ECES
المركز المصري
للدراسات الاقتصادية
The Egyptian Center
for Economic Studies

ECONOMIC LENS

Issue 27
20 September 2026

The Emerging Risk of Cyber Security: Middle East and Egypt

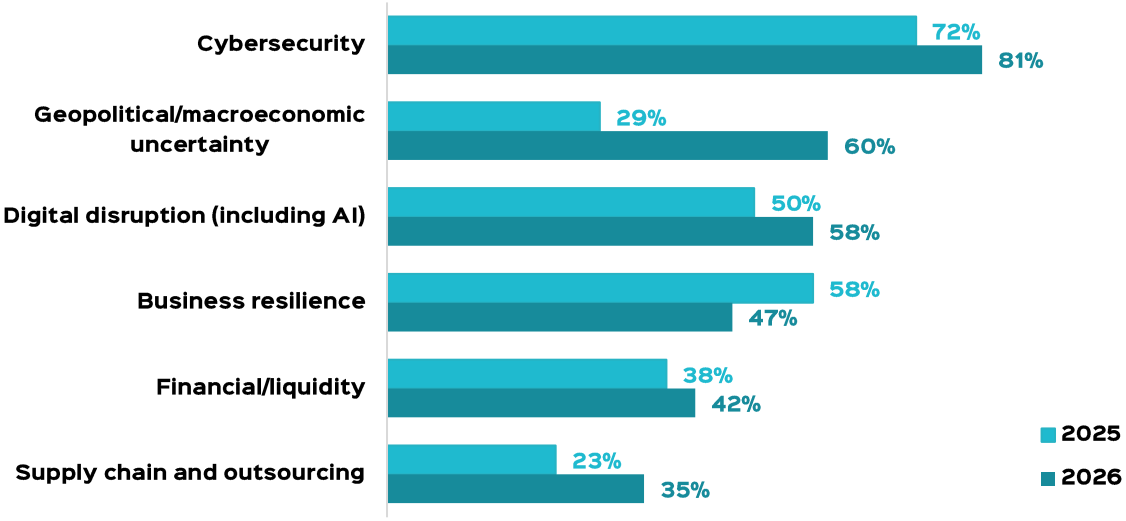
Why address this topic now?

While the regional war that began in February 2026 has dominated the discussion of risk in the Middle East, it is not the risk that organizations in the region rank first. The Internal Audit Foundation and the Arab Confederation of Internal Auditors (ARABCIA) recently published Risk in Focus 2026/2027: Middle East, an annual survey that identifies the five most significant risks facing organizations in each region of the world.[1] The 2026 edition draws on responses from 3,285 Chief Audit Executives (CAEs) in 132 countries, of which 296 responses came from 15 Middle Eastern countries. Egypt contributed 39 of these responses, which makes it the fourth largest national sample in the region after Oman, Bahrain and the UAE. In addition to the survey, the report relies on two regional roundtables with 20 participants and three in-depth interviews.

The report examines 16 risk areas, and its main finding is that the conflict between the U.S., Israel and Iran reshaped the regional risk ranking within a single year. The share of Middle Eastern CAEs that placed geopolitical and macroeconomic uncertainty among their top five risks doubled from 29% in 2025 to 60% in 2026, which is the highest level recorded in any region. Cybersecurity was a top risk in both years which rose by 9 percentage points to 81% in 2026.

[1] Internal Audit Foundation and Arab Confederation of Internal Auditors (ARABCIA), Risk in Focus 2026/2027: Hot Topics for Internal Auditors, Middle East (2026).

Figure 1. Middle East: top risks, 2025 vs 2026 (share of CAEs selecting each risk among their five highest risks)



Source: Prepared by the author based on Risk in Focus 2026/2027, Exhibit 1.1 (n = 296).

The report reveals that Cybersecurity is also the highest ranked risk in every region covered by the survey. Globally, 80% of CAEs listed cybersecurity among their top five risks in 2026, which is an increase of seven percentage points over 2025. As we can see from Figure 2, the ratings range from 72% in Asia Pacific to 86% in Europe, which indicates that the perception of this risk does not depend on the level of income or digital maturity of a region. The report notes that the largest annual increases were recorded in Africa (+11 percentage points), Asia Pacific (+10) and the Middle East (+9). This convergence suggests that cybersecurity is now perceived as a structural risk of operating in a digital economy rather than a sector-specific or regional concern.

Figure 2. Cybersecurity as a Top 5 risk by region, 2026 (share of CAEs)

Source: Risk in Focus 2026/2027, Exhibit 1.2 (n = 3,285).

The report describes a risk displacement effect, in which risks such as business resilience, governance and organizational culture fell in the ranking not because their importance fell, but because more urgent risks took their place. Despite this displacement, cybersecurity was not pushed down the ranking, and it remained the highest rated risk in the region for the fourth consecutive year. Not only is cybersecurity ranked as the highest risk it has not changed is positioning despite the increase in geopolitical risk.

The purpose of this Economic Lens is to highlight the importance of cybersecurity to the economy and explains its positioning in Egypt and the Middle East and what must be done to mitigate that risk.

Why does cybersecurity matter for the economy?

Cybersecurity is defined as the protection of networks, systems and digital services from unauthorized access, disruption or damage. For example, a ransomware attack that disables a retailer's payment system can halt sales entirely even when no customer data is stolen, which shows that protecting systems matters independently of protecting information. This protection has become an economic issue because payments, trade, energy, logistics and government services now depend on digital infrastructure. A successful attack therefore creates costs that go beyond the affected firm, such as interrupted services, lost transactions and reduced confidence in digital channels. According to IBM's Cost of a Data Breach Report 2025, the global average cost of a data breach was $4.44 million, up from $3.86 million in 2020.[2] At the global level, these costs are extremely large. Cybersecurity Ventures estimates the annual global cost of cybercrime at $10.5 trillion in 2026, and expected to rise to $15.63 trillion by 2029.

While cybersecurity is often treated as a technical cost, it is also a condition for digital transformation and investment. Financial inclusion, e-government, fintech and AI adoption all depend on the willingness of households and firms to use digital channels. Third-party and supply chain compromise was the most frequent cause of breaches in the Middle East (17% of incidents), which indicates that the security of one firm depends on the security of its suppliers.[4] Therefore, cybersecurity has the characteristics of a shared infrastructure, where underinvestment by some firms imposes costs on others.

Are cybersecurity and data security the same risk?

While the two terms are often used interchangeably, cybersecurity and data security are not the same function. Cybersecurity protects systems and networks from attack, regardless of what they contain. Data security and data protection are concerned with the information itself, including who is permitted to collect it, where it is stored, how long it is kept, and whether it can be transferred abroad.

[2] IBM, Cost of a Data Breach Report 2025.
[4] IBM Newsroom MEA, “Cost of a Data Breach 2025: Middle East findings.” Converted at the official peg of SAR 3.75 per U.S. dollar.

An organization can therefore have strong network defenses and still misuse or over-collect personal data, and it can comply with data protection rules while remaining exposed to ransomware.

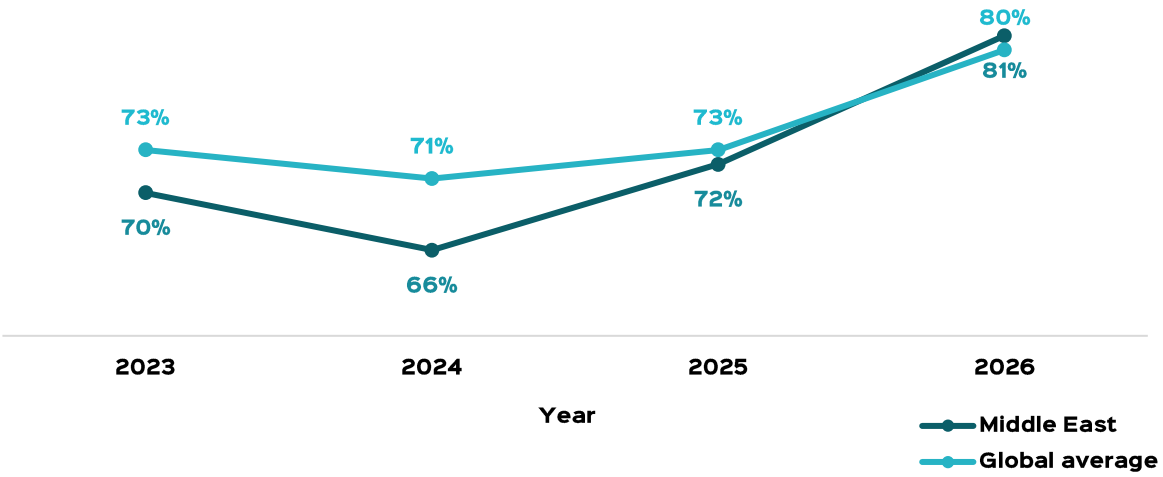
The Risk in Focus report mentions this separation, although only indirectly. The survey itself combines the two, since the risk area is described to respondents as "cybersecurity and data security," which means that the 81% rating covers both. However, the report notes that regulators in Saudi Arabia asked a financial institution to segregate its cyber and data chiefs into separate roles, which required the hiring of an additional senior expert. The same CAE reported that compliance-related costs for cybersecurity increased by 40% over the past year, partly due to this additional hiring. The report also discusses data protection under digital disruption rather than under cybersecurity. It notes that several jurisdictions in the region restrict cross-border data transfers, which often require regulatory approval and must respect the principle of data minimization.

This separation is important for three reasons. Firstly, the two risks are governed by different rules and regulators, since cybersecurity is supervised by national cybersecurity authorities, while data protection is supervised by data protection authorities with their own licensing and penalties. Secondly, separate roles reduce the conflict of interest that arises when the official responsible for operating systems is also responsible for judging whether data is being used lawfully. For example, a cybersecurity officer may prefer to retain detailed customer activity logs for several years to investigate incidents, while a data protection officer is required to ask whether retaining this personal data for such a period is necessary and lawful. Thirdly, the adoption of AI raises the value of data governance, because AI tools depend on large volumes of data that may be processed outside the country.

Has the perception of Cybersecurity in the Middle East changed in the past few years?

The Risk in Focus report shows that In the Middle East, 81% of CAEs rated cybersecurity as a top five risk, compared to 72% in 2025 and 66% in 2024. Figure 3 shows that the region was below the global average until 2025 and moved above it in 2026. The global average for cybersecurity risk was higher than the Middle East up until 2025 but this changed in 2026 with the risk being higher at 81% than the average of 80%. This is due to an increase in digitization in region which provides more opportunities for attacked, but also due to the war in the Gulf which triggered an increase of cybersecurity attacks.

Figure 3. Cybersecurity risk rating, 2023-2026 (share of CAEs selecting cybersecurity as a Top 5 risk)



Source: Prepared by the author based on Risk in Focus 2026/2027, Exhibits 1.1 and C.2.

This increase has been observed by private cybersecurity experts. According to CloudSEK there has been an increase in ransomware activity in the region from 17 threat intelligence feeds in April 2025 to 357 in June 2026 (CloudSEK, 2026). Mastercard similarly reports that cyberattacks across Eastern Europe, the Middle East and Africa rose by 13% between March 2025 and March 2026, and that the Middle East alone accounted for 49% of the total increase.

What are governments and the private sector doing in the Middle East?

Governments in the region have mainly responded through the creation of central cybersecurity authorities and binding controls. The National Cybersecurity Authority (NCA) of Saudi Arabia was established in 2017 to protect vital interests, national security and sensitive infrastructure.[6] The UAE established its Cybersecurity Council in 2020 and adopted a National Cybersecurity Strategy for 2025-2031 that is built on six pillars, including governance, national resilience, emerging technology security, public-private partnerships and talent development.[7] As a result, eight Arab states were classified in Tier 1 of the Global Cybersecurity Index 2024.[8]

Despite this progress, the regional picture is uneven. Kuwait, Tunisia, Algeria and Libya were classified in Tier 3, while Iraq, Lebanon, Syria, Sudan and Palestine were classified in Tier 4 and Yemen in Tier 5.[9]

[6] National Cybersecurity Authority (Saudi Arabia), "About NCA," https://nca.gov.sa/en/vision-and-mission/.
[7] Eventus Security, "UAE National Cybersecurity Strategy 2025-2031."
[8] Telecom Review, "Assessing Arab States in the ITU's GCI 2024."
[9] Telecom Review, "Assessing Arab States in the ITU's GCI 2024."

Table 1. Arab countries by tier in the ITU Global Cybersecurity Index 2024

Tier	Arab countries
Tier 1 (Role-modelling)	Egypt, Bahrain, Morocco, Oman, Qatar, UAE, Saudi Arabia
Tier 2 (Advancing)	None
Tier 3 (Establishing)	Algeria, Kuwait, Libya, Tunis
Tier 4 (Evolving)	Iraq, Lebanon, Palestine, Syria, Sudan
Tier 5 (Building)	Yemen

Source: Global Cybersecurity Index 2024, as reported by Telecom Review.[10]

The ITU also identifies a cyber-capacity gap in the region, which is characterized by limitations in skills, staffing, equipment and funding. This is because the countries with the weakest rankings are also those most affected by conflict and fiscal pressure. It is important to point out that attackers can use weakly protected countries and suppliers as entry points to better protected ones, which limits the benefit of national strategies that are not accompanied by regional cooperation.

The private sector has responded mainly through higher spending and stronger assurance. Cybersecurity spending across the Gulf countries is projected to double and exceed $32.7 billion (AED 120 billion) by 2030, with the UAE and Saudi Arabia accounting for more than 60% of the total (Grand View Research, 2025).[11] The Risk in Focus report notes that financial institutions are hiring additional specialists and contracting more service providers in response to regulatory requirements, as reported by CAEs in roundtables. Internal audit functions have also shifted their effort, since 78% of CAEs in the region listed cybersecurity as a top five audit priority in 2026 compared to 69% in 2025, and the share reaches 87% in financial services.[12]

What Egypt needs to do to protect itself from increasing cybersecurity risk

Egypt has built its institutional framework for cybersecurity gradually over the past two decades. The Egyptian Computer Emergency Readiness Team (EG-CERT) was established in 2009 under the National Telecom Regulatory Authority (NTRA) to provide incident response, analysis and early warning for government, financial entities and other critical information infrastructure sectors. The Egyptian Supreme Cybersecurity Council (ESCC) was established in 2014 with a mandate to develop and oversee the national strategy for responding to cyber threats. The legal framework was then extended through the Anti-Cyber and Information Technology Crimes Law No. 175 of 2018. The council issued the National Cybersecurity Strategy 2023-2027, which includes programs for legislative

[10] Telecom Review, "Assessing Arab States in the ITU's GCI 2024."
[11] Khaleej Times, "Gulf cybersecurity spend to top Dh120 billion by 2030" (19 November 2025), citing Grand View Research. The figure covers the whole Gulf region and is reported in UAE dirhams by the source; converted at the official peg of AED 3.6725 per U.S. dollar.
[12] Internal Audit Foundation and Arab Confederation of Internal Auditors (ARABCIA), Risk in Focus 2026/2027: Hot Topics for Internal Auditors, Middle East (2026). All survey figures in this issue are drawn from this report unless otherwise stated.

development, national partnerships, research and innovation, community awareness, cyber defenses and international cooperation.[17]

The financial sector has its own arrangements, which are led by the Central Bank of Egypt (CBE). The CBE established the Egypt Financial Computing Incident Response Team (EG-FinCIRT) to prevent and mitigate incidents and to exchange information among banks. EG-FinCIRT became the first sectoral center in Egypt to join the global Forum of Incident Response and Security Teams (FIRST) in May 2023.[18] This sectoral approach is consistent with the findings of the Risk in Focus report, since financial services record the highest cybersecurity risk rating in the region.

Regarding data security, Egypt followed the same separation discussed above, since data protection is governed by a separate law and a separate regulator. The Personal Data Protection Law No. 151 was issued in 2020, but its executive regulations were only issued in November 2025 through Decree No. 816 of 2025, more than five years later.[19] The regulations empower the Personal Data Protection Center to license and supervise data controllers, and they require the appointment of a data protection officer, the notification of breaches within 72 hours, and a permit for cross-border transfers of personal data. Organizations were given a one-year grace period, which means that enforcement is expected to begin in late 2026, with penalties for violating it. Despite the importance of this reform, the five-year delay in issuing the regulations is an example of the gap between legislation and execution, and many firms are likely to enter the enforcement period without prior experience of compliance.

While government action has focused on institutions and laws, the private sector response is visible in spending and training. The Egyptian cybersecurity market is estimated at $257 million in 2026 and is projected to reach $452 million by 2031 (Mordor Intelligence, 2026).[20] The biggest driver of this growth is the National Cybersecurity Strategy, which is accelerating public sector spending. Banking and financial services account for the largest share of demand (31%), and large enterprises account for about 68% of spending. Private initiatives have also targeted skills, such as the Information Security Academy launched by the Export Development Bank of Egypt and the Egyptian Banking Institute, and the cybersecurity major introduced by the American University in Cairo.[21] However there is still shortage of specialist, combined with the concentration of spending in large firms, indicates that small and medium-sized enterprises remain the least protected from cybersecurity threats.

[17] Ministry of Communications and Information Technology, “National Cybersecurity Strategy 2023-2027”; Egyptian Supreme Cybersecurity Council; EG-CERT.
[18] Egypt Today, “CBE’s financial sector cybersecurity center joins global cybersecurity forum” (17 May 2023); Central Bank of Egypt, “EG-FinCIRT acquires the membership of OIC-CERT” (January 2024).
[19] Kennedys, “Egypt’s Personal Data Protection Law: the compliance countdown has begun” (2026); Baker McKenzie, “Egypt: Important Data Protection Update” (January 2026).
[20] Mordor Intelligence, “Egypt Cybersecurity Market” (2026).
[21] EnterpriseAM, “The cyber threats facing Egypt and how to address them” (4 December 2024), citing Kaspersky data for H1 2024.

What is the way forward?

Overall, the evidence indicates that cybersecurity is perceived as the highest organizational risk globally, in the Middle East and, by extension, in Egypt, and that the regional conflict and the adoption of AI have increased this risk rather than displaced it. While Egypt has a strong formal framework, as reflected in its Tier 1 classification, the main challenge is the translation of this framework into implemented capacity. The following points summarize the policy implications for Egypt:

- Close the gap between commitment and capacity: The ESCC should prioritize the areas where Egypt scores lowest, namely cyber crisis management and cybercrime prosecution, through national crisis exercises and specialized investigative units.
- Treat cybersecurity and data security as separate but coordinated functions: The ESCC, EG-CERT, the CBE and the Personal Data Protection Center should coordinate breach reporting requirements, so that firms do not face duplicate efforts when a single incident is both a cyberattack and a personal data breach.
- Reduce the cost of compliance for smaller firms: The Personal Data Protection Center could let small firms share a single data protection officer and phase in enforcement gradually, since the Saudi experience shows that requiring separate specialists raises costs that smaller firms can least afford.
- Expand the supply of specialists: The Ministry of Communications and Information Technology, universities and banks should scale up training, since the current number of graduates is far below market demand.
- Strengthen risk governance within firms: Boards and audit committees should require regular reporting on cyber risk maturity, third-party exposure and AI use, since less than half of organizations in the region describe their cybersecurity governance as mature.
- Deepen regional cooperation: Information sharing between national and sectoral response teams should be extended, because state-linked attacks on critical infrastructure and the uneven capacity across Arab countries create shared exposure.

Ultimately, the key is not the number of strategies and laws that are issued, but the speed and consistency with which they are implemented. The delay in issuing the executive regulations of the Personal Data Protection Law shows that the cost of slow execution is a prolonged period of uncertainty for firms. Therefore, cybersecurity should be treated as part of the investment climate and of economic resilience, and not only as a technical matter.