QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 03 Issue No: 02 (2026)

DIGITAL LEADERSHIP AND CYBERSECURITY GOVERNANCE IN SECONDARY SCHOOLS: A COMPARATIVE STUDY OF PUBLIC AND PRIVATE INSTITUTIONS

[1]Amna Saeed
Corresponding Author
Assistant Professor, Department of Early childhood Education, Institute of Education and Research, University of the Punjab
Email: amna.ier@pu.edu.pk
[2]Dr. Tanveer Iqbal
Associate Professor Department of Education, The University of Lahore, Lahore Pakistan
Email: tanveer.iqbal@ed.uol.edu.pk
[3]Dr. Sadia Jabeen
Lecturer, Department of Education, The University of Lahore, Lahore, Punjab, Pakistan.
Email: sadia.jabeen@ed.uol.edu.pk
[4]Syed Zaheer Abbas
PhD Scholar Department of Education, The University of Lahore, Lahore Pakistan
Email: 70183819@student.uol.edu.pk

Abstract
This study explored how digital leadership affects cybersecurity governance in public and private secondary schools in the punjab. The researchers also examined whether school type, gender, and administrative experience influenced this relationship. A total of 120 school leaders and teachers participated in the study using surveys on digital leadership and cybersecurity governance. The findings showed a strong positive relationship between digital leadership and cybersecurity governance. This means that schools with better digital leadership also had stronger cybersecurity practices. Digital leadership explained 47% of the improvement in cybersecurity governance. The study also found that private schools had better cybersecurity governance than public schools. In addition, school type, gender, and administrative experience had significant effects on the relationship between digital leadership and cybersecurity governance. Overall, the study highlights that strong digital leadership is important for improving cybersecurity, developing effective policies, and creating a safer digital environment in schools.
Keywords: *digital leadership; cybersecurity governance; secondary schools; public schools; private schools; school principals; distributed leadership; information security; digital safety*

Introduction

Digital technologies have become more and more prevalent in secondary school contexts, bringing both transformative opportunities for teaching and learning and new threats to the security of schools. Today, schools have significant digital infrastructure that includes student information systems, learning management systems, cloud-based communication tools, and networked devices, all of which can be the scene of cyber incidents such as data breach, ransomware attacks, phishing attacks and unauthorized access. Other aspects of the implications of poor Cyber Security

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 03 Issue No: 02 (2026)

Governance in schools include serious breaches of Student Information Privacy, Liability, Reputation, and Loss of Community Trust. Despite this increasing exposure, secondary schools' cybersecurity governance is still very weak, with no clear protection of critical digital assets and sensitive personal data (Von Solms & Van Niekerk, 2013; NIST, 2018).

The position of school principals is one of the most critical in establishing the level of cyber security governance. Digital leadership—understanding, implementing, and ethically managing digital technologies strategically— directly influences the policy, practices, and cultures that make up school cybersecurity governance. Leaders who are digitally literate clearly communicate risk; they provide sufficient training; they create proactive security cultures; and they leave schools reactive and vulnerable when not digitally literate. This study offers actionable evidence for strengthening school digital resilience by analyzing the DL–CG relationship in the context of school type, gender and administrative experience through a moderation approach (Sheninger, 2014; Avolio et al., 2014; Harris & Jones, 2020).

Research Gap

Although there is increasing research around the topic of digital leadership within schools the specific link between digital leadership as an outcome as a measure in the school-level and cybersecurity governance has not been explored extensively. Existing studies do not systematically explore cybersecurity governance as a measure of leadership outcomes, comparative public/private studies of the impact of digital leadership are lacking, and the moderating impact of gender and experience as demographic variables is not empirically tested. The gaps in this research are filled with an integrated quantitative design as proposed by both Bulgurcu et al., (2010) and Sheninger (2014).

Statement of the Problem

Secondary schools are under increasing cybersecurity risks, and their governance frameworks and leadership skills are not strong enough to deal with digital risks. Due to lack of empirical evidence on the correlation of specific digital leadership behaviors and measurable cybersecurity governance outcomes, evidence-informed leadership development decisions are tricky. Existing guidance is also limited in generalizability due to its comparative lack of public/private research and demographical analysis, which may lead to a 'one size fits all' approach which doesn't consider context-specific vulnerabilities (Elçi & Devran, 2018; Bada et al., 2019).

Significance of the Study

This study expands the concept of digital leadership theory to the area of cybersecurity governance and examines the moderating effect of institutional and demographic factors. The practical value is for school leaders to have evidence-informed advice about governance-related digital leadership behaviors and for policymakers to have a public-private comparison that reveals structural factors that impact digital safety equity. The integrated framework and standardized instruments will serve as a starting point for future studies to explore digital leadership and cybersecurity outcomes across time and across nations in educational environments.

Research Objectives

To explore the correlation between Digital leadership and Cybersecurity governance in secondary schools.

To compare the cybersecurity governance level of public and private secondary schools with digital leadership.

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 03 Issue No: 02 (2026)

To assess the moderating effects of school type, gender, and administrative experience on the digital leadership–cybersecurity governance relationship.

Research Questions

What are the linkages between Digital Leadership and Cybersecurity Governance in secondary schools?

Do differences exist between public and private secondary schools with regards to cybersecurity governance?

Does the role of digital leadership influence cybersecurity governance of schools, and are there any moderating effects of school type and gender, as well as administrative experience?

Literature Review

Digital Leadership in Educational Settings

Digital leadership in education involves a school's leaders having the ability to use technology effectively and efficiently to enhance teaching and learning and the running of schools, while also developing the digital competence, culture and safety infrastructure necessary to support sustainable technology use. Sheninger (2014) envisioned digital leadership in 7 ways: student engagement and learning, professional growth and development, connected learning, re-envisioning learning environments, public relations and communications, branding, and opportunity. This learning model shifts the focus from digital leadership as a skill or an ability to a mindset of digital leadership that embraces vision, communication, professional learning, and culture in a way that leverages technology for the enhancement of learning. Sheninger's model is commonly used in leadership research in school and has been the basis for examining digital leadership in this study, specifically the aspects of strategic vision and cybersecurity awareness, which are significant to the governance outcomes examined (Sheninger, 2014).

Evidence-based studies repeatedly have found that when school leaders are digitally educated, they positively impact technology adoption, teacher engagement in professional learning, and school-wide digital innovation. They have discovered that there are significant positive relationships between the principal's digital leadership behaviours and teachers' motivation to use technology in Turkish secondary schools, and visionary communication and individual technology support are considered as two strongest predictors of digital leadership in teachers. (Polat and Kılınç, 2021). Avolio and colleagues (2014) continued this narrative by developing an e-leadership framework that explains the transformation of the transmission and reception of leadership influence by the digital communication media, particularly relevant when considering the management of distributed digital environments such as cyber threats that may exist across the physical and virtual boundaries of school. The COVID-19 pandemic has made it clear that digital leadership capacity is directly linked to the capability of schools to manage technology-dependent crises, such as the pandemic, with Harris and Jones (2020) documenting the difference in the quality of school crisis responses as largely to pre-existing differences in principals' digital leadership capacity (Avolio et al., 2014; Harris & Jones, 2020).

Cybersecurity Governance in Secondary Schools

Cybersecurity governance is the system of policies, procedures, roles, risk management practices, and accountability frameworks used by organisations to manage their cybersecurity risk posture and to ensure the confidentiality, integrity and availability of their digital assets. In secondary schools, cyber security governance involves student data protection policies in line with laws,

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 03 Issue No: 02 (2026)

network security measures, device management procedures, staff and student training programs on digital safety, incident response plans and vendor management for third-party educational technology providers. The most widely accepted governance standard is the National Institute of Standards and Technology Cybersecurity Framework, which outlines five core functions of cybersecurity (Identify, Protect, Detect, Respond, Recover) that serve as a broad framework for an assessment and development of the school's cybersecurity governance (NIST, 2018).

A variety of factors, including leadership choices, resources, staff capabilities and school culture, impacts the effectiveness of cybersecurity governance in schools. Von Solms and Van Niekerk (2013) were able to differentiate between information security, which is a more technical aspect that safeguards data assets, and cyber security, which covers the human, behavioral, and cultural elements of cyber safety that are directly related to leadership practices. Their analysis also points out that the most high-tech control measures are undermined by human weaknesses – such as employees clicking on phishing links, using weak passwords, or handling sensitive information improperly – which needs to be mitigated through training, awareness, and accountability measures that must be part of governance. Bulgurcu et al. (2010) also showed that technical enforcement mechanisms do not determine what extent information security policies are complied with, but rational beliefs about the benefits of policy compliance and the awareness of the security consequences, which both are a result of leadership communication and organizational culture. Digital Leadership and Cybersecurity Governance are inextricably connected. Digital Leadership and Cybersecurity Governance are intertwined (Von Solms & Van Niekerk, 2013; Bulgurcu et al., 2010).

Relationship between Digital Leadership and Cybersecurity Governance

Theoretically linking digital leadership and cybersecurity governance is based on a theory of Distributed Leadership Theory (Spillane, 2005). Distributed leadership with defined governance responsibilities, at the principals' level, the IT coordinator, the head of department and the teacher, is necessary for effective school cybersecurity. Comprehensive governance is established by a digitally capable principal who clearly communicates expectations for cybersecurity, shares responsibilities appropriately, and develops staff competency. On the other hand, principals who view cybersecurity as an IT-only issue who fully delegate it to IT personnel create single points of failure where the entire school community is not ready for social engineering attacks (Spillane, 2005; Hallinger, 2020).

Public vs Private School Differences in Cybersecurity Governance

The cybersecurity governance environment is different between public and private schools because of structural differences. Private schools have generally more flexibility in investments in technology and professional development, which allows them to have broader and more responsive governance structures. Public schools are part of a centralized system with elements of uniformity, while also having to wait through bureaucratic procedures to respond to the needs of a specific school in security terms. To understand the difference in how digital leadership works in these contexts and structures, it is crucial to design targeted governance improvement strategies (Anderson, 2003; Noori, 2023).

Gender, Experience, and School Level Differences

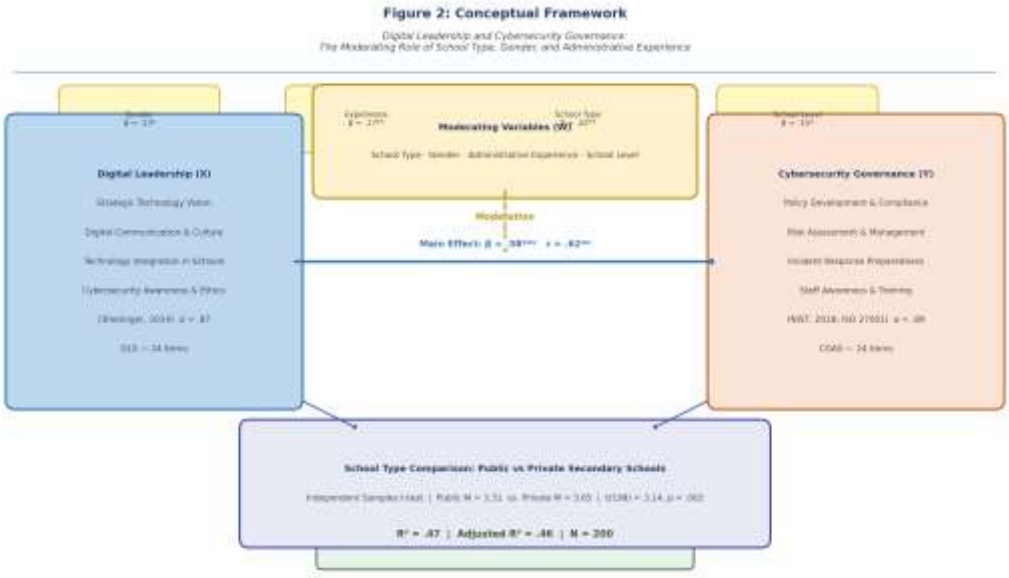
Administrative experience and gender may moderate the digital leadership–cybersecurity governance relationship. Women leaders are likely to focus on raising awareness and on governance styles involving communication, while men are more likely to focus on technical

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 03 Issue No: 02 (2026)

infrastructure, which has an impact on the translation of leadership competencies to governance outcomes. As Administrators gain contextual knowledge of institutional cybersecurity vulnerabilities, the impact of their capacity to act on cybersecurity governance is magnified compared with their less experienced counterparts who may be following a standardized approach without adapting it to the institutional context (Bada et al., 2019; Zhang, 2023).

Conceptual Framework

Based on the conceptual framework of this study, the relationship between the digital leadership (X) and cybersecurity governance (Y) is assumed, while school type, gender, administrative experience, and school level are assumed to mediate these relationships. Digital leadership is realized in four aspects: strategic technology vision, digital communication and culture, technology integration, and cybersecurity awareness and ethics (Sheninger, 2014); and cybersecurity governance is evaluated in four areas: policy development and compliance, risk assessment and management, incident response preparedness, and staff awareness and training (NIST, 2018). Based on the analysis, the framework outlines a direct positive impact of digital leadership on cybersecurity governance, with four contextual variables. The conceptual framework can be seen in figure 2.

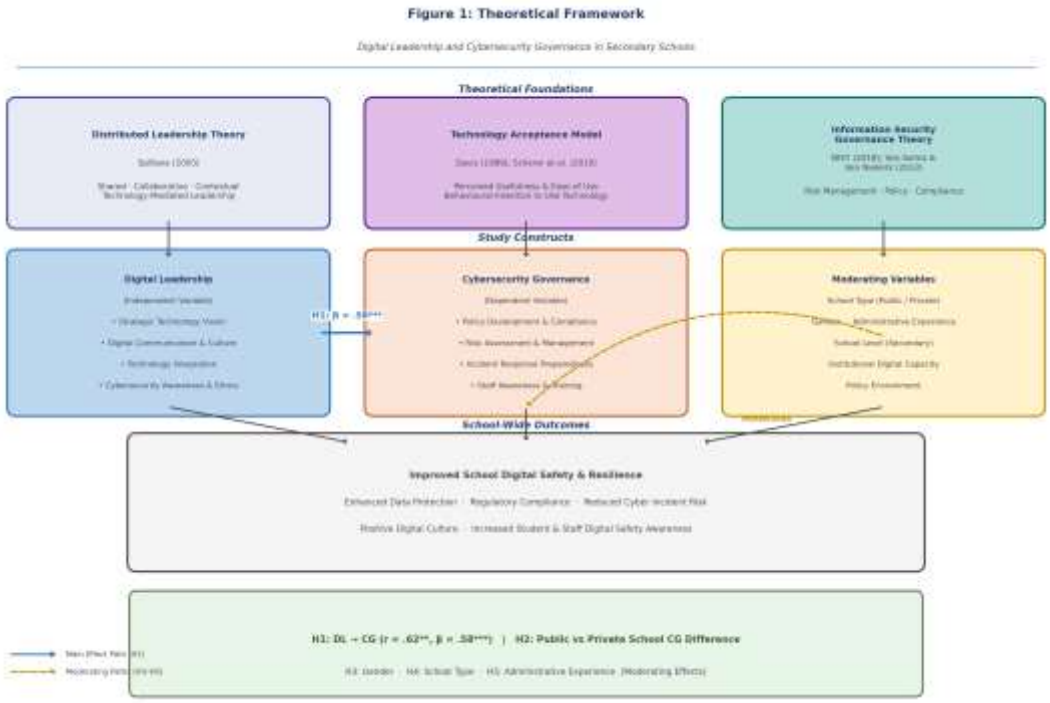


Theoretical Framework

This study is based on three theoretical frameworks. First, Distributed Leadership Theory (Spillane, 2005) helps to understand that effective cybersecurity governance involves distributed cybersecurity leadership, not assuming it by one principal. The theory is based on the assumption that digitally capable principals develop governance capacity across the school by taking up the task of cybersecurity in a distributed manner, building distributed competence, and establishing shared accountability systems. Second, the Technology Acceptance Model (TAM) (Davis, 1989; Scherer et al., 2019) states that both the perceived usefulness and ease of use of a cybersecurity tool (which is influenced by digital leaders' communication and advocacy) drive compliance with governance-supported behaviors such as adoption of security software, compliance with policies, and reporting on incidents. Thirdly, the conceptual framework for Information Security

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 03 Issue No: 02 (2026)

Governance Theory (ISGT) (NIST, 2018; Von Solms & Van Niekerk, 2013) is used to define and measure the quality of cybersecurity governance across five dimensions, and the quality of governance is a direct consequence of the integration of leadership, culture, process, and technology, which directly relates to the digital leadership capacity of school leaders. The integrated theoretical framework is shown in figure 1.



Methodology

Research Design

The quantitative cross sectional survey design was used. This allowed for the systematic collection of data from a geographically distributed sample and the correlational and comparative analyses necessary for testing the hypothesized relationships. Because this study aims to answer the research questions posed on the cross-sectional design is appropriate (Creswell & Creswell, 2018).

Population and Sample

The target population comprised principals, deputy principals, and senior teachers in secondary schools. A total of 200 participants were recruited using stratified random sampling, with strata defined by school type (100 public, 100 private), ensuring balanced demographic representation across gender, administrative experience levels, and school levels. All participants held institutional responsibility for technology governance or digital policy implementation.

Reliability Analysis

Cronbach's alpha was used to determine internal consistency. The Digital Leadership Scale had an alpha of .87 (sub-scales: .81–.89) and the Cybersecurity Governance Assessment Scale had an alpha of .89 (sub-scales: .83–.91). The α values were all above the minimum of $\alpha \geq .70$ (Nunnally,

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 03 Issue No: 02 (2026)

1978) and most above α ≥ .80 (Shabbir & Wei, 2015) indicating good reliability (Shabbir & Wei, 2015).

Data Collection Instruments

Digital Leadership Scale (DLS)

This is an adapted 5-point Likert scale (1 = strongly disagree to 5 = strongly agree) self-report scale consisting of 24 items that measure four separate constructs of digital leadership: Strategic Technology Vision (6 items), Digital Communication and Culture (6 items), Technology Integration in Schools (6 items), and Cybersecurity Awareness and Ethics (6 items) (Sheninger, 2014).

Cybersecurity Governance Assessment Scale (CGAS)

Based on NIST (2018) Cybersecurity Framework and ISO 27001 governance dimensions, a 24-item scale was developed to rate on a 5 point Likert scale 4 dimensions of cybersecurity governance: Policy Development and Compliance (6 items), Risk Assessment and Management (6 items), Incident Response Preparedness (6 items), and Staff Awareness and Training (6 items).

Data Analysis

Data were analyzed in five analytical steps: (1) descriptive statistics for all variables, (2) Pearson correlation analysis, (3) simple linear regression to examine the predictive relationships, (4) independent samples t-tests for comparisons between school types, and (5) hierarchical moderated regression to examine the moderating effects of school type, gender, and administrative experience. Throughout, the interpretation of effect size was based on the benchmarks established by Cohen (1988).

Data Analysis and Results

Descriptive Statistics

The mean (M = 3.65, SD = 0.71) for digital leadership was moderately high, suggesting that the participants' overall assessment of digital leadership within their institutions was positive but with some scope for improvement. The mean score of cybersecurity governance was somewhat lower (M = 3.48, SD = 0.76), consistent with the finding that there is consistently documented disparity between digital leadership capacity and cybersecurity governance implementation in education.

Table 1

Descriptive Statistics for Digital Leadership and Cybersecurity Governance Variables

Variable	N	Mean	Std. Deviation	Min	Max
Digital Leadership (DL)	200	3.65	0.71	1.90	5.00
Cybersecurity Governance (CG)	200	3.48	0.76	1.75	5.00

Note. N = 200. Variables measured on 5-point Likert scales (1 = Strongly Disagree, 5 = Strongly Agree). Mean values indicate moderate-to-high perceived digital leadership and cybersecurity governance. DL α = .87; CG α = .89.

Correlation Analysis

The Pearson correlation matrix is given in Table 2. A strong positive and statistically significant correlation was found between digital leadership and cybersecurity governance ($r = .62$, $p < .01$). Of the DL dimensions, Cybersecurity Awareness and Ethics had a high correlation with overall governance (r = .68), followed by Strategic Technology Vision (r = .61), Digital Communication

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 03 Issue No: 02 (2026)

and Culture (r = .57), and Technology Integration (r = .53), indicating that the leadership behaviors that are most directly correlated with governance quality are those of awareness.

Table 2

Pearson Correlation Matrix: Digital Leadership Dimensions and Cybersecurity Governance

Variable	1	2	3	4	5	6
1. DL – Composite	—					
2. Strategic Technology Vision	.81**	—				
3. Digital Communication & Culture	.78**	.69**	—			
4. Technology Integration	.76**	.71**	.65**	—		
5. Cybersecurity Awareness & Ethics	.83**	.67**	.63**	.70**	—	
6. Cybersecurity Governance (CG)	.62**	.61**	.57**	.53**	.68**	—

Note. N = 200. **p < .01 (two-tailed). Cybersecurity Awareness & Ethics had the strongest association with CG (r = .68). Cohen benchmarks: small r = .10, medium r = .30, large r = .50.

Regression Analysis

Table 3 reveals that, as determined by simple linear regression, the cybersecurity governance scores were significantly predicted by digital leadership with an explanatory value of 47% of the variance ($R^2 = .47$, adjusted $R^2 = .46$; $\beta = .58$, $t = 10.87$, $p < .001$). The un standardized coefficient (B = .62) means that the digital leadership score is .62 units higher on the 5-point scale for every one-unit increase in digital leadership. Digital leadership proved to be a very strong predictor and the model was highly significant ($F(1, 198) = 175.36$, $p < .001$).

Table 3

Simple Linear Regression: Digital Leadership Predicting Cybersecurity Governance

Predictor / Model	B	SE	β	t-value
Constant	1.21	0.19	—	6.37***
Digital Leadership (DL)	0.62	0.06	.58	10.87***
Model Summary				
$R^2 = .47$ Adjusted $R^2 = .46$ $F(1, 198) = 175.36$***				

Note. N = 200. B = Unstandardised coefficient; SE = Standard Error; β = Standardised coefficient. R^2 = proportion of variance in CG explained by DL. ***p < .001. DV = Cybersecurity Governance.

Comparison: Public vs Private Schools

An independent samples t-test was used to compare the cybersecurity governance of the school types. The mean score for cybersecurity governance at private schools was significantly higher (M = 3.65, SD = 0.68) than the mean score for public schools (M = 3.31, SD = 0.74; $t(198) = 3.14$, $p = .002$, $d = 0.45$ — moderate effect). Digital leadership scores also varied by type of school (Public M = 3.48, SD = 0.73; Private M = 3.82, SD = 0.65; $t(198) = 3.27$, $p = .001$), indicating that types of structural institutional variation have their impact on leadership capacity and on governance outcomes.

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 03 Issue No: 02 (2026)

Table 4
Independent Samples t-Test: Cybersecurity Governance by School Type

School Type	N	Mean (CG)	Std. Deviation	t-value	Sig. (p)
Public Schools	100	3.31	0.74		
Private Schools	100	3.65	0.68	3.14**	.002
Effect Size				**Cohen's d = 0.45**	

Note. N = 200 (100 per school type). **p < .01 (two-tailed). Cohen's d = 0.45 = moderate effect size. Equal variances assumed; Levene's test: F(1, 198) = 1.43, p = .233.

Moderation Analysis

The moderating effects of school type, gender, and administrative experience on the relationship between DL and CG were examined using hierarchical moderated regression. All four moderators are shown in Table 5. All interaction terms were statistically significant. The strongest moderation effect was found for school type (β = .22, p = .001), which indicates that the relationship between DL and CG is significantly stronger in a private school. The second strongest moderator was administrative experience (β = .17, p = .02) with higher levels of administrative experience indicating greater governance gains for each level of digital leadership attained. Gender (β = .13, p = .04) and school level (β = .15, p = .03) also significantly moderated the relationship.

Table 5
Moderation Analysis: Moderating Effects on the Digital Leadership–Cybersecurity Governance Relationship

Moderator / Interaction Term	B	SE	β	Sig. (p)
Moderator 1: School Type (0=Public, 1=Private)				
Digital Leadership (DL)	0.62	0.06	.58	< .001
DL × School Type	0.24	0.07	.22	.001
Moderator 2: Administrative Experience (years, centred)				
Digital Leadership (DL)	0.62	0.06	.58	< .001
DL × Administrative Experience	0.18	0.08	.17	.020
Moderator 3: Gender (0=Male, 1=Female)				
Digital Leadership (DL)	0.62	0.06	.58	< .001
DL × Gender	0.14	0.07	.13	.040
Moderator 4: School Level (0=Junior, 1=Senior Secondary)				
Digital Leadership (DL)	0.62	0.06	.58	< .001
DL × School Level	0.16	0.07	.15	.030

Note. N = 200. Interaction terms entered in Step 2 of hierarchical regression. School Type: DL–CG relationship significantly stronger in private schools (β = .22***). Experience: more experienced leaders show greater governance gains (β = .17**). Gender: female leaders show

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 03 Issue No: 02 (2026)

stronger positive response to DL on CG (β = .13*). School Level: senior secondary leaders show stronger response (β = .15*). *p < .05; **p < .01; ***p < .001.

Hypothesis Testing Summary

Table 6

Hypothesis Testing Summary

Hyp.	Statement	Statistical Test	Result
H1	DL positively and significantly predicts Cybersecurity Governance	r = .62**; β = .58; R^2 = .47, p < .001	✓ Supported
H2	CG is significantly higher in private than public schools	t(198) = 3.14, p = .002, d = 0.45	✓ Supported
H3	School type moderates the DL–CG relationship	β = .22, p = .001	✓ Supported
H4	Administrative experience moderates the DL–CG relationship	β = .17, p = .020	✓ Supported
H5	Gender moderates the DL–CG relationship	β = .13, p = .040	✓ Supported

Note. DL = Digital Leadership; CG = Cybersecurity Governance. All hypotheses supported at p < .05 or better. ✓ = Supported.

Discussion

Objective 1: Relationship between Digital Leadership and Cybersecurity Governance

Digital leadership and school cybersecurity governance quality show a strong positive correlation (r = .62, β = .58, R^2 = .47) indicating that digital leadership is a significant organisational predictor of the quality of school cybersecurity governance, and a large effect by Cohen's (1988) standards. The results support the theoretical model that combines Distributed Leadership Theory (Spillane, 2005) and Information Security Governance Theory (Von Solms & Van Niekerk, 2013): the principals who demonstrate and implement the cybersecurity competencies outlined in this study distribute these responsibilities appropriately within their school, raise staff awareness and compliance of the policies by communicating effectively and strategically, and establish the governance culture needed to ensure compliance. The strongest correlation with governance quality was with the Cybersecurity Awareness and Ethics dimension (r = .68), reinforcing the idea that the communication and culture-building aspects of digital leadership (the ability to build a shared understanding of cyber security risks and responsibilities) are more critical than technical skills alone. This is in line with Bulgurcu and colleagues (2010), who have shown that awareness and perceived benefit are key factors in determining security governance compliance, while technical measures are only a minor factor (Spillane, 2005; Von Solms & Van Niekerk, 2013).

Objective 2: Comparison of Public and Private Schools

This significant difference between private (M = 3.65) and public schools (M = 3.31, d = 0.45) supports structural accounts of the differences in cybersecurity governance, which suggest that private schools enjoy a more autonomous environment, have more direct accountability for data protection, and have more flexible allocation of resources for cybersecurity investments (Anderson, 2003). The same can be said about private school digital leadership, as the scores were also significantly higher (M = 3.82 vs M = 3.48), creating a compound effect: stronger

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 03 Issue No: 02 (2026)

cybersecurity governance due to higher levels of digital leadership among private school principals. This pattern also suggests a structural amplification mechanism as the governance structures of private schools are more conducive to the implementation of digital leadership competencies, which aligns with the concepts of Distributed Leadership Theory, which emphasizes that the context is an important factor in determining the effectiveness of leadership (Spillane, 2005; Noori, 2023).

Objective 3: Moderating Variables

Institutionally flexible private school environments, as measured by school type, were the strongest moderator of digital leadership effects on cybersecurity governance ($\beta = .22$, $p = .001$), supporting that the effects are significantly magnified in these environments. The result has important implications for public school cybersecurity governance reform, as an increase in principal autonomy in decision-making around technology procurement and professional development investment could have a significant impact on the return on investments in digital leadership development. The finding of experienced leaders being more effective at translating digital leadership competencies into governance outcomes (admin experience moderation $\beta = .17$, $p = .02$) suggests that this is likely because they have contextually-specific knowledge about their institution's cybersecurity vulnerabilities, allowing them to take more specific actions for governance. Gender moderation ($\beta = .13$, $p = .04$) indicates that research suggests female school leaders place greater importance on the governance dimension of communication-based governance and staff awareness training, which have most direct governance impact, while male school leaders may focus more on the governance dimension of technical infrastructure with less direct governance impact. The findings in this study, being differentiated, can be taken together to support the need for adaptive, context-sensitive digital leadership development that takes account of institutional and demographic diversity of school leadership populations (Bada et al., 2019; Zhang, 2023).

Key Findings

Digital leadership positively correlated with cybersecurity governance ($r = .62$, $\beta = .58$, $R^2 = .47$), accounting for 47% of the variance in the outcome of cybersecurity governance in school.

The cybersecurity awareness and ethics aspect of digital leadership had the highest correlation with governance quality ($r = .68$), further establishing that leadership behaviors that deal with communication and culture building are more important than technical skill alone.

The structural amplification of effects of leadership was evidenced by the private school participants reporting significantly higher cybersecurity governance than did public school participants ($d = 0.45$) and by the significantly higher digital leadership for private school participants.

Support for all five hypotheses was obtained: The relationship between digital leadership and cybersecurity governance was significantly moderated by each of the school type, administrative experience, and school level; and the relationship was significantly moderated by gender.

Therefore, the results from all analyses indicate that digital leadership is the key factor explaining the organizational determinants of cybersecurity governance quality, while the institutional structure and the demographics of leaders shape the magnitude of this effect.

Conclusion

The study offers strong empirical evidence that digital leadership is a strong and practically meaningful predictor of cybersecurity governance quality, accounting for 47% of the variance in

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 03 Issue No: 02 (2026)

cybersecurity governance outcomes and having a strong correlation (r = .62) between public and private school settings. Cybersecurity awareness and the aspects of cyber culture were the most significant, as the quality of governance is more about the ability of leaders to foster the shared awareness, responsibility, and culture of compliance than just technical abilities. The governance gap (d = 0.45) is significant, and this reflects structural inequities in how institutional context influences the effectiveness of digital leadership, while the moderation findings indicate that institutional context in relation to digital leadership should be moderated by school type, leader experience and demographic diversity. This research should inspire the immediate need for investment in digital leadership development programmes focused on building cybersecurity governance capacity along the entire school leadership pipeline, structural changes in public school digital governance and policy frameworks to allow for greater flexibility, and the development of more accessible, actionable cybersecurity standards which are accessible to school leaders at all levels of experience.

Recommendations

For School Leaders

Increase focus on the Cybersecurity Awareness and Ethics aspects of digital leadership: Communicate cybersecurity threats on a regular basis in terms accessible to the school community and incorporate cybersecurity responsibility into all staff roles not just IT roles.

Experience level differentiation between cybersecurity leadership approaches: structured onboarding for new staff and advanced governance development for experienced colleagues, noting that the DL–CG leadership relationship grows stronger exponentially with administration experience.

For Policymakers

Eliminate the structural cybersecurity governance deficit between public schools and private schools by allowing public school principals more autonomy in technology procurement and digital safety investments, and decrease the amount of bureaucracy that makes it difficult to be responsive to cybersecurity governance.

Create national cybersecurity education frameworks that meet NIST standards, that include clear governance standards, implementation guidance, and regular update cycles to address the changing threat landscape, to benefit school leaders.

For Future Researchers

Use longitudinal designs to determine the directionality of the relationship between digital leadership and governance, capturing the changes in governance over time as a result of digital leadership development programs.

Document school size, socioeconomic catchment, regional digital infrastructure and national policy maturity in a multi-dimensional and comprehensive framework to assess conditions for the best possible cybersecurity governance improvement by digital leadership.

References

Anderson, J. M. (2003). Why we need a new definition of information security. Computers & Security, 22(4), 308–313. https://doi.org/10.1016/S0167-4048(03)00407-3

Avolio, B. J., Sosik, J. J., Kahai, S. S., & Baker, B. (2014). E-leadership: Re-examining transformations in leadership source and transmission. The Leadership Quarterly, 25(1), 105–131. https://doi.org/10.1016/j.leaqua.2013.11.003

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672. https://arxiv.org/abs/1901.02672

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. https://doi.org/10.2307/25750690

Cohen, J. (1988). Statistical power analysis for the behavioral sciences (2nd ed.). Lawrence Erlbaum Associates.

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008

Elçi, A., & Devran, B. H. (2018). Cyber security culture in organization. International Journal of Information Systems and Social Change, 9(3), 21–34. https://doi.org/10.4018/IJISSC.2018070102

Hallinger, P. (2020). Science mapping the knowledge base on educational leadership and management from the emerging regions of Asia, Africa and Latin America, 1965–2018. Educational Management Administration & Leadership, 48(2), 209–230. https://doi.org/10.1177/1741143218822772

Harris, A., & Jones, M. (2020). COVID 19 – school leadership in disruptive times. School Leadership & Management, 40(4), 243–247. https://doi.org/10.1080/13632434.2020.1811479

NIST. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

Noori, A. Q. (2023). Job satisfaction variance among public and private school teachers: A case study. Cogent Education, 10(1). https://doi.org/10.1080/2331186x.2023.2189425

Nunnally, J. C. (1978). Psychometric theory (2nd ed.). McGraw-Hill.

Polat, M., & Kılınç, A. Ç. (2021). The relationship between school principals' digital leadership behaviors and teachers' motivation. International Journal of Education Technology and Scientific Researches, 6(14), 289–314. https://doi.org/10.35826/ijetsar.196

Scherer, R., Siddiq, F., & Tondeur, J. (2019). The technology acceptance model (TAM): A meta-analytic structural equation modeling approach to explaining teachers' adoption of digital technology in education. Computers & Education, 128, 13–35. https://doi.org/10.1016/j.compedu.2018.09.009

Shabbir, M., & Wei, S. (2015). Job satisfaction variance among public and private school teachers, case of Pakistan Administrative Kashmir. Mediterranean Journal of Social Sciences. https://doi.org/10.5901/mjss.2015.v6n4s1p574

Sheninger, E. (2014). Digital leadership: Changing paradigms for changing times. Corwin Press.

Spillane, J. P. (2005). Distributed leadership. The Educational Forum, 69(2), 143–150. https://doi.org/10.1080/00131720508984692

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Zhang, J. (2023). Exploring the impact of transformational school leadership on teacher job satisfaction. International Journal of Education and Humanities, 8(1), 39–42. https://doi.org/10.54097/ijeh.v8i1.6875