

Article

AI-Supported Dynamic Cyber Risk Assessment for Cyber Situational Awareness: A Cross-Sectional Survey

Mansour Almalki , Liqaa Nawaf  and Fiona Carroll 

School of Technologies, Cardiff Metropolitan University, Western Ave, Cardiff CF5 2YB, UK;
llnawaf@cardiffmet.ac.uk (L.N.); fcarroll@cardiffmet.ac.uk (F.C.)

* Correspondence: m.h.z.almalki@outlook.cardiffmet.ac.uk

Abstract

Small and medium-sized enterprises (SMEs) have limited resources and governance that might restrict their ability to conduct dynamic cyber risk assessment (DCRA) and maintain effective cyber situational awareness (CSA). This study investigates stakeholders' perceptions of CSA, DCRA, and AI-enabled cybersecurity to develop a conceptual framework targeted for SMEs. The online survey was cross-sectional, and 302 completed responses were gathered. The valid sample size for the items ranged from 288 to 299. Out of 293 respondents, 54 (18.4%) indicated prior usage of CSA techniques, 21 (7.2%) reported prior use of DCRA tools, and 226 (77.1%) backed AI in the cybersecurity field. The highest rated DCRA requirements were continuous threat updates, identification of attacks and vulnerabilities, and prioritization of alerts based on risk. The highest rated implementation challenges were accuracy, relevance, and integration with current infrastructure. Four multi-item measures had good-to-outstanding internal consistency ($\alpha = 0.868\text{--}0.926$; $\omega = 0.870\text{--}0.929$), and parallel analysis supported a single factor for each. Exploratory findings suggested that Information Technology (IT) and cybersecurity professionals had greater familiarity with CSA and DCRA than did leaders and managers. There was a moderate-to-strong positive association between familiarity with CSA and DCRA ($\rho = .54$). The framework defines AI as a layer of analytical decision support, DCRA as the process of translating changing evidence into updated and prioritized risk information, and CSA as decision-relevant interpretation and use of that information. This framework will help SMEs to improve CSA and will help their leaders to make the right decisions when dealing with cyber threats.

Keywords: Artificial Intelligence; cyber situational awareness; dynamic cyber risk assessment; organizational readiness; decision support; small and medium-sized enterprises



Academic Editor: Steven Furnell

Received: 3 July 2026

Revised: 28 July 2026

Accepted: 1 August 2026

Published: 3 August 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

The existence of technical controls is not the sole basis for cybersecurity decisions. Decision-makers need to be capable of identifying relevant cybersecurity events, understanding their meaning, and anticipating the possible development of a situation [1]. These skills are crucial for cyber situational awareness (CSA) and the quality of risk-based action [2].

This requirement is challenging for small and medium-sized enterprises (SMEs), which commonly operate with limited budgets, fewer specialist staff, and less formal security governance than large organizations. Such constraints can lead to SMEs relying on

reactive controls and periodic risk reviews even as threats, vulnerabilities, and business dependencies evolve rapidly [2].

A possible approach to close this gap is dynamic cyber risk assessment (DCRA). In practice, DCRA is an iterative update of cyber risk estimates as new operational evidence is generated, rather than as a fixed annual or quarterly outcome. AI may support this process through anomaly detection, threat classification, predictive modeling, evidence correlation, and decision-support functions. However, the value of these techniques depends on data quality, integration, explainability, human oversight, and the organization's capacity to act on the output [3].

Previous work on CSA, DCRA, AI-enabled cybersecurity, and SME readiness has often developed along separate technical or organizational lines. Technical studies tend to evaluate algorithms and architectures, whereas organizational studies emphasize awareness, resources, governance, and adoption. Less survey evidence explains how stakeholders understand the relationship among these concepts, which DCRA capabilities they prioritize, and which implementation barriers they expect in resource-constrained settings. The present study addresses this gap by using stakeholder perceptions to derive requirements for an SME-oriented conceptual framework. Because SME employment was not verified for every respondent, the findings are not presented as a representative estimate of SME readiness.

Four research questions guide the paper. RQ1: How familiar are respondents with CSA and DCRA, and how often do they report using them? RQ2: Which DCRA capabilities and implementation barriers are considered most important? RQ3: What are respondents' views of AI in cybersecurity, and which AI-supported CSA and DCRA capabilities do they expect? RQ4: How can the survey findings be organized into an SME-oriented conceptual framework? The contribution is empirical and conceptual rather than causal: Sections 2 and 3 review the background and methods. Section 4 reports the survey results, Section 5 interprets the findings and presents the framework, and Section 6 concludes the paper.

2. Background and Related Work

Situational awareness (SA) is defined as a process of moving from the perception of relevant elements to the understanding of their meaning to the projection of how the situation may evolve [4]. Within cybersecurity, CSA generalizes this reasoning to the digital environment in which analysts and decision-makers need to interpret incomplete, distributed and rapidly changing evidence [5]:

- Perception: Identifying relevant events, assets, vulnerabilities and indicators in the environment.
- Comprehension: Evaluating the interrelation of these elements with the organization, its mission, and its current exposure.
- Projection: Estimating how the situation might evolve and what action might be needed.

CSA is therefore not simply a dashboard or an alert feed. Technical visibility must be blended with contextual knowledge and human judgment. Research has shown that information overload, poor explanation, and limited user knowledge can degrade decision-making even with security data [5,6].

Risk assessment provides part of that context by linking evidence to likelihood, impact, and organizational priorities. The design challenge is how to refresh that interpretation without overwhelming users or offering automated outputs as the final word.

2.1. Dynamic Cyber Risk Assessment and SME Constraints

Risk assessment is described as the “overall process of risk identification, risk analysis, and risk evaluation” [7]. According to Craigen et al. [8], cybersecurity risk assessment is crucial because it helps identify and reduce potential risks to cyber infrastructure. The assessment is conducted to identify the cyber risks and vulnerabilities of digital environments using different tools, frameworks, and methodologies to protect critical assets from cyber threats.

Moreover, the DCRA should incorporate several key elements such as the application of cybersecurity maturity assessment frameworks, vulnerability scanning of critical cyber systems, cybersecurity metrics, multi-criteria decision-making frameworks, and dynamic simulation approaches. These tools are employed to estimate the level of risk in the cyber infrastructure and improve its overall security. Such methods can be used by organizations to effectively address cyber threats and enhance security in different contexts, including SMEs.

More investments are needed in cybersecurity solutions because of the increasing threats of cybercrime against SMEs. Cybersecurity risk assessment in SMEs is difficult due to the limited resources, expertise, and the rapidly changing nature of cyber threats [9,10]. Furthermore, SMEs struggle to deploy cybersecurity solutions and to comprehend the extent of their cyber risks due to the unavailability of resources and lack of suitable in-house expertise [11].

Moreover, Chandna and Tiwari [12] emphasize that new entrepreneurial endeavors face challenges in addressing online risks owing to their limited resources and capabilities in comparison to well-established firms. The challenges faced by SMEs in addressing cybersecurity issues are compounded by inadequate protective measures and a lack of awareness of the importance of cybersecurity [13]. The lack of resources and relevant in-house expertise in SMEs complicates the adoption of cybersecurity solutions and raises awareness of cyber risks [10,13]. Fortunately, Neri et al. [14] demonstrated that SMEs were increasingly starting to pave the way for organizational cyber readiness by taking more proactive steps to address cyber risks.

2.2. Cyber Situational Awareness and Organizational Readiness in SMEs

According to Tsiodra et al. [15], SMEs face a challenging CSA, representing around 90% of companies globally and more than 50% of employees, according to the World Bank. SMEs are considered an easy target for exploitation by threat actors [15] as they have sensitive and personally identifiable information. SMEs are crucial to economic development [16] and are businesses with fewer than 250 employees. SMEs are increasingly vulnerable to cyberattacks and need to prioritize cybersecurity to protect their businesses. Cybersecurity threats are ever-increasing, and SMEs are desirable targets for cybercriminals. Thus, SMEs must have a robust cybersecurity strategy [17].

According to a recent study by Renaud and Ophoff [18], SMEs are considered to be more prone to cyberattacks, mainly due to their limited resources and lack of situational awareness. Also, Renaud and Ophoff [18] presented the matter of CSA in SMEs and suggested a model created based on Endsley’s theory. The research used data from an online survey of 361 SMEs in the UK, and partial least squares modeling was used to validate the suggested model [18].

In another study, Ncubukezi [19] analyzed the CSA in SMEs in South Africa. The study included 30 SMEs from various business sectors to reflect different views and experiences. Researchers discovered that cybersecurity practices in SMEs differed depending on the business sector. One of the major factors behind this variation was the lack of regulations, standards, procedures or guidelines to encourage the adoption of strong cybersecurity measures in SMEs. As a result, SMEs often suffered from poor cybersecurity that could

lead to economic and reputational damage. The study also highlighted the limitations of existing security measures and their implementation. Furthermore, it was stated that SME employees had inadequate knowledge of the management of cyber attacks, which in turn posed significant threats [19].

The two studies, Renaud and Ophoff [18] and Ncubukezi et al. [19], found some ways to ensure good cybersecurity in SMEs. SMEs should develop detailed rules, regulations, and guidelines to promote good cybersecurity practices among employees.

Also, they should allocate funds for comprehensive cybersecurity training programs to equip employees with the necessary knowledge and skills to detect and counter cyber threats. Furthermore, SMEs need to constantly review and update their security measures to deal with the changing nature of cyber threats, and this desire has not happened without enhancing the CSA for SMEs. Taken together, these studies suggest that SME cybersecurity cannot be reduced to a checklist of tools. Awareness, governance, skills, and the ability to translate technical information into action are interdependent. They also leave open the question of how AI-supported DCRA should be designed so that it strengthens, rather than complicates, CSA in organizations with limited resources.

3. Method

The study adopted a quantitative cross-sectional online survey to explore perceptions of cybersecurity, CSA, DCRA, and AI. The questionnaire consisted of 48 questions in four analytical domains: the cybersecurity environment, CSA and use, DCRA and requirements, and views on AI-supported CSA and DCRA.

3.1. Participants and Recruitment

The survey was opened by 573 people and completed by 302 (52.7%). Among respondents with valid role data ($n = 293$), 118 (40.3%) identified as IT or cybersecurity specialists, and 136 (46.4%) reported leadership responsibilities; these categories were not mutually exclusive. Of valid demographic responses, 202 of 292 (69.2%) identified as male and 89 (30.5%) as female. The largest age group was 35–44 years (69 of 299; 23.1%). A bachelor's degree was reported by 161 of 295 (54.6%), a master's degree by 71 (24.1%), and a doctorate by 28 (9.5%). Of 300 valid employment responses, 180 (60.0%) worked full time, 62 (20.7%) were students, and 29 (9.7%) were retired.

Participants were recruited by email through official organizational contacts and the researcher's professional network. The invitation stated that previous cybersecurity expertise was not required. Recruitment was therefore purposive in reach but self-selected in response. The sample included specialists, leaders, and participants outside specialist or verified SME roles; it is consequently treated as a heterogeneous stakeholder sample rather than a probability sample representative of SMEs, countries, or sectors.

3.2. Questionnaire Development and Measures

Questionnaire development followed the main stages described by Burgess: defining the aims, identifying the intended population, selecting the online mode, drafting and reviewing items, piloting, administering the final instrument, and analyzing the responses [20]. Items were mapped to four domains: cybersecurity context; CSA familiarity, use, and expected benefits; DCRA familiarity, use, system requirements, and implementation challenges; and AI acceptance and expected capabilities for CSA and DCRA.

Some questions were based on previous information-security culture assessment work [21–23] and adapted to the present research questions. The draft was reviewed by academic supervisors and cybersecurity specialists for clarity, relevance, and content

coverage. Before the main survey, a pilot was carried out to identify ambiguous, repetitive or poorly ordered questions.

The instrument combined categorical, yes/no/uncertain, ranking, multiple-response, open-text, and five-point Likert-type questions. Qualtrics routing displayed follow-up items only when relevant. The questionnaire was not designed as a single 48-item psychometric scale; reliability analysis was therefore restricted to four coherent multi-item measures with common response formats. The complete survey questionnaire as implemented in Qualtrics is provided in Appendix A.

3.3. Ethics and Data Management

Ethical approval was granted by Cardiff Metropolitan University under project reference CST_Ethics_App_PhDStudent_MAlmalki_20240613_16. Participants received an information sheet and completed online consent before taking part. Participation was voluntary, responses were kept confidential, and the participant information outlined the withdrawal procedure and the seven-day withdrawal period. Qualtrics was used for secure data collection. Incomplete cases were excluded from the analysis, and the 302 records marked as finished were used.

3.4. Statistical Analysis

Data management was carried out using the IBM SPSS (Version 21) Statistics program. Missing, routed, and out-of-range responses were treated as missing for the relevant item, and the 302 records coded as finished were retained for analysis. Frequencies and percentages were calculated using item-specific valid denominators; multiple-response questions are reported with the number of respondents answering the item and the number or percent selecting each option. Means and standard deviations are for recoded five-point ratings. Higher scores indicate greater importance, familiarity, or criticality.

Internal consistency was evaluated separately for DCRA system-development requirements (Q37; 10 items), DCRA implementation challenges (Q39; 7 items), expected AI capabilities for CSA (Q45; 6 items), and expected AI capabilities for DCRA (Q48; 6 items). Cronbach's alpha, 95% bootstrap confidence intervals, McDonald's omega, corrected item-total correlations, and alpha-if-item-deleted values were tested. The construct structure was assessed through the Kaiser–Meyer–Olkin statistic, Bartlett's test of sphericity, the eigenvalues and parallel analysis, and the one-factor maximum-likelihood models.

Exploratory inferential analyses were conducted to examine role and construct relationships relevant to the research questions. Mann–Whitney U tests were employed to compare specialists and non-specialists and leaders and non-leaders on ordinal CSA and DCRA familiarity scores. We tested associations with reported CSA use, DCRA use, and AI endorsement using Pearson chi-square tests; effect sizes are reported as Cramer's V and rank-biserial correlations. We used Spearman correlations to explore the associations between familiarity and expectations of AI support. We used binary logistic regression to determine if specialist status, leadership status, familiarity with CSA and familiarity with DCRA were independent predictors of AI endorsement. The 12 bivariate tests were performed with Holm's correction.

4. Results

The results are presented by research question. Section 4.2 addresses RQ1 through CSA familiarity and use, Section 4.3 addresses RQ1 and RQ2 through DCRA awareness, requirements, and barriers, Section 4.4 addresses RQ3 through AI acceptance and expected capabilities, Section 4.5 reports reliability and construct-structure evidence, and Section 4.6 reports exploratory associations.

4.1. Cybersecurity Environment Analysis

The 299 valid respondents rated the importance of cybersecurity as high ($M = 4.75$, $SD = 0.60$). In total, 255 (88.5%) of 288 valid responses to the cybersecurity challenge item stated that cybersecurity currently posed significant challenges. The mean ratings of the challenges listed in Table 1 are reported ($n = 285$ valid). The highest rated challenges were adoption of new technologies ($M = 4.36$), poor CSA ($M = 4.34$), and limitations of traditional risk assessment and response approaches ($M = 4.29$).

Table 1. Perceived cybersecurity challenges.

Challenges in Cybersecurity	Mean	Std. Deviation
Adoption of new technologies.	4.36	0.817
Poor CSA.	4.34	0.773
Traditional methods of CRA and responding to evolving threats in cybersecurity.	4.29	0.752
Using AI capabilities in cyberattacks.	4.22	0.905
The lack of cybersecurity professionals.	4.17	0.943
The lack of sufficient employment of AI capabilities in cyber defense.	4.16	0.879
Absence of a legal and regulatory framework for cybersecurity.	3.66	1.201
Valid n	285	

The responses were concentrated toward the upper end of the rating scale, indicating broad agreement that cybersecurity is both important and difficult to manage. The three highest-rated challenges reflect a common concern with organizational adaptation: keeping pace with new technologies, maintaining adequate situational awareness, and responding to threats through approaches that are more flexible than traditional periodic risk assessment.

Of the 290 valid answers, 238 (82.1%) answered that SMEs needed more attention and support on cybersecurity, 48 (16.6%) answered maybe, and four (1.4%) answered no. Table 2 presents the perceived importance of threats. Data breaches ($M = 4.74$), phishing ($M = 4.57$), cloud vulnerabilities ($M = 4.47$), and system vulnerabilities ($M = 4.47$) were rated the highest. Others that rated high were advanced persistent threats ($M = 4.42$), third-party vulnerabilities ($M = 4.35$), and ransomware ($M = 4.34$).

Table 2. Perceived cybersecurity threats.

Threats	Mean	Std. Deviation
Data Breaches	4.74	0.585
Phishing	4.57	0.711
Vulnerability in the Cloud	4.47	0.783
Vulnerabilities in Systems	4.47	0.809
Mobile Attacks	4.44	0.803
Advanced Persistent Threat (APT)	4.42	0.827
Third-Party Vulnerabilities	4.35	0.854
Ransomware	4.34	0.876
IoT Attacks	4.29	0.864
Social Engineering	4.15	0.989
Remote Work Environments	4.12	0.951
Cryptojacking	4.07	0.978
Valid n	293	

Taken together, these ratings indicate that respondents were concerned not only about direct attack types, such as phishing and ransomware, but also about vulnerabilities arising from cloud services, internal systems, and third-party dependencies.

4.2. CSA Awareness, Use, and Expected Benefits

Figure 1 shows CSA familiarity among 296 valid respondents. Overall, 236 (79.7%) reported at least slight familiarity, while 60 (20.3%) selected not familiar at all. The recoded familiarity score averaged 2.90 (SD = 1.30) on a 1–5 scale in which higher scores indicate greater familiarity.

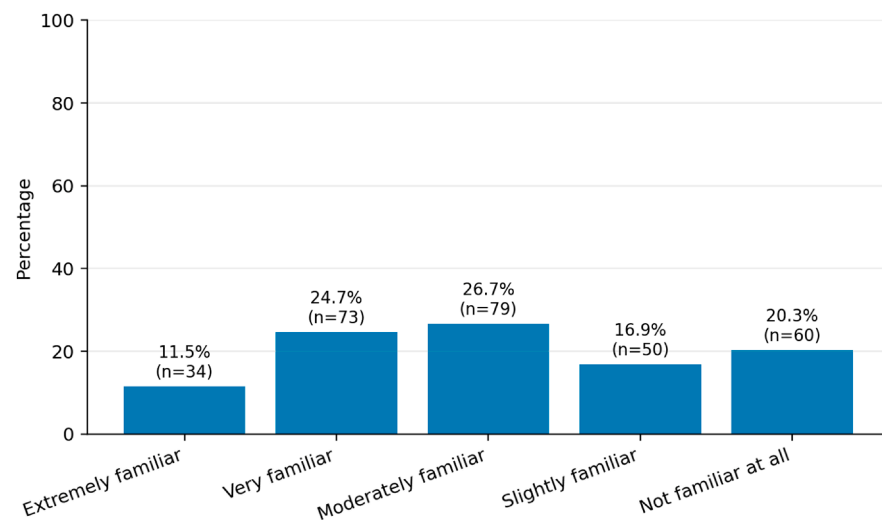


Figure 1. Self-reported familiarity with CSA.

Reported operational use was lower: among 293 valid responses, 54 (18.4%) reported prior CSA use, 57 (19.5%) were unsure, and 182 (62.1%) reported no use. This contrast shows that awareness of CSA was substantially more common than practical experience with it, identifying a clear familiarity–use gap relevant to RQ1.

Among the 54 respondents who reported prior use of CSA, 26 (48.1%) received CSA information automatically through an electronic system, 19 (35.2%) relied on paper-based documents, and nine (16.7%) reported using another source. All 54 respondents completed the update-frequency item.

Within this subgroup, updates were received monthly by 18 respondents (33.3%), weekly by 13 (24.1%), daily by 10 (18.5%), quarterly by seven (13.0%), and yearly by six (11.1%) (Figure 2). Overall, 31 respondents (57.4%) received updates monthly or less frequently, whereas 23 (42.6%) received daily or weekly updates. This indicates that frequent operational updating was not the dominant practice, even among respondents who reported previous CSA use.

For the CSA improvement item, 89 of the 290 valid respondents (30.7%) selected “yes,” 195 (67.2%) selected “maybe,” and six (2.1%) selected “no.” The predominance of “maybe” responses indicates substantial uncertainty about whether CSA requires improvement.

Moreover, the ranking item was completed by 288 respondents. Improved cyber risk assessment and response to evolving threats was ranked first by 180 respondents (62.5%). The remaining first-ranked options were more informed decision-making (57; 19.8%), better resource allocation (25; 8.7%), and improved business continuity (24; 8.3%). Two responses (0.7%) did not produce a classifiable first-ranked option. Figure 3 presents the distribution of first-ranked benefits. The high focus on risk assessment and response to threats shows that respondents associated the improvement of CSA with a better understanding and handling of emerging cyber risks.

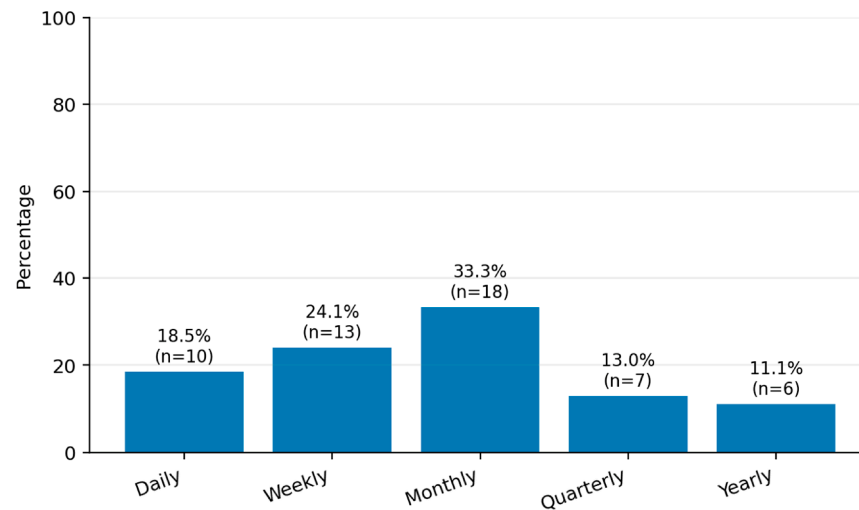


Figure 2. Reported CSA update frequency among respondents reporting prior CSA use.

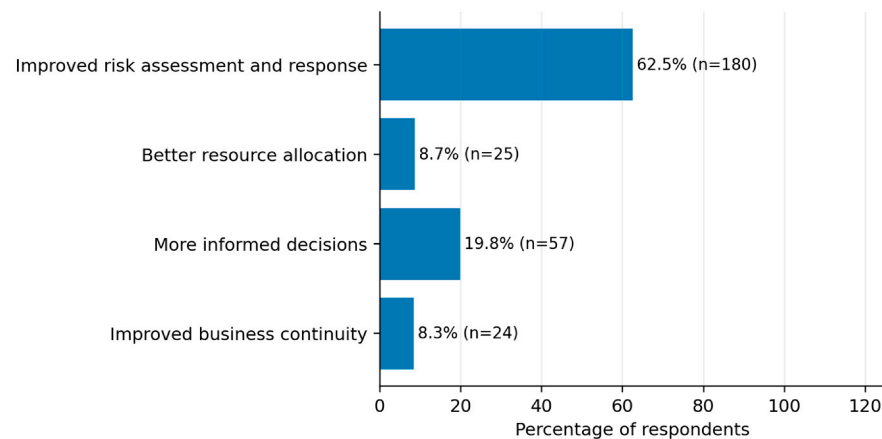


Figure 3. First-ranked anticipated benefit of improving CSA.

4.3. DCRA Awareness, Use, Requirements, and Barriers

Self-reported familiarity with DCRA was mixed among the 296 valid respondents (Figure 4). On the recoded five-point scale, where higher scores indicated greater familiarity, the mean familiarity score was 2.47 (SD = 1.32). One hundred respondents (33.8%) reported no familiarity with DCRA, whereas only 66 (22.3%) described themselves as very or extremely familiar. The remaining 130 respondents (43.9%) reported slight or moderate familiarity. Overall, the distribution indicates that familiarity with DCRA was limited and uneven across the sample and was lower than the previously reported familiarity with CSA.

Only 21 of the 293 valid respondents (7.2%) reported previous use of DCRA, whereas 70 (23.9%) were uncertain and 202 (68.9%) reported no previous use. The use-frequency item was therefore completed by a small conditional subgroup. Among the 21 previous users, eight respondents (38.1%) reported daily use, four (19.0%) weekly use, four (19.0%) monthly use, two (9.5%) quarterly use, and three (14.3%) annual use. The corresponding percentages are presented in Figure 5. Although daily use was the most frequently reported pattern within this subgroup, the very small number of previous users indicates that DCRA had limited reported operational adoption across the wider sample.

For the question asking whether DCRA could enhance CSA, 81 of the 290 valid respondents (27.9%) selected “yes,” 198 (68.3%) selected “maybe,” and 11 (3.8%) selected “no.”

The predominance of “maybe” responses indicates considerable uncertainty about the relationship between DCRA and CSA, rather than clear rejection of the proposed relationship.

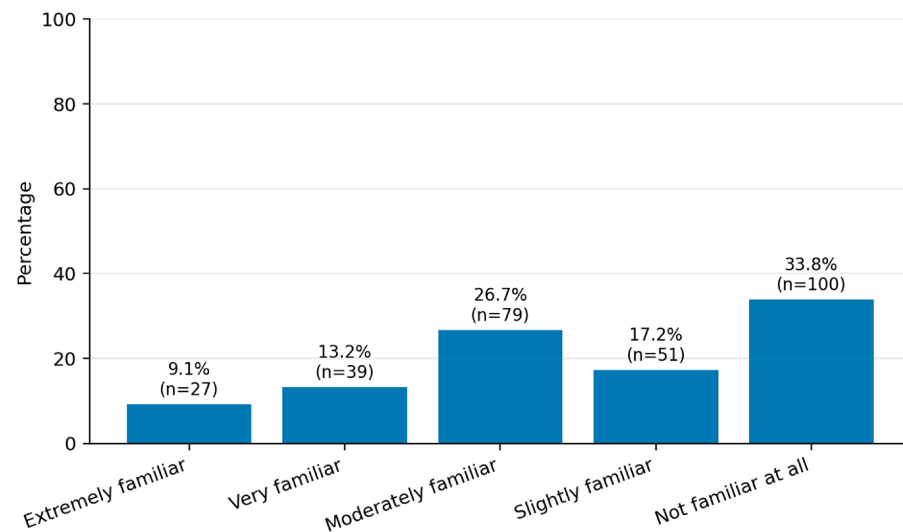


Figure 4. Self-reported familiarity with DCRA.

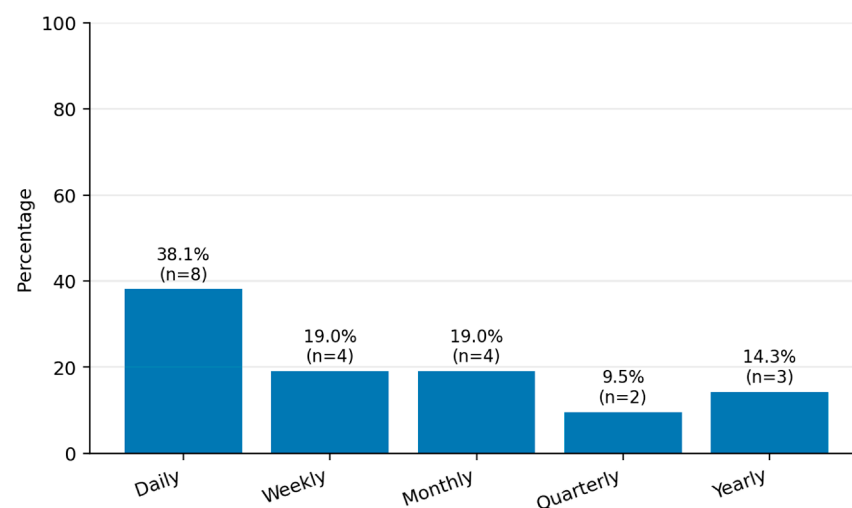


Figure 5. Reported DCRA use frequency among previous users.

The multiple-response follow-up question concerning the mechanisms through which DCRA could enhance CSA was completed by 285 respondents. Percentages in Figure 6 were calculated using these 285 respondents as the denominator and do not sum to 100% because respondents could select more than one option. Early threat identification was the most frequently selected mechanism, reported by 223 respondents (78.2%), followed by increased awareness of the surrounding environment and potential threats (200; 70.2%), informed decision-making (150; 52.6%), adaptability to a changing security landscape (131; 46.0%), and improved resource allocation (117; 41.1%). These findings show that respondents most commonly associated DCRA with earlier threat recognition and improved awareness, whereas resource-allocation benefits were selected less frequently. The identified mechanisms informed the development of the proposed conceptual framework.

For the DCRA improvement item, 108 of the 292 valid respondents (37.0%) selected “yes,” 164 (56.2%) selected “maybe,” and 20 (6.8%) selected “no.” The predominance of “maybe” responses indicates considerable uncertainty about whether existing DCRA approaches require improvement.

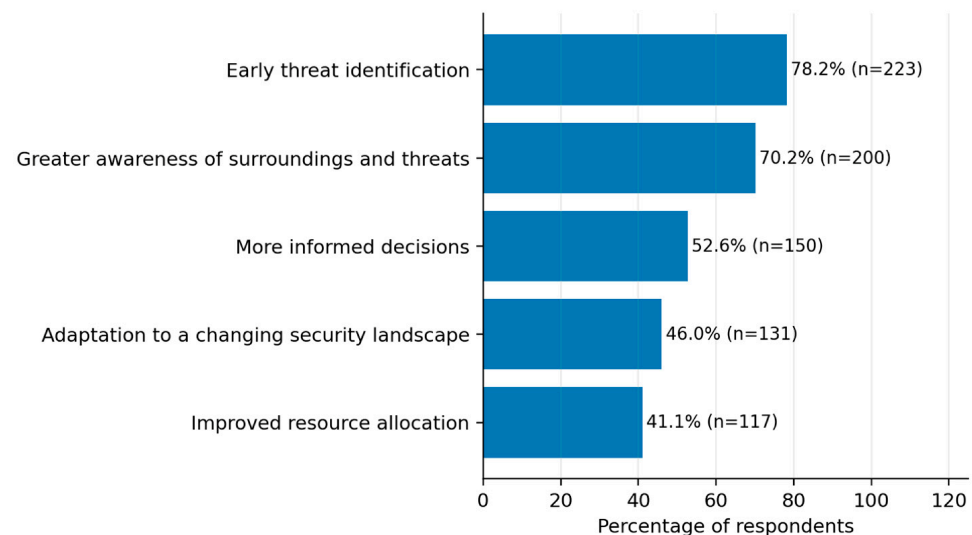


Figure 6. Reported ways DCRA could support CSA.

Table 3 reports the ratings of ten DCRA development requirements among respondents with complete data for this routed measure (valid $n = 274$). Continuous updating of threat information received the highest rating ($M = 4.39$), followed by the identification of attacks and vulnerabilities ($M = 4.37$) and risk-based alert prioritization ($M = 4.31$). The concentration of the highest ratings on continuous updating, threat identification, and prioritization indicates that respondents placed the greatest importance on capabilities that support timely and adaptive risk assessment.

Table 3. DCRA system-development requirements.

Requirement	Mean	Std. Deviation
Continuously update understanding of threats	4.39	0.837
Identify potential attacks and vulnerabilities	4.37	0.860
Prioritize alerts based on risk	4.31	0.883
Process real-time data streams	4.25	0.896
Retain human intervention	4.22	0.926
Adapt to organizational needs and risk profile	4.20	0.863
Generate real-time reports	4.16	0.897
Be easy to use	4.16	0.970
Automate routine tasks	4.16	0.942
Integrate data from diverse sources	4.10	0.991
Valid n	274	

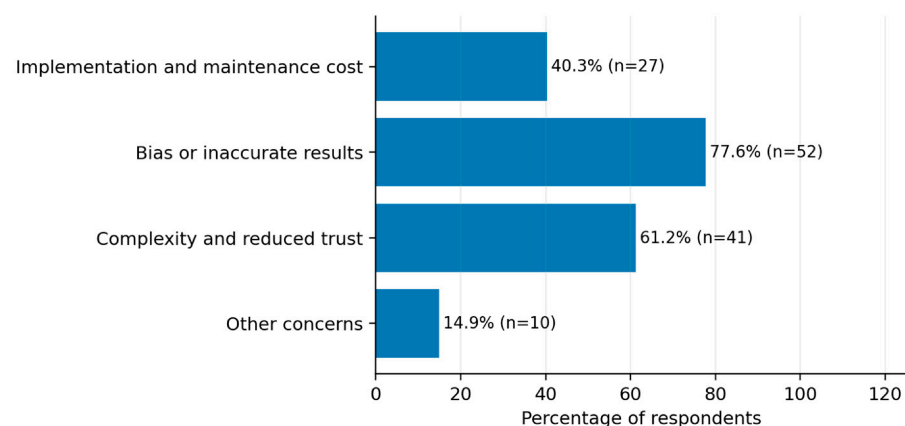
Table 4 presents the perceived DCRA implementation challenges for the same complete-case subgroup (valid $n = 274$). Accuracy and relevance ($M = 4.16$) and integration with existing infrastructure ($M = 4.16$) received the highest mean ratings, followed by adaptability to evolving threats ($M = 4.12$) and system complexity ($M = 4.12$). These results indicate that respondents were concerned both with the technical reliability of DCRA outputs and with the practical difficulty of integrating and maintaining adaptive systems within existing organizational environments. In the follow-up item, 99.3% of respondents indicated that no additional major challenges needed to be added. This percentage refers only to respondents' assessment of the comprehensiveness of the listed challenges.

Table 4. Perceived DCRA implementation challenges.

Implementation Challenge	Mean	Std. Deviation
Accuracy and relevance	4.16	0.916
Integration with existing infrastructure	4.16	0.949
Adaptability to evolving threats	4.12	0.946
System complexity	4.12	0.904
Cost	4.09	0.992
Human expertise integration	4.08	0.982
Balancing security with usability	4.07	0.992
Valid <i>n</i>		274

4.4. Perceptions of AI and Expected CSA/DCRA Capabilities

Among the 293 valid responses, 226 respondents (77.1%) endorsed the use of AI technologies in cybersecurity, whereas 67 (22.9%) did not. Among those who did not endorse AI, the most frequently selected concern was the potential for bias or inaccurate results (52; 77.6%), followed by system complexity and reduced trust in AI-supported decisions (41; 61.2%), implementation and maintenance costs (27; 40.3%), and other concerns (10; 14.9%) see Figure 7. Because respondents could select more than one concern, the percentages do not sum to 100%. The pattern indicates that opposition to AI was driven more strongly by concerns about reliability, transparency, and trust than by cost alone. These responses are relevant to the governance and design requirements of AI-enabled cybersecurity systems but should not be interpreted as evidence of the actual frequency of specific AI adoption failures.

**Figure 7.** Reasons for not endorsing AI in cybersecurity.

Among the 226 respondents who endorsed AI, automation of routine tasks and the perceived ability of AI to analyze data rapidly and accurately were each selected by 179 respondents (79.2%). Reduced cost and effort were selected by 140 respondents (61.9%), while 133 (58.8%) selected the development of advanced services and three (1.3%) reported other reasons see Figure 8. Because respondents could select more than one reason, the percentages do not sum to 100%. The pattern indicates that support for AI was driven primarily by expectations of operational efficiency and enhanced analytical capacity, rather than by cost reduction alone.

For AI-supported CSA, 169 of the 296 valid respondents (57.1%) selected “yes,” 103 (34.8%) selected “maybe,” and 24 (8.1%) selected “no.” The six-item expected-capability measure was conditional on the relevant survey route, and 170 respondents provided complete responses to all six items.

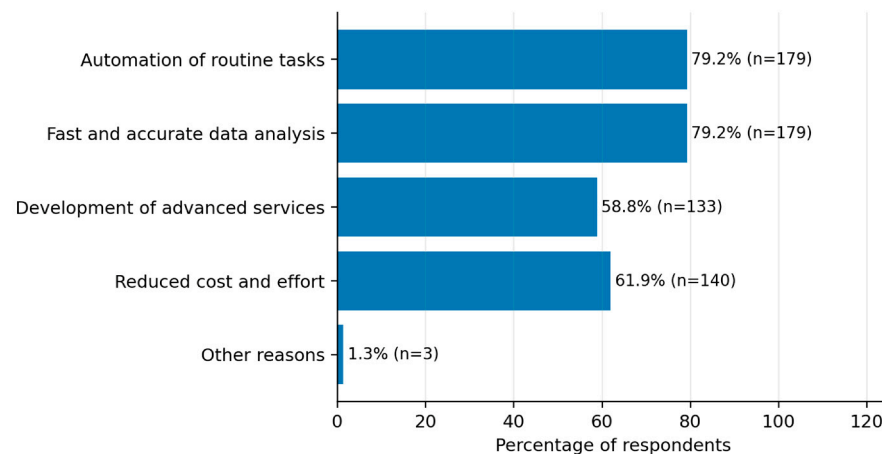


Figure 8. Reasons for endorsing AI in cybersecurity.

As shown in Table 5, monitoring and analyzing vast volumes of data and providing advanced capabilities in threat detection, anomaly detection, prediction, and response received the joint-highest mean ratings ($M = 4.52$). Providing powerful proactive cyber threat intelligence for classification and interpretation followed closely ($M = 4.50$), followed by empowering employees to respond promptly to security incidents and prevent cyberattacks ($M = 4.48$). Providing real-time insights and alerts about potential risks received a mean rating of 4.37, while ensuring that cybersecurity processes are transparent and easy to understand received the lowest, although still high, rating ($M = 4.27$). The consistently high ratings indicate that respondents primarily associated AI-supported CSA with improved analytical capacity, earlier threat recognition, and support for interpreting complex cybersecurity information.

Table 5. Expected AI Capabilities for enhancing CSA.

Expected Capability	Mean	Std. Deviation
Monitor and analyze vast volumes of data.	4.52	0.747
Providing advanced capabilities in threat detection, anomaly detection, prediction, and response.	4.52	0.673
Providing powerful proactive cyber threat intelligence for classification and interpretation.	4.50	0.771
Empower employees to respond promptly to security incidents and prevent cyber attacks.	4.48	0.740
Providing real-time insights and alerts about potential risks.	4.37	0.791
Cybersecurity processes should be transparent and easy to understand.	4.27	0.820
Valid <i>n</i>		170

For AI-supported DCRA, 136 of the 296 valid respondents (45.9%) selected “yes,” 132 (44.6%) selected “maybe,” and 28 (9.5%) selected “no.” The near-equal proportions of affirmative and uncertain responses indicate considerable uncertainty about AI’s potential contribution to DCRA, although outright rejection was limited. The six-item expected-capability measure was conditional on an affirmative response, and all 136 eligible respondents provided complete data. Within this subgroup, continuous threat analysis received the highest mean rating ($M = 4.57$), followed by prediction of future attacks ($M = 4.43$) and data processing and prioritization ($M = 4.40$); see Table 6. The results indicate that the respondents associated AI-supported DCRA mainly with the continuous interpretation

of changing threat conditions, anticipation of potential attacks, and prioritization of large amounts of risk information.

Table 6. Expected AI capabilities for enhancing DCRA.

Expected Capability	Mean	Std. Deviation
Continuous threat analysis.	4.57	0.707
Predict future attacks.	4.43	0.813
Data processing and prioritization.	4.40	0.864
Helping cybersecurity specialists focus on proactive defense.	4.38	0.851
Improved risk assessments.	4.38	0.816
Integration with other security tools.	4.24	0.937
Valid <i>n</i>		136

4.5. Reliability and Construct-Structure Assessment

Reliability and construct-structure analyses were conducted for four multi-item measures. Complete-case sample sizes differed because Qualtrics routing did not present every measure to every respondent.

All four measures showed good to excellent internal consistency. Cronbach's alpha ranged from 0.868 to 0.926 and McDonald's omega from 0.870 to 0.929. KMO values ranged from 0.858 to 0.929, and all Bartlett tests were significant ($p < 0.001$). Parallel analysis retained one factor for each measure; the first observed eigenvalues ranged from 3.71 to 6.10, and standardized one-factor loadings ranged from 0.548 to 0.817.

No item was removed on reliability grounds: corrected item-total correlations ranged from 0.525 to 0.777, and alpha-if-item-deleted values did not provide a substantive basis for removing an item (Table 7). These results support internal consistency and empirical unidimensionality for the specified measures.

Table 7. Reliability and construct-structure results for the four multi-item measures.

Construct Structure	α/ω	Complete-Case <i>n</i>	Multi-Item Measure
KMO 0.929; Bartlett $\chi^2(45) = 1753.00, p < 0.001$; $\lambda_1 = 6.10$; PA = 1; loadings 0.610–0.817	α 0.926 [0.898, 0.945]; ω 0.929	274	DCRA requirements (Q37; 10 items)
KMO 0.862; Bartlett $\chi^2(21) = 813.96, p < 0.001$; $\lambda_1 = 3.93$; PA = 1; loadings 0.548–0.808	α 0.868 [0.838, 0.895]; ω 0.870	273	DCRA challenges (Q39; 7 items)
KMO 0.895; Bartlett $\chi^2(15) = 509.00, p < 0.001$; $\lambda_1 = 3.89$; PA = 1; loadings 0.738–0.810	α 0.890 [0.822, 0.930]; ω 0.891	170	AI capabilities for CSA (Q45; 6 items)
KMO 0.858; Bartlett $\chi^2(15) = 376.74, p < 0.001$; $\lambda_1 = 3.71$; PA = 1; loadings 0.688–0.785	α 0.875 [0.793, 0.923]; ω 0.876	136	AI capabilities for DCRA (Q48; 6 items)

4.6. Exploratory Associations Between Professional Background and Key Survey Outcomes

Exploratory analyses examined whether cybersecurity specialization and leadership responsibility were associated with familiarity with, and previous use of, CSA and DCRA. Mann–Whitney U tests were used for the ordinal familiarity measures, chi-square tests were used for categorical use outcomes, and Spearman's rank correlation was used to examine the relationship between CSA and DCRA familiarity. Holm adjustment was applied to the reported bivariate tests to reduce the risk of false-positive findings from multiple comparisons. Effect sizes are given along with adjusted *p*-values to indicate the practical magnitude of the associations. Cybersecurity specialists were more familiar with CSA and DCRA than non-specialists, with moderate rank-biserial effects ($r = 0.38$ and $r = 0.31$, respectively).

Specialist status was also associated with previous use of CSA (Cramer's $V = 0.31$) and DCRA (Cramer's $V = 0.24$). Differences by leadership status were smaller: leadership responsibility was associated with CSA familiarity ($r = 0.21$), DCRA familiarity ($r = 0.27$), and previous DCRA use (Cramer's $V = 0.17$). CSA and DCRA familiarity were moderately and positively related (Spearman's $\rho = 0.54$). All associations reported in Table 8 remained statistically significant after Holm adjustment. These results indicate that professional IT and cybersecurity experience was more clearly related to familiarity and previous use than to general support for AI adoption. The findings are exploratory and cross-sectional and should therefore be interpreted as associations rather than causal effects. An additional exploratory logistic regression of AI endorsement is reported in Table A1 in Appendix B.

Table 8. Exploratory associations among professional background, familiarity, and previous use.

Analysis	Valid n	Statistic	Effect Size	Raw p	Holm-Adjusted p	Interpretation
Specialist status vs. CSA familiarity	293	$U = 14,223.5$	Rank-biserial $r = 0.38$	<0.001	<0.001	Moderately greater familiarity among specialists
Specialist status vs. DCRA familiarity	293	$U = 13,565.5$	Rank-biserial $r = 0.31$	<0.001	<0.001	Moderately greater familiarity among specialists
Leadership status vs. CSA familiarity	293	$U = 12,946.5$	Rank-biserial $r = 0.21$	0.001	0.005	Small difference by leadership responsibility
Leadership status vs. DCRA familiarity	293	$U = 13,577.5$	Rank-biserial $r = 0.27$	<0.001	<0.001	Small-to-moderate difference by leadership responsibility
Specialist status $\times$ CSA use	293	chi-square(2) = 28.10	Cramer's $V = 0.31$	<0.001	<0.001	Moderate association with previous CSA use
Specialist status $\times$ DCRA use	293	chi-square(2) = 16.28	Cramer's $V = 0.24$	<0.001	0.002	Small-to-moderate association with previous DCRA use
Leadership status $\times$ DCRA use	293	chi-square(2) = 8.12	Cramer's $V = 0.17$	0.017	0.049	Small association with previous DCRA use
CSA familiarity vs. DCRA familiarity	296	Spearman's $\rho = 0.54$	Moderate positive association	<0.001	<0.001	Higher CSA familiarity accompanied higher DCRA familiarity

Note. U = Mann–Whitney U statistic; r = rank-biserial correlation; V = Cramer's V ; ρ = Spearman's rank correlation. Holm-adjusted p -values account for multiple bivariate comparisons.

5. Discussion

This study examined stakeholder perceptions of CSA, DCRA, and AI-enabled cybersecurity, and used the resulting evidence to develop an SME-oriented conceptual framework. Three interconnected findings emerged. First, self-reported familiarity with CSA and DCRA was substantially more common than reported operational use. Second, respondents placed high importance on adaptive DCRA capabilities while simultaneously identifying reliability, integration, adaptability, and complexity as major implementation barriers. Third, support for AI was high overall but conditional on accuracy, transparency, trust, cost and human oversight. Taken together, these results suggest that the adoption of AI-enabled DCRA is not a mere technical issue. It is a socio-technical process shaped by organizational readiness, operational practices, data quality, governance, and the ability of decision-makers to interpret and act on system outputs.

The discussion is organized around the four research questions. The findings are interpreted as evidence of respondents' perceptions and expectations rather than as proof of technical effectiveness, organizational capability, or causal relationships.

5.1. Familiarity and Operational Use of CSA and DCRA

RQ1 examined respondents' familiarity with CSA and DCRA and their reported use of these concepts. The results reveal a clear distinction between conceptual recognition and operational adoption. However, most respondents reported at least some familiarity with CSA, and fewer than one-fifth reported previous operational use. Familiarity with DCRA was lower, and reported DCRA use was particularly limited. This pattern suggests that recognizing a concept does not necessarily mean that it has been embedded in formal processes, tools, reporting arrangements, or decision routines.

This familiarity–use gap is consistent with previous SME cybersecurity research showing that awareness of cybersecurity concepts does not necessarily lead to formal implementation. Earlier studies have associated this gap with limited specialist expertise, insufficient training, constrained resources, and the absence of structured cybersecurity processes [2,14,18,19]. The present findings extend this literature by demonstrating that the same distinction applies specifically to CSA and DCRA: respondents were more likely to recognize these concepts than to report using them operationally.

Several explanations may account for this pattern. Respondents may have encountered CSA or DCRA terminology through professional guidance, training, academic materials, or cybersecurity products without applying the concepts through a formally identified system. Organizations may also perform activities resembling situational awareness or dynamic risk assessment without using those labels. Conversely, some respondents may recognize the terminology without possessing detailed knowledge of its operational requirements. Familiarity should therefore not be treated as direct evidence of competence or organizational maturity.

Nevertheless, the difference between familiarity and use is operationally important. Awareness-building alone is unlikely to result in effective adoption. Organizations also require defined responsibilities, reliable data sources, assessment procedures, escalation arrangements, and mechanisms for incorporating risk information into decisions. For SMEs, the challenge may therefore be less about introducing additional terminology and more about translating CSA and DCRA into manageable and repeatable practices that fit existing resources and workflows.

The particularly low reported use of DCRA is compatible with previous research indicating that dynamic assessment approaches can be difficult to operationalize because they require continuous evidence collection, system integration, analytical capacity, and clearly defined decision processes [24,25]. The present survey cannot determine which of these conditions caused the low reported adoption, but it identifies a practical gap between the expected value of dynamic assessment and respondents' reported exposure to it.

5.2. Expected DCRA Capabilities and Implementation Barriers

RQ2 asked about capabilities for DCRA and expected implementation barriers. The most important capabilities were continuous threat updating, attack and vulnerability identification, and risk-based alert prioritization. These preferences show that DCRA should provide timely and actionable information.

This emphasis on continuous updating and risk re-prioritization is consistent with the literature that sees dynamic assessment as iterative revision of risk estimates in response to new evidence and changes in context [24,25]. These priorities reinforce the difference between DCRA and traditional periodic cyber risk assessment: the expected value is not

simply to produce a risk score, but to revise the interpretation and priority of risks as conditions change.

However, accuracy and relevance, integration with existing infrastructure, adaptability to evolving threats, and system complexity were also identified by respondents as the most important implementation challenges. These findings are not contradictory. Rather, they identify a central design requirement: the same features that make DCRA attractive can also make it difficult to implement. For example, continuous updating may improve responsiveness but can also generate additional noise when data are incomplete, poorly integrated, or interpreted without adequate context.

These concerns reflect implementation problems identified in prior research on dynamic risk assessment cybersecurity adoption [11,24–26]. Previous work has also emphasized that technically sophisticated assessment methods may provide limited operational value when their evidence, assumptions, and results cannot be understood by decision-makers [2].

Automated prioritization can support decision-making only when users can understand why a particular event or risk has received a given priority. A useful DCRA process must therefore connect updated evidence to an understandable risk rationale. It should communicate the source, relevance, confidence, and potential implications of the evidence included in the assessment. Even in cases of ambiguous evidence, high stakes, or automated outputs that conflict with the organization's existing knowledge, human review is still necessary.

Integration is especially important for SMEs, which may operate heterogeneous or legacy systems and lack dedicated personnel to maintain complex analytical infrastructures. An SME-oriented DCRA approach should therefore minimize unnecessary complexity, support incremental implementation, and align with existing security and business processes. The study consequently contributes a stakeholder-informed interpretation of DCRA requirements: continuous analysis and prioritization should be considered together with integration, explainability, relevance, and human review rather than as separate design concerns.

5.3. Conditional Support for AI-Enabled Cybersecurity

RQ3 examined respondents' views of AI and their expectations regarding AI-supported CSA and DCRA. More than three-quarters of valid respondents endorsed the use of AI in cybersecurity. Support was primarily associated with automation, rapid analysis of large data volumes, and the development of more advanced analytical services. The findings suggest that AI was viewed by the respondents mainly as a means of enhancing analytical capacity and relieving the burden of repetitive processing.

The high level of general support is in line with literature describing the potential contribution of AI to automated analysis, anomaly detection, threat classification, pattern recognition and cybersecurity decision support [2,27]. However, the present findings qualify this expectation. Respondents who did not endorse AI most frequently identified bias or inaccurate results, system complexity, reduced trust, and implementation cost.

These concerns are consistent with research suggesting that AI-enabled cybersecurity systems are susceptible to poor data quality, opaque decision-making, adversarial manipulation, false positives, and governance weaknesses [28,29]. Support for AI should therefore not be taken as a sign of unconditional technological optimism. It is a conditional acceptance, depending on whether the outputs of AI are deemed reliable, understandable, and suitable for operational decisions. The conditional capability measures support this interpretation further. Respondents expect AI to be able to contribute to anomaly detec-

tion, threat identification, large-volume analysis, continuous threat monitoring, prediction support, and risk prioritization.

The findings therefore support positioning AI as a decision-support capability rather than as an autonomous replacement for human judgment. Previous research similarly emphasizes that automated cybersecurity analysis requires human expertise to interpret contextual information, assess possible consequences, and determine an appropriate organizational response [2,30]. The present study adds stakeholder evidence to this position: respondents' support was strongest when AI was associated with analytical assistance, while opposition was driven primarily by concerns about reliability, transparency, and trust.

5.4. Uncertainty as an Indicator of Readiness

A notable finding across several survey items was the high proportion of respondents selecting "maybe" or expressing uncertainty. This occurred in relation to whether CSA required improvement, whether DCRA could enhance CSA, whether existing DCRA approaches required improvement, and whether AI could enhance DCRA.

This pattern can be interpreted in relation to organizational-readiness and technology-adoption research. Previous studies indicate that adoption decisions are influenced not only by perceived usefulness but also by organizational knowledge, available expertise, governance, compatibility, resources, and confidence in the technology [11,14,30]. Respondents with limited practical exposure to CSA, DCRA, or AI-enabled assessment may therefore have lacked a sufficiently stable basis for providing a definite judgment.

This finding extends the readiness discussion by identifying uncertainty itself as a relevant design consideration. An SME-oriented approach should not assume that prospective users already share a stable understanding of CSA, DCRA, or AI-supported risk assessment. Clear terminology, practical examples, staged implementation, and traceable explanations may therefore be required before users can evaluate or rely on dynamic risk outputs.

5.5. Development and Contribution of the Conceptual Framework

RQ4 considered how the findings could be organized into an SME-oriented conceptual framework. The proposed framework connects cybersecurity evidence, AI-enabled decision support, DCRA, CSA, human oversight, and organizational readiness. The structure is based on the survey results and previous literature. The CSA component is based on the research on perception, comprehension, and projection of relevant situational information [4,5]. The DCRA component is based on the research on continuous or near-real-time risk updating [24,25,31]. The AI-enabled decision-support component is informed by literature describing automated analysis, anomaly detection, threat classification, and prioritization [27,29]. Human oversight and organizational readiness are included because previous studies and the present findings both identify expertise, governance, transparency, infrastructure, and resources as conditions affecting operational adoption [11,30].

The survey findings informed the framework in several ways. High ratings for continuous threat updating, attack and vulnerability identification, and risk-based prioritization informed the DCRA component. Expectations concerning anomaly detection, large-volume analysis, prediction support, and threat intelligence informed the AI-enabled decision-support component. Concerns about bias, accuracy, complexity, integration, and trust informed the human-oversight and governance requirements. Finally, the familiarity–use gap and the frequency of uncertain responses informed the emphasis on organizational readiness, staged adoption, and understandable outputs.

As shown in Table 9, the framework requirements were not derived from a single survey item. Instead, they were developed by combining related findings across familiarity,

reported use, DCRA requirements, implementation barriers, and expectations regarding AI-supported CSA and DCRA. The mapping provides traceability between the empirical evidence and the proposed framework.

Table 9. Mapping survey evidence to conceptual-framework requirements.

Framework Component	Design Implication	Survey Evidence
Organizational-readiness and user-interface layer.	Simple terminology, staged adoption, and training.	Low reported CSA use and rare DCRA use.
Evidence ingestion and DCRA update cycle.	Refresh risk as evidence changes.	Continuous updating rated highest.
Anomaly detection and threat-classification services.	Automated identification and contextual analysis.	Attack/vulnerability identification.
Risk scoring, triage, and explanation output.	Rank events by risk and uncertainty.	Risk-based prioritization.
Governance and assurance controls.	Calibration, interfaces, drift review, and human oversight.	Accuracy, integration, adaptability, and complexity barriers.
Explainability and human-in-the-loop decisions.	Expose provenance, confidence, and review points.	Transparency and human intervention rated important.

These requirements were organized into the conceptual model shown in Figure 9. The model positions AI as a decision-support capability, DCRA as the process through which changing evidence is converted into updated and prioritized risk information, and CSA as the decision-oriented capability supported by that information. Organizational readiness, human oversight, and feedback influence the operation of the framework across its stages.

The framework's contribution lies in connecting technical and organizational bodies of research that are frequently considered separately. Technical studies commonly examine AI algorithms, detection performance, risk models, and system architectures, whereas organizational studies focus on awareness, expertise, governance, resources, readiness, and technology adoption [11,24]. The proposed framework integrates these perspectives by positioning DCRA as the process through which AI-supported analysis may be converted into updated and prioritized risk information, and CSA as the decision-oriented capability through which that information is perceived, interpreted, and used.

This relationship remains conceptual rather than causally established. The cross-sectional survey did not test whether AI improved DCRA performance, whether DCRA mediated the relationship between AI and CSA, or whether the framework reduced cybersecurity incidents. The model should therefore be interpreted as a stakeholder-informed set of proposed relationships and design requirements requiring further evaluation through operational deployment, longitudinal research, and studies involving verified SME samples.

Overall, the study contributes empirical evidence concerning stakeholder familiarity, reported use, expectations, and concerns, together with a conceptual integration of AI-enabled analysis, dynamic risk assessment, situational awareness, human oversight, and organizational readiness. Its principal implication is that AI-enabled DCRA should not be evaluated solely through technical performance. Its operational value also depends on whether the resulting risk information is relevant, explainable, trusted, compatible with existing processes, and usable within the resource constraints of the intended organization.

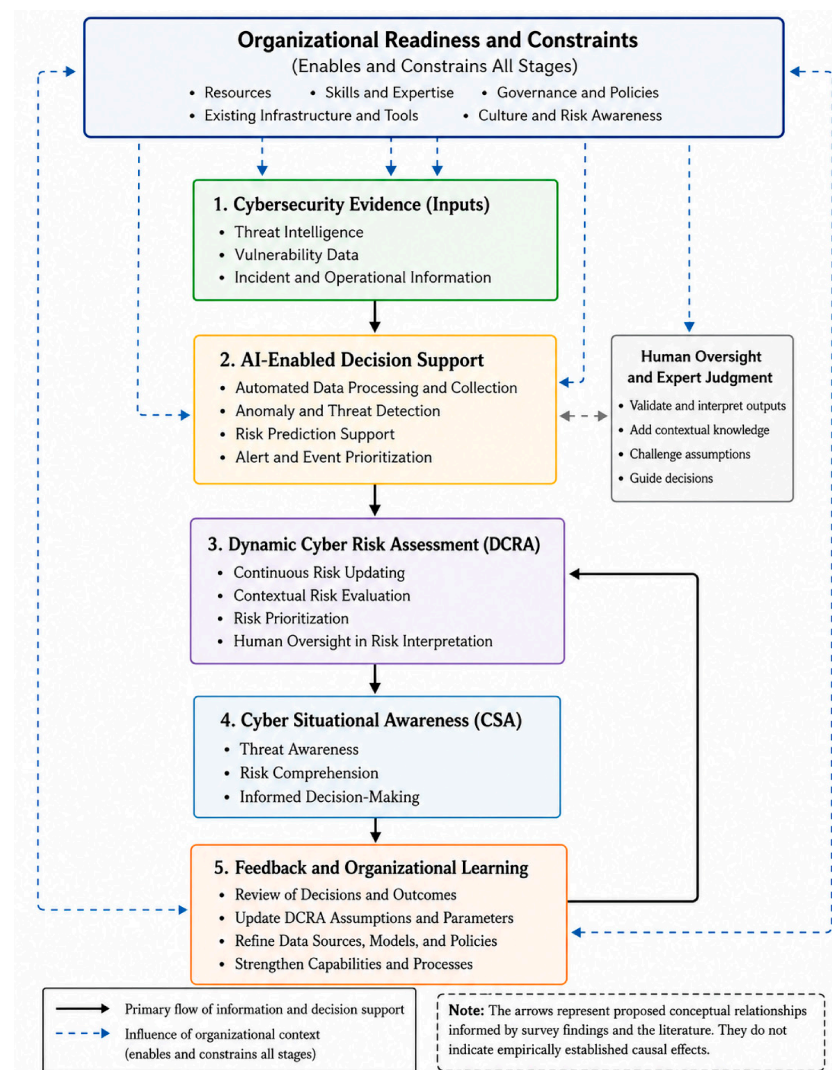


Figure 9. SME-oriented conceptual framework.

5.6. Limitations

The study has several limitations. First, it used a cross-sectional, self-selected sample. Second, responses were self-reported and may be affected by interpretation, recall, or social-desirability bias. Third, several follow-up measures were conditional, producing different denominators and small subgroups. Fourth, a small number of finished records contained missing or out-of-range codes, which were excluded item by item. Finally, the reliability and one-factor results apply only to four specified measures and do not establish criterion validity.

6. Conclusions

This study examined stakeholder perceptions of CSA, DCRA, and the potential role of AI in supporting these capabilities. The survey findings were used to develop an SME-oriented conceptual framework that connects cybersecurity evidence, AI-enabled decision support, dynamic risk updating, human interpretation, and organizational readiness.

In regard to RQ1, the results show a significant difference between the conceptual familiarity and the reported operational application. Although a substantial share of respondents reported some familiarity with CSA, only 18.4% reported previous use. The disparity was greater for DCRA users, of whom only 7.2% reported previous use. These results suggest that the knowledge of CSA and DCRA terminology has not always been

translated into established organizational procedures, tools, or decision routines. The results therefore indicate an implementation gap rather than a knowledge gap.

For RQ2, the major requirements for the development of DCRA were continuous threat updates, identification of attacks and vulnerabilities, and risk-based prioritization of alerts, which also reflect stakeholders' expectations for timely, adaptable, and actionable risk information rather than periodic or static assessments. The respondents reported accuracy and relevance, integration with existing infrastructure, adaptability to evolving threats, and system complexity as the primary barriers to implementation. This combination suggests that the operational value of DCRA is not only a function of the frequency of risk updates but also of the reliability, understandability, compatibility, and usability of the resulting information within the available organizational resources. RQ3 revealed broad yet conditional support for AI. Respondents requested anomaly detection, threat classification, prediction, large-volume analysis, and prioritization, but also cited concerns of bias, trust, cost, and complexity.

RQ4 was addressed by organizing these findings into a framework in which AI supports evidence analysis, DCRA converts changing evidence into prioritized risk information, and CSA represents the human and organizational interpretation used for decisions. Future research should evaluate the framework through technical comparison and longitudinal field studies. Relevant outcomes include decision quality, response time, false-positive burden, user understanding, calibration, maintenance effort, and cybersecurity outcomes over time.

Practical Recommendations

The findings support the following practical recommendations for organizations and researchers working with SMEs:

- Establish shared, operational definitions and requirements of CSA and DCRA before introducing automation.
- Introduce dynamic assessment gradually, beginning with critical assets and traceable evidence.
- Use AI for analysis and prioritization while retaining human risk ownership and approval.
- Connect DCRA outputs to clear CSA communication, escalation, and feedback processes.
- Match deployment scope to available data, skills, budget, integration capacity, and maintenance effort.
- Maintain a documented cycle for model drift, threat intelligence, standards, regulatory change, and user feedback.
- Validate the framework through comparative, longitudinal, and operational studies in verified SME environments.

Author Contributions: Conceptualization and methodology, M.A., L.N. and F.C.; investigation, data curation, formal analysis, visualization, and writing—original draft, M.A.; supervision and writing—review and editing, L.N. and F.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was approved by Cardiff Metropolitan University (reference CST_Ethics_App_PhDStudent_MAlmalki_20240613_16).

Informed Consent Statement: Informed consent was obtained electronically from all participants before participation.

Data Availability Statement: The anonymized data supporting the findings of this study are available from the corresponding author upon reasonable request. The data are not publicly available because they were collected from human participants and are subject to the conditions of the ethical approval and participant consent. Access may be provided only where it is consistent with applicable ethical and institutional requirements.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

SMEs	Small and medium-sized enterprises.
DCRA	Dynamic cyber risk assessment.
CSA	Cyber situational awareness.
AI	Artificial intelligence.

Appendix A. Initial Qualtrics Survey Questions

English ▼

(Questions about you)

Your Views Matter!

The research aims to evaluate the viewpoints regarding the utilisation of AI to enhance cyber situational awareness and enable dynamic cyber risk assessment.

Almalki at Cardiff Metropolitan University is conducting the research project.

You have been cordially invited to take part in this survey as one of numerous individuals recruited via email.

Your previous expertise is not required.

The survey should take approximately 20 minutes to complete.

Thank you for agreeing to participate in this research.

PARTICIPANT INFORMATION SHEET

Project reference number: CST_Ethics_App_PhDStudent_MAlmalki_20240613_16

Before making a decision, it is crucial for you to comprehend the purpose of the study and its requirements. We urge you to read the following information attentively to make an informed decision.

What is the purpose of the study?

This is an online survey exploring users' views on how to enhance cyber situational awareness (CSA) and dynamic cyber risk assessment (DCRA). Data collection will occur in July 2024. The participants' views will help the researcher understand users' perceptions of CSA and DCRA and influence the development of a new method.

Do I have to take part?

Participation in the project is voluntary and requires you to complete and accept the Participant Consent Form before you can take part. You have the right to withdraw from the investigation at any point during the data collection process by simply closing your web browser. If you wish to withdraw your data from the study once it has been collected, you may do so within seven days of the data collection process by emailing the Principal Investigator at st20252905@cardiffmet.ac.uk and quoting the study reference number and your withdrawal code from the survey. After the 7-day withdrawal period, it will not be possible to extract your data as all data will be anonymised. If you require more information on the actions that the University will take upon receiving a withdrawal request, a Participant Withdrawal Form is available.

Are there any risks associated with taking part?

No risks are expected for the participants in this study. The Principal Investigator will be happy to answer any queries about what the study involves.

Are there any benefits associated with taking part?

Additionally, your feedback will help influence the development of a new ML-dependent method.

What will happen to the results of the research project?

The study's purpose is to enhance the design and user experience of a new CSA and DCSA. It aims to collect data and insights on users' perspectives on them. The findings will be shared through project reports and academic channels like conferences and journals.

How will my data and my privacy be protected?

Once data collection has finished, all data will be anonymised within a 7-day withdrawal period by removing the only way to link responses to a participant - the withdrawal code created by the participant in the survey. The data collected will only be used for research purposes after it has been fully anonymised. All data will be stored securely on the account of st20252905@cardiffmet.ac.uk from Cardiff Metropolitan University. Any data held elsewhere will be deleted. Only data that is required for the completion of the study will be collected, and it will include no personal identifiers. Once the collection of your data has finished and the 7-day withdrawal period has passed, it will not be possible to extract your data from the data set as all data is anonymous. The anonymous data will be held for ten years after the project's completion.

Who is involved in the project? Almalki, a researcher at Cardiff Metropolitan University, is conducting this research project. If you have any questions or need further information, please email the Principal Investigator, Almalki, at st20252905@cardiffmet.ac.uk

☐ I confirm that I have read and understood the information sheet for this study and agree to participate in it.

Please indicate your age.

- ☐ 18-24 years old
- ☐ 25-34 years old
- ☐ 35-44 years old
- ☐ 45-54 years old
- ☐ 55-64 years old
- ☐ 65+ years old

Please indicate your gender.

- ☐ Male
- ☐ Female
- ☐ Prefer to self-describe (please specify)

Please indicate your educational degree.

- ☐ High school
- ☐ Bachelor degree
- ☐ Master degree
- ☐ Doctorate degree
- ☐ Other (please specify)

Please indicate your employment state.

- ☐ Working full-time
- ☐ Working part-time
- ☐ Distance working
- ☐ Unemployed
- ☐ Study
- ☐ Retired
- ☐ Other (please specify)

Please indicate the name of your home country.

Please indicate the country in which you currently reside.

Are you an IT or cybersecurity specialist?

- ☐ Yes
- ☐ No

Do you hold a leadership position?

- ☐ Yes
- ☐ No

(Cybersecurity questions)

Now, we would like to ask you some questions about cybersecurity.

How important do you think cybersecurity is?

- ☐ Extremely important
☐ Very important
☐ Moderately important
☐ Slightly important
☐ Not at all important

Do you believe that there are currently challenges within the realm of cybersecurity?

- ☐ Agree
☐ Neither agree nor disagree
☐ Disagree

We understand the importance of addressing challenges in cybersecurity.

What are the significant challenges you see in cybersecurity?

	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
Poor cyber situational awareness	☐	☐	☐	☐	☐
Increasing the adoption of innovative technologies	☐	☐	☐	☐	☐
Traditional cybersecurity approaches in risk assessment and responding to evolving threats	☐	☐	☐	☐	☐
The lack of cybersecurity specialists	☐	☐	☐	☐	☐
Employing AI capabilities in the cyber attack	☐	☐	☐	☐	☐
The lack of sufficient employment of AI capabilities in cyber defence	☐	☐	☐	☐	☐
Absence of a legal and regulatory framework for cybersecurity	☐	☐	☐	☐	☐

Do you believe there are additional challenges in cybersecurity that were not mentioned in the previous question?

☐ No

☐ Yes (please specify)

Do you think Small and Medium Enterprises (SMEs) need more attention and support in terms of cybersecurity?

☐ Yes

☐ Maybe

☐ No

Which sectors below do you believe are critical and require more attention regarding cybersecurity?

	Extremely critical	Very critical	Moderately critical	Slightly critical	Not critical at all
Financial services sector	☐	☐	☐	☐	☐
Healthcare and public health	☐	☐	☐	☐	☐
sector	☐	☐	☐	☐	☐
Government facilities sector	☐	☐	☐	☐	☐
Energy sector	☐	☐	☐	☐	☐
Food and agriculture sector	☐	☐	☐	☐	☐
Transportation systems sector	☐	☐	☐	☐	☐
Communications and IT	☐	☐	☐	☐	☐
sector					
Water and wastewater					
systems					

Do you believe that there are other sectors that require more attention and support in terms of cybersecurity, which were not mentioned in the previous question?

☐ No

☐ Yes (please specify)

Of the following threats, what do you consider to be significant threats in the field of cybersecurity?

Extremely significant	Very significant	Moderately significant	Slightly significant	Not significant at all
--------------------------	---------------------	---------------------------	-------------------------	------------------------------

Data Breaches	☐	☐	☐	☐	☐
Remote Work Environments	☐	☐	☐	☐	☐
Mobile Attacks	☐	☐	☐	☐	☐
Phishing	☐	☐	☐	☐	☐
Ransomware	☐	☐	☐	☐	☐
Cryptojacking	☐	☐	☐	☐	☐
IoT Attacks	☐	☐	☐	☐	☐
Social Engineering	☐	☐	☐	☐	☐
Vulnerability in the Cloud	☐	☐	☐	☐	☐
Third-Party Vulnerabilities (Vendors, Contractors, Partners)	☐	☐	☐	☐	☐
Vulnerabilities in systems					
Advanced persistent threat (APT)					

Do you believe that there are additional significant threats in the field of cybersecurity that were not mentioned in the previous question? Your insights will help us identify potential threats.

- ☐ No
- ☐ Yes (please specify)

(Cyber situational awareness questions)

Now, we would like to ask you some questions about cyber situational awareness (CSA).

A comprehensive understanding of the cyber environment is needed to assess the potential impact of risk on the business effectively.

Do you agree?

- ☐ Strongly disagree
- ☐ Somewhat disagree
- ☐ Neither agree nor disagree
- ☐ Somewhat agree
- ☐ Strongly agree

"The CSA concept involves understanding an organisation's IT environment, cybersecurity threats, and potential impact. It helps organisations make informed decisions, prioritise resources, and respond effectively to cyber incidents."

How familiar are you with the concept of CSA?

- ☐ Extremely familiar
- ☐ Very familiar
- ☐ Moderately familiar
- ☐ Slightly familiar
- ☐ Not familiar at all

Have you ever utilised the concept of a CSA?

- ☐ Yes
- ☐ No
- ☐ I do not know

How do you usually get information about the state of CSA?

- ☐ Paper documents
- ☐ Automatic via electronic system
- ☐ Other (please specify)

What software do you use to get information on the CSA state?

How often do you get updates about the CSA state?

- ☐ Daily
- ☐ Weekly
- ☐ Monthly
- ☐ Quarterly
- ☐ Yearly

Do you believe that CSA needs to be improved?

- ☐ Yes
- ☐ Maybe
- ☐ No

What advantages do you anticipate will be driven by enhancing CSA?

(Please drag and drop options in order of importance (1 = very important and 4= least important))

Enhance cybersecurity risk assessment and the response to evolving threats

Better Resource Allocation

Making wised decisions

Improved Business Continuity

Do you believe that there are other advantages to enhancing CSA that were not mentioned in the previous question?

- ☐ No
- ☐ Yes (please specify)

(Dynamic cyber risk assessment questions)

Now, we would like to ask you some questions about dynamic cyber risk assessment (DCRA).

"DCRA is the continuous process of identifying and assessing risks to the cyber environment dynamically and in real-time to aid in making informed decisions that are key to protecting systems effectively. Moreover, it enhances resilience against cyber threats".

How familiar are you with the concept of DCRA?

- ☐ Extremely familiar
- ☐ Very familiar
- ☐ Moderately familiar
- ☐ Slightly familiar
- ☐ Not familiar at all

Have you utilised a DCRA before?

- ☐ Yes
- ☐ No
- ☐ I don't know

Which DCRA software or system did you use?

How often do you deal with DCRA?

- ☐ Daily
- ☐ Weekly
- ☐ Monthly
- ☐ Quarterly
- ☐ Yearly

In your opinion, could using DCRA enhance CSA?

- ☐ Yes
- ☐ Maybe
- ☐ No

How can DCRA enhance CSA?

(You can select more than one answer).

- ☐ Identifying potential threats early and responding more effectively
- ☐ Increase the awareness of individuals of surroundings and potential threats
- ☐ Empower to make informed decisions
- ☐ To be more suitable for situations where the security landscape is constantly shifting
- ☐ Improved resource allocation (decrease the need for a high budget or more specialists)

Do you believe that there are other ways DCRA can enhance CSA that were not mentioned in the previous question?

- ☐ No
- ☐ Yes (please specify)

Do you believe that DCRA needs to be improved?

- ☐ Yes
☐ No
☐ I do not know

What aspects do you believe are essential to consider when developing the DCRA system?

	Extremely critical	Very critical	Moderately critical	Slightly critical	Not critical at all
Integrate data from diverse sources.	☐	☐	☐	☐	☐
Process real-time data streams.	☐	☐	☐	☐	☐
Identify potential attacks and	☐	☐	☐	☐	☐
vulnerabilities.	☐	☐	☐	☐	☐
Continuously update understanding of	☐	☐	☐	☐	☐
threats.	☐	☐	☐	☐	☐
Automating routine tasks.	☐	☐	☐	☐	☐
Implementing a system to prioritise	☐	☐	☐	☐	☐
alerts based on risk.	☐	☐	☐	☐	☐
Human intervention should remain an	☐	☐	☐	☐	☐
essential aspect.	☐	☐	☐	☐	☐
Adapt to the specific needs and risk					
profile.					
Generate real-time reports.					
Easy to use.					

Are there other significant aspects essential to consider when developing the DCRA system that were not mentioned in the previous question?

- ☐ No
☐ Yes (please specify)

When seeking to implement a new dynamic approach to cyber risk assessment, what challenges do you foresee encountering?

	Extremely critical	Very critical	Moderately critical	Slightly critical	Not critical at all
System complexity	☐	☐	☐	☐	☐
Cost	☐	☐	☐	☐	☐
Accuracy and Relevance	☐	☐	☐	☐	☐
Integration with existing infrastructure	☐	☐	☐	☐	☐
Human expertise	☐	☐	☐	☐	☐
integration	☐	☐	☐	☐	☐
The adaptability of the evolving threats	☐	☐	☐	☐	☐
Balancing security with usability	☐	☐	☐	☐	☐

Are there other challenges you foresee encountering in implementing a new dynamic approach to cyber risk assessment that were not mentioned in the previous question?

☐ No

☐ Yes (please specify)

(Artificial Intelligence questions)

Now, we would like to ask you some questions about using artificial intelligence (AI).

Would you endorse the use of AI in cybersecurity systems?

☐ Yes

☐ No

Why would you not endorse the use of AI in cybersecurity systems?
(You can select more than one answer).

AI can be expensive to implement and maintain.

AI can be biased if the data it is trained on is biased; this can lead to unfair or inaccurate results.

- ☐ AI systems can be complex and challenging to understand; this can make it hard to trust their decisions.
- ☐ Other (please specify)

☐

Why would you endorse the use of AI in cybersecurity systems?

(You can select more than one answer).

- ☐ AI automates tasks, freeing up human employees to focus on more creative or strategic work.
- ☐ AI is fast and accurate in analysing data to identify patterns and trends that humans might miss.
- ☐ AI can be used to develop services that humans might not be able to do.
- ☐ AI reduces cost and effort.
- ☐ Other (please specify)

Would you believe that using AI could enhance CSA?

- ☐ Yes
- ☐ No
- ☐ I do not know

What do you think is the most important factor for using AI to enhance CSA?

	Extremely crucial	Very crucial	Moderately crucial	Slightly crucial	Not crucial at all
Providing advanced capabilities in threat detection, detecting anomalies, prediction, and response.	☐	☐	☐	☐	☐
The cybersecurity processes are more transparent and easy to understand.	☐	☐	☐	☐	☐
Monitor and analyse vast amounts of data.	☐	☐	☐	☐	☐
Provide powerful, proactive cyber threat intelligence to classify and interpret potential threats.	☐	☐	☐	☐	☐
Providing real-time insights and alerts about potential risks.	☐	☐	☐	☐	☐
Empower employees to respond promptly to security incidents and effectively prevent cyber-attacks.					

Do you believe there are significant factors for using AI to enhance CSA that were not mentioned in the previous question?

- ☐ No
- ☐ Yes (please specify)

Can the utilisation of AI enhance DCRA processes?

- ☐ Yes
- ☐ No
- ☐ I do not know

What do you think is the most important factor for using AI to enhance DCRA processes?

	Extremely crucial	Very crucial at all	Moderately Continuous Threat Analysis.	Slightly crucial	Not crucial
Data Processing and Prioritisation.	☐	☐	☐	☐	☐
Predict Future Attacks.	☐	☐	☐	☐	☐
Improved Risk Assessments.	☐	☐	☐	☐	☐
Integration with Other Security Tools.	☐	☐	☐	☐	☐
Helping the Cybersecurity Specialists to Focus on	☐	☐	☐	☐	☐
Proactive Defense.	☐	☐	☐	☐	☐

Do you believe there are other significant factors for using AI to enhance the DCRA process that were not mentioned in the previous question?

- ☐ No
- ☐ Yes (please specify)

(Share your thoughts on the survey topics)

Is there anything else that you would like to share with us on the survey topics?

- ☐ No
- ☐ Yes (please specify)

Powered by Qualtrics

Appendix B. Exploratory Logistic Regression of AI Endorsement

A binary logistic regression was conducted as an additional exploratory analysis to examine whether specialist status, leadership status, CSA familiarity, and DCRA familiarity independently predicted endorsement of AI in cybersecurity (complete-case $n = 293$). The

model was statistically significant overall, (likelihood-ratio chi-square(4) = 12.17, $p = 0.016$) but its explanatory contribution was limited (McFadden's R-squared = 0.039). None of the four predictors was independently significant after the remaining variables were controlled. The model therefore provides no basis for attributing AI endorsement to a single professional role or familiarity variable. AI endorsement may instead depend on organizational, practical, and attitudinal factors that were not fully measured in the survey. The complete regression estimates, confidence intervals, and interpretations are presented in Table A1.

Table A1. Binary logistic regression predicting endorsement of AI in cybersecurity.

Predictor	Odds Ratio	95% Confidence Interval	p	Interpretation
Cybersecurity specialist status	1.46	[0.76, 2.81]	0.260	Not independently associated with AI endorsement
Leadership status	1.64	[0.89, 3.03]	0.114	Not independently associated with AI endorsement
CSA familiarity	0.99	[0.76, 1.28]	0.918	No independent association
DCRA familiarity	1.24	[0.95, 1.61]	0.106	Positive tendency, but not statistically significant

Note. Complete-case $n = 293$. Overall model: likelihood-ratio chi-square(4) = 12.17, $p = 0.016$; McFadden's R-squared = 0.039. Odds ratios above one indicate higher estimated odds of AI endorsement, but the effect is not statistically significant when its confidence interval includes one and $p > 0.05$.

References

- Wang, K.; Guo, X.; Yang, D. Research on the Effectiveness of Cyber Security Awareness in ICS Risk Assessment Frameworks. *Electronics* **2022**, *11*, 1659. [\[CrossRef\]](#)
- Bada, M.; Nurse, J.R. Developing Cybersecurity Education and Awareness Programs for Small- And Medium-Sized Enterprises (SMEs). *Inf. Comput. Secur.* **2019**, *27*, 393–410. [\[CrossRef\]](#)
- Carias, J.F.; Borges, M.R.S.; Labaka, L.; Arrizabalaga, S.; Hernantes, J. Systematic Approach to Cyber Resilience Operationalization in SMEs. *IEEE Access* **2020**, *8*, 174200–174221. [\[CrossRef\]](#)
- Endsley, M.R. Toward a Theory of Situation Awareness in Dynamic Systems. *Hum. Factors J. Hum. Factors Ergon. Soc.* **1995**, *37*, 32–64. [\[CrossRef\]](#)
- Jiang, L.; Jayatilaka, A.; Nasim, M.; Grobler, M.; Zahedi, M.; Babar, M.A. Systematic Literature Review on Cyber Situational Awareness Visualizations. *IEEE Access* **2022**, *10*, 57525–57554. [\[CrossRef\]](#)
- Chaudhary, S.; Gkioulos, V.; Katsikas, S. Developing metrics to assess the effectiveness of cybersecurity awareness program. *J. Cybersecur.* **2022**, *8*, tyac006. [\[CrossRef\]](#)
- Ross, R.; Winstead, M.; McEvilly, M. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018.
- Craigen, D.; Diakun-Thibault, N.; Purse, R. Technology Innovation Management Review: Defining Cybersecurity. *Technol. Innov. Manag. Rev.* **2014**, *4*, 13–21. [\[CrossRef\]](#) [\[PubMed\]](#)
- van Haastrecht, M.; Sarhan, I.; Shojafar, A.; Baumgartner, L.; Mallouli, W.; Spruit, M. A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs. In Proceedings of the ARES 2021: The 16th International Conference on Availability, Reliability and Security, Virtual, 17–20 August 2021; pp. 1–12.
- Trantidou, T.; Bravos, G.; Valoggia, P.; Skourtis, I.; Falelakis, M.; Poullos, K.; Spais, I.; Ioannidis, S.; Oudin, T.; Costa, R.; et al. SENTINEL-Approachable, Tailor-Made Cybersecurity and Data Protection for Small Enterprises. In Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience (CSR), Virtual, 27–29 July 2022; pp. 112–117.
- Hasani, T.; O'reilly, N.; Dehghantanha, A.; Rezania, D.; Levallet, N. Evaluating the Adoption of Cybersecurity and Its Influence on Organizational Performance. *SN Bus. Econ.* **2023**, *3*, 97. [\[CrossRef\]](#) [\[PubMed\]](#)
- Chandna, V.; Tiwari, P. Cybersecurity and the New Firm: Surviving Online Threats. *J. Bus. Strat.* **2021**, *44*, 3–12. [\[CrossRef\]](#)
- Shojafar, A.; Järvinen, H. Classifying SMEs for Approaching Cybersecurity Competence and Awareness. In Proceedings of the ARES 2021: The 16th International Conference on Availability, Reliability and Security, Virtual, 17–20 August 2021; pp. 1–7.
- Neri, M.; Niccolini, F.; Pugliese, R. Assessing SMEs' Cybersecurity Organizational Readiness: Findings from an Italian Survey. *Online J. Appl. Knowl. Manag.* **2022**, *10*, 1–22. [\[CrossRef\]](#) [\[PubMed\]](#)

15. Tsiodra, M.; Panda, S.; Chronopoulos, M.; Panaousis, E. Cyber Risk Assessment and Optimization: A Small Business Case Study. *IEEE Access* **2023**, *11*, 44467–44481. [\[CrossRef\]](#)
16. Hutton, G. *Business Statistics*; Briefing paper number 06152; The House of Commons Library: London, UK, 2022.
17. Lewis, S. Cyber Attack Warning for SMEs as Risks Heighten amid COVID-19 Pandemic. *Professional Jeweller*, 18 August 2020.
18. Renaud, K.; Ophoff, J. A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organ. Cybersecur. J. Pract. Process People* **2021**, *1*, 24–46. [\[CrossRef\]](#)
19. Ncubekezi, T.; Mwansa, L.; Rocaries, F. A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses. In Proceedings of the 2020 15th International Conference for Internet Technology and Secured Transactions (ICITST), Virtual, 8–10 December 2020; pp. 1–6.
20. Burgess, T.F. *A General Introduction to the Design of Questionnaires for Survey Research*; University of Leeds: Leeds, UK, 2001.
21. Da Veiga, A.; Martins, N. Information security culture: A comparative analysis of four assessments. In Proceedings of the 8th European Conference on IS Management and Evaluation, Gent, Belgium, 11–12 September 2014; pp. 49–57.
22. Da Veiga, A. An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. *Inf. Comput. Secur.* **2018**, *26*, 584–612. [\[CrossRef\]](#)
23. Da Veiga, A.; Martins, N. The value of using a validated information security culture instrument. In Proceedings of the 8th European Conference on IS Management and Evaluation, Gent, Belgium, 11–12 September 2014; pp. 146–154.
24. Cheimonidis, P.; Rantos, K. Dynamic Risk Assessment in Cybersecurity: A Systematic Literature Review. *Futur. Internet* **2023**, *15*, 324. [\[CrossRef\]](#)
25. Riesco, R.; Villagr , V.A. Leveraging Cyber Threat Intelligence for a Dynamic Risk Framework. *Int. J. Inf. Secur.* **2019**, *18*, 715–739. [\[CrossRef\]](#)
26. Angelelli, M.; Arima, S.; Catalano, C.; Ciavolino, E. Cyber-Risk Perception and Prioritization for Decision-Making and Threat Intelligence. *arXiv* **2023**, arXiv:2302.08348. [\[CrossRef\]](#)
27. Raimundo, R.; Ros rio, A.T. The Impact of Artificial Intelligence on Data System Security: A Literature Review. *Sensors* **2021**, *21*, 7029. [\[CrossRef\]](#) [\[PubMed\]](#)
28. Hamon, R.; Junklewitz, H.; Garrido, J.S.; Sanchez, I. Three Challenges to Secure AI Systems in the Context of AI Regulations. *IEEE Access* **2024**, *12*, 61022–61035. [\[CrossRef\]](#)
29. Naik, B.; Mehta, A.; Yagnik, H.; Shah, M. The Impacts of Artificial Intelligence Techniques in Augmentation of Cybersecurity: A Comprehensive Review. *Complex Intell. Syst.* **2021**, *8*, 1763–1780. [\[CrossRef\]](#)
30. Perozzo, H.; Zaghloul, F.; Ravarini, A. CyberSecurity Readiness: A Model for SMEs Based on the Socio-Technical Perspective. *Complex Syst. Inform. Model. Q.* **2022**, *33*, 53–66. [\[CrossRef\]](#)
31. Zhu, Q.; Qin, Y.; Zhou, C.; Gao, W. Extended Multilevel Flow Model-Based Dynamic Risk Assessment for Cybersecurity Protection in Industrial Production Systems. *Int. J. Distrib. Sens. Netw.* **2018**, *14*, 155014771877956. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.