# Cybersecurity Talent Retention Challenges in the Malaysian Energy Industry: A Qualitative Structured Review

**Faizul Amri Md Yusof[1]* , Norain Ismail[2]**

**Faculty of Technology Management and Technopreneurship, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia**

***Corresponding Author**

**DOI: https://doi.org/10.47772/IJRISS.2026.100700873**

**Received: 02 August 2026; Accepted: 07 August 2026; Published: 14 August 2026**

## ABSTRACT

Malaysia's energy industry is increasingly dependent on connected information technology and operational technology systems, creating greater reliance on a limited and highly specialised cybersecurity workforce. Retaining these professionals remains difficult due to occupational pressure, limited career growth, compensation concerns, inadequate support and competition for scarce skills. Their departure may weaken cyber capability and operational continuity, yet direct evidence from Malaysia's energy industry remains limited. This review identifies the principal challenges affecting cybersecurity talent retention and examines their implications for Malaysian energy organisations. A qualitative structured review with scoping-oriented evidence mapping and thematic synthesis was conducted using 50 sources retained from an initial evidence base of 215 academic publications, professional and institutional reports, and policy documents. The retained sources were organised using a Population–Concept–Context framework and classified according to source type, evidential role and contextual proximity to the Malaysian energy setting. Five interconnected retention challenges were identified: occupational stress, career stagnation, compensation inequity, inadequate organisational support and talent scarcity. The synthesis indicates that workforce scarcity may concentrate responsibilities among a small number of specialists, increase occupational strain and amplify the effects of limited career progression, perceived reward inequity and insufficient organisational support. The review proposes a cyber-talent attrition cycle in which talent scarcity contributes to workload concentration and employment dissatisfaction, leading to turnover, loss of technical capacity and tacit organisational knowledge, and further intensification of workforce scarcity. The findings position cybersecurity retention as an operational-resilience and cyber-risk governance concern rather than solely a human-resource issue. Energy organisations should therefore integrate workload, succession, career development, reward fairness and knowledge-continuity indicators into workforce and cyber-risk management. However, because no direct employee-level study of cybersecurity talent retention in the Malaysian energy industry was identified, the proposed five-challenge framework and attrition cycle require empirical validation.

**Keywords:** cybersecurity talent; employee retention; Malaysian energy industry; occupational stress; talent scarcity

## INTRODUCTION

Energy systems are undergoing rapid digital transformation. Smart grids, cloud platforms, industrial Internet of Things devices, advanced analytics, artificial intelligence and renewable-energy technologies are increasing the connectivity of assets that were previously isolated. Although these developments improve operational visibility, efficiency and decision-making, they also expand the potential attack surface and place cybersecurity at the centre of operational continuity, public safety and national resilience [1–3, 34].

Effective cybersecurity in this environment depends not only on technical controls but also on a stable and capable workforce with knowledge of organisational processes, industrial systems and sector-specific risks. Cybersecurity professionals in energy organisations may be required to operate across both information technology and operational technology environments. Their responsibilities therefore combine information-

security and cybersecurity expertise with an understanding of engineering constraints, legacy infrastructure, safety requirements and continuous operations [4–6]. The loss of experienced personnel may consequently weaken institutional knowledge, incident-response readiness, security governance and operational resilience [15–17, 21, 22].

The global shortage of cybersecurity professionals has made suitably qualified personnel increasingly difficult to recruit and retain. Earlier and more recent workforce studies describe a persistent mismatch between the demand for cybersecurity capability and the supply of appropriately prepared professionals [7–11, 18–20, 48]. In Southeast Asia and Malaysia, digital growth, regulatory development and competition among financial services, telecommunications, technology and critical-infrastructure organisations place additional pressure on the labour market [12–14]. For Malaysian energy organisations, this scarcity may increase workload concentration, occupational pressure and external employment opportunities for existing cybersecurity personnel, thereby heightening retention risks [15–17, 21, 22, 32, 44, 49, 50].

Malaysia's digital-economy development, energy transition and evolving cybersecurity regulation are further increasing demand for specialist capability. The Malaysia Digital Economy Blueprint, Malaysia Cyber Security Strategy 2020–2024 and Cyber Security Act 2024 establish a policy environment in which critical-infrastructure organisations are expected to strengthen cybersecurity governance and resilience [35–37]. Malaysian studies involving technology and highly skilled employees also identify career opportunities, reward fairness, organisational support and employment conditions as relevant to retention [24, 38, 39, 47]. Broader retention research also identifies compensation fairness and supervisor support as relevant considerations [45].

Retention must be distinguished from recruitment. Filling a vacancy does not eliminate workforce risk if experienced employees leave before their system knowledge, professional relationships and incident history are transferred. This risk is especially significant in energy organisations, where cybersecurity personnel may hold tacit knowledge of operational dependencies, legacy systems and compensating controls that cannot be replaced quickly through external recruitment. Research on scarce skills and specialist retention indicates that organisational support, professional embeddedness, career development and advancement opportunities influence whether employees remain or leave [15–17]. Research on perceived organisational support and job embeddedness further explains how supportive employment practices, organisational attachment and professional embeddedness may influence retention [25–31].

Despite the importance of the issue, the relevant evidence remains fragmented across several bodies of literature. Cybersecurity workforce research often concentrates on education, competencies, recruitment and workforce shortages. Prominent workforce studies and frameworks have focused principally on cybersecurity education, competency development, recruitment pipelines and skills shortages [7–14, 18–20, 48]. By comparison, the organisational conditions influencing the continued employment of experienced cybersecurity professionals—including occupational stress, career progression, reward fairness and organisational support—have received less integrated attention, particularly within the Malaysian energy industry [21, 22, 25–28, 32, 49, 50]. General employee-retention research examines compensation, organisational support, engagement and job embeddedness, while energy-sector literature frequently focuses on technical resilience or broader scarce-skills management [1–6, 15–17, 25–31, 34, 43, 45–47]. Relatively few studies integrate these perspectives into a coherent explanation of how occupational, organisational and labour-market pressures jointly influence cybersecurity talent retention in energy and critical-infrastructure settings, particularly within the Malaysian context.

Direct empirical evidence examining cybersecurity professionals employed in Malaysia's energy industry remains limited. Existing cybersecurity-workforce, specialist-retention and energy-sector research has not sufficiently explained how occupational demands, organisational employment conditions and labour-market pressures interact in this setting. This review addresses that gap by integrating multidisciplinary evidence, distinguishing direct findings from transferable evidence and examining five interconnected retention challenges within the Malaysian energy context.

Accordingly, this review aims to identify and synthesise the principal challenges affecting the retention of cybersecurity professionals in energy and critical-infrastructure organisations and to interpret their implications for the Malaysian energy industry. It addresses the following research question:

What challenges affect cybersecurity talent retention in energy and critical-infrastructure organisations, and what are their implications for the Malaysian energy industry?

The review contributes to the literature in three ways. First, it consolidates multidisciplinary evidence from cybersecurity workforce, employee-retention and energy-sector research. Second, it identifies five interconnected retention challenges: occupational stress, career stagnation, compensation inequity, inadequate organisational support and talent scarcity. Third, it proposes a review-derived cyber-talent attrition cycle linking workforce scarcity, workload concentration, occupational strain, reduced organisational commitment, external mobility, turnover, knowledge loss and further scarcity. Through this synthesis, the review connects cybersecurity talent retention with operational resilience, knowledge continuity and critical-infrastructure protection, positioning retention not solely as a human-resource concern but also as a cyber-resilience and operational-risk priority.

## Literature Context

### Cybersecurity Workforce Scarcity and Retention

Cybersecurity workforce research consistently identifies shortages of qualified personnel and persistent gaps between education, job requirements and professional practice [7, 18, 19]. Recent studies indicate that the gap between workforce demand and supply reflects a persistent structural shortage rather than a temporary labour-market imbalance [10, 11, 20]. This shortage is particularly significant among experienced professionals capable of managing complex incidents and coordinating across technical, operational and managerial functions.

Workforce scarcity therefore creates both recruitment and retention challenges, as organisations compete for a limited pool of specialists while placing greater responsibilities on existing personnel. Where demand exceeds supply, cybersecurity professionals have greater access to external opportunities. The departure of experienced personnel may also increase workloads, weaken institutional knowledge and intensify pressure on the remaining workforce. Existing studies indicate that retention is influenced by professional development, organisational conditions, employment expectations, perceived external opportunities and compensation considerations [21, 22]. Workforce scarcity should therefore be understood as both a recruitment and retention problem because employee departures may reinforce the pressures already affecting the remaining workforce.

### Retention in Specialist Technology Work

Specialist-employee retention research consistently identifies career development, reward fairness, organisational support and professional embeddedness as important influences on employees' decisions to remain. Employees are more likely to stay where they perceive credible progression opportunities, recognition of expertise, fair employment conditions and strong organisational fit [17, 23–31]. Conversely, limited advancement, weak support and attractive external alternatives may increase turnover intention.

In cybersecurity roles, organisational attachment may develop through specialist projects, trusted working relationships and familiarity with complex systems. However, isolated teams, contractor-heavy arrangements and weak internal career pathways may reduce these attachment mechanisms. These organisational and professional conditions provide the basis for interpreting career stagnation, compensation inequity and inadequate organisational support in the subsequent analysis.

### Occupational Demands in Cybersecurity Work

Cybersecurity work is characterised by evolving threats, continuous vigilance, unpredictable incidents and accountability for potentially serious failures. These demands may be intensified by limited staffing, restricted budgets and incomplete organisational support, contributing to exhaustion, reduced job satisfaction and turnover

intention [32]. This indicates that occupational stress is not an isolated employee-wellbeing issue; when high job demands are not matched by adequate organisational resources, they may directly weaken retention and reinforce existing workforce shortages.

The Job Demands–Resources model explains that strain becomes more likely when sustained demands, including workload, time pressure, alert volume and incident responsibility, are not balanced by adequate staffing, autonomy, technical resources, recognition and recovery opportunities [33]. In understaffed cybersecurity teams, talent scarcity may therefore increase occupational stress by concentrating critical responsibilities among a limited number of specialists.

### Cybersecurity Work in the Energy Industry

Cybersecurity in the energy industry links digital protection with operational continuity, public safety and potentially significant physical consequences. Information technology and operational technology convergence requires professionals to reconcile different technological lifecycles, operating priorities and risk tolerances [4, 5]. Digital transformation, renewable-energy integration and increased system connectivity further expand this complexity [2, 34]. Thus, energy-sector cybersecurity roles may impose unusually broad technical and operational demands, increasing pressure on a limited specialist workforce and making the retention of experienced personnel especially important for organisational resilience.

These conditions may amplify retention pressures because energy-sector cybersecurity professionals work within continuous operations, legacy infrastructure and high-consequence environments. Their departure may remove system-specific knowledge and weaken incident-response readiness, making workforce instability an operational-resilience concern rather than solely a staffing issue [15, 16].

The findings are interpreted through four complementary perspectives, namely the Job Demands–Resources model, perceived organisational support, social exchange and job embeddedness [25–31, 33, 44]. The relevance of occupational demands and organisational resources to cybersecurity professionals is further supported by research on stress within the cybersecurity profession [32]. Together, these perspectives help explain how occupational demands, organisational resources, employment exchanges and attachment to the organisation may shape employees' decisions to remain or leave. They are applied only after the themes have been developed and are used as interpretive aids rather than as formally tested variables or predetermined categories imposed on the evidence.

## REVIEW METHODOLOGY

### Review Design

This study employed a qualitative, structured and scoping-oriented review design. The approach was selected because the research question spans several evidence domains, including cybersecurity workforce research, employee-retention studies, energy-sector literature, Malaysian policy and labour-market documents, and organisational-behaviour theory. The review aimed to integrate conceptually related but methodologically heterogeneous evidence and to identify recurring retention challenges rather than estimate pooled statistical effects.

The review does not claim exhaustive systematic coverage. Its evidence base was reconstructed retrospectively from an existing collection of 215 academic publications, professional and institutional reports, and policy documents, rather than generated through a prospectively registered and fully reproducible database-search protocol. The retained sources were reassessed against the review objective, research question and eligibility criteria, and presented as a structured qualitative synthesis.

### Population–Concept–Context Framework

The review question and source-selection process were guided by the Population–Concept–Context framework presented in Table 1.

Table 1. Population–Concept–Context framework

| Element | Scope |
|---|---|
| Population | Cybersecurity professionals, information-security specialists, cybersecurity engineers, analysts, managers and comparable specialist technology employees |
| Concept | Challenges affecting employee retention, turnover intention, intention to remain, workforce stability and knowledge continuity |
| Context | Energy, utilities, oil and gas, renewable energy, critical infrastructure and Malaysian high-skilled technology employment |

The population was defined broadly enough to include comparable specialist occupations where direct cybersecurity-retention evidence was limited. The concept focused on occupational, organisational and labour-market conditions that may influence whether professionals remain with or leave an organisation. The primary context was energy and critical infrastructure, while Malaysian technology-workforce evidence was included where it provided relevant contextual insight.

**Evidence Selection**

The initial evidence pool consisted of 215 academic publications, professional and institutional reports, and policy documents covering cybersecurity, employee retention, organisational behaviour, energy and critical infrastructure, and the Malaysian policy and labour-market environment. These sources were retrospectively reassessed against the review objective, research question and predefined source-retention criteria.

Sources were retained according to two complementary sets of source-retention criteria.

Substantive evidence criteria

Sources were retained where they:

1. directly examined cybersecurity workforce retention, turnover intention or intention to remain;
2. addressed one or more of the emerging retention-challenge domains;
3. examined specialist-technology or energy-sector workforce retention; or
4. provided relevant evidence on occupational stress, career development, compensation, organisational support or talent scarcity.

Contextual, theoretical and methodological criteria

Sources were also retained where they:

1. provided relevant Malaysian labour-market, regulatory or critical-infrastructure context;
2. contributed an established theoretical explanation of retention behaviour; or
3. supported the review design, evidence classification or thematic-analysis process.

Sources were not carried forward where they were primarily technical and lacked a workforce connection, duplicated evidence already represented elsewhere, focused exclusively on recruitment without retention relevance, were peripheral to the research question, or did not contribute substantively, contextually, theoretically or methodologically to the review.

All 215 sources were retrospectively reviewed for relevance to the research question and to the substantive, contextual, theoretical and methodological requirements of the review. Sources with a potentially relevant contribution were assessed in greater detail. Retention decisions were recorded according to each source's contribution to the findings, Malaysian or energy-sector context, theoretical interpretation or methodological process. Sources were retained only where their contribution could be clearly linked to one or more of these roles.

Fifty sources were retained for substantive, contextual, theoretical or methodological use. The remaining 165 entries were not incorporated into the present review. Because the initial evidence base had not been created through a prospectively logged screening protocol, these exclusions are not presented as a formal PRISMA screening process. Instead, the figures provide transparent retrospective evidence accounting.

Table 2. Retrospective evidence accounting

| Evidence stage | Number | Interpretation |
|---|---|---|
| Initial evidence base | 215 | Broad multidisciplinary collection of academic publications, professional and institutional reports, and policy documents |
| Sources retained in the manuscript | 50 | Sources used for substantive, contextual, theoretical or methodological purposes |
| Sources not carried forward | 165 | Sources outside the final scope, duplicative in contribution, primarily technical, peripheral to retention or not required for the present review |

The 50 retained sources did not perform identical functions. Peer-reviewed empirical studies and reviews primarily supported substantive findings. Theoretical publications guided interpretation, policy and institutional documents established the Malaysian and sectoral context, and methodological sources supported the review process.

**Data Charting**

A structured charting process was used to organise information from each retained source. The charted fields included:

- author and publication year;
- publication type;
- country or regional relevance;
- sector;
- study design;
- professional or employee group;
- retention issue;
- principal findings;
- energy-sector relevance;
- Malaysian relevance;
- contextual proximity;
- contribution to one or more challenge themes; and
- methodological or interpretive limitations.

The charting process facilitated comparison across sources drawn from different disciplines, sectors and research designs. It also supported the distinction between direct cybersecurity-retention evidence, contextually close evidence and broader transferable specialist-retention evidence. The resulting classifications informed the aggregate evidence characteristics presented in Table 5 and the thematic synthesis reported in the Results.

**Thematic Synthesis**

The thematic synthesis involved five iterative stages: familiarisation with the retained evidence, initial coding, grouping of related codes, development of descriptive categories and consolidation into final challenge themes. Braun and Clarke's guidance on thematic analysis informed the repeated movement between source material, emerging codes and higher-order themes [40, 41].

The synthesis followed a combined deductive–inductive approach. The research question and established retention literature provided an initial analytical direction, while the final themes were refined through repeated comparison with the retained evidence. This process produced five principal challenges: occupational stress, career stagnation, compensation inequity, inadequate organisational support and talent scarcity.

Table 3. Development of codes and final challenge themes

| Illustrative source issue | Initial code | Descriptive category | Final challenge |
|---|---|---|---|
| Persistent vigilance, incident pressure and reduced sleep quality | Emotional exhaustion | Work demands | Occupational Stress |
| Restricted specialist advancement and need to change employers for promotion | Technical career ceiling | Career opportunity | Career Stagnation |
| Perceived internal–external pay gap or inadequate recognition of expertise | Reward unfairness | Employment exchange | Compensation Inequity |
| Responsibility without adequate authority, staffing or leadership support | Support deficit | Organisational conditions | Inadequate Organisational Support |
| Limited workforce supply and aggressive cross-industry recruitment | External labour pull | Labour-market conditions | Talent Scarcity |

Source selection, data charting and initial thematic coding were undertaken primarily by the first author, while the second author provided supervisory and critical review of the thematic structure and manuscript interpretation. The findings were therefore treated as interpretive rather than mechanically reproducible, and repeated comparison between themes and cited sources was used to reduce unsupported interpretation.

**Evidence Strength and Contextual Proximity**

The retained evidence was assessed according to substantive strength and contextual proximity. Peer-reviewed empirical studies and systematic reviews were prioritised for claims concerning retention challenges. Established theories and meta-analyses supported interpretation, while legislation, policy documents and institutional reports established regulatory, sectoral and labour-market context. Professional and commercial commentary was used only as supplementary evidence.

Table 4. Evidence hierarchy used in the review

| Evidence category | Typical source | Primary role | Caution |
|---|---|---|---|
| High substantive strength | Peer-reviewed empirical studies; systematic reviews | Support challenge identification and relationships | Consider study design, sample quality and contextual fit |

| Evidence category | Typical source | Primary role | Caution |
|---|---|---|---|
| High interpretive strength | Established theory, meta-analysis and major conceptual studies | Explain organisational, exchange and embeddedness mechanisms | Does not directly establish effects in Malaysian energy organisations |
| Contextual evidence | Legislation; government policy; institutional reports | Establish regulation, sector conditions and workforce trends | Does not provide employee-level causal evidence |
| Supplementary evidence | Professional or commercial commentary | Illustrate current practice concerns | Used cautiously and not as sole support for a finding |

Contextual proximity was classified into six categories: direct Malaysian energy-sector cybersecurity evidence; Malaysian cybersecurity, technology or related specialist-employment evidence; international energy or critical-infrastructure evidence; general cybersecurity-workforce evidence; general technology or specialist-retention evidence; and theory, methodology, policy or broader contextual evidence.

The classification prevented evidence from adjacent occupations, sectors or countries from being treated as directly equivalent to Malaysian energy-sector evidence. Claims based mainly on transferable sources were therefore expressed cautiously using terms such as “suggests,” “may indicate” and “is likely to be relevant.”

### Review Rigour and Limitations

Review rigour was supported through explicit eligibility criteria, structured data charting, retention of a code-to-theme audit trail and repeated comparison of interpretations with the cited evidence. The review also distinguished direct, contextually close and transferable evidence.

The principal limitations were the retrospective construction of the evidence base, heterogeneity of the retained sources, limited direct Malaysian energy-sector evidence and the potential influence of reviewer judgement. These constraints limit claims of completeness, causality and direct generalisability and are discussed further in the Limitations section.

## RESULTS

### Characteristics of the Evidence Base

The review retained 50 sources published between 1986 and 2025. Based on the source-level classification undertaken during data charting, the evidence base comprised 18 empirical studies, 11 review or meta-analytic publications, nine theoretical or conceptual sources, six policy or institutional documents, four professional or supplementary sources and two methodological publications. Empirical and review studies provided the principal support for the substantive findings, while theoretical publications guided interpretation of organisational support, social exchange, job embeddedness and work-demand mechanisms. Policy and institutional sources were used primarily to establish Malaysian regulatory, sectoral and labour-market conditions.

The contextual proximity of the evidence varied. There is no retained source that directly examined cybersecurity talent retention among employees working specifically in Malaysian energy organisations. Five sources provided Malaysian cybersecurity, technology or related specialist-employment evidence, ten addressed international energy or critical-infrastructure settings, 16 concerned the wider cybersecurity workforce and 13 provided transferable evidence from technology or specialist-retention research. The remaining six sources contributed theory, methodology, policy or broader contextual framing.

Primary challenge coding assigned the greatest number of sources to talent scarcity, followed by inadequate organisational support, career stagnation, occupational stress and compensation inequity. These counts represent each source's principal analytical contribution only. Several sources also supported secondary themes; therefore, the primary classifications should not be interpreted as the total number of sources relevant to each challenge. Occupational stress was informed by a smaller body of directly relevant cybersecurity evidence, whereas career, compensation and organisational-support findings drew more extensively on transferable technology and organisational research.

Table 5. Characteristics of the retained evidence

| Characteristic | Number | Percentage | Interpretation |
|---|---|---|---|
| Total retained sources | 50 | 100.0% | Sources used for substantive, theoretical, contextual or methodological purposes |
| Empirical studies | 18 | 36.0% | Main source of participant- and organisation-level evidence |
| Review and meta-analytic studies | 11 | 22.0% | Synthesised existing cybersecurity and retention evidence |
| Theoretical or conceptual publications | 9 | 18.0% | Supported conceptual interpretation |
| Policy and institutional sources | 6 | 12.0% | Established Malaysian, regulatory and workforce context |
| Professional or supplementary sources | 4 | 8.0% | Provided conference, professional or emerging-practice insight |
| Methodological publications | 2 | 4.0% | Supported thematic synthesis |
| Direct Malaysian energy-sector cybersecurity evidence | 0 | 0.0% | Most directly aligned evidence; no employee-level study was identified |
| Malaysian cybersecurity, technology or related specialist-employment evidence | 5 | 10.0% | Contextually close Malaysian evidence |
| International energy or critical-infrastructure evidence | 10 | 20.0% | Sector-specific transferable evidence |
| General cybersecurity-workforce evidence | 16 | 32.0% | Occupation-specific cybersecurity evidence |
| General technology or specialist-retention evidence | 13 | 26.0% | Transferable technology and specialist-retention evidence |
| Theory, methodology, policy or broader contextual evidence | 6 | 12.0% | Theoretical, methodological and policy support |

Note: Source type and contextual proximity were classified independently. Each source was assigned one primary category within each classification, and each classification therefore totals 50. Primary challenge classifications identify the principal contribution of each source and do not exclude secondary contributions to other themes.

**Overview of the Five Challenges**

The synthesis identified five interconnected retention challenges: occupational stress, career stagnation, compensation inequity, inadequate organisational support and talent scarcity. These operate across employee, organisational and labour-market levels. Scarcity may concentrate responsibilities and increase occupational pressure, while weak career opportunities, reward inequity and inadequate support can reduce employees' willingness to remain. Table 6 summarises the principal indicators, likely retention consequences and relevance to energy organisations.

Table 6. Five cybersecurity talent-retention challenges and their implications

| Challenge | Key indicators | Likely retention consequence | Energy-sector relevance |
|---|---|---|---|
| Occupational Stress | Excessive workload, continuous vigilance, incident pressure, on-call duties and sleep disruption | Burnout, withdrawal and intention to leave | Continuous operations and high-consequence failures intensify pressure |
| Career Stagnation | Restricted specialist progression, weak development pathways and limited internal mobility | External job search to obtain professional advancement | Small OT-security teams may provide few senior specialist roles |
| Compensation Inequity | Below-market pay, salary compression and inadequate recognition of certification, expertise or on-call responsibility | Greater responsiveness to external employment offers | Energy organisations compete with finance, technology, consulting and international employers |
| Inadequate Organisational Support | Insufficient staffing, limited authority, inadequate tools, weak leadership understanding and low recognition | Reduced commitment, weaker organisational attachment and withdrawal | Professionals may remain accountable for risks they lack the authority or resources to address |
| Talent Scarcity | Workforce shortages, prolonged vacancies, aggressive recruitment and key-person dependency | High mobility and repeated knowledge loss | Combined information-technology and operational-technology expertise is difficult and slow to replace |

**Occupational Stress**

Occupational stress emerged as the most immediate employee-level challenge. Cybersecurity professionals operate in an adversarial environment characterised by evolving threats, continuous monitoring requirements, unpredictable incidents and accountability for potentially serious security failures. Singh et al. [32] describe cybersecurity work as involving continuous change, expanding mandates and substantial responsibility. Reeves, Pattinson and Butavicius [49] found meaningful relationships among cybersecurity roles, burnout and sleep quality, while Rangarajan et al. [50] characterise burnout as a socio-technical problem that can weaken workforce effectiveness and continuity.

In energy and critical-infrastructure organisations, these demands may be intensified by the potential consequences of failure. Cyber incidents can disrupt service availability, equipment, public safety and regulatory compliance. Continuous operations may also increase on-call responsibilities and reduce opportunities for recovery.

Occupational stress becomes a retention challenge when sustained job demands are not balanced by adequate organisational resources. High workload does not automatically result in turnover, but prolonged pressure combined with insufficient staffing, limited recovery time, weak supervisory support or inadequate professional control may contribute to emotional exhaustion, reduced job satisfaction and increased openness to alternative employment. In this respect, the evidence is consistent with the Job Demands–Resources model, which suggests that strain intensifies when job demands exceed the resources available to employees [33].

Direct cybersecurity evidence supports the relationship between occupational stress, burnout and workforce continuity. However, the extent to which these relationships operate specifically among Malaysian energy-sector cybersecurity professionals requires empirical investigation.

**Career Stagnation**

Career stagnation refers to the perception that continued employment provides insufficient opportunities for professional growth, advancement or meaningful role development. Cybersecurity professionals invest substantially in technical expertise, certifications and continuous learning. They may therefore expect access to challenging assignments, structured development opportunities and visible progression pathways. Where advancement depends primarily on movement into general management, experienced specialists may feel required to leave technical work or change employers to progress.

Chai and Kim [21] connect cybersecurity career decisions to the wider professional environment, while specialist technology-retention studies identify advancement, skills development and meaningful career opportunity as important reasons for remaining with an organisation [23, 38, 42]. The evidence suggests that employees are more likely to remain where professional development is linked to credible internal progression rather than offered only as a temporary or isolated benefit.

This challenge may be especially relevant in operational-technology cybersecurity. Energy-sector teams may be comparatively small, and organisations may provide only a limited number of senior technical positions. This can create a specialist career ceiling in which the organisation depends heavily on an employee's expertise but does not provide an equivalent route to greater status, responsibility or reward.

Professional development may also generate a development–mobility paradox. Training and certification strengthen organisational capability and can signal support, but they also increase the employee's market value and external employability. Development is therefore more likely to support retention when accompanied by internal career opportunities, recognition, role enrichment and appropriate rewards. Evidence concerning this challenge is drawn mainly from cybersecurity-career studies and transferable technology-retention research rather than direct Malaysian energy-sector studies.

**Compensation Inequity**

Compensation inequity concerns employees' perceptions that their expertise, responsibilities or contribution are not recognised fairly through financial and non-financial rewards. The issue is broader than absolute salary. Employees may compare their remuneration with that of colleagues, recently recruited employees, market benchmarks, competitors and international opportunities. They may also consider whether certification costs, specialist expertise, on-call duties and high-consequence responsibilities are recognised appropriately.

Retention literature consistently identifies reward fairness as an important influence on employee decisions [43–46]. Malaysian technology-sector research similarly indicates that remuneration forms part of a broader combination of factors shaping retention [38]. In a labour market characterised by persistent cybersecurity demand, perceived internal–external pay gaps can make employees more receptive to alternative employment.

Cybersecurity workforce scarcity may also create salary compression. Long-serving employees may receive only slightly higher remuneration than newly recruited specialists, even though they possess greater organisational and system-specific knowledge. Energy-sector professionals may additionally perceive that operational-technology expertise, critical-infrastructure accountability or out-of-hours responsibilities are insufficiently reflected in their reward arrangements.

Compensation inequity interacts with career stagnation and organisational support. Employees may accept moderate remuneration where they experience strong professional growth, meaningful work and credible organisational recognition. However, where limited progression and weak support accompany perceived reward unfairness, external offers may become more attractive. Compensation should therefore be interpreted as part of the broader employment exchange rather than as an isolated cause of turnover.

### Inadequate Organisational Support

Inadequate organisational support describes an employment environment in which cybersecurity professionals perceive that their contribution, well-being or operational requirements receive insufficient attention. Perceived organisational support research shows that employees form beliefs about whether their organisation values their contribution and provides the resources and treatment necessary for them to perform effectively [25–28]. Malaysian research involving government-linked companies and the oil and gas sector also identifies organisational support as relevant to talent retention [39, 47].

Within cybersecurity teams, inadequate support may be experienced through insufficient staffing, delayed investment, inadequate tools, limited access to training, weak leadership understanding, low recognition of preventive work or accountability without corresponding authority. Professionals may identify serious vulnerabilities but lack the budget, operational influence or decision rights necessary to resolve them. This creates an accountability–support imbalance in which employees remain responsible for preventing failure despite having incomplete control over the conditions that produce risk.

Inadequate organisational support may also weaken job embeddedness. Employees are less likely to develop strong organisational attachment when cybersecurity functions are isolated from strategic decision-making, treated primarily as a cost or blamed following incidents. Conversely, visible executive sponsorship, professional autonomy, meaningful employee participation and cross-functional inclusion may strengthen employees' fit with the organisation and increase the perceived sacrifice associated with leaving.

The evidence supporting this challenge is derived primarily from organisational-support theory, general retention studies and contextually relevant Malaysian employment research. Its specific operation within Malaysian energy cybersecurity teams remains to be tested directly.

### Talent Scarcity

Talent scarcity operates both as an external labour-market condition and as an internal source of work pressure. Cybersecurity workforce studies consistently report that the supply of suitably qualified professionals remains insufficient relative to organisational demand [7–11, 48]. Regional studies indicate that organisations across Southeast Asia face similar constraints as digitalisation increases demand for advanced cybersecurity capability [12, 14].

For Malaysian energy organisations, talent scarcity may be intensified by competition with financial services, telecommunications, technology companies, consulting firms and international employers. Remote-working arrangements and cross-border employment can further expand the range of opportunities available to experienced professionals. The relevant cybersecurity labour market is therefore increasingly international, which may reduce the usefulness of comparing remuneration and career conditions only with other domestic energy organisations.

Scarcity may also create key-person dependency. When a small number of specialists understand legacy infrastructure, operational dependencies and previous incidents, their departure removes both technical capacity and tacit knowledge. Remaining employees may then absorb additional monitoring, response, project and compliance responsibilities.

Talent scarcity therefore operates as both a labour-market condition and an outcome of turnover. Limited workforce supply increases pressure on existing personnel, while employee departure further reduces capability and intensifies workload. This reciprocal relationship underpins the cyber-talent attrition cycle developed in the Discussion.

## DISCUSSION

The review identifies five interconnected challenges affecting cybersecurity talent retention in energy and critical-infrastructure organisations: occupational stress, career stagnation, compensation inequity, inadequate

organisational support and talent scarcity. Together, these challenges show that retention is shaped by the interaction of demanding work conditions, internal employment arrangements and external labour-market opportunities.

Cybersecurity studies provide the most direct support for occupational stress and talent scarcity, while career, compensation and support findings draw partly on transferable technology and organisational research. The resulting framework is therefore evidence-informed but requires direct validation among cybersecurity professionals in Malaysia's energy industry.

**Cyber-Talent Attrition Cycle**

The central analytical contribution of the review is the proposed cyber-talent attrition cycle. The cycle integrates the five challenges into a mutually reinforcing workforce-risk process rather than treating them as independent causes of turnover. It is presented as a review-derived analytical framework and not as a causal model tested within a single empirical study.

The cycle may begin with talent scarcity, which can leave cybersecurity teams understaffed and prolong vacancies. When available work is concentrated among a limited number of experienced employees, monitoring, incident response, compliance, project and on-call responsibilities increase. Sustained workload concentration may contribute to occupational stress, reduced recovery and emotional exhaustion.

Where these pressures occur alongside restricted career progression, perceived compensation inequity or inadequate organisational support, employees may experience weaker organisational attachment and reduced reasons to remain. Strong external demand can then convert dissatisfaction into mobility by providing accessible opportunities in competing sectors, international organisations or remote roles. Employee departure subsequently removes both technical capacity and tacit organisational knowledge. Remaining employees absorb additional responsibilities, increasing key-person dependency, workload concentration and the possibility of further turnover.

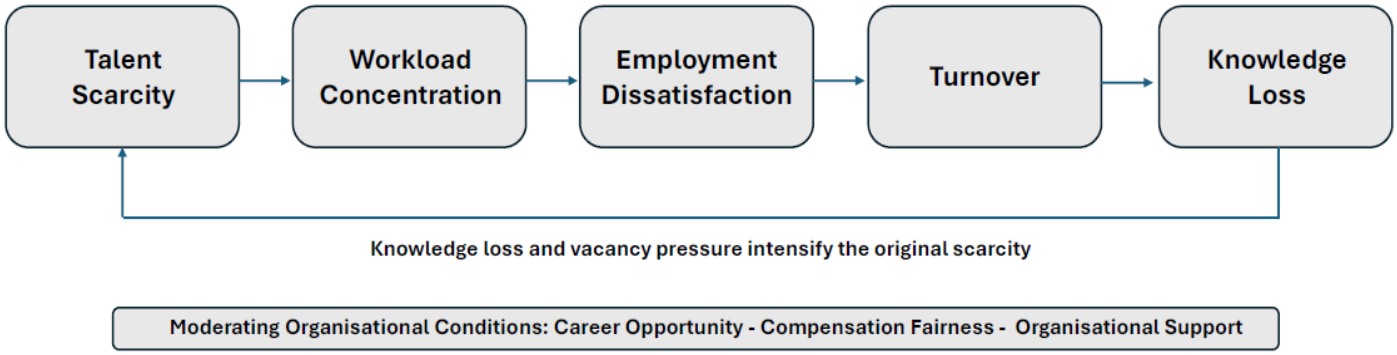


Figure 1. Proposed cyber-talent attrition cycle.

Note: The cycle is a review-derived analytical synthesis and has not yet been empirically validated within the Malaysian energy industry.

Table 7. Mechanisms in the cyber-talent attrition cycle

| Stage | Mechanism | Organisational consequence |
|---|---|---|
| 1. Talent scarcity | Insufficient supply and prolonged vacancies | Work is concentrated among existing specialists |
| 2. Workload concentration | More monitoring, incidents, projects and compliance per employee | Occupational stress and reduced recovery |

| Stage | Mechanism | Organisational consequence |
|---|---|---|
| 3. Employment dissatisfaction | Career, reward and support expectations are not met | Lower commitment and greater openness to offers |
| 4. Turnover | Employees move to competitors or international roles | Vacancy and loss of tacit system knowledge |
| 5. Knowledge loss | Remaining staff absorb undocumented responsibilities | Greater scarcity, key-person risk and operational vulnerability |

Note: The stages represent a review-derived analytical synthesis.

**Theoretical Interpretation**

The cyber-talent attrition cycle integrates four complementary theoretical perspectives. First, the Job Demands–Resources model explains how talent scarcity and workload concentration may produce occupational strain when staffing, autonomy, recovery time and managerial support are insufficient [33]. Under this perspective, persistent demands may contribute to exhaustion when employees do not have adequate organisational resources to manage them.

Second, perceived organisational support explains how employees assess whether the organisation values their contribution, recognises their expertise and responds to their professional and well-being needs [25–27]. Where cybersecurity professionals perceive strong organisational support, they may develop greater commitment and stronger reasons to remain. Conversely, inadequate resources, weak recognition and limited managerial attention may encourage withdrawal.

Third, social exchange theory provides a basis for understanding how reward fairness, career investment and organisational treatment influence employee reciprocity [28, 44]. Employees who perceive a balanced employment exchange may respond through stronger commitment and continued membership, whereas persistent imbalance may increase openness to external employment.

Fourth, job embeddedness explains how organisational fit, professional relationships and the perceived sacrifices associated with departure influence retention [29–31]. Cybersecurity professionals may become embedded through trusted working relationships, specialist projects and familiarity with complex systems. However, weak internal career opportunities or limited organisational attachment may reduce the perceived cost of leaving.

Together, these perspectives indicate that cybersecurity turnover is unlikely to result from a single condition. Instead, it may arise through the interaction of excessive work demands, insufficient organisational resources, perceived employment-exchange imbalance and weakened organisational embeddedness. The cyber-talent attrition cycle therefore connects external workforce scarcity with internal employment conditions and explains how turnover may reinforce future workload and capability risks.

**Distinctiveness of the Malaysian Energy Industry**

The Malaysian energy context gives the five challenges a distinctive configuration. First, digital transformation, renewable-energy integration and increasing system connectivity expand the range of information technology and operational technology assets requiring protection. Second, critical-infrastructure regulation increases governance, reporting and capability expectations. Third, experienced cybersecurity professionals may move to financial services, telecommunications, consulting or technology organisations with more mature cybersecurity functions, flexible work arrangements or stronger reward structures. Fourth, combined IT–OT expertise is scarce and highly context-dependent, making replacement slower and more difficult than conventional vacancy measures may suggest.

Workforce instability in this environment may produce consequences beyond recruitment cost. Employee departure can weaken monitoring continuity, incident-response readiness, control ownership and knowledge

transfer, particularly where only a small number of employees understand legacy systems and operational dependencies.

These findings imply that cybersecurity retention should not be treated solely as an employee-engagement or human-resource performance issue. It should also be incorporated into cyber-risk governance, operational-resilience planning and critical-knowledge management. General retention programmes may be insufficient where they do not address the specialist demands, responsibilities and career expectations associated with cybersecurity work.

The review extends existing retention research by connecting employee departure with cybersecurity capability and operational resilience. Its principal contribution is not the identification of individual retention factors, which are established in the wider literature, but their integration into a cyclical explanation of workforce risk.

The proposed cyber-talent attrition cycle shows how scarcity may increase workload, how organisational deficiencies can convert pressure into turnover, and how turnover can remove tacit knowledge and further intensify scarcity. This positions retention as a mechanism affecting organisational capability rather than solely as an employee or human-resource outcome.

**Organisational Opportunities**

The findings indicate several opportunities for energy organisations to strengthen cybersecurity workforce stability. These opportunities correspond directly to the five identified challenges and should be implemented as an integrated retention approach rather than as isolated initiatives.

Table 8. Organisational opportunities corresponding to the five challenges

| Challenge | Organisational opportunity | Illustrative actions |
|---|---|---|
| Occupational stress | Reduce unmanaged job demands | Staffing reviews; sustainable on-call rosters; post-incident recovery; workload monitoring; access to confidential support |
| Career stagnation | Create credible specialist careers | Dual technical-managerial ladders; OT-security competencies; mentoring; role rotations; promotion criteria linked to expertise |
| Compensation inequity | Improve reward fairness | Market benchmarking; specialist allowances; certification recognition; transparent grades; on-call compensation |
| Inadequate organisational support | Strengthen support and authority | Board visibility; adequate tools and budget; employee participation; recognition of prevention; clear decision rights |
| Talent scarcity | Build capacity and knowledge continuity | Graduate pipelines; apprenticeships; university partnerships; succession plans; documentation; role shadowing; communities of practice |

These opportunities should be interpreted as evidence-informed responses rather than proven interventions. Direct evaluations within Malaysia's energy industry remain limited, and organisations should therefore monitor whether their initiatives produce measurable improvements.

Relevant indicators may include:

- voluntary turnover;
- vacancy duration;
- unplanned overtime;
- on-call frequency;

- internal promotion rates;
- training and certification utilisation;
- employee perceptions of support and reward fairness;
- succession-plan coverage; and
- concentration of critical knowledge among individual employees.

Monitoring these indicators would allow organisations to assess whether retention initiatives are reducing workforce risk rather than merely increasing programme activity.

**Practical And Policy Implications**

Energy organisations should incorporate cybersecurity workforce stability into cyber-risk governance and operational-resilience reporting. Indicators such as turnover, vacancy duration, overtime, succession coverage and concentration of critical knowledge can provide early warning of capability risk. Workforce capacity should also be considered when approving digital-transformation, cloud, renewable-energy and IT–OT programmes.

Human-resource and cybersecurity leaders should jointly design specialist career pathways, reward structures, development arrangements, workload controls and succession plans. Cybersecurity leaders can define technical role requirements and operational criticality, while HR functions can support consistent workforce planning, progression and compensation practices.

At policy level, technical cybersecurity regulation should be supported by workforce-development and retention initiatives. Universities, employers, professional bodies and government agencies should collaborate on energy-specific cybersecurity education, operational-technology training, apprenticeships, professional pathways and mid-career conversion. The success of these initiatives should be assessed through capability, progression and retention outcomes rather than training participation alone.

**Future Research**

Future research should collect primary evidence from cybersecurity professionals employed in Malaysian electricity, oil and gas, renewable-energy, utility and other critical-infrastructure organisations. Semi-structured interviews could examine how the five challenges are experienced across career stages, organisational types and technical roles. Such research could also identify retention factors that may not be visible in the existing international and cross-sector literature.

Quantitative studies could test the relative influence of occupational stress, career opportunity, compensation fairness, organisational support and external labour-market demand on intention to remain and actual turnover. The proposed cyber-talent attrition cycle could be tested using longitudinal or structural models that examine whether talent scarcity increases workload and whether workload, organisational conditions and external opportunities subsequently influence employee departure.

Comparative research is also needed across:

- information-technology and operational-technology cybersecurity roles;
- government-linked and private-sector organisations;
- permanent employees and contractors;
- early-career and experienced professionals;
- Malaysian and other ASEAN energy organisations; and
- different energy subsectors.

Longitudinal studies should evaluate whether specialist career ladders, workload controls, compensation changes, succession arrangements and supervisor-support interventions produce sustained retention improvements. A further priority is to investigate whether turnover is associated with cyber-resilience outcomes such as incident-response speed, audit findings, control continuity, recovery performance and knowledge-transfer effectiveness.

### Limitations

This review was reconstructed retrospectively from an existing evidence base of 215 academic publications, professional and institutional reports, and policy documents rather than generated through a newly executed and fully reproducible database search. It therefore cannot claim exhaustive coverage of all relevant studies.

Direct empirical evidence concerning cybersecurity talent retention in Malaysia's energy industry was limited. Several findings were consequently informed by Malaysian technology-sector studies, international cybersecurity research and broader specialist-retention literature. Although contextual proximity was considered, evidence transferred from adjacent settings may not fully reflect the experiences of Malaysian energy-sector professionals.

The retained sources also varied in design and methodological strength. Policy, institutional and professional materials were used primarily for context, while substantive findings were based mainly on empirical and review evidence.

Finally, source selection and thematic coding involved researcher judgement, and the proposed attrition cycle has not been empirically validated. The framework should therefore be treated as a foundation for future investigation rather than a confirmed causal model.

## CONCLUSION

This review identified five interconnected challenges affecting cybersecurity talent retention in energy and critical-infrastructure organisations: occupational stress, career stagnation, compensation inequity, inadequate organisational support and talent scarcity. Together, they show that workforce stability is shaped by the interaction of job demands, organisational conditions and external labour-market pressures.

The review proposes a cyber-talent attrition cycle in which scarcity concentrates responsibilities, increases occupational strain and, when combined with weak career opportunities, reward inequity or inadequate support, contributes to turnover. Employee departure can then remove technical capacity and tacit organisational knowledge, placing further pressure on the remaining workforce.

For energy organisations, cybersecurity retention should therefore be treated as a cyber-risk, operational-resilience and knowledge-continuity issue rather than solely as a human-resource concern. Malaysian energy organisations should prioritise sustainable workloads, specialist career pathways, fair rewards, organisational support, succession planning and knowledge-transfer arrangements.

Because no direct employee-level study of cybersecurity talent retention in the Malaysian energy industry was identified, the five-challenge framework and proposed attrition cycle require empirical validation.

## ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to Universiti Teknikal Malaysia Melaka (UTeM) for supporting this study.

### Author Contributions

Faizul Amri Md Yusof: Conceptualisation, evidence selection, data charting, thematic analysis, writing—original draft, and manuscript revision. Norain Ismail: Methodological guidance, critical review, and manuscript revision. Both authors reviewed and approved the final manuscript.

### Funding Declaration

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

**Conflict Of Interest**

The authors declare that they have no conflict of interest.

**Ethical Considerations**

The data supporting this study were derived from documentary sources comprising academic publications, professional and institutional reports, and policy documents.

**Data Availability**

The aggregate evidence classifications supporting this review are presented in the manuscript. Additional working materials used for data charting and thematic synthesis are available from the corresponding author upon reasonable request.

# REFERENCES

1. Wallis, T., Paul, G. and Irvine, J. (2022). Organisational contexts of energy cybersecurity. In Computer Security: ESORICS 2021 International Workshops (Lecture Notes in Computer Science, Vol. 13106, pp. 384–402). Springer. https://doi.org/10.1007/978-3-030-95484-0_22
2. Saeed, S., Gull, H., Aldossary, M. M., Altamimi, A. F., Alshahrani, M. S., Saqib, M., Zafar Iqbal, S. and Almuhaideb, A. M. (2024). Digital transformation in energy sector: Cybersecurity challenges and implications. Information, 15(12), Article 764. https://doi.org/10.3390/info15120764
3. Venkatachary, S. K., Prasad, J., Alagappan, A., Andrews, L. J. B., Raj, R. A. and Duraisamy, S. (2024). Cybersecurity and cyber-terrorism challenges to energy-related infrastructures: Cybersecurity frameworks and economics—Comprehensive review. International Journal of Critical Infrastructure Protection, 45, Article 100677. https://doi.org/10.1016/j.ijcip.2024.100677
4. Murray, G., Johnstone, M. N. and Valli, C. (2017). The convergence of IT and OT in critical infrastructure. In C. Valli (Ed.), Proceedings of the 15th Australian Information Security Management Conference (pp. 149–155). Edith Cowan University. https://doi.org/10.4225/75/5a84f7b595b4e
5. Moussamir, M. and Dolezilek, D. (2013). The demands and implications of IT and OT collaboration. In PAC World Africa Conference Proceedings. Schweitzer Engineering Laboratories.
6. Siemers, B., Attarha, S., Kamsamrong, J., Brand, M., Valliou, M., Pirta-Dreimane, R., Grabis, J., Kunicina, N., Mekkanen, M., Vartiainen, T. and Lehnhoff, S. (2021). Modern trends and skill gaps of cyber security in smart grid: Invited paper. In IEEE EUROCON 2021—19th International Conference on Smart Technologies (pp. 565–570). IEEE. https://doi.org/10.1109/EUROCON52738.2021.9535632
7. Assante, M. J. and Tobey, D. H. (2011). Enhancing the cybersecurity workforce. IT Professional, 13(1), 12–15. https://doi.org/10.1109/MITP.2011.6
8. Crumpler, W. and Lewis, J. A. (2019). The cybersecurity workforce gap. Center for Strategic and International Studies. https://www.csis.org/analysis/cybersecurity-workforce-gap
9. Burrell, D. N. (2020). An exploration of the cybersecurity workforce shortage. In Information Resources Management Association (Ed.), Cyber warfare and terrorism: Concepts, methodologies, tools, and applications (pp. 1072–1081). IGI Global. https://doi.org/10.4018/978-1-7998-2466-4.ch063
10. Jerman Blažič, B. (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
11. ISC2. (2024). 2024 ISC2 Cybersecurity Workforce Study. ISC2. https://www.isc2.org/research
12. Dillon, R. and Tan, K.-L. (2024). Cybersecurity workforce landscape, education, and industry growth prospects in Southeast Asia. Journal of Tropical Futures, 1(2), 172–181. https://doi.org/10.1177/27538931231176903
13. PIKOM. (2024). Growing threat: Cybersecurity landscape in Malaysia 2024. PIKOM. https://pikom.org.my/2024/FOCS/PIKOM_Cybersecurity_Report.pdf
14. Gerth, F., Tan, A. W. K., Kwa, P. T. H. and Roche, O. P. (2025). Cybersecurity job requirements in Asian countries: An analysis of workforce trends and future implications. Journal of Applied Economic Sciences, 20(2/88), 192–206. https://doi.org/10.57017/jaes.v20.2(88).02

15. Mabuza, P. F. and Gerwel Proches, C. N. (2014). Retaining core, critical and scarce skills in the energy industry. The Indian Journal of Industrial Relations, 49(4), 635–648.
16. Steiner, S., Cropley, M., Simonds, L. and Heron, R. (2020). Reasons for staying with your employer: Identifying the key organizational predictors of employee retention within a global energy business. Journal of Occupational and Environmental Medicine, 62(4), 289–295. https://doi.org/10.1097/JOM.0000000000001820
17. Živković, A., Pap Vorkapić, A. and Franjković, J. (2024). Charting a path to sustainable workforce: Exploring influential factors behind employee turnover intentions in the energy industry. Sustainability, 16(19), Article 8511. https://doi.org/10.3390/su16198511
18. Dodge, R. C., Toregas, C. and Hoffman, L. J. (2012). Cybersecurity workforce development directions. In N. Clarke and S. Furnell (Eds.), Proceedings of the Sixth International Symposium on Human Aspects of Information Security and Assurance (HAISA 2012) (pp. 1–12). University of Plymouth.
19. Caulkins, B., Marlowe, T. and Reardon, A. (2019). Cybersecurity skills to address today's threats. In T. Z. Ahram and D. Nicholson (Eds.), Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity (pp. 187–192). Springer. https://doi.org/10.1007/978-3-319-94782-2_18
20. Davies, G., Mison, A. and Eden, P. (2022). Addressing the skills shortage in cybersecurity. Proceedings of the 17th International Conference on Cyber Warfare and Security, 17(1), 544–551. https://doi.org/10.34190/iccws.17.1.69
21. Chai, S.-M. and Kim, M.-K. (2012). A road to retain cybersecurity professionals: An examination of career decisions among cybersecurity scholars. Journal of the Korea Institute of Information Security & Cryptology, 22(2), 295–316. https://doi.org/10.13089/JKIISC.2012.22.2.295
22. Ishmael, A. and Halawi, L. (2023). Retention of qualified cybersecurity professionals: A qualitative study. Journal of Computer Information Systems, 63(1), 204–215. https://doi.org/10.1080/08874417.2022.2049018
23. Thomas, S. J. (2015). Exploring strategies for retaining information technology professionals: A case study [Doctoral dissertation, Walden University]. Walden Dissertations and Doctoral Studies, 219.
24. Teoh, W. M. Y., Yuen, Y. Y., Chong, S. C. and Chong, C. W. (2024). Talent retention for sustainable high-skilled employment in information and communication industry. Journal of Infrastructure, Policy and Development, 8(15), Article 9710. https://doi.org/10.24294/jipd9710
25. Eisenberger, R., Huntington, R., Hutchison, S. and Sowa, D. (1986). Perceived organizational support. Journal of Applied Psychology, 71(3), 500–507. https://doi.org/10.1037/0021-9010.71.3.500
26. Rhoades, L. and Eisenberger, R. (2002). Perceived organizational support: A review of the literature. Journal of Applied Psychology, 87(4), 698–714. https://doi.org/10.1037/0021-9010.87.4.698
27. Kurtessis, J. N., Eisenberger, R., Ford, M. T., Buffardi, L. C., Stewart, K. A. and Adis, C. S. (2017). Perceived organizational support: A meta-analytic evaluation of organizational support theory. Journal of Management, 43(6), 1854–1884. https://doi.org/10.1177/0149206315575554
28. Allen, D. G., Shore, L. M. and Griffeth, R. W. (2003). The role of perceived organizational support and supportive human resource practices in the turnover process. Journal of Management, 29(1), 99–118. https://doi.org/10.1177/014920630302900107
29. Mitchell, T. R., Holtom, B. C., Lee, T. W., Sablynski, C. J. and Erez, M. (2001). Why people stay: Using job embeddedness to predict voluntary turnover. Academy of Management Journal, 44(6), 1102–1121. https://doi.org/10.5465/3069391
30. Lim, G. M. and Wong, S. F. (2009). Understanding retention of IT professionals in vendor organizations: A job embeddedness model. Journal of Outsourcing and Organizational Information Management, 2009, Article 102112.
31. Zhang, M., Fried, D. D. and Griffeth, R. W. (2012). A review of job embeddedness: Conceptual, measurement issues, and directions for future research. Human Resource Management Review, 22(3), 220–231. https://doi.org/10.1016/j.hrmr.2012.02.004
32. Singh, T., Johnston, A. C., D'Arcy, J. and Harms, P. D. (2023). Stress in the cybersecurity profession: A systematic review of related literature and opportunities for future research. Organizational Cybersecurity Journal: Practice, Process and People, 3(2), 100–126. https://doi.org/10.1108/OCJ-06-2022-0012
33. Bakker, A. B. and Demerouti, E. (2007). The Job Demands–Resources model: State of the art. Journal of Managerial Psychology, 22(3), 309–328. https://doi.org/10.1108/02683940710733115

34. Kumar, K., Pandey, N. K., Verre, F. and Shah, R. (2025). Cybersecurity challenges in the digitization and integration of renewable energy systems: A review. IEEE Transactions on Engineering Management, 72, 3042–3054. https://doi.org/10.1109/TEM.2025.3586557
35. Economic Planning Unit, Prime Minister's Department. (2021). Malaysia Digital Economy Blueprint. Government of Malaysia. https://www.mydigital.gov.my/wp-content/uploads/2023/08/Malaysia-Digital-Economy-Blueprint_ENG.pdf
36. National Cyber Security Agency. (2020). Malaysia Cyber Security Strategy 2020–2024. National Security Council, Prime Minister's Department, Government of Malaysia.
37. Malaysia. (2024). Cyber Security Act 2024 (Act 854). Commissioner of Law Revision, Malaysia. https://lom.agc.gov.my/ilims/upload/portal/akta/outputaktap/2177706_BI/Act%20854.pdf
38. Ramachandaran, S. D., Vasudevan, A., Sagadavan, R., John, S. and Onn, T. Y. (2024). The determinants of talent retention in the information technology services sector in Malaysia. International Journal of Management and Sustainability, 13(2), 283–298. https://doi.org/10.18488/11.v13i2.3656
39. Isa, A., Ibrahim, H. I., Rafidi, M. M., Khalid, N. H., Gopal, V., Haque, R. and Qazi, S. (2025). The effect of perceived organizational support on retention of talent at Government-Linked Companies (GLCs). Journal of Cultural Analysis and Social Change, 10(3), 2272–2280. https://doi.org/10.64753/jcasc.v10i3.2742
40. Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
41. Braun, V. and Clarke, V. (2021). One size fits all? What counts as quality practice in (reflexive) thematic analysis? Qualitative Research in Psychology, 18(3), 328–352. https://doi.org/10.1080/14780887.2020.1769238
42. Costa, L. A., Dias, E., Ribeiro, D., Fontão, A., Pinto, G., Pereira dos Santos, R. and Serebrenik, A. (2024). An actionable framework for understanding and improving talent retention as a competitive advantage in IT organizations. In Proceedings of the 2024 IEEE/ACM 46th International Conference on Software Engineering: Companion Proceedings (ICSE-Companion '24) (pp. 290–291). Association for Computing Machinery. https://doi.org/10.1145/3639478.3643073
43. Kossivi, B., Xu, M. and Kalgora, B. (2016). Study on determining factors of employee retention. Open Journal of Social Sciences, 4(5), 261–268. https://doi.org/10.4236/jss.2016.45029
44. Harden, G., Boakye, K. G. and Ryan, S. D. (2018). Turnover intention of technology professionals: A social exchange theory perspective. Journal of Computer Information Systems, 58(4), 291–300. https://doi.org/10.1080/08874417.2016.1236356
45. Oladimeji, K. A. (2024). Applying organizational support lenses for employee retention: The role of supervisor support and compensation fairness. Journal of Technology Management and Business, 11(1), 98–110.
46. Krishna Prakash, M., Vijay Raja, R. and Vishnu Kumar, S. (2025). Factors influencing employee retention in the IT sector: A comprehensive review of recognition, compensation, work environment, and job autonomy. Asian Journal of Interdisciplinary Research, 8(2), 56–88. https://doi.org/10.54392/ajir2524
47. Salleh, R., Khalid Ali, K., Kumar, V., Abd Razak, S. N. and Khan, M. L. (2023). Perceived organizational support and talent retention of women engineers in the Malaysian oil and gas sector: A conceptual framework. Journal of Hunan University Natural Sciences, 50(1), 186–197. https://doi.org/10.55463/issn.1674-2974.50.1.19
48. Tomić Rotim, S. and Komnenić, V. (2020). Cybersecurity talent shortage. Annals of Disaster Risk Sciences, 3(2). https://doi.org/10.51381/adrs.v3i2.26
49. Reeves, A., Pattinson, M. and Butavicius, M. (2024). The sleepless sentinel: Factors that predict burnout and sleep quality in cybersecurity professionals. Information and Computer Security, 32(4), 477–491. https://doi.org/10.1108/ICS-11-2023-0222
50. Rangarajan, A., Nobles, C., Dykstra, J., Cunningham, M., Robinson, N., Hollis, T., Paul, C. L. and Gulotta, C. (2025). A roadmap to address burnout in the cybersecurity profession: Outcomes from a multifaceted workshop. In A. Moallem (Ed.), HCI for Cybersecurity, Privacy and Trust: Proceedings of HCI-CPT 2025 (Lecture Notes in Computer Science, Vol. 15814, pp. 125–140). Springer. https://doi.org/10.1007/978-3-031-92833-8_8