الغزاوي ومشاركوه
AlGhazzawi & Partners

CYBERSECURITY LESSONS, SAUDI ARABIA 2025:

BUILDING STRONGER DIGITAL RESILIENCE IN 2026

The year 2025 was a defining period for cybersecurity in the Kingdom of Saudi Arabia. As we push forward with Vision 2030's ambitious agenda, characterized by massive digital transformation and rapid technological integration, the threat landscape has responded in kind. We witnessed a shift from opportunistic attacks to highly targeted, sophisticated campaigns aimed at critical infrastructure, high-value data, and the digital supply chain.

Introduction

The key lesson from 2025 is clear: cybersecurity is no longer a peripheral IT concern; it is a fundamental pillar of corporate governance, legal compliance, and strategic business continuity. For legal and business leaders in the Kingdom, 2026 must be the year where passive defense is abandoned in favor of a proactive, resilient strategy rooted in the governance frameworks established by the National Cybersecurity Authority (NCA).

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

In practical terms, major incidents are increasingly assessed not only by technical impact, but by questions of compliance readiness, governance oversight, and defensible decision-making under Saudi regulatory expectations (including ECC-aligned implementation and evidence of ongoing assurance).

Key Cybersecurity Developments in 2025

The developments of the past year can be categorized into two critical areas: the evolution of the threat actor and the maturation of the regulatory framework.

The Evolving Threat Landscape

2025 confirmed that threat actors are becoming faster, more specialized, and alarmingly effective at leveraging legitimate tools and access points.

- **SUPPLY CHAIN INFILTRATION:**
  The rise in successful attacks targeting third-party vendors, software providers, and managed service providers (MSPs) was a major theme. These attacks bypassed traditional perimeter defenses by exploiting the weak links in a company's extended digital ecosystem. A breach in a small vendor became a systemic risk for their largest clients.

  This also created direct governance and compliance exposure: under the NCA model, organizations are expected to manage cybersecurity risks across their extended ecosystem, making vendor weaknesses a potential contractual liability and, depending on circumstances, a reportable regulatory concern.

- **RANSOMWARE-AS-A-SERVICE (RAAS) SOPHISTICATION:**
  Ransomware groups continued to professionalize, adopting a (triple-extortion) model, encrypting data, exfiltrating data, and then targeting the victim's clients or partners for further pressure. This shifted the incident response focus from mere data recovery to managing profound reputational and legal crises.

  Beyond operational recovery, ransomware increasingly triggers legally sensitive steps: notification timelines, stakeholder communications, coordination with authorities, and evidence preservation; areas where "technical containment" does not necessarily equal regulatory compliance.

- **AI AND DEEPFAKE UTILIZATION:**
  Malicious actors began to effectively leverage Generative AI tools to create hyper-realistic phishing campaigns (vishing and deepfake social engineering) that targeted executives and high-value employees. This made the human element the most vulnerable point in the defense chain.

  For leadership, this elevates cyber risk into an executive accountability issue: awareness programs, escalation protocols, and decision controls must be auditable and aligned to local expectations, not treated as generic training checkboxes.

What These Developments Mean for 2026

The convergence of evolving threats and stringent compliance requirements dictates a new strategic posture for 2026.

- **ENHANCED LEGAL AND BOARD LIABILITY FOR CYBERSECURITY IN SAUDI ARABIA:**
  The biggest shift is the recognition that cyber risk is fiduciary risk. As the frameworks for cybersecurity compliance for businesses in Saudi Arabia mature, the liability for a catastrophic breach increasingly falls on the board and executive leadership. Law firms are already seeing litigation and regulatory inquiries pivot from technical failures to questions of cybersecurity governance in Saudi Arabia and due diligence. Did the board allocate sufficient resources? Was the Chief Information Security Officer (CISO) empowered? Were audits conducted against local standards (e.g., ECC)?

  In regulatory practice, the core question becomes: can the organization demonstrate implemented (not paper) compliance, board oversight, and a defensible trail of decisions, controls, and assurance activities.

- **DIGITAL RESILIENCE OVER MERE PREVENTION:**
  The focus must shift from an unachievable goal of 100% prevention to digital resilience, the ability to anticipate, withstand, recover, and adapt quickly from an attack. This involves implementing robust and regularly tested Incident Response Plans (IRP) that factor in legal notification requirements, data privacy stipulations, and regulatory reporting mandates within the Kingdom.

  A resilient IRP should be legally informed: it must anticipate evidence preservation, escalation authority, regulatory coordination, and documentation requirements, so readiness is measured by compliance response capability as much as technical recovery speed.

- **THE VISION 2030 CATALYST:**
  Every digital transformation project under Vision 2030, from smart cities to FinTech innovations, introduces a new entry point for threat actors. Security is no longer an afterthought added at the end of a project; it must be Security by Design, integrated from the initial planning stages to ensure that growth is not achieved at the expense of stability.

  This also strengthens the compliance dimension: transformation programs should map security requirements to applicable national controls and sectoral expectations at the design stage, so delivery remains defensible under regulatory scrutiny.

2026 Executive Action Plan

The Roadmap for achieving digital resilience is structured around four strategic imperatives:

Governance and Oversight

- **MANDATE BOARD ENGAGEMENT:** Appoint a digitally-aware board member or committee to oversee cyber risk.
- **INSIST ON REGULAR REPORTING:** Mandate quarterly compliance reports that specifically detail the organization's adherence to the NCA's ECC controls outlined in the ECC-EN.pdf document.
- **GOAL:** Elevate cyber risk management to a strategic, executive-level accountability, fulfilling fiduciary duties. To make oversight practical, reporting should connect cyber posture to legal exposure and business continuity (e.g., ECC-aligned metrics rather than generic KPIs).

Compliance and Cybersecurity Regulatory Audits in Saudi Arabia

- **END "PAPER COMPLIANCE":** Move beyond theoretical compliance checks.
- **COMMISSION EXTERNAL AUDITS:** Engage independent, third-party auditors to stress-test systems specifically against the NCA's ECC requirements.
- **GOAL:** Accurately measure the true security posture, identify actual implementation gaps, and ensure compliance with KSA legal obligations.Audit outputs should be usable as defensible evidence of due diligence, showing implementation, remediation tracking, and clear accountability.

Supply Chain Security

- **TIGHTEN VENDOR CONTRACTS:** Require all key third-party vendors to sign contracts with strict security clauses covering liability and breach notification.
- **ENSURE ALIGNMENT:** Mandate that vendor controls align with the security requirements dictated by the ECC framework, where applicable.
- **GOAL:** Mitigate systemic risk by securing the weakest links in the organization's extended digital ecosystem. In 2026, supply chain security is as much contractual and governance work as it is technical: clear obligations, escalation, audit rights, and incident cooperation terms reduce both operational and legal exposure.

Technology and Architecture

- **ADOPT ZERO TRUST (ZTA):** Assume the enemy is inside and migrate to a Zero Trust Architecture.
- **VERIFY EVERYTHING:** Implement controls that verify every user, device, and application attempting to access network resources, regardless of their location..
- **GOAL:** Contain the blast radius of any breach and prevent attackers from moving laterally (sideways) within the network. When deploying these architectures, keep documentation and accountability in mind: technical controls should translate into clear internal policies and traceable enforcement.

Executive Checklist: What You Need to Ask Your Team Right Now

The questions an executive asks are a direct reflection of the organization's cybersecurity maturity. Every senior leader and General Counsel should be asking their CISO or IT Director the following essential questions:

- **COMPLIANCE:**
  "Can we definitively demonstrate our adherence to the NCA's Essential Cybersecurity Controls (ECC compliance) and relevant sector-specific regulations (e.g., SAMA)? When was the last independent audit?"
- **RESPONSE READINESS:**
  "How quickly can we legally notify all required local authorities and affected parties following a confirmed breach, and have we successfully run a full-scale, legally-informed, multi-departmental incident response simulation this quarter?"

- **FINANCIAL MITIGATION:**
  "What is our current cyber insurance coverage, and does the policy language cover modern risks like business interruption from ransomware and the costs associated with regulatory fines under KSA law?"

- **TALENT & AWARENESS:**
  "What is our strategy for attracting and retaining qualified Saudi cyber professionals, and is our mandatory staff training program specifically tailored to defend against ٢٠٢٥'s most common threats (e.g., AI-driven deepfakes)?"

- **BUDGETING:**
  "How is our security spending allocated between prevention, detection, and recovery/resilience capabilities, and is the budget scaled appropriately to the risk of our digital transformation projects?"

  Add a governance lens: "Are our ECC compliance metrics embedded into leadership reporting, and can we evidence oversight, escalation, and decision-making if reviewed by regulators?"

Conclusion

The transition to digital resilience in Saudi Arabia in 2026 is fundamentally a shift in corporate governance and legal foresight. The path to achieving Vision 2030 cybersecurity compliance, in addition to its ambitious goals, is paved not just with technology investment but with absolute legal clarity.

Successfully implementing the mandatory ECC framework, managing complex supply chain risks, and navigating the inevitable regulatory scrutiny require more than technical execution; they demand an integrated legal and strategic approach. Enterprises must translate technical controls into clear legal policies, establish defensible contracts with partners, and build governance structures that stand up under regulatory investigation. The organizations that successfully achieve this integration, aligning their cyber strategy with the precise and evolving legal obligations of the Kingdom, will be the true leaders of the digital economy, ensuring their growth is both rapid and secure.

Disclaimer:
This article reflects regulatory and governance trends and is provided for informational purposes only. It does not constitute legal advice.