INFORMATION SYSTEMS MANAGEMENT

Security as a Subscription: Can Vulnerability Management as a Service Close the Kingdom's Cybersecurity Skills Gap by 2030?

Muhammad Tehami Nadeem

Published November 2026

Abstract

Organisations in the Kingdom of Saudi Arabia must find, rank and fix technical vulnerabilities continuously, yet the specialists who can do this are scarce everywhere and especially scarce in small firms. Vulnerability management offered as a subscription service promises to pool that scarce expertise and automate much of the routine work. This paper examines whether, and under what conditions, such a service can narrow the national skills gap before 2030. The method is an integrative synthesis, conducted systematically, of thirty journal papers (2020–2025) that passed peer review and deal with the shortage of skills, vulnerability assessment and prioritisation, automated testing and security outsourcing, read alongside three public documents from the national cybersecurity regulator. Two studies serve as anchors: a survey of cybersecurity practices and attack damage in Saudi small enterprises, and a model that prioritises vulnerabilities using externally visible network information. The synthesis produces a three-tier service model and a division of responsibilities between provider and client. It finds that the service can absorb discovery, scoring and much of the testing workload, but that contract design, client-side coordination and retained in-house judgement decide whether exposure actually falls. An illustrative capacity comparison with invented figures shows the pooling effect. The answer to the title question is a qualified one: the service can narrow the gap, not close it. The analysis draws solely on published sources and involves no primary or proprietary data.

1 Introduction

Every organisation that runs networked systems inherits a stream of newly disclosed vulnerabilities. Keeping pace with it requires people who can scan systems, interpret findings, judge which flaws matter most, coordinate fixes and confirm that the fixes worked. Those people are in short supply. Studies from Europe describe recruiting, retaining and maintaining enough cybersecurity professionals as a constant battle that extends to managerial as well as technical roles (Blažič, 2021), and a comparison of four knowledge frameworks began from the observation that organisations worldwide struggle to recruit staff with the necessary knowledge (Dkaidek & Rashid, 2024).

Saudi Arabia faces the same pressure while pursuing rapid digital transformation. According to the regulator, the workforce exceeded 21,000 specialists in 2024, up 9% on the previous year (Table 1, D2), yet demand is driven by every government entity and by the many private firms that are now digital. Small firms are the hardest case. A survey of 282 respondents representing small Saudi enterprises found that firms with an inspection team and a recovery plan suffered less financial harm from attacks, and that contact with cybersecurity authorities and an inspection team had significant effects on restoration time (Alharbi et al., 2021). Few small firms can employ such a team themselves.

Vulnerability management as a service is one response. Instead of building an internal function, an organisation subscribes to a provider that runs discovery scans, scores and ranks findings, tests

exploitability and advises on remediation, often through a shared platform and pooled analysts. The model is attractive because routine parts of the work can be automated and because one team of specialists can serve many clients. Whether it reduces risk, and whether it can make a material difference to a national skills gap, is less clear.

This paper examines those questions. It builds on two anchor studies. The first is the Saudi small-enterprise survey just described (Alharbi et al., 2021), which links specific practices to attack outcomes. The second is a model that prioritises vulnerabilities using network environment variables gathered from open sources, with input data obtained from an Internet search engine for connected devices (Reyes et al., 2022). The former shows why expertise matters; the latter shows how much of the work can be automated with information that is also available to attackers.

The study has one aim: to assess whether vulnerability management delivered as a subscription can narrow the Kingdom's cybersecurity skills gap by 2030 and to specify the conditions under which it would do so. The objectives are (O1) to identify which vulnerability management tasks are most demanding of scarce skills and which can be automated or pooled; (O2) to determine, from the outsourcing literature, the contractual and organisational conditions under which a provider's work reduces a client's risk; and (O3) to propose a service model with a clear division of responsibilities and judge its evidence base. Three research questions follow. RQ1: Which parts of vulnerability management can a service provider absorb, and which depend on the client? RQ2: What conditions make outsourced vulnerability work effective? RQ3: Can such services plausibly narrow the national skills gap by 2030, and what else is needed?

The remainder of the paper covers the background, the method, the findings for each question, the proposed model with an illustrative capacity comparison, a discussion of implications and limits, and the conclusions.

2 Background

2.1 A shortage that education alone will not fix in time

Responses to the skills gap have focused on education. Analysis of European curricula and commercial courses found missing topics in both higher education programmes and private training, and discussed problems of common accreditation and competence certification (Blažič, 2021). A comparison of European skills frameworks called for frameworks that are broader and more adaptable, covering neglected areas such as smaller firms and emerging domains such as the security of artificial intelligence (Almeida, 2025). Guidance for university curriculum development has been assembled from internationally recognised documents and frameworks in response to a reported worldwide shortage of proficient experts (Ramezanian & Niemi, 2024).

Training for operational roles is also changing. In critical infrastructure, where once isolated networks are becoming exposed and the supply of cyber workers is insufficient, a game-based training platform built on historical incidents was designed to help facility owners and operators assess their posture and apply cybersecurity frameworks (Ashley et al., 2022). In the Kingdom, a fuzzy multi-criteria assessment examined segment-wise competency development in cybersecurity policy and compared three decision methods (Alhakami, 2024). All of these efforts take years to change the size of the workforce. Services that make better use of existing specialists could act faster.

2.2 Vulnerability management as a skilled discipline

Vulnerability management is often described as scanning and patching, but its difficult parts are judgement and coordination. Scoring is the first difficulty. The Common Vulnerability Scoring System is central to practice, yet its algorithm is not justified formally or empirically, and using it directly as a risk score contradicts its own specification (Spring et al., 2021). A critique went further, arguing that inconsistencies in the specification and a lack of correlation with exploitation in the wild leave the system unable to describe severity, let alone risk (Howland, 2023). Data-driven alternatives have multiplied, and a survey of the field set out a taxonomy and best practices for assessment and prioritisation based on machine learning (Le et al., 2023).

Data quality is a second difficulty. Not all detected vulnerabilities have base scores in the current version of the standard, which led to the use of machine learning to convert older vectors to the newer format (Nowak et al., 2023). The same team then examined whether the environmental scores enabled by the converter improve prioritisation compared with older base scores, measuring changes in mitigation times and exposure (Balsam et al., 2025). Coordination is a third difficulty. A four-year longitudinal study of 132 delayed patching tasks in two healthcare organisations found that coordination delays were the most prominent cause and that most delays occurred during deployment (Dissanayake et al., 2022). These findings matter for a service model: scoring can be centralised, but deployment remains in the client's hands.

2.3 The economics of security outsourcing

Security outsourcing has been studied mainly through formal models of managed security service providers. When security depends on the efforts of both provider and client and those efforts are private, a double moral hazard problem can arise under the bilateral refund contracts that are common in the industry; monitoring contracts solve it only when variable monitoring costs are negligible, whereas liability contracts can solve it more generally (Wu et al., 2021). A model of the interaction between a provider and a strategic hacker found that not all information assets are worth protecting and that optimal efforts do not necessarily rise with efficiency (Wu et al., 2020). In supply chains, security externalities and information leakage risk affect whether firms should share a provider (Wu et al., 2025), and competition between client firms changes the provider's benefits in ways that depend on technology similarity (Gao & Gong, 2022).

Operational studies of service delivery are fewer but relevant. A decision-support model for outsourcing alert analysis to on-demand analysts showed that a security operations centre could deliver scalable services that meet agreed service levels (Shah et al., 2020). A maturity and capability method for security operations centres, based on a define-measure-analyse-improve-control cycle, offered a service-oriented route to continuous improvement and was demonstrated in a case study (Acartürk et al., 2021). Together these studies suggest that outsourced security work can be organised efficiently, but that its value to the client depends on incentives, information and the client's own effort.

2.4 The Saudi organisational setting

Saudi evidence points to uneven capability. In a mixed-methods study of ten Saudi universities, few participants said that risks were assessed regularly and dealt with promptly once found, and participants were concerned about weak policies and procedures and insufficient training (Alhumud et al., 2023). A national awareness survey of 1,230 participants found that 32.5% had no idea about phishing attacks and that only 29.2% of the 21.7% who had been victims reported the crime

(Alzubaidi, 2021). These figures concern individuals rather than organisations, but they indicate the human background against which technical controls operate.

The regulatory baseline is clear. The national Essential Cybersecurity Controls require government entities and operators of critical national infrastructure to run a vulnerability management programme that includes, at a minimum, regular assessment and detection, grading of findings by severity, remediation in line with that grading and the associated risk, patches checked in a non-production environment and links with reliable sources of new vulnerability information, and they include separate subdomains on penetration testing and on third-party cybersecurity (Table 1, D1). Supply is not the obstacle: the regulator's 2024 economic report counted 353 providers of cybersecurity products, solutions and services and listed managed security operations among the market segments (Table 1, D3). A subscription model would therefore operate within existing obligations and an existing supply base.

Table 1. Public documents from the national regulator consulted for this study (not counted among the thirty reviewed articles)

Code	Document	Year	Content used in this study
D1	Essential Cybersecurity Controls (ECC-2:2024), National Cybersecurity Authority	2024	Scope covers government entities and private owners or operators of critical national infrastructure; vulnerability management subdomain (2-10) requires regular detection, severity grading, risk-informed fixing, pre-tested patches and reliable vulnerability feeds; separate subdomains on penetration testing and third-party cybersecurity
D2	Key Economic Indicators in the Cybersecurity Sector in the Kingdom 2025, National Cybersecurity Authority	2025	Cybersecurity workforce exceeded 21,000 specialists in 2024, growth of 9% on the previous year; women represent 32% of the workforce
D3	Report on Key Economic Indicators in the Cybersecurity Sector 2024, National Cybersecurity Authority	2024	353 providers of cybersecurity products, solutions and services; managed security operations listed among market segments

3 Method

3.1 Approach

The study is a systematic integrative review followed by a service-design step. An integrative review suits the question because the relevant evidence is scattered across workforce studies, technical work on scoring and testing, formal economic models and organisational surveys, and because these sources use incompatible measures. The design step translates the synthesis into a service model and a responsibility matrix, which are then assessed against the evidence.

3.2 Identifying and selecting studies

The literature was gathered in November 2026. Keyword searches of a freely accessible scholarly index covered the cybersecurity skills shortage and workforce, vulnerability assessment and prioritisation, scoring systems, patch management, automated penetration testing, managed security services and outsourcing, small-enterprise security and Saudi organisational cybersecurity. Records were checked against the registration data deposited by publishers to confirm identifiers and years

and to exclude retracted items. Eligible items were refereed journal papers dated 2020 to 2025 that addressed one or more of these themes and offered an abstract or text detailed enough to code. Thirty articles met the criteria. The two anchors (Alharbi et al., 2021; Reyes et al., 2022) were selected because one provides Saudi evidence on how practices affect outcomes and the other demonstrates automated, context-aware prioritisation.

3.3 Analysis

Each article was coded for the vulnerability management task it concerns (discovery, scoring and prioritisation, validation and testing, remediation, governance and reporting), the skill demand it implies, its evidence type and its setting. Tasks were then classified by how far they can be automated, pooled across clients or must remain with the client. Evidence for each element of the resulting model was rated supportive, mixed or limited. Three public documents from the national regulator were consulted for obligations and market facts; they appear in Table 1 and are not among the thirty articles. The capacity comparison in Section 5.3 uses invented numbers to show the logic of pooling. No primary, survey or proprietary data were collected, and no real organisation is described.

4 Findings

4.1 What a provider can absorb and what stays with the client (RQ1)

Discovery is the most automatable task. External exposure can be quantified from open sources, and the anchor model calculated a risk factor for each vulnerability from network environment variables collected through an Internet device search engine, with a prototype that automated extraction, correlation and calculation (Reyes et al., 2022). The results showed that prioritisation was possible using only the information available to an attacker. A provider can run such collection across all clients from one platform.

Scoring and prioritisation can also be centralised, and here the case for a specialist service is strong, because the methods are complex and improving. LICALITY combined threat modelling with a neuro-symbolic model to estimate both the likelihood and the criticality of exploitation, and in two case studies it reduced the remediation work required by the standard score for future threats by factors of 2.89 and 1.85 (Zeng et al., 2022). ILLATION learned risk patterns from adversaries, severity and the network environment and assessed 1,000 vulnerabilities in about 4.5 minutes on a general-purpose computer in a simulated network (Zeng et al., 2024). Environmental scoring, enabled by vector conversion, adds client context to the ranking (Nowak et al., 2023; Balsam et al., 2025). Few organisations could build or maintain such tools alone; a provider can.

Testing is partly automatable. Manual penetration testing is labour-intensive and needs highly skilled practitioners, and given the shortage of experts, automation has been proposed through a self-organising architecture for testing real systems (Skandylas & Asplund, 2025). A survey of path planning in automated testing described rapid progress in methods for choosing efficient attack paths (Chen et al., 2024). These tools extend the reach of each human tester but do not remove the need for one.

Remediation and governance stay largely with the client. The longitudinal evidence on patching delays shows that coordination and deployment, not identification, are where time is lost (Dissanayake et al., 2022), and these steps require access to systems, change approvals and business knowledge that a provider does not hold. Asset knowledge is also a client responsibility, since

environmental scoring depends on accurate information about what each system does. For RQ1, then, the division is fairly sharp: finding and ranking weaknesses, and a large share of testing, can move to the provider, whereas fixing them, supplying asset context and accepting residual risk cannot.

4.2 Conditions for outsourced work to reduce risk (RQ2)

The outsourcing models identify incentive design as the first condition. Because provider and client efforts are private, refund-style contracts invite each side to rely on the other; liability arrangements, which reward well-protected clients and penalise breaches, can align efforts, and monitoring by a third party works only when its variable cost is low (Wu et al., 2021). For a vulnerability service, this implies that contracts should tie fees or credits to agreed outcomes such as time to remediate critical findings, with responsibility for deployment delays clearly assigned.

The second condition is scope. A provider facing a strategic attacker may rationally leave less valuable assets less protected (Wu et al., 2020), and where client firms share a provider or interdependent assets, security externalities and leakage risk alter the optimal arrangement (Wu et al., 2025; Gao & Gong, 2022). Clients therefore need to state which assets are in scope and how their criticality is ranked, rather than leave this to the provider.

The third condition is service management. Alert analysis can be delivered at scale within service levels when the work is modelled and scheduled properly (Shah et al., 2020), and maturity assessment gives providers and clients a shared basis for improvement (Acartürk et al., 2021). The fourth condition is a capable client counterpart. The Saudi small-enterprise survey found that awareness, knowledge of potential damage and professionals' salaries were related to loss of sensitive data (Alharbi et al., 2021), which suggests that the client's own people still shape outcomes. Evidence from British organisations points the same way: investment in cybersecurity systems followed existing capabilities and experienced attacks (Fernandez De Arroyabe et al., 2023), and among 240 small firms neither incidents nor impacts drove implementation, which reflected market failure and information asymmetry (Arroyabe et al., 2024). A service cannot help a client that does not recognise the need for it.

In short, outsourced vulnerability work reduces risk when contracts align incentives around remediation outcomes, when scope and criticality are set by the client, when the provider manages its service to measurable levels and when the client retains enough capacity to act on findings.

4.3 Can the service narrow the gap by 2030? (RQ3)

The answer has two parts. On the supply side, subscription services multiply the effect of each specialist. Automated discovery, data-driven prioritisation and automated testing let a small team serve many clients, and the reduction in remediation work reported for likelihood-based ranking suggests that clients would also spend less effort on low-value fixes (Zeng et al., 2022). Pooling is particularly valuable for small firms, which are described as a blind spot in information security management because of their size, scope and finances (Antunes et al., 2021). An association-led programme based on an international management standard benefited fifty Portuguese small firms through stronger management and better staff awareness (Antunes et al., 2021), which shows that shared delivery can reach organisations that would never build their own function.

On the demand side, the evidence sets limits. Remediation remains a client task, and small firms face financial, technical and organisational barriers that call for awareness programmes tailored to sector and role (Rawindaran et al., 2025). Saudi findings on infrequent risk assessment and insufficient

training (Alhumud et al., 2023) and on low public awareness (Alzubaidi, 2021) imply that many clients lack the counterpart capacity on which outsourcing depends. A subscription can relocate scarce skills but cannot substitute for the basic knowledge needed to commission, understand and act on the service.

The evidence therefore supports a qualified answer. Subscription services can narrow the skills gap by concentrating specialist work and automating routine tasks, and this effect could be felt well before 2030 because it does not depend on new graduates. They cannot close the gap on their own, because the client-side roles they create, such as coordinators who own remediation and managers who accept risk, must still be filled, and because education and training remain the only route to a larger pool of specialists (Ramezanian & Niemi, 2024; Dkaidek & Rashid, 2024).

4.4 Risks that a subscription introduces

Outsourcing also creates exposure of its own. A provider that scans and tests many clients holds detailed knowledge of their weaknesses, privileged credentials for authenticated scanning and, in higher tiers, the ability to change systems. That concentration makes the provider an attractive target and turns a single breach into a breach of many clients. The supply-chain model shows that information leakage between firms sharing a provider is a real consideration in choosing whether to share one (Wu et al., 2025). The Essential Cybersecurity Controls address this through a dedicated third-party cybersecurity subdomain, which a buyer should apply to any vulnerability service (Table 1, D1).

Three further risks follow from the evidence. The first is false assurance. Reports full of severity counts can create an impression of control while the most likely attack paths remain open, which is the central criticism of severity scores used as risk measures (Spring et al., 2021; Howland, 2023). The second is dependence. If all analysis sits with the provider, the client loses the ability to judge the provider's work or to change supplier, and the incentive problems identified in the outsourcing models become harder to manage (Wu et al., 2021). The third is mismatch between automated testing and fragile systems. Automated tools can choose efficient attack paths (Chen et al., 2024), but production systems that cannot tolerate disruption need agreed rules of engagement. Each risk can be reduced by contract terms and client oversight, and none is a reason to avoid the model, but together they explain why the client cannot be a passive buyer.

5 A tiered service model for the Kingdom

5.1 Three service tiers

The synthesis suggests three tiers (Figure 1). Tier 1, visibility, provides continuous external and internal discovery, asset reconciliation and scheduled authenticated scanning, with findings scored by severity and exposure. It suits small firms with little internal capability and is almost entirely automated, drawing on open-source exposure data in the manner of the anchor model (Reyes et al., 2022). Tier 2, prioritisation and assurance, adds likelihood-based ranking using threat information and client context, periodic automated and expert-led penetration tests, remediation guidance for each priority finding and monthly reporting against agreed service levels (Zeng et al., 2022; Skandylas & Asplund, 2025). Tier 3, managed remediation, adds co-managed patch coordination, verification scanning after fixes and integration with the client's change process and operations centre, and is intended for larger entities and operators subject to the national controls.

All tiers share three features. The first is a common evidence trail that maps each activity to the minimum requirements of the national controls, so that subscribing helps clients demonstrate compliance (Table 1, D1). The second is outcome-based reporting, centred on time to remediate by priority class rather than on counts of findings. The third is a skills component: each subscription includes role-based awareness and coaching for the client's coordinator, reflecting evidence that tailored awareness changes small-firm behaviour (Rawindaran et al., 2025).

Choosing a tier is itself a judgement. A practical rule drawn from the findings is to match the tier to the client's ability to act on what the service produces. An organisation with no one able to deploy fixes should start at Tier 1 and use the coaching component to build a coordinator before moving up; an organisation with a change process but no specialists gains most from Tier 2; and an operator with its own operations centre but too few analysts can use Tier 3 to add capacity without giving up control. Movement between tiers should be expected as client capability grows, which is one way in which the service can contribute to the national workforce rather than merely substitute for it.

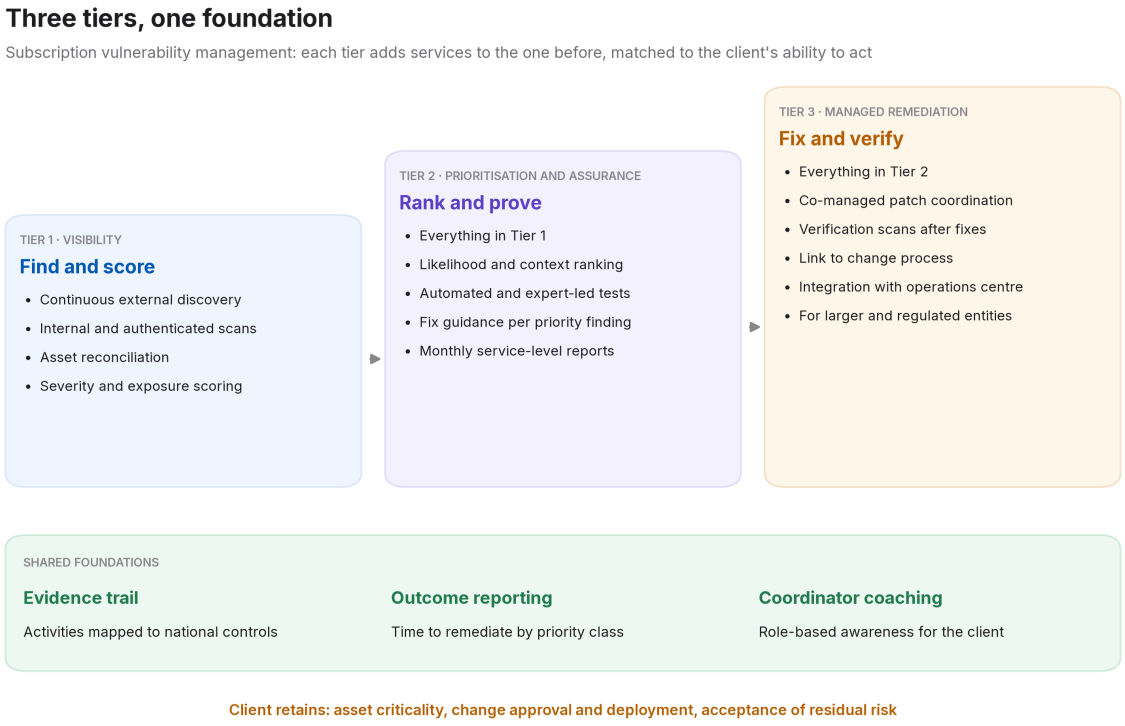

Figure 1. Three-tier subscription model for vulnerability management, with shared foundations

5.2 Dividing responsibilities

Table 2 sets out the division of responsibilities. The provider owns the platform, discovery, scoring method, testing and reporting. The client owns the asset register, the business criticality of systems, approval and deployment of changes and the acceptance of residual risk. Shared items, notably the definition of scope, the remediation targets and the treatment of exceptions, are fixed in the contract. In line with the outsourcing models, the contract should link a part of the fee to agreed remediation outcomes and should assign responsibility for delays explicitly (Wu et al., 2021).

The matrix also guards against two failure modes found in the evidence. One is the provider rationally underprotecting assets it judges to be of low value (Wu et al., 2020), which client-set critic-

ality counters. The other is the coordination delay at deployment (Dissanayake et al., 2022), which named client owners and service-level clocks address.

Table 2. Division of responsibilities in a subscription vulnerability management service

Activity	Provider	Client	Contract mechanism	Evidence
Asset register and business criticality	Reconciles discovered assets	Owns register and sets criticality	Scope schedule, reviewed quarterly	Mixed
Discovery and scanning	Runs external and internal discovery and scans	Grants access and approves windows	Coverage target per asset class	Supportive
Scoring and prioritisation	Applies likelihood and context-based ranking	Supplies environmental context	Documented method and priority classes	Supportive
Validation and testing	Runs automated and expert-led tests	Approves rules of engagement	Test frequency by tier	Mixed
Remediation	Advises and verifies fixes	Approves and deploys changes	Time-to-remediate targets with fee link	Mixed
Risk acceptance and exceptions	Records and reports	Accepts residual risk formally	Exception register and expiry dates	Limited
Compliance evidence and skills	Maps work to national controls; coaches coordinator	Names and trains a coordinator	Reporting format and coaching hours	Limited

5.3 Illustrative capacity comparison

Figure 2 illustrates the pooling effect with invented numbers. It does not estimate national demand or describe any provider. Consider twelve hypothetical small and medium-sized organisations, each needing vulnerability management. If each builds an in-house function, each needs at least one specialist, so twelve specialists are required, and each organisation's specialist must also cover tasks for which there is too little volume to build expertise. Under a pooled subscription with automated discovery and ranking, the same work might be handled by an assumed four specialists at the provider, plus a part-time coordinator in each client at an assumed 0.2 of a full-time post, for a total of 6.4 full-time equivalents, of whom only four need deep specialist skills.

The example shows two things. First, pooling and automation reduce the number of scarce specialists needed. Second, they do not reduce the client-side requirement to zero; the coordinators, though less specialised, still have to be found and trained. Real ratios will depend on client size, technology and service tier, and the values here are assumptions for illustration only.

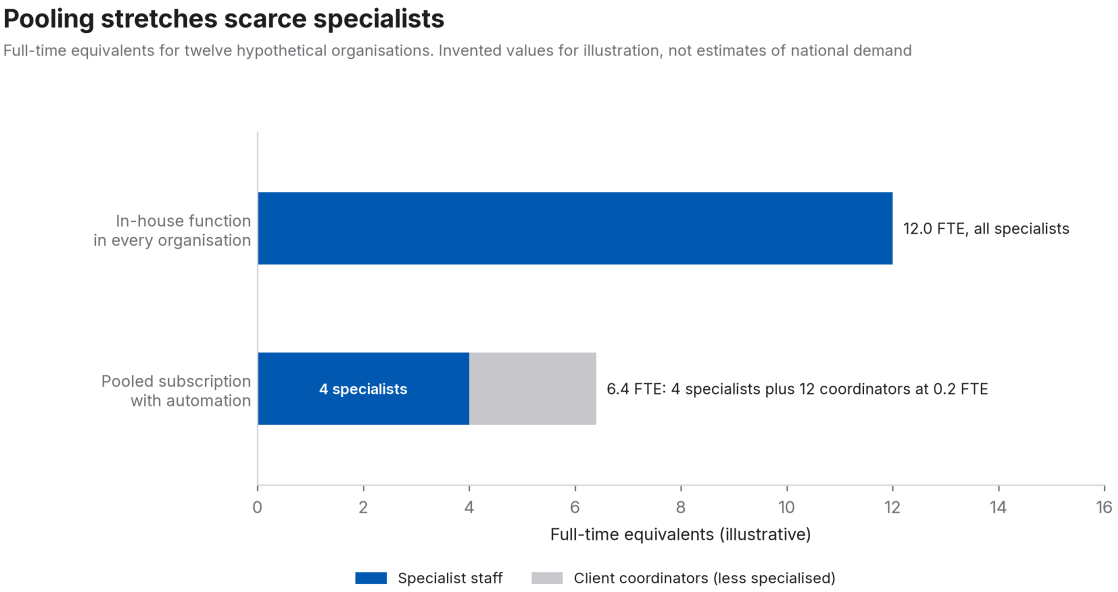

Figure 2. Illustrative full-time staff needed for twelve hypothetical organisations under in-house and pooled models (invented values)

6 Discussion

6.1 Contribution

The anchor studies approach the problem from opposite directions. Alharbi et al. (2021) show that practices requiring expertise, such as inspection teams and recovery planning, reduce harm in Saudi small enterprises, and Reyes et al. (2022) show that a large share of prioritisation can be automated from externally visible data. The present review connects these points through the outsourcing and workforce literature and argues that the decisive question is not whether a service can do vulnerability work, which it plainly can, but whether contracts and client capacity allow that work to reduce exposure. The tiered model and responsibility matrix translate this argument into a form that buyers, providers and regulators can use.

Evidence strength differs across the model. Support is strongest for automated discovery and data-driven prioritisation, which rest on several technical studies with evaluations (Reyes et al., 2022; Zeng et al., 2022, 2024; Le et al., 2023). Evidence on contract design is mixed, because it comes from formal models rather than field studies (Wu et al., 2020, 2021). Evidence that subscription services improve outcomes for Saudi clients is limited, as no study in the sample evaluated such a service directly.

6.2 Implications for buyers, providers and policy

Buyers should subscribe to the tier that matches their capacity to act, not the tier with the most features, and should insist on outcome-based reporting. A firm that cannot deploy fixes gains little from sophisticated ranking. Providers should design contracts that share responsibility for remediation outcomes and should build client coaching into the service, since the client's coordinator is the bottleneck. Policymakers could encourage pooled services for small firms, for example through sector associations, following the association-led model that worked for small Portuguese firms (An-

tunes et al., 2021), and could define a common reporting format linked to the national controls so that service evidence can support compliance reviews.

For workforce planning, the model implies a shift in demand rather than its disappearance. Fewer deep specialists would be needed per organisation, but more coordinators with working knowledge of vulnerability management would be needed in client organisations. Training programmes and competency frameworks should therefore include this coordinating role explicitly, alongside specialist pathways (Almeida, 2025; Alhakami, 2024).

Progress towards 2030 should also be measured in a way that reflects exposure rather than activity. Useful indicators would include the share of small and medium-sized organisations covered by a recognised vulnerability service, the median time to remediate findings in the highest priority class and the number of trained client coordinators. The regulator's existing economic reporting already tracks the workforce and the supply base (Table 1, D2 and D3); adding outcome measures of this kind would show whether pooled services are actually reducing risk rather than simply growing the market.

6.3 Limitations

The review covers thirty English-language journal articles and does not include industry reports, which hold much of the practical evidence on managed services. Several key studies use simulated networks or formal models, and their results may not transfer to Saudi organisations. Saudi evidence in the sample concerns small enterprises, universities and individual awareness, not the public sector or critical infrastructure. The capacity comparison is illustrative and should not be read as an estimate. Future work should evaluate subscription services in Saudi organisations directly, measuring remediation times before and after adoption, and should study how contract terms affect client and provider effort in practice.

7 Conclusion

A subscription service can stretch the Kingdom's scarce cybersecurity specialists further, and it can do so sooner than education alone. Providers are in a strong position to take over the finding and ranking of weaknesses and a good part of the testing, particularly where ranking is automated and sensitive to context (RQ1). Whether that effort lowers risk depends on contracts that reward fixes, on clients defining what matters, on managed service levels and on a client side able to act (RQ2). By 2030 such services could narrow the skills gap materially, but they will not close it, because remediation, asset knowledge and risk acceptance remain client tasks and the pool of specialists still has to grow (RQ3). The practical recommendation is to treat the subscription as a partnership with defined client roles, not as a purchase that transfers the problem.

References

[1] Acartürk, C., Ulubay, M., & Erdur, E. (2021). Continuous improvement on maturity and capability of security operation centres. *IET Information Security*, 15(1), 59–75. https://doi.org/10.1049/ise2.12005

[2] Alhakami, W. (2024). Enhancing cybersecurity competency in the Kingdom of Saudi Arabia: A fuzzy decision-making approach. *Computers*, Materials & Continua, 79(2), 3211–3237. https://doi.org/10.32604/cmc.2023.043935

[3] Alharbi, F., Alsulami, M., AL-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia. *Sensors*, 21(20), Article 6901. https://doi.org/10.3390/s21206901

[4] Alhumud, T. A. A., Omar, A., & Altohami, W. M. (2023). An assessment of cybersecurity performance in the Saudi universities: A total quality management approach. *Cogent Education*, 10(2), Article 2265227. https://doi.org/10.1080/2331186x.2023.2265227

[5] Almeida, F. (2025). Comparative analysis of EU-based cybersecurity skills frameworks. *Computers & Security*, 151, Article 104329. https://doi.org/10.1016/j.cose.2025.104329

[6] Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, 7(1), Article e06016. https://doi.org/10.1016/j.heliyon.2021.e06016

[7] Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, 1(2), 219–238. https://doi.org/10.3390/jcp1020012

[8] Arroyabe, M. F., Arranz, C. F., Fernandez De Arroyabe, I., & Fernandez de Arroyabe, J. C. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society*, 78, Article 102670. https://doi.org/10.1016/j.techsoc.2024.102670

[9] Ashley, T. D., Kwon, R., Gourisetti, S. N. G., Katsis, C., Bonebrake, C. A., & Boyd, P. A. (2022). Gamification of cybersecurity for workforce development in critical infrastructure. *IEEE Access*, 10, 112487–112501. https://doi.org/10.1109/access.2022.3216711

[10] Balsam, A., Walkowski, M., Nowak, M., Oko, J., & Sujecki, S. (2025). Automatic CVSS-based vulnerability prioritization and response with context information and machine learning. *Applied Sciences*, 15(16), Article 8787. https://doi.org/10.3390/app15168787

[11] Blažič, B. J. (2021). The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. *Technology in Society*, 67, Article 101769. https://doi.org/10.1016/j.techsoc.2021.101769

[12] Chen, Z., Kang, F., Xiong, X., & Shu, H. (2024). A survey on penetration path planning in automated penetration testing. *Applied Sciences*, 14(18), Article 8355. https://doi.org/10.3390/app14188355

[13] Dissanayake, N., Zahedi, M., Jayatilaka, A., & Babar, M. A. (2022). Why, how and where of delays in software security patch management: An empirical investigation in the healthcare sector. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2), 1–29. https://doi.org/10.1145/3555087

[14] Dkaidek, Z., & Rashid, A. (2024). Bridging the cybersecurity skills gap: Knowledge framework comparative study. *IEEE Security & Privacy*, 22(5), 88–95. https://doi.org/10.1109/msec.2024.3428892

[15] Fernandez De Arroyabe, I., Arranz, C. F., Arroyabe, M. F., & Fernandez de Arroyabe, J. C. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Computers & Security*, 124, Article 102954. https://doi.org/10.1016/j.cose.2022.102954

[16] Gao, X., & Gong, S. (2022). An economic analysis of information security outsourcing with competitive firms. *Managerial and Decision Economics*, 43(7), 2748–2758. https://doi.org/10.1002/mde.3560

[17] Howland, H. (2023). CVSS: Ubiquitous and broken. *Digital Threats: Research and Practice*, 4(1), 1–12. https://doi.org/10.1145/3491263

[18] Le, T. H. M., Chen, H., & Babar, M. A. (2023). A survey on data-driven software vulnerability assessment and prioritization. *ACM Computing Surveys*, 55(5), 1–39. https://doi.org/10.1145/3529757

[19] Nowak, M. R., Walkowski, M., & Sujecki, S. (2023). Support for the vulnerability management process using conversion CVSS base score 2.0 to 3.x. *Sensors*, 23(4), Article 1802. https://doi.org/10.3390/s23041802

[20] Ramezanian, S., & Niemi, V. (2024). Cybersecurity education in universities: A comprehensive guide to curriculum development. *IEEE Access*, 12, 61741–61766. https://doi.org/10.1109/access.2024.3392970

[21] Rawindaran, N., Jayal, A., & Prakash, E. (2025). Cybersecurity framework: Addressing resiliency in Welsh SMEs for digital transformation and Industry 5.0. *Journal of Cybersecurity and Privacy*, 5(2), Article 17. https://doi.org/10.3390/jcp5020017

[22] Reyes, J., Fuertes, W., Arévalo, P., & Macas, M. (2022). An environment-specific prioritization model for information-security vulnerabilities based on risk factor analysis. *Electronics*, 11(9), Article 1334. https://doi.org/10.3390/electronics11091334

[23] Shah, A., Ganesan, R., Jajodia, S., & Cam, H. (2020). An outsourcing model for alert analysis in a cybersecurity operations center. *ACM Transactions on the Web*, 14(1), 1–22. https://doi.org/10.1145/3372498

[24] Skandylas, C., & Asplund, M. (2025). Automated penetration testing: Formalization and realization. *Computers & Security*, 155, Article 104454. https://doi.org/10.1016/j.cose.2025.104454

[25] Spring, J., Hatleback, E., Householder, A., Manion, A., & Shick, D. (2021). Time to change the CVSS? *IEEE Security & Privacy*, 19(2), 74–78. https://doi.org/10.1109/msec.2020.3044475

[26] Wu, Y., Duan, J., Dai, T., & Cheng, D. (2020). Managing security outsourcing in the presence of strategic hackers. *Decision Analysis*, 17(3), 235–259. https://doi.org/10.1287/deca.2019.0406

[27] Wu, Y., Tayi, G. K., Feng, G., & Fung, R. Y. K. (2021). Managing information security outsourcing in a dynamic cooperation environment. *Journal of the Association for Information Systems*, 22(3), 827–850. https://doi.org/10.17705/1jais.00681

[28] Wu, Y., Wang, N., Dai, T., & Cheng, D. (2025). Information security outsourcing strategies in the supply chain considering security externality. *Journal of the Operational Research Society*, 76(3), 482–497. https://doi.org/10.1080/01605682.2024.2368611

[29] Zeng, Z., Huang, D., Xue, G., Deng, Y., Vadnere, N., & Xie, L. (2024). ILLATION: Improving vulnerability risk prioritization by learning from network. *IEEE Transactions on Dependable and Secure Computing*, 21(4), 1890–1901. https://doi.org/10.1109/tdsc.2023.3294433

[30] Zeng, Z., Yang, Z., Huang, D., & Chung, C.-J. (2022). LICALITY—Likelihood and criticality: Vulnerability risk prioritization through logical reasoning and deep learning. *IEEE Transactions on Network and Service Management*, 19(2), 1746–1760. https://doi.org/10.1109/tnsm.2021.3133811