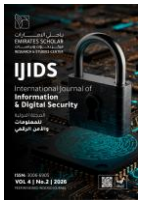

International Journal of Information & Digital Security
Vol 4 Issue 1 (2026)
Pages 14 - 22
Available at
www.emiratesscholar.com

Cybersecurity in the Gulf Cooperation Council: An Analytical Review of the Threat Landscape, Critical-Infrastructure Risk, and National Strategies

Johann Schmidt, Arjun Reddy
Technical University of Munich - Germany, Indian Institute of Technology Delhi - India

ARTICLE INFO

KEYWORDS
cybersecurity; Gulf Cooperation Council; critical infrastructure; operational technology; national cybersecurity strategy; Shamoon; ITU Global Cybersecurity Index

HOW TO CITE
Schmidt, J., & Reddy, A. (2026). Cybersecurity in the Gulf Cooperation Council: An Analytical Review of the Threat Landscape, Critical-Infrastructure Risk, and National Strategies. International Journal of Information & Digital Security, 4(1), 14-22.
https://doi.org/10.54878/5x1zz198

ABSTRACT

The states of the Gulf Cooperation Council (GCC) are pursuing some of the world's most ambitious programmes of digital transformation while simultaneously operating the strategic energy infrastructure on which the global economy depends, a combination that makes the region both a leader in digital adoption and an exceptionally attractive target for cyber-attack. This analytical review examines the cybersecurity situation of the GCC across three dimensions. First, we characterize the threat landscape, arguing that the region faces an unusually severe mix of state-sponsored operational-technology sabotage, exemplified by the Shamoon wiper attacks on Saudi Aramco and RasGas, alongside ransomware, social-engineering, and the expanding attack surface of smart-city and Internet-of-Things deployment. Second, we analyse critical-infrastructure and operational-technology risk, noting that while the GCC energy sector is relatively advanced in adopting global frameworks such as the NIST Cybersecurity Framework and IEC 62443, other sectors, including water utilities and transport, lag in maturity, and IT/OT convergence continues to expand exposure. Third, we assess national strategies and governance, observing that Saudi Arabia and the United Arab Emirates now rank among the global leaders on the ITU Global Cybersecurity Index, yet the region still suffers from fragmented policy, limited intra-regional cooperation, a shortage of skilled professionals, and persistent human-factor weaknesses documented in empirical studies of Gulf organizations. We frame the analysis with a standard risk formulation and a sectoral maturity comparison, and we conclude that the GCC's principal cybersecurity challenge is no longer awareness or investment, both of which are substantial, but the integration of governance, workforce, and OT security into a coherent and cooperative regional posture. The review is analytical and is weighted toward the energy sector and the larger GCC economies, where the evidence base is deepest.

Double-blind peer review by independent reviewers.

Received: 09 Jan 2026, Accepted: 29 May 2026, Published: 21 Jun 2026

*Corresponding author: johann.schmidt@tum.de

1. Introduction

The Gulf Cooperation Council, comprising Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates, occupies an unusual position in the global cybersecurity landscape. On one hand, its member states are among the most aggressive adopters of digital technology in the world, pursuing national visions, Saudi Arabia's Vision 2030, the UAE's digital-government and smart-city programmes, and their counterparts across the region, that place connectivity, data, and automation at the centre of economic diversification. On the other, the region operates a concentration of strategically vital energy infrastructure, producing and moving a substantial share of the world's oil and gas, whose disruption would carry consequences far beyond the region itself. The intersection of rapid digitization, great wealth, critical energy assets, and acute geopolitical tension produces a threat profile that is, in important respects, distinctive.

That distinctiveness is not merely theoretical. In 2012 the Shamoon wiper malware destroyed data on some thirty thousand workstations at Saudi Aramco and propagated to other regional energy firms including RasGas, in what remains one of the most consequential destructive cyber-attacks ever publicly documented (Bronk & Tikk-Ringas, 2013). The episode announced that the region's critical infrastructure was both a target and, in the operational-technology domain, dangerously exposed. In the years since, the volume and sophistication of attacks against GCC organizations have risen sharply, and the region's governments have responded with substantial investment, dedicated national authorities, and, in the cases of Saudi Arabia and the UAE, world-leading rankings on international readiness indices (Alshabib & Martins, 2022).

The economic dimension sharpens the point. Industry measurements have for several years placed the Middle East among the regions with the highest average cost per data breach in the world, a reflection of the value of the data and assets at stake, the concentration of high-value organizations, and the sophistication of the attacks the region attracts. When the potential losses include not only breached records but the disruption of energy production and export, on which several national economies overwhelmingly depend, the aggregate exposure is of a different order from that of most comparably sized economies. Cybersecurity in the GCC is therefore not only a technical or a security matter but a macroeconomic and strategic one, which is precisely why the region's governments have elevated it to the level of national policy.

This review provides an analytical account of that situation for readers concerned with information and digital security. It is organized around three questions. What is the shape of the threat landscape the GCC faces, and why is it distinctive? How exposed is the region's critical and operational-technology infrastructure, and how mature are its defences? And how effective are the national strategies and governance arrangements that GCC states have built, and where do they fall short? We approach these questions comparatively and analytically, framing the discussion with standard risk concepts and a sectoral maturity lens, and we draw throughout on the growing regional literature, including work published in this journal on information security and national digital investment (Habbal, 2023) and on cybersecurity for the Gulf Arab community (Abdelmajid, 2023).

2. Scope and Method

This is an analytical review supported by a structured search of the academic and policy literature on cybersecurity in the GCC and the wider Middle East. We drew on peer-reviewed studies of the regional threat landscape, national strategies, and human factors; on documented incident analyses; and on the global frameworks and indices against which regional performance is commonly assessed. Our aim is to synthesize and interpret this evidence rather than to catalogue every study, and the review is deliberately weighted toward the energy sector and the larger GCC economies of Saudi Arabia, the UAE, and Qatar, where the evidence base is deepest and the strategic stakes highest. We frame the synthesis with standard diagnostic tools, a risk decomposition and a sectoral maturity comparison, so that the analysis is structured rather than merely narrative, while acknowledging that much operational detail in this domain is, by its nature, not publicly reported.

3. Why the GCC Threat Profile Is Distinctive

A structured analysis of the region's risk begins with the factors that make it a preferred target, because they explain the shape of the threat landscape that follows. Four are decisive. The first is strategic energy infrastructure: the GCC's oil and gas facilities are of global economic and geopolitical significance, which makes them attractive to state and state-aligned actors seeking leverage or disruption rather than mere financial gain. The second is the speed and breadth of digitization: national visions have driven the rapid deployment of digital government, smart cities, and Internet-of-Things systems, expanding the attack surface faster than security practice and workforce capacity have grown (Tubaishat

ISSN: 3006-6905 - https://doi.org/10.54878/5x1zz198

et al., 2020). The third is wealth: the region's affluent economies and organizations are lucrative targets for financially motivated cybercrime, including ransomware. The fourth is geopolitical tension: the GCC sits within one of the world's most contested regions, and cyberspace has become an arena in which those tensions are expressed, raising the likelihood of state-sponsored operations against regional targets.

These four factors interact to produce a threat profile in which high-consequence, state-linked attacks on operational technology coexist with high-volume, financially motivated crime and a rapidly enlarging IoT attack surface. It is the combination, rather than any single element, that distinguishes the GCC, and it is why analyses grounded in the region nonetheless carry lessons for other rapidly digitizing, resource-rich, or geopolitically exposed states (Alshabib & Martins, 2022).

4. The Threat Landscape

Against that structural backdrop, the region's threats fall into a small number of recurring categories, mapped in Figure 1 and detailed in Table 1. The most consequential is state-sponsored or state-aligned attack on operational technology and critical infrastructure. The Shamoon campaigns are the defining example: a destructive wiper that rendered tens of thousands of machines inoperable at Saudi Aramco and spread to other energy firms, with later variants recurring in 2016–2017, demonstrating both the intent to cause disruption rather than theft and the vulnerability of converged IT/OT environments (Alghamdi, 2021; Bronk & Tikk-Ringas, 2013).

Alongside this sit the threats common to all digitized economies but sharpened by the region's wealth. Ransomware has grown into a leading concern, with attackers encrypting both IT and, increasingly, OT systems and combining encryption with data theft in double-extortion schemes. Phishing and social engineering remain the most common initial vector, exploiting the human factor that empirical studies of Gulf organizations repeatedly identify as a weak point (Saeed, 2023). The proliferation of smart-city and IoT deployments introduces large numbers of often poorly secured devices, expanding the attack surface in ways that dedicated studies of GCC smart cities have flagged (Tubaishat et al., 2020; Andrade et al., 2020). And supply-chain and insider threats, harder to quantify, complete a landscape in which the region must defend against the full spectrum of adversaries, from opportunistic criminals to sophisticated state actors.

4.1 Case analysis: Shamoon and the operational-technology lesson

The Shamoon episode repays closer analysis because it crystallizes the region's distinctive risk. On 15 August 2012 a wiper virus spread across the corporate network of Saudi Aramco, overwriting the master boot records and data of roughly thirty thousand workstations and forcing the company to disconnect its network for days while it recovered; the same malware struck the Qatari gas producer RasGas shortly after (Bronk & Tikk-Ringas, 2013). Two features mark the attack as a template rather than an aberration. First, its purpose was destruction, not theft or ransom: the objective was to disrupt and to signal, which is the signature of a state-aligned rather than a criminal actor and which raises the stakes of defence from confidentiality to availability and safety. Second, although the destruction fell on IT workstations rather than on the industrial control systems directly, the incident exposed how thoroughly corporate and operational networks had become intertwined, and how a compromise of the former could threaten the latter (Alghamdi, 2021).

The analytical lesson the region drew, and that the subsequent recurrence of Shamoon-class malware in 2016 and 2017 reinforced, is that critical-infrastructure operators must treat availability and OT integrity as first-order security objectives, must segment IT from OT rigorously, and must plan for destructive attacks and not only for data breaches. Much of the GCC energy sector's subsequent investment in OT security, and its comparatively advanced adoption of frameworks such as IEC 62443, can be read as a direct response to the lesson Shamoon taught (Al Araimi et al., 2026). The episode thus functions in the region's cybersecurity history much as a sentinel event functions in safety engineering: a costly demonstration that reshaped priorities.

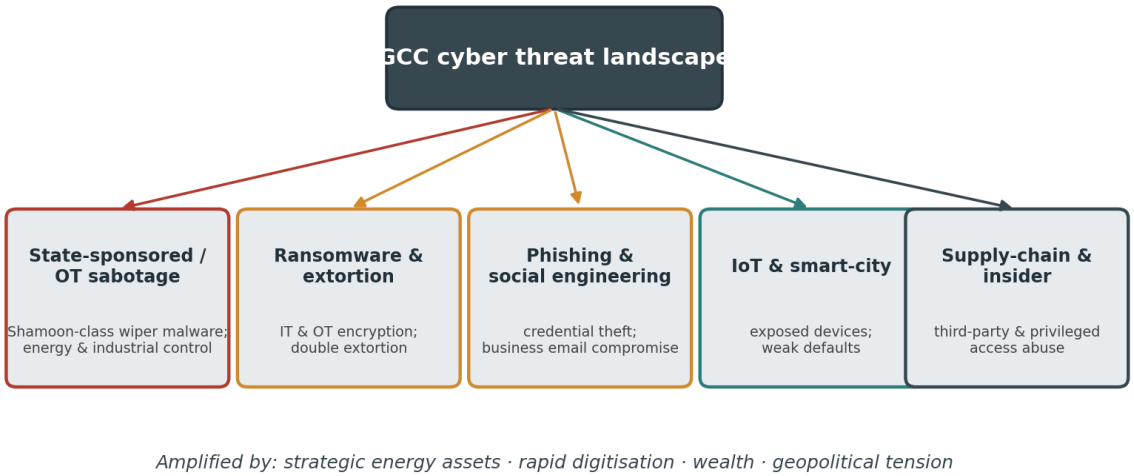

Figure 1. The GCC cyber threat landscape: principal categories and the structural factors that amplify them.

Table 1. Principal threat categories facing the GCC, with vectors and regional relevance.

Threat category	Typical vector	GCC relevance / example
State-sponsored OT sabotage	Wiper malware; ICS intrusion.	Shamoon attacks on Saudi Aramco & RasGas.
Ransomware & extortion	Phishing; RDP; double extortion.	Wealthy targets; IT and OT encryption.
Phishing / social engineering	Email; credential theft; BEC.	Leading initial vector; human-factor weakness.
IoT & smart-city	Exposed devices; weak defaults.	Rapid smart-city / IoT deployment.
Supply-chain & insider	Third-party & privileged access.	Large vendor ecosystems; expatriate workforce.

5. Critical-Infrastructure and Operational-Technology Risk

Because the region's highest-consequence risk lies in its critical infrastructure, the state of operational-technology security deserves separate analysis. Operational technology, the industrial control and safety systems that run energy, water, and transport, was historically isolated from external networks, but the convergence of IT and OT that digital transformation entails has connected these once-air-gapped systems to the wider network and exposed legacy equipment, never designed for a hostile network environment, to remote attack. Assessments of GCC critical-infrastructure operators find that the energy sector is relatively advanced in adopting global OT frameworks, the NIST Cybersecurity Framework, NIST SP 800-82, the IEC 62443 standards, and capability-maturity models such as C2M2, but that other sectors, notably water utilities and municipal transport, lag well behind, and that barriers including a shortage of skilled OT professionals, siloed IT and OT organizations, and fragmented national policy impede progress (Al Araimi et al., 2026).

This unevenness is itself a systemic risk, because critical services are interdependent and an adversary will target the weakest link. Figure 2 depicts the maturity gradient across sectors in illustrative terms drawn from the reviewed literature. The analytical implication is that the region's considerable investment in securing its flagship energy assets is necessary but not sufficient: a water utility or transport system compromised through weaker defences can cause cascading harm, and can serve as a

foothold into better-defended networks. Raising the floor of OT maturity across all critical sectors, rather than only the ceiling in energy, is therefore where much of the region's remaining infrastructure risk resides.

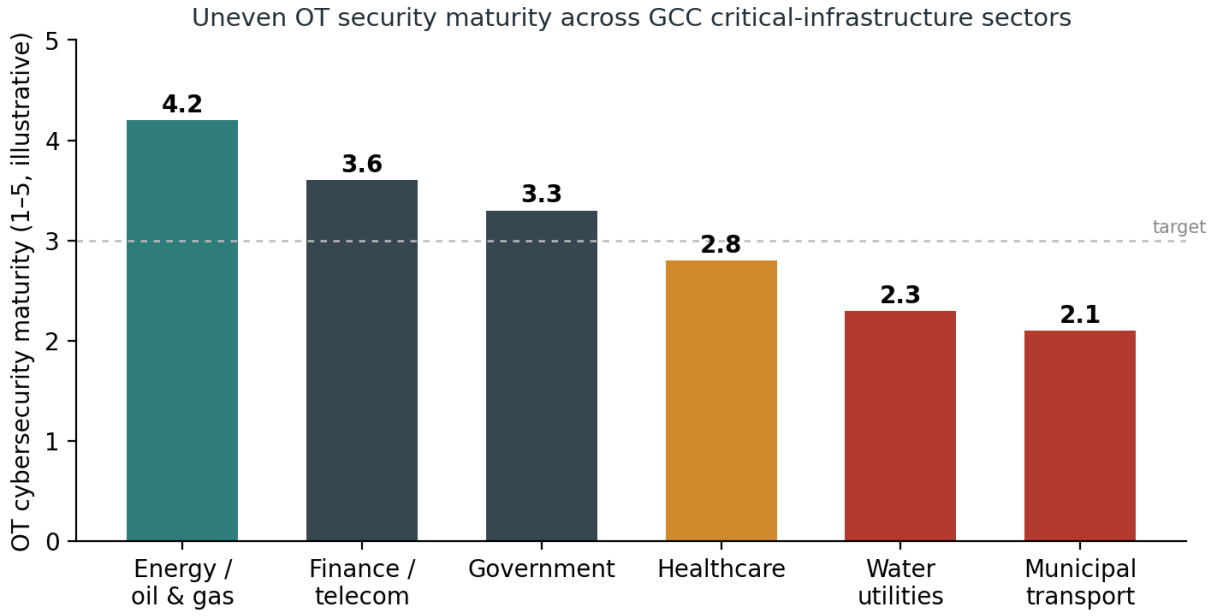

Figure 2. Illustrative OT-security maturity across GCC critical-infrastructure sectors, synthesised from the reviewed literature.

What raising that floor requires is, in outline, well established, and it is worth stating because it converts a diagnosis into a programme. Rigorous segmentation between IT and OT, and among OT zones, limits the lateral movement on which destructive attacks such as Shamoon depend. Continuous monitoring of OT networks, historically neglected because these systems were assumed to be isolated, provides the visibility without which intrusions go undetected for months. The gradual adoption of zero-trust principles, in which no device or user is trusted by default, hardens the converged environment against both external and insider threats. And disciplined patching, asset inventory, and incident-response planning, difficult in OT environments where availability is paramount and downtime for updates is costly, close the basic hygiene gaps that adversaries most often exploit. None of these controls is exotic; the challenge in the GCC, as elsewhere, is to implement them consistently across every critical sector rather than only in the best-resourced ones, and to staff them with the OT-security professionals the region is still working to produce (Al Araimi et al., 2026).

6. National Strategies and Governance

GCC governments have responded to this threat environment with sustained investment and institution-building, and by some measures with conspicuous success. Saudi Arabia established a National Cybersecurity Authority in 2017 and, together with the United Arab Emirates, now ranks among the global leaders on the International Telecommunication Union's Global Cybersecurity Index, both countries placing in the world's top five in the 2020 edition, a remarkable position for economies that only recently prioritized the domain (International Telecommunication Union, 2021). The UAE has created a dedicated Cybersecurity Council and national electronic-security authority, Qatar a national cyber-security agency, and the smaller states their own centres and computer emergency response teams. Table 2 summarizes the principal national arrangements.

Table 2. National cybersecurity governance across GCC states (illustrative).

State	Principal authority / instrument	Note
Saudi Arabia	National Cybersecurity Authority (est. 2017); national strategy.	Top-tier ITU GCI 2020 ranking.
United Arab Emirates	UAE Cybersecurity Council; national electronic-security authority.	Top-tier ITU GCI 2020 ranking.

Qatar	National Cyber Security Agency; national strategy.	Major-event-driven investment.
Bahrain	National Cyber Security Centre.	Financial-sector focus.
Oman	CERT (OCERT); national programme.	Early regional CERT.
Kuwait	National Cyber Security Center / CERT.	Developing framework.

Governance has also extended into law. In recent years GCC states have enacted comprehensive data-protection and cybercrime legislation, including national personal-data-protection laws in Saudi Arabia and the United Arab Emirates and specialized regimes in financial free zones, moving the region toward the kind of legal infrastructure that mature cyber ecosystems require. This legislative turn matters analytically because regulation shapes incentives: mandatory breach notification, accountability for data controllers, and penalties for negligence push organizations to invest in security that they might otherwise defer, and they create the reporting that a national picture of threat depends upon. The regional literature on aligning national policy with digital-economy objectives situates this legal development within the broader project of building a secure environment for national digital investment (Habbal, 2023). The remaining challenge is less the existence of law than its consistent enforcement and its harmonization across a bloc whose members legislate independently.

Yet capability at the national level coexists with a structural weakness at the regional level. A detailed study drawing on interviews with GCC cybersecurity policymakers found that, despite individual national strengths, the region suffers from limited strategic cooperation and a lack of dialogue to tackle common threats, so that adversaries who operate transnationally face defenders who largely do not (Alshabib & Martins, 2022). Cyber threats do not respect borders, and the absence of deep intra-GCC information-sharing, coordinated incident response, and harmonized policy leaves collective gaps that no single national authority, however capable, can close. Strengthening regional cooperation is thus, on the evidence, the highest-value governance improvement available to the bloc.

7. The Human Factor

Technology and governance notwithstanding, the evidence consistently identifies people as the decisive variable, and here the regional literature is unusually rich. A study of information-security behaviour among Saudi business employees found that they did not perceive several important security constructs as relevant, a gap that can translate directly into exploitable behaviour, and recommended layered measures at both organizational and individual levels (Saeed, 2023). A moderated-mediation analysis of Saudi organizations found that employees' perceptions of organizational responsibility strongly shaped their own security behaviour, underlining that security culture is set from the top (Asfahani, 2024). And a comparative study of the technology-savvy UAE population, analysed through Hofstede's cultural framework, found that human factors in cybersecurity behaviour differ in culturally specific ways from Western populations, cautioning against importing awareness programmes wholesale rather than adapting them to the regional context (Shah et al., 2023). The analytical lesson is that awareness and culture are not soft addenda to a technical problem but central determinants of risk, and that in the GCC they must be addressed in a culturally grounded way, a point the regional literature on educating Gulf communities has also emphasized (Abdelmajid, 2023).

8. An Analytical Risk Framing

It is useful to draw the strands together with the standard vocabulary of risk analysis, because doing so clarifies where the region's exposure actually lies. Cyber risk is conventionally decomposed as a function of threat, vulnerability, and impact,

$$\text{Risk} = f(\text{Threat} \times \text{Vulnerability} \times \text{Impact}),$$

and the GCC scores high on all three terms: threat is elevated by wealth, energy assets, and geopolitics; vulnerability by rapid digitization, OT exposure, uneven sectoral maturity, and human-factor weaknesses; and impact by the strategic and economic centrality of the assets at risk. Because the three multiply rather than add, the region's aggregate risk is high even where individual defences are strong, and reducing it requires progress on every term rather than excellence on one. For prioritization, security economics offers the annualized loss expectancy,

$$\text{ALE} = \text{SLE} \times \text{ARO},$$

the product of the single-loss expectancy of an incident and its annualized rate of occurrence, which directs

investment toward the combinations of high impact and high frequency, precisely the profile of ransomware against wealthy targets and of state-sponsored attacks on high-value infrastructure. This framing makes explicit why the GCC's response, though well funded, must be balanced across the risk terms: investment concentrated on the threat or impact side, without commensurate reduction of vulnerability through OT maturity, workforce development, and human-factor programmes, leaves the product stubbornly large.

9. Challenges and Gaps

Synthesizing the analysis, five gaps stand out as the region's principal remaining challenges. The first is the skills shortage: demand for qualified cybersecurity and, especially, OT-security professionals far outstrips supply, constraining every other improvement (Al Araimi et al., 2026). The second is IT/OT organizational silos, which leave the converged systems that matter most defended by teams that do not fully understand one another. The third is uneven sectoral maturity, with critical services outside energy lagging dangerously. The fourth is fragmented regional cooperation, which cedes an advantage to transnational adversaries (Alshabib & Martins, 2022). The fifth is the human factor, where culturally grounded awareness and security culture remain works in progress (Saeed, 2023; Shah et al., 2023). Table 3 pairs these challenges with the responses the evidence supports.

Table 3. Principal GCC cybersecurity challenges and evidence-supported responses.

Challenge	Consequence	Response
Skills shortage	Constrains all other improvements.	Workforce development; OT-security training.
IT/OT silos	Converged systems poorly defended.	Integrated IT/OT governance and teams.
Uneven sectoral maturity	Weakest sector sets systemic risk.	Raise OT maturity floor beyond energy.
Fragmented cooperation	Advantage to transnational attackers.	Regional information-sharing & joint response.
Human factor	Behaviour undermines controls.	Culturally grounded awareness; security culture.

10. Discussion

The analysis supports a clear and, in its way, optimistic conclusion. The GCC has moved, in little more than a decade, from the shock of Shamoon to a position of substantial national capability, with two of its members ranked among the world's most cyber-ready states and its flagship energy sector adopting the best global frameworks. The region's cybersecurity problem is therefore no longer principally one of awareness or investment, both of which are now considerable, but one of integration and coordination: of connecting strong national capabilities into a cooperative regional posture, of extending the maturity of the energy sector to water, transport, and health, of closing the workforce gap that constrains everything else, and of addressing the human factor in a culturally grounded way. These are hard problems, but they are problems of execution and coordination rather than of recognition or resource, which is a more tractable position than many regions occupy.

Two implications deserve emphasis. First, because cyber risk multiplies threat, vulnerability, and impact, and because the region's threat and impact terms are structurally high and largely fixed, the most controllable lever is vulnerability, and within it the unglamorous foundations of OT maturity, workforce, and human factors rather than headline technology. Second, because adversaries operate across borders while defence remains largely national, the single highest-value collective step is deeper regional cooperation, an argument the GCC-focused literature makes repeatedly and which the bloc's shared language, institutions, and threat environment make unusually feasible (Alshabib & Martins, 2022; Abdelmajid, 2023). The region has built the national foundations; the task now is to connect and complete them.

Table 4. A prioritised roadmap for strengthening GCC cybersecurity, by horizon.

Priority	Near-term action	Longer-term action
Workforce	Expand IT/OT security training and certification.	Build regional talent pipelines and centres of excellence.
OT security	Extend energy-sector frameworks to water, transport, health.	Set GCC-wide OT maturity benchmarks.
Regional cooperation	Establish intra-GCC threat-intelligence sharing.	Coordinate incident response and harmonise policy/law.
Human factor	Deploy culturally grounded awareness programmes.	Embed security culture and top-down accountability.
Governance & law	Enforce data-protection and breach-notification regimes.	Harmonise regulation and align with national visions.

Two emerging developments will test the region's posture in the coming years and deserve anticipatory attention. The first is the weaponization of artificial intelligence by attackers, which promises more convincing phishing, faster vulnerability discovery, and adaptive malware, and which will raise the tempo of attack in ways that manual defence cannot match; the same technology, deployed defensively for anomaly detection and automated response, is part of the answer, but it shifts the contest onto terrain where the workforce and data gaps identified above bite hardest. The second is the longer-horizon threat that quantum computing poses to the cryptography on which today's digital security rests, a prospect that has begun to prompt attention to quantum-safe protocols and key distribution, including within this journal's own literature. For a region investing so heavily in long-lived digital and physical infrastructure, beginning the migration toward cryptographic agility and post-quantum readiness is a prudent hedge rather than a premature one.

These developments reinforce rather than alter the review's central argument. Whether the threat is a wiper today or an AI-augmented campaign tomorrow, the region's resilience will rest on the same foundations: a capable and sufficient workforce, mature and consistently applied OT security, a security-conscious culture, sound governance and law, and, binding these together, genuine regional cooperation. The GCC has shown that it can build national capability at remarkable speed; extending that capability across sectors, embedding it in people and institutions, and sharing it across borders is the work that will determine whether the region's digital ambitions rest on secure foundations.

11. Limitations

This review is analytical and interpretive rather than empirical, and it inherits the limits of a domain in which much operational information is, for good reasons, not public. Threat and incident data are incomplete and often drawn from vendor or media sources of uncertain reliability, and the sectoral maturity comparison we present is an illustrative synthesis of the reviewed literature rather than a measured index. The evidence base is uneven across the bloc, concentrated in Saudi Arabia, the UAE, and Qatar and thinner for the smaller states, so regional generalizations are better supported for some members than others. The field also evolves rapidly, as adversaries, technologies, and national institutions change, so specific claims about capability and posture are necessarily time-bound. These constraints qualify the detail of the analysis without unsettling its central conclusions about the region's distinctive risk profile and the primacy of integration and cooperation.

12. Conclusion

The Gulf Cooperation Council presents a cybersecurity paradox: a region that is simultaneously among the world's most digitally ambitious and most acutely targeted, and that has responded with capability that is impressive at the national level yet incomplete at the regional and sectoral one. Its threat landscape is distinctively severe, combining state-sponsored sabotage of critical energy infrastructure, exemplified by the Shamoon attacks, with the ransomware, social-engineering, and IoT threats common to all digital economies but sharpened by the region's wealth and exposure. Its defences are, in the leading states and the energy sector, genuinely strong, but they are undercut by uneven sectoral maturity, a skills shortage, IT/OT silos, human-factor weaknesses, and, above all, limited regional cooperation. The path forward, on the evidence, is not more recognition or more spending but better integration: connecting national strengths into a coordinated regional posture, raising the floor of critical-infrastructure security across every sector, building the workforce, and grounding awareness in the region's own

ISSN: 3006-6905 - https://doi.org/10.54878/5x1zz198

culture. The GCC has demonstrated that a determined state can build world-class cybersecurity capability quickly; the remaining challenge is to make that capability collective, complete, and resilient.

References

Abbadi, D. (2024). Morocco's cybersecurity strategy between challenges and aspirations. International Journal of Information & Digital Security, 2(1).

Abdelmajid, N. (2023). The necessity of cybersecurity for community safety: The proposal of the Safe Family Program for educating the Gulf Arab community on information security for both students and parents. International Journal of Information & Digital Security, 1(1).

Al Araimi, A. K., et al. (2026). Assessing OT cybersecurity readiness in critical infrastructure: Global frameworks and GCC applications. In Proceedings of the 2026 5th International Conference on Innovative Practices in Technology and Management (ICIPTM). IEEE.

Alghamdi, M. I. (2021). Impact of cyber attack on Saudi Aramco. Journal of Cybersecurity and Information Management, 7(1), 8–15.

Alshabib, H. N., & Martins, J. T. (2022). Cybersecurity: Perceived threats and policy responses in the Gulf Cooperation Council. IEEE Transactions on Engineering Management, 69(6), 3664–3675. https://doi.org/10.1109/TEM.2020.3035577

Andrade, R. O., Yoo, S. G., Tello-Oquendo, L., & Ortiz-Garcés, I. (2020). A comprehensive study of the IoT cybersecurity in smart cities. IEEE Access, 8, 228922–228941. https://doi.org/10.1109/ACCESS.2020.3046442

Asfahani, A. M. (2024). Perceptions of organizational responsibility for cybersecurity in Saudi Arabia: A moderated mediation analysis. International Journal of Information Security, 23, 1257–1275. https://doi.org/10.1007/s10207-023-00782-z

Bronk, C., & Tikk-Ringas, E. (2013). The cyber attack on Saudi Aramco. Survival, 55(2), 81–96. https://doi.org/10.1080/00396338.2013.784468

Habbal, F. (2023). Impact of information security on national digital investment. International Journal of Information & Digital Security, 1(1).

International Telecommunication Union. (2021). Global Cybersecurity Index 2020. Geneva: International Telecommunication Union.

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity, Version 1.1. Gaithersburg, MD: NIST. https://doi.org/10.6028/NIST.CSWP.04162018

Saeed, S. (2023). Digital workplaces and information security behavior of business employees: An empirical study of Saudi Arabia. Sustainability, 15(7), 6019. https://doi.org/10.3390/su15076019

Shah, M. U., Iqbal, F., Rehman, U., & Hung, P. C. K. (2023). A comparative assessment of human factors in cybersecurity: Implications for cyber governance. IEEE Access, 11, 87970–87984. https://doi.org/10.1109/ACCESS.2023.3305100

Tubaishat, A., & Al-Obeidat, F. (2020). Building a security framework for smart cities: A case study from UAE. In Proceedings of the 2020 5th International Conference on Computer and Communication Systems (ICCCS) (pp. 480–485). IEEE.