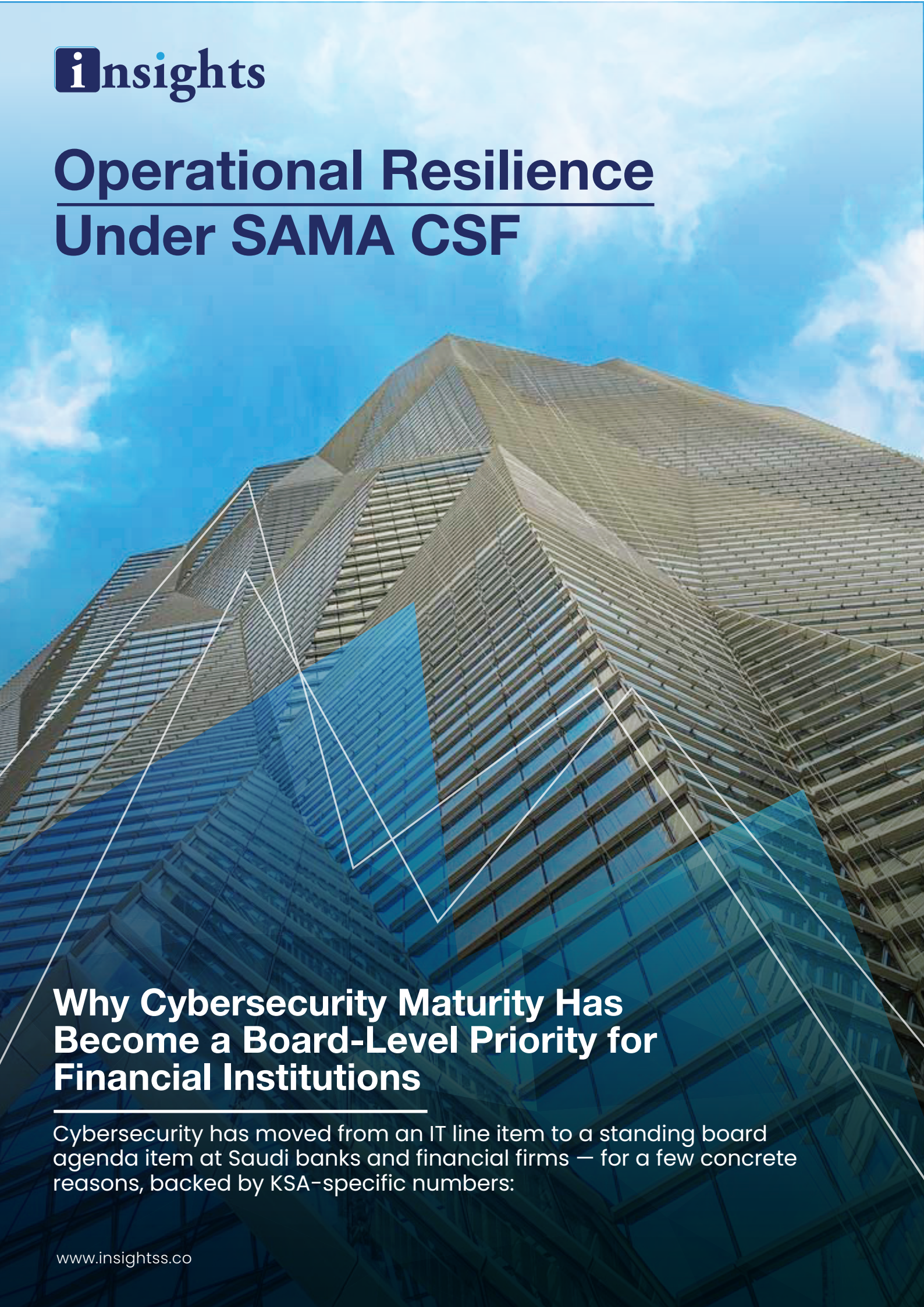
insights

Operational Resilience Under SAMA CSF



Why Cybersecurity Maturity Has Become a Board-Level Priority for Financial Institutions

Cybersecurity has moved from an IT line item to a standing board agenda item at Saudi banks and financial firms — for a few concrete reasons, backed by KSA-specific numbers:

Regulatory pressure has tightened, not loosened

SAMA's 2026 Cyber Security Framework update raised the bar significantly: third-party vendor assurance is now mandatory rather than advisory, and Tier-1 institutions must report to their boards on cybersecurity twice a year instead of once. The framework also aligned with the National Cybersecurity Authority's Essential Cybersecurity Controls, closing gaps that used to let weaker practices slide.

REGULATORY PRESSURE

- Mandatory third-party assurance
- Board reporting twice yearly
- Alignment with NCA Essential Controls

Money is on the line — directly and indirectly

FINANCIAL IMPACT

SAR 25M	SAR 20M	$ 4.88M
regulatory fines	penalties in 2025	Average breach cost

Attack volume keeps climbing

KSA industries — finance, government, and energy chief among them — have logged well over 110 million cyberattacks in recent years, and 2025 alone saw disclosed ransomware hits on Gulf banks, dark-web listings of Saudi bank account data, and DDoS attacks on bank websites.

RISING THREATS

110M+ cyberattacks

Ransomware

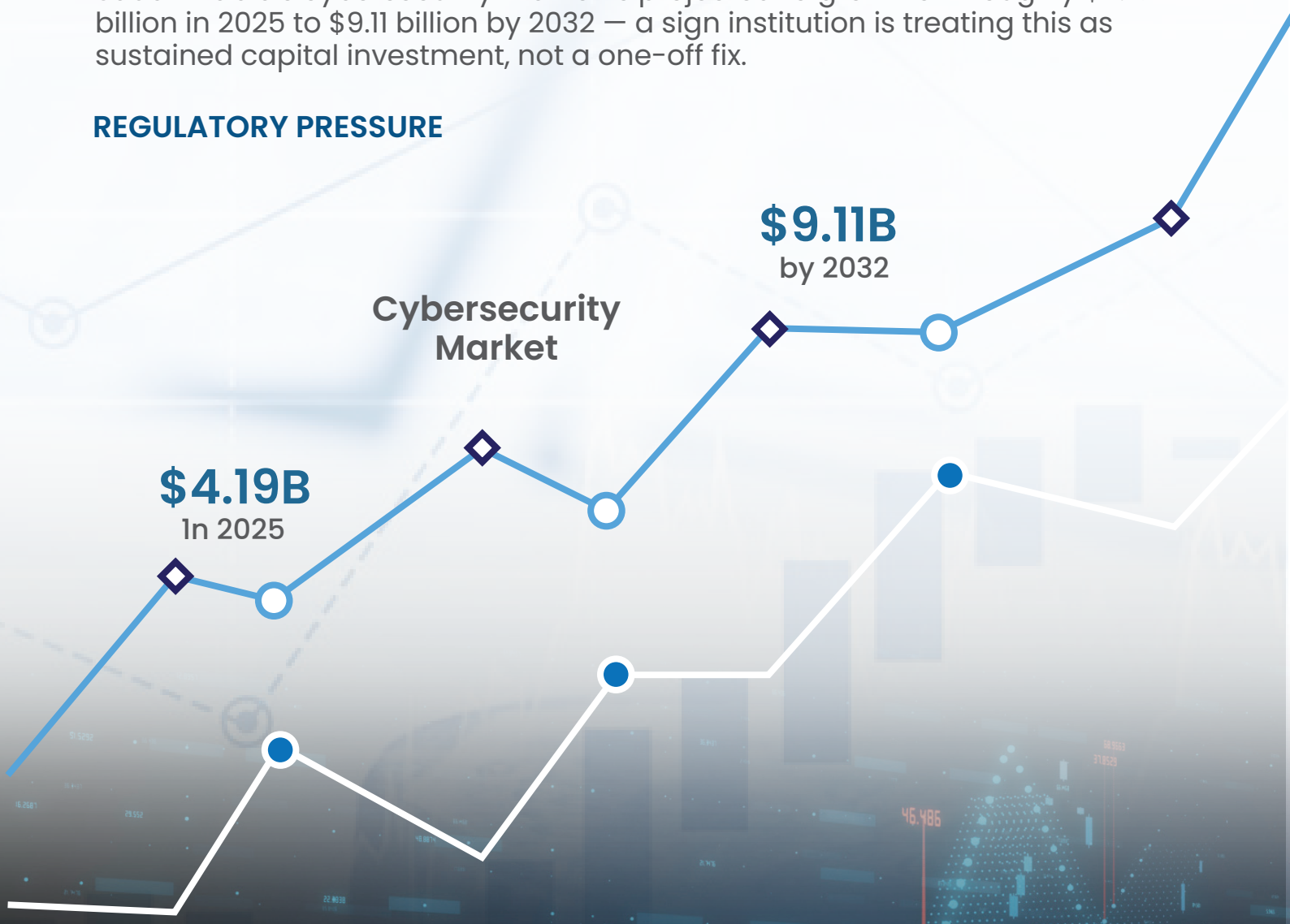
DDoS Attacks

Data Leaks

The market is responding accordingly

Saudi Arabia's cybersecurity market is projected to grow from roughly $4.19 billion in 2025 to $9.11 billion by 2032 — a sign institution is treating this as sustained capital investment, not a one-off fix.

REGULATORY PRESSURE



Net effect: a security failure at a Saudi bank today isn't just an IT incident — it's a regulatory, financial, and reputational event that lands squarely on the board's desk, backed by mandatory governance requirements (board-endorsed strategy, CISO independence, measurable KPIs) rather than best-practice suggestions.

Four Priorities for Strengthening Operational Resilience

MAKE CYBER RESILIENCE A GOVERNANCE RESPONSIBILITY

Operational resilience should be embedded within corporate governance rather than managed solely as an IT initiative. Boards and executive management should regularly review cyber risks, resilience capabilities, and remediation progress as part of broader strategic oversight.

MEASURE MATURITY, NOT JUST COMPLIANCE

Meeting minimum regulatory requirements is only the starting point. Institutions should establish measurable maturity targets, monitor Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs), and use assessment results to drive continual improvement rather than annual compliance exercises.

INTEGRATE CYBER -SECURITY WITH ENTERPRISE RISK MANAGEMENT

Cybersecurity cannot operate independently of operational risk, business continuity, third-party risk, and technology governance. Integrating these disciplines enables management to understand how cyber events could affect critical business services and overall organizational resilience.

BUILD A CULTURE OF CONTINUOUS IMPROVEMENT

Higher maturity organizations continuously evaluate the effectiveness of controls, learn from incidents, conduct regular testing, and strengthen resilience through ongoing governance rather than one-time projects. This shift from reactive compliance to continuous improvement is a defining characteristic of mature organizations under the SAMA CSF.

How Insights Helps Financial Institutions

At Insights Financial & Management Consulting, we help financial institutions move beyond regulatory compliance by strengthening their operational resilience capabilities through:

- SAMA CSF Maturity Assessments
- Cybersecurity Governance Reviews
- Operational Resilience Assessments
- Enterprise Risk Management Integration
- Business Continuity and Crisis Management Reviews
- Third-Party Risk Assessments
- Board and Executive Cyber Governance Advisory

Our approach combines governance, regulatory expertise, and risk management practices to help institutions build resilient operating models aligned with SAMA's regulatory expectations.

Key Takeaway

As Saudi Arabia's financial sector continues its digital transformation, operational resilience has become a strategic capability rather than a regulatory obligation. Institutions that continuously measure, strengthen, and integrate cybersecurity maturity into enterprise governance will be better positioned to manage disruption, maintain stakeholder confidence, and support sustainable growth

REFERENCE LINKS:

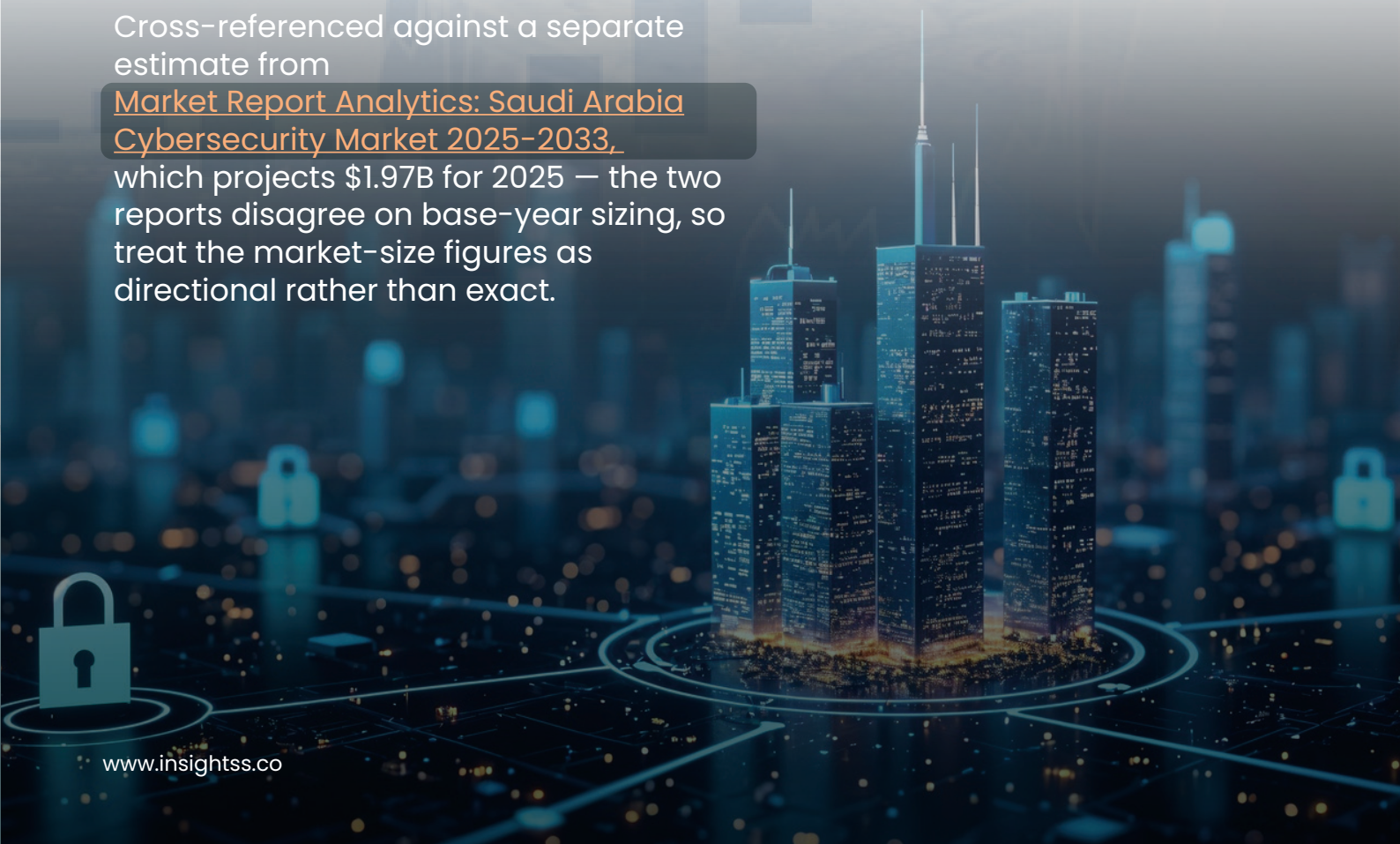
- **Money is on the line — directly and indirectly**
  CMS Law: Data protection and cybersecurity laws in Saudi Arabia

- **Attack volume (110M+ attacks)**
  MarkNtel Advisors: Saudi Arabia Cyber Security Market Size & Outlook 2026-2032

- **Specific 2025 incidents**
  CYFIRMA: Cyber Threat Landscape Report – Saudi Arabia

- **Market size projections ($4.19B in 2025—$9.11B by 2032)**
  MarkNtel Advisors: Saudi Arabia Cyber Security Market Size & Outlook

Cross-referenced against a separate estimate from Market Report Analytics: Saudi Arabia Cybersecurity Market 2025-2033, which projects $1.97B for 2025 — the two reports disagree on base-year sizing, so treat the market-size figures as directional rather than exact.



2026

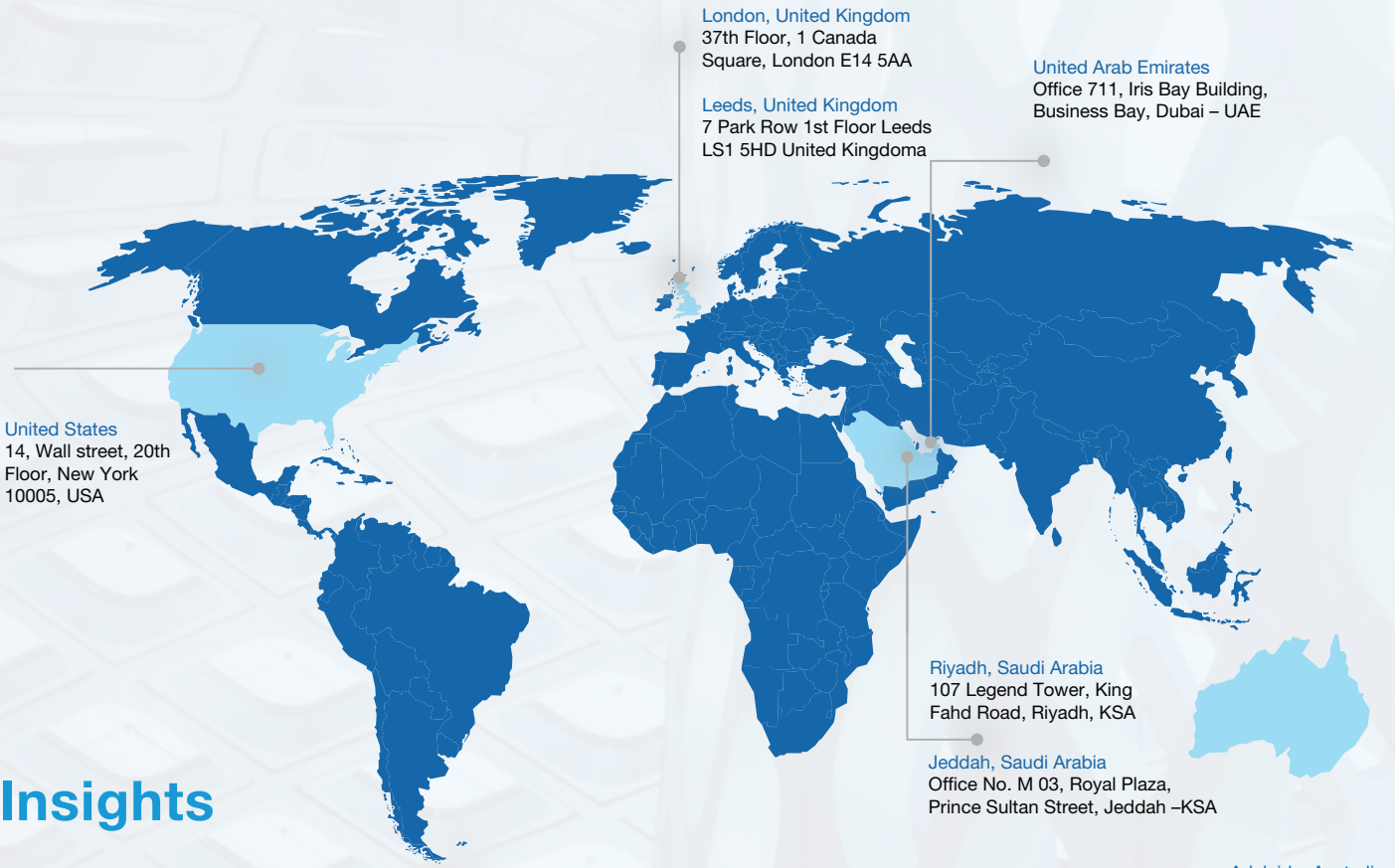
Contact Us

For further information, clarification and discussion concerning the contents, please contact our Real Estate Strategic Consultancy team:

Khawaja Soha Butt
Partner - Financial & Risk Advisory
: sbutt@insightss.co

Nick Whitford
Senior Vice President
: nwhitford@insightss.co

Ameer Abbas
Vice President - Financial & Risk Advisory
: aabbas@insightss.co



Insights

: +966 53 775 0075
: info@insightss.co
: www.insightss.co