International Research Journal of Management Science & Technology



ISSN 2250 – 1959(0nline)
2348 – 9367 (Print)

An Internationally Indexed Peer Reviewed & Refereed Journal

www.IRJMST.com
www.isarasolutions.com

Published by iSaRa Solutions

IMPACT OF PERCEIVED ORGANISATIONAL SUPPORT IN DETERMINING CYBER RESILIENCE AMONG PERSONNEL INVOLVED IN SECURITY DUTIES

Major General ZIS Yazdani (Retd) , Prof (Dr) Musheer Ahmad
Department of Business Administration, Khwaja Moinuddin Chisti Language University, Lucknow

Abstract

1. Cyber resilience has emerged as a critical human, organisational, and operational capability as security organisations become increasingly dependent on networked information systems, digital communications, and technology-enabled decision-making. The present paper examines how Perceived Organisational Support (POS) influences cyber resilience among personnel involved in security duties. The paper builds on Protection Motivation Theory (PMT) and Social Exchange Theory (SET) to establish that technical controls and formal cyber policies cannot by themselves guarantee resilient behaviour. Personnel must also believe that the organisation values their contribution to cyber security, provides appropriate training and resources, supports timely reporting, and backs responsible decisions during cyber incidents. Such perceptions strengthen confidence, discretionary effort, vigilance, learning, and adaptive behaviour.

2. The paper adopts a conceptual and literature-based approach to analyze how POS influences the cognitive and psychological appraisal of security operators. The analysis indicates that POS strengthens cyber resilience through five principal mechanisms: institutional commitment, resource enablement, psychological safety and trust, reciprocity and discretionary effort, and organisational learning. Conversely, weak support increases security fatigue, reduces incident reporting, encourages workarounds, and creates an efficacy gap between awareness of threats and the capability to act upon that awareness. The paper proposes practical measures including visible leadership commitment, role-specific training, scenario-based exercises, simplified security procedures, rapid feedback after reporting, recognition of positive security behaviour, non-punitive learning from inadvertent errors, and incorporation of human-factor indicators into organisational cyber-readiness assessments. The paper concludes that resilient security personnel are not produced by fear or compliance alone; they are developed when threat awareness is matched by competence, workable systems, and credible institutional support.

***Keywords*:** Perceived Organisational Support; Cyber Resilience; Security Personnel; Protection Motivation Theory; Social Exchange Theory; Cybersecurity Self-Efficacy; Incident Reporting; Cybersecurity Culture; Human Factors.

1. Introduction

1.1. The nature of security operations has changed substantially with the digitisation of command, communication, intelligence, logistics, surveillance, training, and administrative functions. Modern military and security organisations depend on interconnected systems that improve speed and situational awareness but simultaneously create additional points of exposure. Cyberspace has therefore become a strategic environment in which disruption, espionage, manipulation, and denial can affect mission effectiveness without necessarily producing a conventional physical attack. Cyber

resilience represents a comprehensive mission requirement extending across acquisition, operational use, performance, and training, rather than a narrow information-technology function.

1.2. Cyber resilience is broader than traditional cyber security. Cyber security generally emphasises protection, prevention, and reduction of the probability of compromise, whereas cyber resilience emphasises the capacity to anticipate, withstand, absorb, respond to, recover from, and adapt to adverse cyber events while sustaining essential functions. ENISA's work on the human aspects of cyber security stresses that technical measures operate in a workplace context in which people face competing demands, limited time, and resource constraints. It recommends enabling secure behaviour through skills, support, and organisational design rather than relying primarily on threat awareness or punishment. NIST's human-centred cybersecurity programme similarly emphasises the interaction of people, process, and technology and the importance of empowering people as active partners in cyber security.

1.3. The human dimension is particularly important in security duties because personnel frequently operate under time pressure, uncertainty, hierarchy, and mission urgency. A security operator may identify an unusual communication, suspicious attachment, abnormal system behaviour, or possible compromise but still hesitate to report it if the organisational climate suggests that reporting mistakes will lead to blame. Conversely, a person who believes that the organisation values his or her contribution, provides reliable systems and training, and supports responsible action is more likely to exercise judgement, report anomalies, and persist with secure practices when those practices impose operational inconvenience.

1.4. This issue is central to Perceived Organisational Support (POS). Eisenberger et al. conceptualised POS as employees' global beliefs concerning the extent to which the organisation values their contributions and cares about their well-being. The concept has subsequently been linked to organisational commitment, performance, well-being, and other employee outcomes. A large meta-analysis covering 558 studies found that leadership, organisational context, human-resource practices, and working conditions contribute to POS and that POS is associated with positive employee attitudes, performance, and well-being (Kurtessis et al., 2017).

1.5. In security environments, POS should not be interpreted simply as welfare or general human-resource support. Cyber-related POS concerns the degree to which personnel perceive that their organisation is serious about cyber preparedness, provides usable protective resources, develops competence, communicates clear procedures, responds constructively to incidents, and supports them when they take appropriate protective action. POS functions as an organisational determinant that complements individual threat and coping appraisals derived from PMT.

1.6. The specific objective of this paper is to examine how POS strengthens or weakens cyber resilience among personnel involved in security duties. The paper concentrates on the mechanisms through which organisational support shapes perceptions, motivation, and behaviour. It also identifies practical ways in which security institutions can improve personnel perceptions of organisational support and thereby strengthen resilient cyber behaviour.

2. Perceived Organisational Support: Concept and Features

2.1. POS originated in organisational support theory and is closely related to Social Exchange Theory. Blau proposed that social relationships involve reciprocal exchanges in which favourable treatment tends to generate an obligation to reciprocate. Eisenberger et al. applied this logic to the employment relationship, arguing that employees develop a general perception of whether their organisation values them and cares about their welfare. When support is perceived as genuine and sustained, employees are more likely to reciprocate through commitment and behaviours that advance organisational objectives.

2.2. POS is a perceptual construct. The same formal policy may produce different perceptions among personnel depending on how consistently it is implemented, how leaders behave, and whether the policy fits operational realities. A security organisation may possess extensive cyber policies and sophisticated technical systems, yet personnel may perceive low support if training is inadequate, security tools are unreliable, procedures are cumbersome, or reports of cyber incidents are met with disproportionate blame. Conversely, relatively simple arrangements generate strong POS when leadership is visible, resources are dependable, and personnel receive timely assistance.

2.3. Five key features of POS are especially relevant to cyber resilience:

2.3.1. Institutional Commitment: Personnel need evidence that cyber readiness is a command priority rather than an administrative requirement delegated exclusively to technical specialists. Leadership messages, participation in exercises, allocation of training time, and attention to cyber readiness during operational planning all communicate organisational priorities.

2.3.2. Resource Enablement: Support is credible only when personnel have the means to perform the desired behaviour. These means include appropriate cyber tools, secure communication systems, updated procedures, access to specialist assistance, training material, and adequate time for cyber-related tasks. Security solutions must make the secure course of action practical and take user needs into account.

2.3.3. Psychological Safety and Trust: Personnel must trust that reporting security anomalies or inadvertent errors will not result in swift punitive action. A climate of psychological safety encourages early reporting and open communication regarding vulnerabilities.

2.3.4. Reciprocity and Discretionary Effort: High POS fosters a strong psychological contract, motivating operators to exert extra-role discretionary effort, such as exercising heightened vigilance during off-peak operational windows or mentoring peers on safe computing practices.

2.3.5. Learning Orientation: Resilient organisations learn from incidents, near misses, and weak signals. A learning-oriented organisation does not remove accountability; rather, it distinguishes deliberate or reckless violations from good-faith mistakes and uses the latter as opportunities to improve training, procedures, and system design.

3. Theoretical Foundation: PMT and SET

3.1. Protection Motivation Theory (PMT) provides the individual-level foundation for understanding cyber-protective behaviour. Rogers, and the subsequent development of PMT, conceptualised protective motivation through threat appraisal and coping appraisal. Threat appraisal involves judgments concerning the seriousness of a threat (perceived severity) and one's vulnerability to it (perceived vulnerability). Coping appraisal involves response efficacy, self-efficacy, and response costs. In cyber security research, these constructs explain compliance intentions and protective behaviour.

PMT - SET INTEGRATION MODEL

Protection Motivation Theory(PMT)	Social Exchange Theory (SET)
- Threat Severity **- Perceived Vulnerability** **- Cybersecurity Self-Efficacy** **- Response Efficacy** **- Response Cost**	**- Institutional Commitment** **- Resource Enablement** **- Psychological Safety** **- Reciprocity / Trust** **- Learning Orientation**

↓

Perceived Organisational Support (POS)

↓

CYBER RESILIENCE OUTCOMES

- **Heightened Vigilance & Adaptive Action**
- **Rapid Incident Reporting & Containment**
- **Discretionary Protective Effort**

3.2. Threat perception is the degree to which personnel recognise the seriousness of a cyber threat. Perceived vulnerability concerns whether the individual believes that he or she, the unit, or the relevant systems could actually be affected. In security duties, threat awareness is necessary but not sufficient. Excessively low threat perception creates complacency, while high threat perception without coping resources produces anxiety or fatalism.

3.3. SET complements PMT by explaining why the organisational environment matters. POS provides a bridge between individual motivation and institutional behaviour. If personnel perceive strong organisational backing, the recommended protective action becomes more than a rule: it becomes part of the reciprocal relationship between the individual and the institution. The person is more likely to believe that reporting, escalation, and temporary disruption of a system will be supported when these actions are necessary to protect the mission.

3.4. The integrated PMT-SET framework proposes that threat perception, perceived vulnerability, cybersecurity self-efficacy, response efficacy, and response cost operate alongside POS in shaping

cyber resilience. Higher POS is directly associated with stronger cyber resilience, serving as an operational catalyst that reinforces positive individual coping appraisals and mitigates perceived response costs.

4. How Organisational Support Influences Security Personnel

4.1. POS influences cyber resilience first by shaping the meaning personnel attach to cyber security. When leaders repeatedly demonstrate that cyber preparedness is a mission requirement, personnel interpret secure behaviour as part of professional duty. When cyber procedures are communicated only as administrative compliance, they are perceived as an additional burden competing with operational tasks.

4.2. POS directly affects personal confidence. Training and organisational assistance increase cybersecurity self-efficacy by giving personnel opportunities to practise rather than merely receive passive information. This is critical because knowledge that is not translated into practical capability may not be available under operational stress. Organisational support and individual coping capability are deeply interconnected.

4.3. POS reduces perceived response cost. A security procedure that requires several cumbersome steps, creates repeated interruptions, or conflicts with operational workflows is perceived as costly. Organisations reduce this cost by simplifying processes, improving interfaces, automating routine controls, and ensuring that security requirements are designed around real work. Security interventions need to fit workplace constraints and should enable rather than obstruct secure behaviour.

4.4. POS further influences discretionary effort. Compliance may be sufficient when rules are directly supervised, but resilience requires personnel to act when a situation falls outside prescribed scripts. This includes reporting a suspicious anomaly that does not fit a known category, seeking specialist advice, isolating a system when authorised, or helping colleagues respond to an incident. Personnel who feel supported are more likely to reciprocate through such discretionary effort.

4.5. The effect is particularly relevant to hierarchical security organisations. Formal authority can compel compliance with prescribed procedures, but it cannot anticipate every cyber scenario. In a rapidly changing threat environment, resilient performance depends on judgment and initiative. POS creates confidence that responsible initiative will be recognised rather than automatically treated as a policy deviation.

4.6. Conversely, low POS creates disengagement. Poor training, insufficient resources, unclear role expectations, inaccessible cyber specialists, or punitive responses generate security fatigue. Personnel know that cyber threats are serious but conclude that they lack the means or organisational backing to address them effectively. This creates an **efficacy gap** between threat awareness and actionable resilience.

5. Organisational Support and Cyber Incident Reporting

5.1. Incident reporting is one of the clearest behavioural pathways through which POS affects resilience. A cyber incident is often first detected by a user or operator rather than by a central security system. The value of the report depends on speed, accuracy, and willingness to escalate. Incident reporting is a critical human factor in organisational cyber resilience, and reporting

behaviour is shaped by interacting cultural, organisational, and individual factors (van der Kleij et al., 2026).

5.2. A supportive reporting climate does not mean an absence of discipline. Rather, it means that personnel can distinguish between deliberate misconduct and honest operational mistakes. If personnel believe that an accidental click, misconfiguration, or mistaken judgement will inevitably lead to administrative blame or disciplinary sanction, they conceal or delay reporting. The resulting loss of detection time is vastly more damaging than the original error.

5.3. For security organisations, a practical principle follows: **"Report early, investigate fairly, learn systematically."** Early reporting should be rewarded through recognition of responsible behaviour. Investigation should establish facts without assuming automatic culpability. Lessons learned must be translated into systemic improvements in training, technology, or procedures. This cycle reinforces POS because personnel observe that their reports lead to constructive organisational action.

6. Findings

6.1. The empirical and theoretical evidence regarding POS and cyber resilience highlights several core findings across existing literature and research frameworks:

Finding Area	Key Insight / Mechanism	Practical Impact
Information Security Compliance	Compliance is driven by cost-benefit beliefs, normative influence, and self-efficacy (Bulgurcu et al., 2010; Ifinedo, 2012).	Confirms PMT applicability; individual appraisals require institutional support to yield action.
Organisations & Support Theory	OST meta-analysis confirms leadership and HR practices as core POS drivers (Kurtessis et al., 2017).	Validates POS as a primary driver of positive work attitudes and extra-role performance.
Operational Relevance	Hierarchy and operational stress amplify reliance on institutional cues.	POS directly impacts self-efficacy, response efficacy, and willing anomaly escalation.
Instrument Reliability	High internal consistency observed across POS and Cyber Resilience scales in pilot testing.	Confirms robust construct validity for assessing human factors in cyber readiness.
The "Efficacy Gap"	High threat awareness paired with low support yields paralysis or unauthorized workarounds.	Emphasizes that technical tools must match operational realities to enable user efficacy.

6.2. First, literature strongly supports the view that organisational context dictates secure behaviour. Bulgurcu, Cavusoglu, and Benbasat (2010) demonstrated that information-security compliance is shaped by beliefs concerning the benefits and costs of compliance, normative influences, and self-efficacy. Ifinedo (2012) similarly found that self-efficacy, response efficacy, and perceived vulnerability were associated with policy compliance. These findings support the integration of PMT variables and reinforce the logic that organisational conditions govern how beliefs convert into action.

6.3. Second, organisational support has a well-established theoretical foundation. Eisenberger et al. (1986) demonstrated that employees form general beliefs regarding whether their organisation values their contributions. Kurtessis et al. (2017), through a meta-analysis of 558 studies, identified leadership, organisational context, human-resource practices, and working conditions as core antecedents of POS.

6.4. Third, POS is particularly relevant in security operations because personnel function within strong hierarchies and under high operational stress. The organisational expression of support includes command emphasis on cyber preparedness, targeted training, usable secure tools, clear incident-response processes, and leadership backing for responsible action. Such support directly strengthens self-efficacy, response efficacy, and willingness to report anomalies.

6.5. Fourth, literature syntheses reveal that personnel who perceive strong institutional investment in digital welfare are significantly more likely to go beyond mandatory procedures. Conversely, an efficacy gap emerges when personnel understand cyber threats but perceive that available institutional tools and procedures do not match threat sophistication, generating frustration and operational workarounds.

7. Discussion

7.1. Cyber resilience among security personnel is fundamentally a socio-technical outcome. Technology establishes structural capabilities and constraints, while people interpret situations, make decisions, and execute procedures. Organisational support shapes the climate in which these decisions occur. A resilient operator within an unsupportive system is constrained; conversely, a supportive organisation amplifies individual capabilities.

7.2. POS should be viewed as complementary to PMT rather than as a substitute for it. Threat perception creates urgency, vulnerability creates personal relevance, self-efficacy creates confidence, response efficacy creates belief in protective measures, and low response cost makes secure behaviour feasible. POS creates the organisational conditions under which these individual perceptions convert into sustained operational behaviour.

7.3. This systemic relationship follows a logical sequence and can be be illustrated as a chain : leadership commitment → resource availability and training→ stronger self-efficacy and response efficacy → lower perceived response cost → greater willingness to report and act → faster organisational learning → stronger cyber resilience.

7.4. Cyber resilience cannot be reduced to simple compliance. Compliance is essential, but resilience requires adaptive capacity when standard operating assumptions fail. Security personnel must recognise unfamiliar threats, communicate uncertainty, seek specialist assistance, and sustain essential functions while systems are degraded. These adaptive behaviours require deep institutional trust.

7.5. Hierarchical security structures intensify this dynamic. Command hierarchies enable rapid coordination and discipline, but operators may hesitate to report operational anomalies upward if fear of reprisal dominates. Cyber resilience requires a balance between strict accountability and psychological learning. The institution must maintain operational standards while ensuring that an operator's first instinct is to report and contain rather than conceal.

8. Practical Implications

8.1. Senior Leadership Ownership: Senior commanders must visibly own cyber resilience. Institutional leaders should communicate that cyber security is integral to overall mission assurance rather than an administrative duty offloaded to IT specialists. Leadership participation in cyber exercises provides a clear signal of institutional commitment.

8.2. Role-Specific, Scenario-Based Training: Generic, annual awareness briefings are insufficient. Security operators face distinct threat vectors depending on whether they operate in command, intelligence, communications, or logistics functions. Training must feature scenario-based exercises, including degraded-environment drills where operators practice maintaining core functions while digital systems are compromised.

8.3. Reduction of Response Cost: Security procedures should be continuously audited to eliminate unnecessary friction, duplication, and operational delay. Automating routine protective controls and designing security requirements around actual operational workflows reduces response costs and increases user adoption.

8.4. Credible Reporting Channels: Incident reporting mechanisms must be transparent, rapid, and easily accessible. Personnel require immediate feedback following a report so they know their initiative yielded concrete action, reinforcing positive social exchange.

8.5. Recognition of Positive Security Behaviour: Organisations should actively recognize early anomaly detection, proactive exercise participation, and security improvements. Formal recognition reinforces the social-exchange relationship and confirms that cyber resilience is a valued operational contribution.

8.6. Human-Factor Metrics in Assessments: Technical audits (e.g., patch management, firewall logs) must be paired with human-factor indicators. Tracking self-efficacy, reporting confidence, response costs, and perceived support yields a comprehensive profile of organisational readiness.

9. Methods to Enhance Perception of Organisational Support

9.1 Strategic Framework: Institutionalizing Support

9.2 Cyber Support Charter: Codify institutional commitments—guaranteeing modern equipment, continuous training, non-punitive incident reporting, and prompt technical backing.

9.3 Unit-Level Cyber Engagements: Implement regular operational huddles to discuss recent threat trends, exercise findings, and practical security obstacles.

9.4 Competence-Focused Practical Exercises: Transition from passive compliance lectures to active rehearsal in compromised environments to build coping efficacy.

9.5 Transparent Post-Incident Feedback: Distribute summary reports following cyber incidents detailing structural fixes and policy improvements stemming from operator reports.

9.6 Resilience-by-Design Acquisition: Enforce usability and secure-by-design standards during technology procurement, ensuring digital tools support human operators under high stress.

10. Conclusion

10.1. Cyber resilience among security personnel is fundamentally a human and organisational capability supported by technology. Perceived Organisational Support explains why individuals operating under identical formal rules display varying degrees of vigilance, incident reporting, adaptation, and operational recovery.

10.2. The integrated PMT-SET framework provides a robust analytical model. PMT highlights individual threat and coping appraisals (severity, vulnerability, self-efficacy, response efficacy, response cost), while SET explains how institutional reciprocity, psychological safety, and trust foster discretionary effort. POS bridges these domains, signaling that the organisation values human contributions and stands behind operators during operational stress.

10.3. High POS strengthens cyber resilience by raising operational confidence, lowering perceived response costs, encouraging discretionary effort, accelerating early incident reporting, and enabling continuous learning. Conversely, low POS generates security fatigue, encourages unapproved workarounds, fosters fear of blame, and suppresses incident reporting.

10.4. Ultimately, security organisations cannot demand resilient cyber behaviour without cultivating the conditions that render such behaviour achievable. Resilient operators are developed when threat awareness is matched by professional competence, usable systems, and credible institutional support.

11. Recommendations

11.1. Establish Leadership Ownership: Embed cyber readiness into routine operational reviews, command evaluations, and mission assurance frameworks.

11.2. Deploy Scenario-Based Training: Focus training on degraded-environment simulations that test decision-making, reporting, and mission continuity under digital disruption.

11.3. Cultivate a Just Reporting Culture: Clearly differentiate between deliberate policy violations and inadvertent operational errors, incentivizing early, good-faith reporting.

11.4. Minimize System Operational Friction: Audit and streamline security protocols, automating routine safeguards to lower response costs for operators.

11.5. Enhance Self-Efficacy: Provide practical, hands-on rehearsal and clear feedback loops to build operator confidence in threat mitigation.

11.6. Formalize After-Action Learning: Implement transparent post-incident reviews so personnel see tangible operational improvements resulting from reported events.

11.7. Monitor Human-Factor Indicators: Incorporate periodic assessments of POS, self-efficacy, and security fatigue into readiness reporting alongside technical audits.

11.8. Integrate Resilience into Acquisition: Mandate user-centric design, graceful system degradation, and ergonomic software interfaces during technology procurement.

11.9. Validate Socio-Technical Models: Conduct ongoing empirical research across varied security sectors to continuously refine the measured impact of POS on adaptive performance.

11.10. Combine Survey and Behavioural Metrics: Augment self-reported perceptions with objective behavioural data, such as simulated exercise response times and incident reporting trends.

Acknowledgement

The author gratefully acknowledges the Editor and the reviewers for their constructive comments, critical observations, and valuable suggestions during the preparation and refinement of this research paper. Their insights have significantly enhanced the conceptual clarity, theoretical discipline, and practical relevance of this work.

References

1. Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), 613–643.
2. Bada, M., Sasse, M. A., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *In International Conference on Cyber Security for Sustainable Society*.
3. Blau, P. M. (1964). *Exchange and Power in Social Life*. New York: Wiley.
4. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523–548.
5. Caesens, G., Stinglhamber, F., Demoulin, S., & De Wilde, M. (2019). Perceived organizational support and employees' well-being: The mediating role of organizational dehumanization. *European Journal of Work and Organizational Psychology*, 28(5), 695–709.
6. Ebbers, S., & van der Kleij, R. (2026). Beyond phishing: A human-centered exploration of cyber incident reporting. *In International Conference on Human Aspects of Information Security, Assurance and Trust* (pp. 335–348). Springer, Cham.
7. Eisenberger, R., Huntington, R., Hutchison, S., & Sowa, D. (1986). Perceived organizational support. *Journal of Applied Psychology*, 71(3), 500–507. https://doi.org/10.1037/0021-9010.71.3.500
8. ENISA. (2018). *Cyber Security Culture Guidelines: Behavioural Aspects of Cybersecurity*. European Union Agency for Cybersecurity.
9. ENISA. (2019). *Behavioural Aspects of Cybersecurity: Cybersecurity Culture Guidelines – Technical Annex: Evidence Reviews*. European Union Agency for Cybersecurity.
10. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007
11. Kurtessis, J. N., Eisenberger, R., Ford, M. T., Buffardi, L. C., Stewart, K. A., & Adis, C. S. (2017). Perceived organizational support: A meta-analytic evaluation of organizational support theory. *Journal of Management*, 43(6), 1854–1884. https://doi.org/10.1177/0149206315575554

12. NIST. (2025). *SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management*. National Institute of Standards and Technology.
13. Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social Psychophysiology*. New York: Guilford Press.
14. Van der Kleij, R., Spinnler, O., Broderick-Hale, J., Hendriks, K., Drenth, A., & van Wijgerden, J. (2026). Cultural, organisational, and individual factors contributing to cyber incident reporting: A systematic literature review. *Computers in Human Behavior*, 109127.
15. Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Journal of Organizational and End User Computing*, 20(4), 69–89.

ISARA INSTITUTE OF MANAGEMENT & PROFESSIONAL STUDIES

WWW.IIMPS.IN

EARN YOUR

MBA



Accreditation & Ranking

UGC / NCTE Approved.

INFO@IIMPS.IN

011-41005174

RESEARCH GATEWAY

STOP PLAGIARISM

1 Submit your content in Word File.

2 Get report in 48 hrs.

3 *Missing content or references will be fixed.

4 Citation for your work.

5 Get accurate user friendly report.

researchgateway.in | info@researchgateway.in

+91-9205579779

AROGYAM ONLINE

Arogyam Ayurveda

Holistic Healing through herbs

100% NATURAL

PARIVARTAN PSYCHOLOGY CENTER

COLOR PSYCHOLOGY : HOW COLOR AFFECT YOUR CHILD

BLUE — Calms your Child's Mind & Body

YELLOW — Promotes Concentration, Stimulates the Memory

PINK — Evokes Empathy, makes your Child Calm

RED — Excites and energizes your Child's body

GREEN — Improves Reading speed and Comprehension

www.parivartan4u.com

Confuse about your children's future?

भारतीय भाषा, शिक्षा, साहित्य एवं शोध

ISSN 2321 – 9726

WWW.BHARTIYASHODH.COM

INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SCIENCE & TECHNOLOGY

ISSN – 2250 – 1959 (0) 2348 – 9367 (P)

WWW.IRJMST.COM

INTERNATIONAL RESEARCH JOURNAL OF COMMERCE, ARTS AND SCIENCE

ISSN 2319 – 9202

WWW.CASIRJ.COM

INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SOCIOLOGY & HUMANITIES

ISSN 2277 – 9809 (0) 2348 - 9359 (P)

WWW.IRJMSH.COM

INTERNATIONAL RESEARCH JOURNAL OF SCIENCE ENGINEERING AND TECHNOLOGY

ISSN 2454-3195 (online)

WWW.RJSET.COM

INTEGRATED RESEARCH JOURNAL OF MANAGEMENT, SCIENCE AND INNOVATION

ISSN 2582-5445

WWW.IRJMSI.COM

JOURNAL OF LEGAL STUDIES,POLITICS AND ECONOMICS RESEARCH

WWW.JLPER.COM