offering offensive and defensive security services including penetration testing, managed detection and response, critical national infrastructure and operational technology protection, and compliance consulting. The company has worked with more than 2,600 organizations worldwide, including governments and enterprises across finance, energy, healthcare and manufacturing.

Microminder Cyber Security
Microminder Cyber Security
+971 4 540 1252
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
X

This press release can be viewed online at: https://www.einpresswire.com/article/942665676

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.