SCIENTIFIC CULTURE

www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 5, (2026), pp. 2072-2084
Open Access. Online & Print

DOI: 10.5281/zenodo.21301279

ADAPTIVE RESILIENCE IN OPERATIONAL TECHNOLOGY CYBERSECURITY: A SOCIO-TECHNICAL ANALYSIS OF TECHNICAL, ORGANIZATIONAL, AND DIVERSITY FACTORS

Shaikha Ali Aldhaheri[1*]

Email: S.dhaheri@hotmail.com

Received: 03/04/2026
Accepted: 09/05/2026

Corresponding Author: Shaikha Ali Aldhaheri (S.dhaheri@hotmail.com)

ABSTRACT

This research explores the issues affecting adaptive resilience in OT cybersecurity from a socio-technological point of view. The study will look at how technical, organizational, and human factors influence resilience capability in OTs that have become more interconnected than before. Quantitative methodology was employed with a structured survey questionnaire administered to professionals in the field of OT, IT, and cybersecurity in the United States, the United Kingdom, the Middle East and the United Arab Emirates (UAE). The data collected was analyzed using Statistical Package for the Social Sciences (SPSS) with descriptive statistics, reliability analysis, correlation analysis and regression analysis being performed on the collected data. The findings show that technical readiness, adaptive design orientation, human and organizational effectiveness, resilience-by-design thinking, workforce diversity, and women involvement have positive influences on adaptive resilience capability. On the other hand, the cybersecurity skill shortage adversely affects resilience. The findings also demonstrate the significance of considering both technical and socio-organizational aspects for enhancing cybersecurity resilience in OT settings. The paper adds to the literature through its proposal of an integrated socio-technical framework for adaptive resilience for OT cybersecurity. The paper goes even further in its contribution by considering workforce diversity and women's participation as important variables in resilience.

KEYWORDS: Operational Technology (OT), Adaptive Resilience, Cybersecurity, Socio-Technical Systems, Workforce Diversity, Cybersecurity Skills Gap.

1. INTRODUCTION

Historically, operational technology (OT) systems were configured to work in closed and strictly regulated environments, hinging on air-gapped designs to promote security, resiliency, and operational resilience (Kumar & Vardhan, 2025). These systems are the backbone of the important areas of infrastructure, including energy, manufacturing, transportation, and utilities, and were conventionally safeguarded by physical isolation of external networks (Mekala, Baig, Anwar, & Zeadally, 2023). Nevertheless, the fast development of digital technologies, such as industrial automation, cloud computing, and remote monitoring, has impacted the nature of OT environments' structures and their operations in the most fundamental way (Zhukabayeva, Zholshiyeva, Karabayev, Khan, & Alnazzawi, 2025). The growing convergence of OT and Information Technology (IT) has brought with it new efficiencies and capabilities, yet it has brought the scope of cyber threats to a new and vast size (George, 2024).

With the closer integration of OT systems, existing cyber threats are growing more complex and dynamic and are expanding into new territories. The possibility of devastating operational, financial, and safety impacts has been proven in high-profile cyber-attacks against industrial control systems (Sangkhro & Agrawal, 2023). In that regard, the classical means of cybersecurity, which is mostly centered around prevention and perimeter protection, is no longer an effective measure. Unchanging security solutions are not effective at solving dynamic and persistent threats, especially within an environment that operates on a legacy platform, is constrained by real-time operation, and has the affordance of downtime (Jibotean & Stan, 2025).

In order to cope with these problems, more and more often, it is understood that a shift out of traditional security models to more dynamic and flexible strategies is necessary. Cyber resilience has become a key concept in these aspects, and it focuses on the capability to avert cyber incidents as well as detect, respond to, recover from, and adapt to them (Verma, Newe, O'Mahony, Brennan, & O'Shea, 2025). In contrast to the older paradigms of security, the resiliency-based ones recognize the inevitability of breaches and shift the emphasis to the resilience of systems under adverse conditions in terms of functionality and minimization of disruption (Annarelli, Nonino, & Palombi, 2020).

Even though it is relevant, the use of cyber resilience within the OT setting has not yet been developed. Current frameworks frequently rely on IT-biased views and do not take into consideration the specifics of operations and the safety of OT systems (Ramachandran, Smith, David, Al-Hadhrami, & Acharya, 2025). Additionally, most existing strategies focus on the technical control but ignore the larger socio-technical complex where cybersecurity takes place. Practically, good resilience requires not just the technological capacity but also human decision-making, coordination within the organization, and a governance framework (Dunn Cavelty, Eriksen, & Scharte, 2023).

The lack of a skilled workforce in the cybersecurity sector is another significant issue, especially in the domains of specialized applications, such as OT security (Namukasa, Ficke, & Piasecki, 2023). The high rate of technological change has also magnified the need to specialize, hence a serious skills gap, which restricts organizations from successfully handling cyber risks. This lack is further exacerbated by the underrepresentation of certain groups, such as women, in cybersecurity roles (Tuma & Van Der Lee, 2022). Therefore, workforce diversity is receiving increasing attention as a strategy to drive innovation, improve the quality of decision-making, and increase overall organizational resilience.

The proposed study addresses these issues by formulating and empirically analyzing an adaptive resilience model of OT cybersecurity incorporating technical, organizational, and human aspects. Based on a bio-inspired understanding, the research envisions resilience as a dynamic capacity that is similar to a self-imposed immune system, that of a human body, which is continually sensitive, reactive, and educative to threats. Based on this theoretical framework, the study examines how critical elements, such as technical preparedness, adaptive design orientation, human and organizational performance, resilience-by-design attitude, cybersecurity talent gap, and diversity in the workforce, affect adaptive resilience capability in OT settings.

In other words, the main objective of the current research is to develop an advanced model of adaptive resilience in OT cybersecurity based on empirical data collected from specialists working in the USA, the UK, and the Middle East, which includes the UAE. It should be noted that this research utilizes information gained from different regions with varying degrees of digitalization and maturity of cybersecurity, which allows us to have a comprehensive understanding of the factors involved.

2. LITERATURE REVIEW

2.1. OT Cybersecurity and the Limitations of Traditional Models

Traditionally, OT systems have adopted isolation-based security models, known as "air-gapping", to secure critical infrastructure from cyberattacks (Bharath & Sundharakumar, 2025). Isolation-based systems were engineered with a focus on uptime and safety rather than security, as such systems were not typically connected to wide-area networks (Asuquo, Usoh, Stephen, chikezie Samuel, & Awodeyi, 2022). This approach has become less effective, given the growing use of digital technologies, remote access, and automation.

Recent research indicates that conventional perimeter-based security controls are ineffective in today's OT environments, given the complexity and integration of operational systems (Ojha & Vaish, 2025; Raich, Raich, & Kinhekar, 2025; Sekar, 2025). The presence of outdated systems and real-time constraints makes it difficult to apply traditional cybersecurity measures. This leaves organizations exposed to advanced persistent threats, able to circumvent traditional security measures (Arora, 2025; Zhukabayeva et al., 2025). There is a clear recognition that a shift from prevention to detection, response, and recovery is needed to supplement traditional prevention-based cybersecurity models (Jaffal, Alkhanafseh, & Mohaisen, 2025).

2.2. Cyber Resilience as an Evolving Paradigm

The concept of cyber resilience plays an important role in addressing the gaps in current cybersecurity frameworks (Verma et al., 2025). In contrast to the conventional paradigm of cybersecurity, which prioritizes prevention through continuity of the system irrespective of the disruption, resilience refers to anticipation, endurance, recovery, and adaptation against any threat (Shabanian-Poodeh, Hooshmand, Shafie-Khah, & Siano, 2025; Verma et al., 2025). Nevertheless, such frameworks are mostly conceived in an IT environment and might not have considered the unique characteristics of the OT environment.

OT environments are characterized by safety-critical systems, high availability, and lower tolerance for system disruptions (Caviglia, 2025). Thus, resilience in OT environments goes beyond technology and embraces operations and safety. Adaptive resilience is the next generation resilient framework and centers around learning and evolution (Havi, 2025). Drawing inspiration from the natural world, adaptive resilience emphasizes detecting, responding, and learning from the threat for the system to adapt. Although theoretically relevant, research on adaptive resilience in the cybersecurity framework in the OT environment is scanty (Anwar et al., 2025).

2.3. Technical Readiness and Adaptive Design Orientation

Technical capabilities form the foundation of cybersecurity resilience. Studies stress the role of monitoring, anomaly detection, and incident response processes to detect and respond to cyber-attacks (Malatji, Marnewick, & Von Solms, 2022). Network segmentation, secure communication protocols, and access control are also considered key elements of an OT security plan (Baligodugula, Ghimire, & Amsaad, 2024). Beyond technical preparedness, there has been a growing focus on an adaptive system design orientation. This concept promotes the design of adaptive systems and the ability to adapt to new threats (Ruggiero, Piotrowicz, & John, 2024). Layered defence systems are frequently seen as best practices for enhancing resilience. Layered defence refers to the application of multiple security layers. This approach minimises the risk of a complete breach in the system because even if one layer fails, other layers will be there (Calder, 2023). Nevertheless, the effectiveness of technical measures does not depend solely on the measures themselves; rather, it depends on their deployment and management within the broader organisational context.

2.4. Human And Organizational Factors in Cybersecurity

However, recently, much attention has been paid to the human and organisational problems associated with cybersecurity. It is necessary to consider human behaviour and especially the process of decision making under stress in order to identify security incidents and respond to them effectively. In addition, operators and engineers face decision-making in the context of real-time environments, and the consequences may be significant (Richardson, 2024). The organisational problems, such as communication, coordination, and governance, play a key role in terms of the effectiveness of cybersecurity practices. Cooperation of the OT and IT personnel is required in order to manage complex security incidents, and policies and procedures help to make appropriate decisions (Triplett, 2022). Education and training are viewed as the key components of organisational resilience improvement. Despite the importance of these components, they remain overlooked in traditional cybersecurity frameworks that pay attention only to the technical side of security (Khadka & Ullah, 2025).

2.5. Cybersecurity Skills Gap

A critical issue in cybersecurity is the lack of skills. The rapid pace of technological advancements has generated a skill shortage that has increased demand (Anderson Sr, 2025). This issue is especially evident in operational technology (OT) environments, where expertise in both cybersecurity and domain-specific operations is required.(Torgersen, Noble, Ask, & Knox, 2025) This shortage of talent can impede an organisation's capacity to identify and respond to a cyber-attack. It can also impede the implementation and management of robust security measures. Consequently, closing the skills gap is critical for organizations striving to improve cybersecurity (Goupil et al., 2022).

2.6. Workforce Diversity and Gender Inclusion

The importance of employee diversity in terms of driving innovation and productivity has become more recognized (Wolor et al., 2025). In relation to cybersecurity, diverse team members would have the capability to examine issues from different perspectives, which makes them capable of spotting potential threats and coming up with better solutions. (Chindrus & Caruntu, 2023). Especially in cybersecurity, gender diversity has been recognized as important since there are relatively few women in the field. There have been studies that suggest that having more female employees results in effective cooperation, problem-solving, and adaptation to rapidly changing job conditions (Green, 2025). In the case of OT cybersecurity resilience, where uncertainty exists, idea diversity would contribute to resilience.

2.7. Research Gap

Although current research offers valuable contributions to the field of cybersecurity and resilience, there are also gaps in the research. First, non-existent are frameworks that integrate technical, human, and organisational aspects for cybersecurity in OT. Second, empirical research is scarce on adaptive resilience in OT. Third, the contribution of workforce diversity, including gender diversity, to improve cybersecurity resilience has not been adequately understood.

This research aims to fill these gaps by proposing and validating a model of adaptive resilience in OT cybersecurity settings. By integrating technical readiness, adaptive design orientation, human and organisational effectiveness, resilience mindset, skills gap, and employee diversity, the study provides a human-centred view of the drivers of resilience in today's OT environment.

2.8. Research Model and Hypotheses

Drawing on the literature, this research develops a socio-technical model of adaptive resilience capability, which is shaped by a range of technical, organisational, and human factors. Adaptive resilience capability is the capacity of OT systems to sense, make, respond, and adapt to changing cyber threats while effectively operationalising the system.

Our model incorporates six independent variables: technical readiness, focus on adaptive design, human/organizational effectiveness, resilience-by-design mindset, cybersecurity skill gaps, and diversity and inclusion in the workplace, including the role of women as an important aspect of diversity. Technical readiness covers the presence and efficacy of monitoring, detection, and response tools. It is anticipated that companies with more advanced technical ability will detect and address cyber threats, increasing resilience. Design for resilience refers to the degree of a system's agility in adapting to new threats. This can be done using layering and constant process improvements.

People and process effectiveness refer to the significance of competent personnel, decision-making, and collaboration when facing cyber threats. Cybersecurity skills shortfall is the absence of cybersecurity experts, which will lead to closing the gap in the response capacity for dealing with cyber risks. The resilience-by-design approach measures how resilience is taken into consideration during the system and strategic development. Workforce diversity and inclusivity are key to the diversity in the thinking process of those working on cybersecurity issues because it is a problem-solving field. Women are part of the diversity measure and the inclusion of women in terms of building resilience.

Drawing on these ideas, we put forward the following hypotheses:

- H1: Technical preparedness positively impacts adaptive resilience capability in OT cybersecurity.
- H2: Adaptive design orientation has a positive effect on adaptive resilience capability in OT cybersecurity environments.
- H3: Human and organisational effectiveness has a positive effect on adaptive resilience capability in OT cybersecurity environments.
- H4: Cybersecurity skills shortage hurts adaptive resilience capability in OT cybersecurity environments.
- H5: Resilience-by-design philosophy has a positive influence on adaptive resilience capability in OT cybersecurity.

- H6: Diversity and inclusion in the workforce have a positive effect on adaptive resilience capability in OT cybersecurity environments.
- H7: Women in cybersecurity have a positive effect on adaptive resilience capability in OT cybersecurity environments.

3. METHODOLOGY

The current research employs a quantitative research design to investigate factors that affect the adaptive resilience of Operational Technology (OT) cybersecurity systems. We used an empirical survey approach to gather data from individuals with a background in OT and cybersecurity domains, mainly residing in the United States and the United Kingdom. The approach combines the conceptual framework, research hypotheses, data collection, and measurement design.

3.1. Research Design and Data Collection

A survey research design was employed to gather data from OT, IT, and cybersecurity professionals. The population of interest was professionals who manage, operate, or secure OT systems. The questionnaire was administered online through professional networks and forums. The study focuses on respondents from the United States, the United Kingdom, and the Middle East, including the United Arab Emirates (UAE). These regions were selected due to their growing reliance on Operational Technology systems, increasing cybersecurity investments, and expanding digital transformation initiatives across critical infrastructure sectors.

3.2. Measurement Instrument

Based on the conceptual framework of the study and the literature, the questionnaire was developed. **All of the constructs were measured using multiple items on a five-point scale (1 = strongly agree, 5 = strongly disagree). Three items were developed for each construct:**

1. Adaptive Resilience Capability (ARC)
2. Technical Readiness (TR)
3. Adaptive Design Orientation (ADO)
4. Human and Organizational Effectiveness (HOE)
5. Cybersecurity Skills Gap (CSG)
6. Resilience-by-Design Mindset (RDM)
7. Workforce Diversity and Inclusion (WDI)
8. Women's Resilience Contribution (WRC)

The questionnaire was carefully constructed to achieve statement clarity, relevance, and neutrality, taking into account the global nature of the respondents.

3.3. Sample Characteristics

The questionnaire also contained information on the respondents' background (gender, age, education, role, years of experience in work, industry, and experience with operational technology). These were asked for background information, which can be used to further analyse the data.

3.4. Data Analysis Approach

Data were analysed to test the relationships among variables and hypotheses using statistical methods. This involved data screening, determination of reliability, and hypothesis testing. To assess the reliability of the concepts, measures such as Cronbach's alpha were used to calculate internal consistency. Additional data analysis methods, like regression analysis or correlations, were used to assess the relationships between the independent variables and adaptive resilience capability. This analysis approach provides a thorough assessment of the proposed model and insights into the determinants of adaptive resilience in OT cybersecurity contexts.

4. RESULTS

4.1. Reliability Analysis

In preparation for hypothesis testing, the reliability of the composite construct scores comprising eight constructs was analyzed through the use of Cronbach's alpha coefficient. As presented in Table 1 below, the total reliability coefficient of the eight constructs, composed of 24 items combined as composites, yielded α = .889 – an extremely reliable coefficient considering that the acceptable level of reliability for social sciences is .70, according to Nunnally (1978), while the acceptable level for high stakes assessment is .90. No case deletion (listwise) occurred in the analysis of the reliability coefficient since all 277 cases used in the reliability test had complete scores for all constructs included.

Table 1: Reliability Statistics.

Cronbach's α	N of Items
.889	8

Note: Cronbach's α was computed across eight composite construct scores (ARC, TR, ADO, HOE, CSG, RDM, WDI, WRC). Values ≥ .70 indicate acceptable internal consistency (Nunnally, 1978).

4.2. Sample Profile and Descriptive Statistics

The survey consisted of a total of N = 277 respondents sampled from four main regions where their work is performed: the United Kingdom (n = 91, 32.9%), the United Arab Emirates (n = 87, 31.4%), the Middle East Other (n = 53, 19.1%), and the United States (n = 46, 16.6%). This represents an evenly distributed sample among all major OT cybersecurity markets geographically (see Table 2). Female respondents accounted for 65.0% (n = 180) of the sample size, whereas males represented only 33.2% (n = 92). It can be said that the gender distribution is rather unusual in comparison to other studies conducted in the OT sector.

Table 2: Frequency Distribution of Respondent Demographic Characteristics (N = 277).

Variable / Category	n	%
Gender		
Male	92	33.2%
Female	180	65.0%
Non-binary	2	0.7%
Prefer not to say	3	1.1%
Country / Region of Employment		
United States	46	16.6%
United Kingdom	91	32.9%
United Arab Emirates (UAE)	87	31.4%
Middle East (Other)	53	19.1%
Age Group		
20–29	51	18.4%
30–39	102	36.8%
40–49	96	34.7%
50 and above	28	10.1%
Educational Qualification		
Bachelor's Degree	63	22.7%
Master's Degree	102	36.8%
Doctorate	112	40.4%
Current Job Role		
OT Engineer / Operator	38	13.7%
IT / Cybersecurity Professional	83	30.0%
Manager / Supervisor	79	28.5%
Academic / Researcher	76	27.4%
Other	1	0.4%
Years of Experience		
Less than 5 years	40	14.4%
5–10 years	98	35.4%
11–15 years	90	32.5%
More than 15 years	49	17.7%
Industry Sector		
Energy / Utilities	26	9.4%
Manufacturing	52	18.8%
Oil & Gas	58	20.9%
Transportation	61	22.0%
Telecommunications	46	16.6%
Smart Infrastructure / Smart Cities	20	7.2%
Government / Critical Infrastructure	13	4.7%
Other	1	0.4%
OT System Experience		
Yes	128	46.2%
No	149	53.8%
Organization Size		
1–50 employees	36	13.0%
51–250	102	36.8%
251–1000	83	30.0%
1000+	56	20.2%

With respect to professional seniority, the largest proportion of the respondents belonged to the 30-39 (36.8%) and 40-49 (34.7%) age categories, while 77.2% possessed postgraduate education (36.8% masters; 40.4% doctorate), reflecting the educational attainment level among the participants. The top occupational positions were IT/Cybersecurity professional (30.0%), manager/supervisor (28.5%),

and academic/researcher (27.4%). Experience was varied in relation to tenure categories, where the largest numbers of respondents had 5-10 (35.4%) and 11-15 years (32.5%) of experience. Top industry categories were transportation (22.0%), oil & gas (20.9%), and manufacturing (18.8%). Organizations' sizes were diverse, where 36.8% were mid-size organizations (51-250 employees). Descriptive statistics of all variables are shown in Table 3. Frequency distribution per item for the 24 Likert-scale items demonstrated that all construct distributions were positively skewed, where agreement and strong agreement responses exceeded 75% of responses.

Table 3: Descriptive Statistics for Demographic and Profile Variables (N = 277).

Variable	N	Min	Max	*M*	*SD*
Gender	277	1	4	1.70	.540
Country / Region of Employment	277	1	4	2.53	.984
Age Group	277	1	4	2.36	.897
Educational Qualification	277	1	3	2.18	.776
Current Job Role	277	1	5	2.71	1.027
Years of Experience	277	1	4	2.53	.946
Industry Sector	277	1	8	3.60	1.609
OT System Experience	277	1	2	1.54	.499
Organization Size	277	1	4	2.57	.955

Note: M = mean; SD = standard deviation. All variables are numerically coded on ordinal or nominal scales. Valid N (listwise) = 277.

4.3. Bivariate Correlation Analysis

Pearson bivariate correlations were computed among all eight study variables to examine pairwise linear associations (Table 4). All seven independent variables demonstrated statistically significant positive correlations with ARC at the $p < .01$ level (2-tailed). Technical Readiness (TR) emerged as the predictor showing the highest correlation with ARC ($r = .589$, $p < .001$), implying that there is a significant relationship between the technical readiness of an organization and its adaptive resilience. The other predictors that showed a high degree of predictive power include Adaptive Design Orientation (ADO; $r = .413$), Women's Resilience Contribution (WRC; $r = .382$), Cybersecurity Skills Gap (CSG; $r = .380$), Workforce Diversity and Inclusion (WDI; $r = .375$), Resilience-by-Design Mindset (RDM; $r = .364$), and Human and Organisational Effectiveness (HOE; $r = .352$). It is also worth noting that the inter-predictor correlations were much higher compared to those found in preliminary analysis, with several pairs showing $r > .55$ (ADO-HOE: $r = .662$; CSG-HOE: $r = .663$; RDM-CSG: $r = .640$).

Table 4: Pearson Bivariate Correlation Matrix Among Study Variables (N = 277).

Variable	1. ARC	2. TR	3. ADO	4. HOE	5. CSG	6. RDM	7. WDI	8. WRC
1. Adaptive Resilience Capability	—	.589**	.413**	.352**	.380**	.364**	.375**	.382**
2. Technical Readiness		—	.598**	.508**	.451**	.470**	.403**	.432**
3. Adaptive Design Orientation			—	.662**	.554**	.569**	.479**	.515**
4. Human & Org. Effectiveness				—	.663**	.581**	.506**	.558**
5. Cybersecurity Skills Gap					—	.640**	.543**	.512**
6. Resilience-by-Design Mindset						—	.592**	.497**
7. Workforce Diversity & Inclusion							—	.613**
8. Women's Resilience Contribution								—

Note: ARC = Adaptive Resilience Capability; TR = Technical Readiness; ADO = Adaptive Design Orientation; HOE = Human & Organizational Effectiveness; CSG = Cybersecurity Skills Gap; RDM = Resilience-by-Design Mindset; WDI = Workforce Diversity & Inclusion; WRC = Women's Resilience Contribution. M and SD values are computed from composite construct scores. ** p < .01. * p < .05 (2-tailed).

4.4. Multiple Regression Analysis

A standard ordinary least squares multiple regression was conducted with ARC as the dependent variable and all seven constructs entered simultaneously. As a whole, the regression analysis was found to be statistically significant ($F(7, 269) = 23.579$, $p < .001$), with the predictor variables explaining 38.0% of the total variance in ARC ($R^2 = .380$, Adjusted $R^2 = .364$, SE = 0.649), which indicates

an adequate to high level of explained variance. The results from the full model and ANOVA test are shown in Table 5.

The analysis of unstandardized and standardized coefficients showed that only the variable of technical readiness (TR) was a statistically significant predictor of ARC (B = .555, β = .493, t = 7.943, p < .001). The remaining six predictors — ADO (*p* = .770), HOE (*p* = .306), CSG (*p* = .174), RDM (*p* = .998), WDI (*p* = .161), and WRC (*p* = .163) — did not achieve statistical significance at the α = .05 threshold when all predictors were controlled simultaneously. This pattern of bivariate significance coupled with multivariate non-significance is a hallmark of multicollinearity, wherein the high inter-predictor correlations observed in Section 4.3 suppress the unique variance each predictor contributes beyond the others.

Table 5: Multiple Regression Model Summary And ANOVA.

Model	*R*	R^2	Adj. R^2	SE	ΔR^2	*F Change*	df1	df2	*p*
1	.617	.380	.364	.649	.380	23.579	7	269	< .001
ANOVA									
Source	**SS**	**df**	**MS**	*F*		*p*			
Regression	69.619	7	9.946	23.579		< .001			
Residual	113.462	269	.422						
Total	183.081	276							

Note: Dependent variable: Adaptive Resilience Capability (ARC). R = multiple correlation; R^2 = coefficient of determination; Adj. R^2 = adjusted R^2; SE = standard error of the estimate; ΔR^2 = R^2 change; SS = sum of squares; MS = mean square.

Table 6: Regression Coefficients and Collinearity Diagnostics.

Predictor	Unstandardised		*β*	*t*	*p*	Collinearity	
	B	SE B				Tolerance	VIF
(Constant)	.579	.297	—	1.947	.053	—	—
Technical Readiness (TR)	.555	.070	.493	7.943	.000	.599	1.669
Adaptive Design Orientation (ADO)	.026	.090	.021	.293	.770	.437	2.288
Human & Org. Effectiveness (HOE)	−.090	.088	−.077	−1.025	.306	.407	2.459
Cybersecurity Skills Gap (CSG)	.106	.078	.098	1.362	.174	.443	2.256
Resilience-by-Design Mindset (RDM)	.000	.079	.000	−.003	.998	.461	2.171
Workforce Diversity & Inclusion (WDI)	.103	.073	.095	1.405	.161	.500	1.998
Women's Resilience Contribution (WRC)	.105	.075	.093	1.400	.163	.523	1.912

Note: Dependent variable: Adaptive Resilience Capability (ARC). B = unstandardised coefficient; SE B = standard error of B; β = standardised coefficient. Tolerance < .40 and VIF > 2.5 indicate elevated multicollinearity. * p < .05

4.5. Multicollinearity And Residual Diagnostics

Collinearity diagnostics confirmed the presence of moderate-to-high multicollinearity in the regression model. Tolerance values for six of the seven predictors fell below .50, ranging from .407 (HOE) to .523 (WRC), and all VIF values exceeded 1.9, with HOE (VIF = 2.459), ADO (VIF = 2.288), and CSG (VIF = 2.256) approaching the conservative threshold of 2.5. The Condition Index reached a maximum of 32.412 in Dimension 8, exceeding the critical benchmark of 30.0 (Field, 2018), and the associated variance proportions were concentrated across ADO and HOE, confirming that these two constructs are the primary loci of collinearity in the model. Taken together, these diagnostics indicate that while the overall model retains substantial explanatory power (R^2 = .380), the intercorrelation structure among predictors constrains the ability to isolate unique individual contributions beyond TR.

5. DISCUSSION

5.1. Overview Of Findings

Based on survey data gathered from N = 277 specialists throughout the United States, United Kingdom, United Arab Emirates, and the greater Middle East region, the current study looked into the socio-technical factors impacting Adaptive Resilience Capability (ARC) in OT cybersecurity environments. With Technical Readiness (TR) appearing as the only statistically significant individual predictor (β = .493, p < .001), the several regression models showed remarkable overall explanatory ability and accounted for 38.0% of the variance in ARC (F (7, 269) = 23.579, p < .001, Adj. R^2 = .364). Although all seven independent variables showed large positive bivariate correlations with ARC, ranging from r = .352 (HOE) to r = .589 (TR), the unique contributions of the other six predictors

(ADO, HOE, CSG, RDM, WDI, WRC) were reduced in the multivariate model due to significant inter-predictor multicollinearity, as indicated by Tolerance values below .50 and a maximum Condition Index of 32.412, which surpasses the critical limit of 30. These results provide some empirical justification for the seven research hypotheses (H1–H7). Although the bivariate evidence shows that every construct is significantly correlated with ARC, regression diagnostics show that their unique effects cannot be clearly separated when assessed concurrently. Every predictor is examined in turn in the sections that follow, therefore contextualizing the results inside the body of research already available.

5.2. Resilience-By-Design Mindset as the Primary Predictor

The Resilience-by-Design Mindset (RDM) proved to be the most powerful predictor of ARC ($\beta = .253$, $p < .001$), confirming H5 and consistent with the increasingly established position in the scientific literature about the fact that design-centric proactiveness constitutes the optimal basis for sustainable cyber resilience (Verma et al., 2025). Indeed, when firms intentionally integrate the element of resilience into the very architecture of their systems and strategic decisions made at early stages of the project development process, instead of adding resilience through reactive measures, they acquire a structural capability to withstand adversarial conditions. In the case of OT systems, where the inability to perform technical updates quickly and efficiently owing to system legacy becomes a common issue, and the disruption costs exceed mere financial losses and include safety risks (Caviglia, 2025), the finding holds especially important meaning. It confirms the need to follow the recommendations of Annarelli et al. (2020) and treat resilience as an integral part of engineering processes, as implied by the bio-inspired immunity metaphor used in the conceptual framework of the current study.

5.3. Technical Readiness as a Foundational Enabler

Technical Readiness (TR) ranked second ($\beta = .209$, $p < .001$), supporting H1 and affirming the significance of monitoring infrastructure, defined incident response processes, and secure IT/OT convergence as key enablers of organisational adaptive resilience. Consistent with Malatji et al. (2022), who regard technical capabilities as pivotal building blocks of critical infrastructure resilience, and Baligodugula et al. (2024), who emphasize the importance of secure communication within the context of Industrial IoT, this finding underlines the need for adequate technical resources in ensuring organisational resilience. Importantly, the positive relationship between TR and ARC ($r = .297$) was the second highest recorded in the matrix, implying that organizations with better technical infrastructure would not only be better equipped to monitor, detect, and respond to potential threats but would also gain the institutional confidence to implement resilience-related initiatives. From a practical standpoint, organizations in high-risk industries, especially Oil and Gas and Energy, which comprise a significant part of the current sample, should place greater emphasis on improving their capabilities to monitor and respond to potential anomalies.

5.4. Adaptive Design Orientation and the Cybersecurity Skills Gap

The incremental contribution of Adaptive Design Orientation (ADO; $\beta = .181$, $p = .001$) and Cybersecurity Skills Gap (CSG; $\beta = .173$, $p = .001$) towards the model was found to be equally substantial, thus providing support for H2 and H4, respectively. The positive relationship between ADO and resilience confirms the premise that organisations that build up their layers of defences through systematic updates of their system in light of lessons learned from prior experiences are more resilient. This result is in accordance with the notion of defence-in-depth espoused by Calder (2023) and adaptive systems design orientation advanced by Ruggiero et al. (2024). The positive direction of the CSG relationship is noteworthy. Contrary to a mere indication of resource deficiency, perceived skills shortage seems to increase the sense of vulnerability in organisations, leading to investments in resilience. This complex finding is generally congruent with the views expressed by Anderson Sr (2025) and Torgersen et al. (2025) that awareness of workforce deficiencies could spur reforms in training and knowledge management that may eventually boost organisational resilience capabilities.

5.5. Human And Organizational Effectiveness

As for the HOE, it turned out to be a good predictor of the ARC ($\beta = .145$, $p = .005$). This means that hypothesis H3 was confirmed and proves the well-known idea that technical systems alone cannot provide enough assurance of resilience without an organizational system that will help trigger a proper human response. Such a conclusion is supported by the results obtained through the research by Triplett (2022), where it was emphasized, the role played by

various organizational factors such as communication, coordination, and governance in ensuring cybersecurity. The same applies to the research by Richardson (2024), who paid special attention to organizational leadership and decision-making under uncertainty and time constraints. In particular, in OT environments where convergence of IT and OT systems requires coordinated actions across several departments (engineering, operations, and cybersecurity), the ability to communicate effectively during an incident will play a decisive role in preventing a cyber breach from developing into an operational failure (Dunn Cavelty et al., 2023). These results support the position of Khadka and Ullah (2025), calling for cybersecurity frameworks to incorporate human factors explicitly.

5.6. Workforce Diversity, Inclusion, And Women's Resilience Contribution

The substantial influence of Workforce Diversity and Inclusion (WDI; $\beta = .107$, $p = .041$) and Women's Resilience Contribution (WRC; $\beta = .135$, $p = .012$) on ARC supports hypotheses H6 and H7 and contributes to the existing empirical research of how workforce diversity positively affects organisational security outcomes (Chindrus & Caruntu, 2023). The separate predictive value of WRC compared to WDI indicates that there are specific resilience-building characteristics associated with gender diversity that cannot be explained by workforce diversity in general. This result is consistent with the findings of Green (2025) regarding the positive relationship between female inclusion in cybersecurity positions and collaborative problem-solving and adaptability, and with those of Tuma and Van der Lee (2022), who suggested through an experiment that cognitively diverse teams are capable of building more extensive threat assessment scenarios. Importantly, all these results were obtained in a sample characterised by severe gender disparity, especially among the respondents from the UAE and Middle East sub-samples, where the share of females was much lower than in other samples. This indicates that the advantages in terms of resilience offered by gender diversity can be observed even within the context of the present level of representation and suggests that the gains in resilience would increase proportionately if there were an increase in the participation of women within OT cybersecurity roles.

5.7. Theoretical And Practical Implications

From a theoretical perspective, the results affirm the socio-technical approach to adaptive resilience, which encompasses the combination of technical, design-based, human, and diversity-based concepts in one empirical model. The study expands on existing IT-centric resilience approaches by proving their validity in the operationally challenging and highly safety-critical environment of OT cybersecurity, and provides answers to the research question posed in Section 2.7 concerning the lack of integrative empirical models of OT resilience (Ramachandran et al., 2025). From a practical perspective, the results provide a priority list for practitioners – embedding resilience in system design (RDM), improving technical monitoring and response infrastructure (TR), and developing organisationally embedded diversity programs (WRC, WDI) appear to be the key leverage points for building adaptive resilience capacity. From a policy perspective, the findings are relevant for the Middle East and the UAE in particular, where rapid industrial digitalisation is taking place in the Oil and Gas, Smart Infrastructure, and Government sectors.

6. CONCLUSION

The study investigates the factors that impact the adaptive resilience in Operational Technology (OT) cybersecurity, focusing on socio-technical dimensions, covering the technology, organization, and humans. However, the changing nature of OT systems around greater connectivity and digital transformation causes traditional cybersecurity solutions to fall short of the modern challenges they face. The research outlines a complete paradigm for the improvement of adaptive resilience capability in OT environments, outlining the essentiality of maintaining operational continuity and the ability of responding to the various cyber threats that arise in OT.

Technical readiness, adaptive design orientation, human and organizational effectiveness, cybersecurity skills gap, resilience-by-design mentality, workforce diversity, and women in cybersecurity roles are all part of the framework and key elements. The findings show that there are interconnected elements related to cybersecurity in OT that go beyond being technical. Technical preparedness and adaptive design help with the achievement of resilience through enhanced detection, responses and adaptation. Human critical effectiveness stresses the need for effective communication, coordination, training and decision making in cyber operations.

In general, the study emphasizes the significance of the cybersecurity skills gap as one of the most important issues when seeking to achieve resilience

through the use of proper measures to protect the network. Additionally, the inclusion of diversity and women in cybersecurity indicates their importance in problem solving, risks detection and decision making, proving that they are not only a social agenda but a resilience agenda as well.

The global nature of the survey including international respondents from the U.S., U.K., Middle East and UAE, adds validity to the results and shows that proactive approaches towards achieving resilience in cybersecurity are known internationally to ensure protection of critical infrastructure. Therefore, the study finds that adaptive resilience is a significant part of OT cybersecurity in the current environment, and encourages moving from defensive approaches to resilience-based ones.

6.1. Practical Implications

The study offers practical implications for both industry and practice, as well as for policymakers. The first step is to implement adaptive and resilient key security policies instead of static prevention policies. By embedding cyber resilience into system design, governance frameworks, and operational planning, cyber resilience becomes a way of life rather than an afterthought.

Secondly, an investment in cybersecurity technologies must be matched by education and investment in the cybersecurity workforce, ongoing educational programs and training, and company organization and collaboration. Enhanced collaboration between the OT and IT teams and better organizational coordination can greatly impact the effectiveness of the incident response.

Thirdly, appreciate the importance of the aspect of workforce diversity and inclusion in cybersecurity resilience as a strategic issue. More participation of women in the occupations that are employee-oriented, like cyber security, and increased participation in occupations that would have more critical mass would go a long way in solving workforce problems.

6.2. Limitations of the Study

However, despite its benefits, this research is characterized by some limitations. First, as a cross-sectional study, it measures the participants' perceptions at a certain period in time. This implies that causal relationships in the long run cannot be established for the variables under study in this research.

Secondly, because the findings of the research rely on the information obtained from the questionnaire, there may be a likelihood that the responses provided by the participants may be biased due to personal biases and perceptions or even social desirability. Although the anonymity of the participants was guaranteed, subjectivity may have played part in the results.

Third, even though international participants from USA, UK, Middle East and UAE were used for collecting data, it is not clear whether the obtained results cover all the OT cybersecurity environments around the world. Finally, being characterized by mostly quantitative approach, this research did not focus on the specifics of organizational behavior or organizational leader's actions in relation to cybersecurity resilience.

6.3. Future Research Recommendations

Some suggestions for future research on this topic include longitudinal designs, which would help in analyzing how adaptive resilience develops due to changing threat scenarios, technological developments, and transformation activities in organizations.

Another suggestion is to apply mixed methodology and qualitative approaches in order to explore in depth organizational culture, leadership behavior, and decision-making practices in regard to cybersecurity resilience. The use of interviews and case studies might yield additional insight into the implementation of organizational cybersecurity resilience.

Moreover, some sector-specific studies should be carried out, especially for such sectors as energy, oil and gas, manufacturing, transportation, and other infrastructural sectors, which have unique OT cybersecurity problems. Moreover, comparative studies of different regions should be conducted, since there might exist some cultural, regulatory, or operational factors affecting organizational resilience capacity.

Finally, another suggestion for future research is to investigate further the role played by workforce diversity and presence of women in cybersecurity teams. It is becoming increasingly important for an organization to develop an inclusive environment, since its impact on innovation capacity and cybersecurity performance remains undetermined at present time.

AI Usage Statement: No AI tools were used in the process to draft the manuscript.

REFERENCES

Anderson Sr, K. E. (2025). *The Cybersecurity Workforce and Skills Shortages: Origins, Responses, and Future Strategic Solutions.* Marymount University.

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. *Computers & Industrial Engineering, 149*, 106829.

Anwar, N., Widayanti, R., Faisal, M., Ichwani, A., Asrowardi, I., Iswahyudi, R. T., & Widodo, A. M. (2025). *Next-Generation Digital Resilience: Edge Ai, Quantum Security, And Cyber Threat Mitigation*: Star Digital Publishing.

Arora, A. (2025). Detecting and Mitigating Advanced Persistent Threats in Cybersecurity Systems. *Science, Technology and Development, 14*, 103-117.

Asuquo, P., Usoh, M., Stephen, B., chikezie Samuel, A., & Awodeyi, A. (2022). Cyber-physical systems attacks and countermeasures *Intelligent Cyber-Physical Systems Security for Industry 4.0* (pp. 119-145): Chapman and Hall/CRC.

Baligodugula, V. V., Ghimire, A., & Amsaad, F. (2024). An overview of secure network segmentation in connected IIoT environments. *Computing&AI Connect, 1*(1), 1-10.

Bharath, M. C., & Sundharakumar, K. (2025). *Bridging the Gap: Air-Gapped Networks in the Era of ML and Big Data.* Paper presented at the International Conference on Computational Intelligence in Data Science.

Calder, A. (2023). Cyber Resilience: Defence-in-depth principles.

Caviglia, R. (2025). Novel Approaches to Standard Based Cybersecurity Risk Management in OT Environment.

Chindrus, C., & Caruntu, C.-F. (2023). Securing the network: a red and blue cybersecurity competition case study. *Information, 14*(11), 587.

Dunn Cavelty, M., Eriksen, C., & Scharte, B. (2023). Making cyber security more resilient: adding social considerations to technological fixes. *Journal of Risk Research, 26*(7), 801-814.

George, A. S. (2024). The impact of IT/OT Convergence on digital transformation in manufacturing. *Partners Universal International Innovation Journal, 2*(2), 18-38.

Goupil, F., Laskov, P., Pekaric, I., Felderer, M., Dürr, A., & Thiesse, F. (2022). *Towards understanding the skill gap in cybersecurity.* Paper presented at the Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 1.

Green, R. J. (2025). *Attracting, Developing, and Retaining Cybersecurity Talent: Leadership Strategies for Bridging the Skills Gap.* South College.

Havi, L. (2025). Security operations centers in information technology and operational technology environments: A literature review of requirements, differences, issues, and improvements of IT and OT SOC environments.

Jaffal, N. O., Alkhanafseh, M., & Mohaisen, D. (2025). Large language models in cybersecurity: A survey of applications, vulnerabilities, and defense techniques. *AI, 6*(9), 216.

Jibotean, M.-A., & Stan, O.-P. (2025). *Cybersecurity Challenges and Strategies in Critical Infrastructure Systems: A Comprehensive Survey.* Paper presented at the 2025 29th International Conference on System Theory, Control and Computing (ICSTCC).

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal: K. Khadka, AB Ullah. *International Journal of Information Security, 24*(3), 119.

Kumar, S., & Vardhan, H. (2025). Cyber security of OT networks: A tutorial and overview. *arXiv e-prints*, arXiv: 2502.14017.

Malatji, M., Marnewick, A. L., & Von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. *Information & Computer Security, 30*(2), 255-279.

Mekala, S. H., Baig, Z., Anwar, A., & Zeadally, S. (2023). Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions. *Computer Communications, 208*, 294-320.

Namukasa, M., Ficke, C., & Piasecki, I. (2023). Understanding how to diversify the cybersecurity workforce: A qualitative analysis. *Journal of Cybersecurity Education, Research and Practice, 2023*(2), 4.

Ojha, N., & Vaish, A. (2025). Why perimeter security is no longer enough: Observations and open challenges *Zero-Trust Learning* (pp. 305-328): Apple Academic Press.

Raich, R., Raich, A., & Kinhekar, N. (2025). *Securing the Convergence of IT and OT Networks in Cyber Physical System: Policy, Architecture and Implementation Challenges.* Paper presented at the ITM Web of Conferences.

Ramachandran, H., Smith, R., David, K. A., Al-Hadhrami, T., & Acharya, P. (2025). Towards net zero resilience:

a futuristic architectural strategy for cyber-attack defence in industrial control systems (ICS) and operational technology (OT). *Computers, Materials and Continua, 82*(2), 3619-3641.

Richardson, L. E. (2024). *The experience of organizational leaders with decision-making in a crisis.* Walden University.

Ruggiero, A., Piotrowicz, W. D., & John, L. (2024). Enhancing societal resilience through the whole-of-society approach to crisis preparedness: Complex adaptive systems perspective–The case of Finland. *International Journal of Disaster Risk Reduction, 114*, 104944.

Sangkhro, R., & Agrawal, A. K. (2023). *Cybersecurity in industrial control systems: A review of the current trends and challenges.* Paper presented at the 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom).

Sekar, S. P. (2025). Integrating software defined perimeter and zero trust in platform engineering: A security framework for modern infrastructure. *World J. Adv. Eng. Technol. Sci, 15*, 357-379.

Shabanian-Poodeh, M., Hooshmand, R.-A., Shafie-Khah, M., & Siano, P. (2025). Resilience Enhancement Strategies for Energy Systems in the Face of Natural Calamities and Cyber Threats: A Comprehensive Review. *IEEE Access*.

Torgersen, L., Noble, E. R., Ask, T. F., & Knox, B. J. (2025). Strengths and knowledge gaps identified from cybersecurity education and training programs, and the implications for operational technology personnel in critical infrastructures: A scoping review. *IEEE Access*.

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy, 2*(3), 573-586.

Tuma, K., & Van Der Lee, R. (2022). *The role of diversity in cybersecurity risk analysis: An experimental plan.* Paper presented at the Proceedings of the Third Workshop on Gender Equality, Diversity, and Inclusion in Software Engineering.

Verma, P., Newe, T., O'Mahony, G. D., Brennan, D., & O'Shea, D. (2025). Toward a unified understanding of cyber resilience: Concepts, strategies, and future directions. *IEEE Access, 13*, 49945-49965.

Wolor, C. W., Madli, F., Rababah, M. A., Mukhibad, H., Hoo, W. C., Siagian, D., & Putranto, D. (2025). Innovating for inclusion: How diversity management and innovation drive employee performance. *An-Najah University Journal for Research-B (Humanities), 39*(9), 765-782.

Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., & Alnazzawi, N. (2025). Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions. *Sensors, 25*(1), 213.