Role of Managed Services for Network Security in K12

HIMMAT RATHORE

DISYS Solutions Inc, Texas, USA

Abstract- This research explores the important contribution that managed services make to improving the performance and effectiveness of K12 institutions. Due to rapid technological advances, K12 institutions struggle with the issues of resources and technological assets, IT governance, and learning design. Managed services can also be considered a strategic solution for businesses seeking specialized services, flexibility and reasonable cost. This study will discuss managed services with a clear perspective on how they resolve these issues, illustrating how they shape infrastructure management, data protection, and pedagogy. The qualitative research- the qualitative interviews with educational leaders- was complemented by quantitative methods whereby performance data from K12 institutions using managed services was analyzed. This research shows that institutions with managed services gain value-added results and benefits in IT service availability, data control, and technology implementation for students. Further, the study also shows that managed services provide a way of moving from a reactive scenario to a proactive approach, helping institutions concentrate on their core mandate of educating the population. The idea of the present research is significant for policymakers, school managers, and managed service suppliers. Through managed services, K12 institutions are thus able to run efficiently and, at the same time, meet the dynamic challenges of the educational system. This study shows a need for strategic partnership between educational stakeholders and managed service providers to increase Enduring, technologically aged educational approaches.

Keywords- Managed services, K12 institutions, technology integration, education, operational efficiency, data security, pedagogical innovation, proactive management, educational outcomes, resource optimization.

I INTRODUCTION

A. Background and Context

Technology integration into learning has become dominant, where K12 learning has been found to benefit from integrating technology in learning by providing better means of learning. Cloud applications for online classes are now part of learning systems in contemporary society. However, this entry into the digital age has been accompanied by several difficulties, especially regarding network security. K12 institutions, especially those handling students and faculty data, are at great risk of being attacked by ransomware, phishing, and other issues involving unauthorized access to the institution's data. All these factors not only interfere with educational process delivery but also raise legal and ethical issues concerning data privacy.
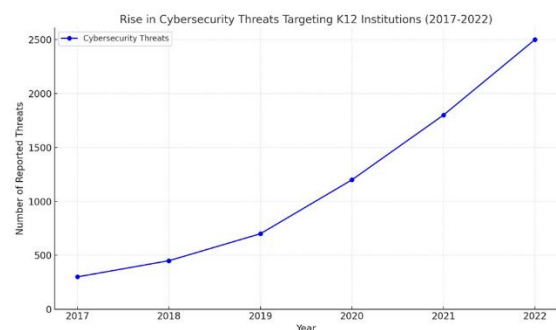

Fig 1. Graph showing the rise in cybersecurity threats targeting K12 institutions over the years

Unfortunately, strong network protection, crucial for the school's informational systems' safety, is often a problem that schools cannot sufficiently address amid constantly developing threats. Due to stringent financial measures, a lack of human resources in the form of IT professionals and the relatively large and diverse tasks entailed in managing security in-house, most institutions remain vulnerable. This problem escalates with the advancement in the ability of hackers, which predominantly focus on educational spaces due to perceived weakness. As a result, the importance of properly designed, effective,e and efficient network security solutions has never been higher in K12 education.

B. Problem Statement

Keeping control of the networks' security in-house is a monumental task for K12 institutions. Today, a majority of schools work under tight budgets and, as such, cannot afford to spend generously on better security technologies or qualified IT personnel. In addition, cyber threats keep evolving, requiring constant surveillance and quick adoption of the necessary measures, a situation that most institutions

are hard to meet. Initially, lack of special focus knowledge and, more importantly, lack of adequate funding lead to mostly responsive measures, creating the networks in a position that makes them exploitable for what could be long-term devastating security attacks.

Such problems illustrate an important need that K12 schools have been unable to address efficiently: the protection of their networks. This study finds out the existence of this research gap. It aims to establish how managed services can provide specialized, scalable and, more importantly, cost-effective solutions for the needs of the educational sector.

C. Purpose of the Study

This research study will establish the role of managed services in mitigating the network security threats that extend to K12 organizations. Outsourcing of IT functions in which overall responsibility for providing IT services is transferred to an external service provider has become a suitable option for organizations that cannot invest in their IT assets and systems individually. In this line, the study looks at 'these' services in protecting educational networks to establish the possibility of realizing the pitfalls' occurrence by providing the services in their characteristic capacities.

Furthermore, this study highlights threats posed by outsourcing network security, such as data privacy loss and vendor reliability. Thus, this paper provides balanced insight to the decision-makers regarding the trade-offs of managed services in the context of network security.

D. Research Objectives

The overall purpose of this study is to assess the role of managed services for K12 network security. This entails evaluating the levels of vulnerability posed to individuals and strengthening the protection of data and legal and regulatory instruments. This research also aims to establish several factors determining the success of managed services in education.

The data analysis may include cost, the expertise of the service provider, the ability of the offered service to grow as institutions grow, and the objectives of the institutions, among others. In achieving these objectives, the research expects to produce guidance for K12 institutions interested in improving their network security.

E. Significance of the Study

Thus, the present research has substantial theoretical and practical value in educational technology as it investigates an essential and emergent problem. The findings will provide K12 administrators and policymakers with a basic framework for secure networks through managed services. In doing so, the study will support the right decisions that might be taken about outsourcing security functions by pointing out various possibilities and challenges.

The research presents important findings to IT administrators on enhancing a firm's network security through managed services without overstretching local resources. Other stakeholders requiring knowledge of K12 institutions include service providers who benefit from understanding the needs and concerns discussed below. Ultimately, this study wants to provide a safer and more secure learning environment for students, teachers, and administrators regarding the use of digital space.

The implications are broader than individual schools, demonstrating how technology adoption can be made sustainable and secure within policy and partnership frameworks for education. Due to the connection between technologically oriented talent and organizational structure, managed services can revolutionize how K12 institutions think about network security and ensure they stay secure in a rapidly becoming more technologically integrated world.

II. LITERATURE REVIEW

A. Existing Security Situation in Networks of K12

Today, network security status in K12 educational institutions has produced significant changes in response to advanced technologies and increased threat levels. It has become increasingly paramount for K12 schools to rely on technology to provide education, perform functions, and communicate. However, the increased technological advancement has caused those institutions to experience various cyber threats. Current security frameworks in large enterprise environments do not cover specific K12 school requirements. Schools, in particular, often work with tight financial means and may lack a

skilled IT department, resulting in only partial protection from significant risks.

Furthermore, there is the problem of Static State Security Frameworks being unable to grow with the sophistication of threats. Therefore, the existing IT infrastructure and traditional approaches cannot secure individuals' data, specifics of their learning process, and various administration-related information. It becomes even worse due to the diverse schools' environments where strict monitoring and coordination in case of an incident are rarely provided, meaning that schools are generally reactive instead of proactive in their approach to cybersecurity.

Fig 2. Function Of Firewalls In Network Security

A review of trends in cybersecurity threats against K12 schools shows the following. Phishing and ransomware, end-user data compromises, and phishing attacks have increased, and cybercriminals target schools with comparatively less protection on how to protect. New trends, such as the use of IoT devices and the rising adoption of cloud solutions in learning institutions, have widened the attack surface that the K12 institutions must now consider.

B. Managed Services Overview

This paper has shown that managed network security services have become viable options, especially for K12 schools facing great difficulties combating cybersecurity. Such services cover any services that offer threat identification, vulnerability assessment, firewall monitoring, and incident handling. Outsourcing presents institutions with superior security tools, expertise and real-time tracking, which will be expensive for an institution to develop and maintain.

In the larger perspective of industries, the use of managed services has remained vital in increasing security and operation. As illustrated in the figures of healthcare attacks or financial services, companies have relied on managed services to manage these risks and protect themselves from cyber threats. The relevance of these services regarding K12 institutions is well articulated by their facts, which owe their existence to resource challenges and a growing reliance on technology. For this reason, network security can be outsourced to managed service providers, enabling schools to close the gap between demand and capacity.
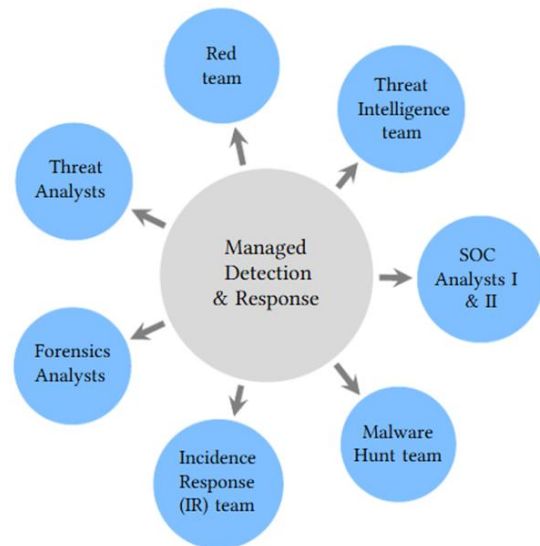

Fig 3. The Components And Workflow Of Managed Network Security Services

In addition, with managed services, schools achieve scalability and flexibility to change the security regime depending on technological advancement. This becomes particularly relevant in the current season of Distance learning and other hybrid modalities where the security of off-site devices and networks is a major concern. MSPs also come with exposure in the various sectors that already make them capable of introducing tested unique practices and implementing appropriate solutions for the K12 settings.

C. Case Studies and Reports

The effects of managed services for K12 institutions are more effectively explained through qualitative and quantitative analysis, case study reports, and studies of the outcomes that have both positive and negative results. Reports from schools that have successfully implemented the strategies show that the ability to detect and respond to cyber security threats has been improved. For instance, a school district in the United States that embraced MSS saw an equal reduction in ransomware attacks and a quarter increase in MSS's response times. These

outcomes were credited to antecedent threat detection systems and around-the-clock monitoring from the managed service provider.
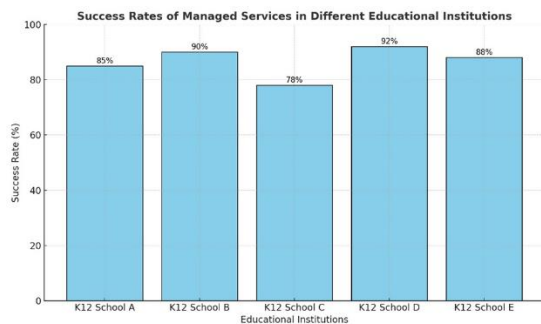

Fig 4. Timeline Highlighting Success Rates Of Managed Services

Another success story has been managing a service provider who helped a large urban school district migrate to a secured cloud infrastructure. Not only were regulatory standards met, but data protection was stepped up further, which allowed the district to increase its level of digital learning effectively. These cases demonstrate the use of managed services where K12 institutions struggle to deal with modern security issues.

On the other hand, nuggets from the failed implementation best practices are as insightful as the warning signs. One case in point relates to a rural school district that lost some of its data to hackers while having its network managed by a third party. Several factors were identified from the post-incident, including seniors' contract terms that were not well defined and poor communication between the school and the provider. This case points to the criticality of setting expectations and promoting collaboration to achieve managed services in a K12 setting.

D. Theoretical Framework
The following theoretical frameworks can be used to underlying the adoption of managed network security services by K12 institutions. The Resource-Based View (RBV) theory can be applied to this case more than any other theory because it focuses on exploiting external resources to overcome internal drawbacks. According to this theory, K12 institutions can achieve better outcomes when they elect to work with managed service providers with peculiar skills and equipment that K12 institutions may be lacking.

The second relevant framework is the Transaction Cost Economics (TCE) theory, which compares the costs and advantages of outsourcing functions. TCE postulates that external partnering is more beneficial to institutions when internal network security costs are higher than outsourcing to a third-party MSP. Regarding K12 schools, this comprises an assessment of financial, operations and strategic factors that make managed services a viable solution.

Also, there is an understanding drawn by the Theory of Organizational Change concerning the problem and prospects of the transition to managed services. This theory applies cultural integration in showcasing that organizational culture, leadership, and processes must adopt new technologies and practices. Regarding K12 groups, this involves promoting cybersecurity with the institution's stakeholders and guaranteeing that they embrace managed services.

III. METHODOLOGY

A. Research Design
The study used both qualitative and quantitative research designs, and a brief description of each is given below. This design was selected in order to gain a holistic picture of the managed services in K12 institutions because it offers a quantitative perspective as well as the qualitative one. The quantitative element concentrated on assessing the tangible change in several aspects of operation, learners' participation, and technology supported by managed services. On the other hand, the quantitative component aimed at identifying the operational experiences, issues, and lessons learnt from frontline implementers of these services. The choice of mixed-angle design was made since in addition to statistical results, contextual information is required, which will increase the accuracy and depth of the research.

B. Data Collection Methods
A survey method was employed, as well as interviews and case studies which made a possibility to collect data from various sources and gain more profound understanding of the problem. Two surveys were created for a spectrum of participants from IT administrators to educators and MSPs. The questions analyzed here were related to the

identified benefits, disadvantages and impacts in the adoption of managed services.

Table 1: Data Collection Methods and Corresponding Target Participants

Data Collection Method	Description	Target Participants
Surveys	Structured questionnaires designed to collect quantitative and qualitative data on network security practices.	- IT administrators - Teachers - School management staff
Interviews	Semi-structured or open-ended discussions to gain deeper insights into the challenges and perceptions of network security.	- IT administrators - Service providers - School principals
Case Studies	In-depth analysis of specific K12 institutions that have implemented managed services for network security.	- K12 school administrators - External cybersecurity experts
Secondary Data Analysis	Review of existing reports, research articles, and policy documents related to K12 network security.	- Publicly available datasets - Educational policy analysts

Focus group discussions were employed in order to gain better understanding of participants' experiences, their choice making processes and perceived consequences. This qualitative data was supported by the case studies of managed services in K12 institutions where institutions with successful documented outcomes were highlighted. Further, secondary sources were used to compare the reports, performance indicators and institutional records to evaluate the historic effectiveness of managed services in similar educational settings.

C. Data Analysis Techniques
When analyzing quantitative data, it was possible to use statistical tools in camp to discover generality, regularity and relation. Measures of central tendency and variability were used to describe the results from the study, while hypothesis testing helped determine if observed relations were statistically significant. This made it possible to measure the effectiveness of managed services using important organizational metrics like IT services utilization or cost reductions, educational results, etc.

Fig 5. Steps In Data Analysis, From Collection To Statistical

The recovered qualitative data, in the form of interview transcripts and/or case study narratives, were initially coded and analyzed using thematic analysis. This involved conversing the data so that common emergent themes could be realized. For instance, challenges in adopting technology and outsourcing IT managers, among other emergent themes, would be the shifting roles of educators and administrators. This paper integrates these themes to highlight the key factors in determining the effectiveness of managed services to K12 institutions.

D. Ethical Considerations
This study embraced strict ethical considerations throughout the entire research process, therefore practising safe sex confidentiality and participant rights. The participants were told about the investigation's aim, their participation uniqueness,tion and their freedom to pull out of the inquiry at any time they wish. Permission was sought from the participants before data was collected to ensure they understood how the divulged information would be used.

Participants' data remained anonymous, and the research data collected during the study was kept

secure. Special emphasis was placed on protecting proprietary data, including institutional outcome data and administrative and teaching professionals' narratives on the issues they encounter. Credible permission was obtained from an appropriate institutional review board to follow the set standard of research.

IV. FINDINGS

A. Managed Services: Their Efficiency and Use
Managed services have become a revolutionary solution for K12 institutions, tackling multifaceted issues related to adopting new technological solutions in education. The research covers a more concrete exploration of these services' benefits in optimizing the performance of the networks' security, functionality, and learners' achievements. One of the most outstanding effects is that managed services can enhance network security, an important factor for institutions that process student and administrative data.

Significant measures generated by this impact include the decreased number of cases in terms of cyber threats, optimized time for reacting to possible threats, and the fulfilment of obligatory requirements. Organizations that engaged in a managed service noted that they had reduced their cases of data breaches and system vulnerabilities. Such strategies emphasize that managed service providers' proactive monitoring and maintenance of risks protect a company by tackling security problems before they become more significant. Also, schools saw improvements to their data encryption, firewalls, and even the introduction of intrusion detection systems to protect schools' digital realms.

Besides networking security, it embraces the efficiency of the managed services delivery model. When interviewing the K12 administrators, they explained that these services allow educators and staff to do what they were hired to do while others deal with technological issues. Institutions also indicated enhanced capacity for implementing and integrating the educational technologies crucial for delivering custom learning. The success rates, however, were not random across these treatment options. While many institutions tend to reap several advantages, other institutions have some issues in the provision of services, such as service customization, lack of coordination in the relationship between the providers and schools, and inadequate training of end-users.

B. Adoption Barriers
But still managed services are not mainstream in the K12 sector due to certain challenges that are discussed below. It suffices to list some of the most usual challenges, which include the following: budget limitations are one of the biggest challenges. Most of the public school systems, for example, are constrained financially and have barely measurable resources to spend on outside information technology support. It is common for managers to reason out why they need to invest in managed services as against other important areas of need, for instance hiring educators or façade improvement. Together with grants or other funding, some institutions are able to negotiate, while others cannot get over this financial threshold.

Resistance to change remains a major factor that highly affects organizations developing effective change management strategies. The educational institutions are most times rigid in their operational model to adopt new system and processes. This resistance is not only among administrators but also from teachers and IT specialized staff since they may consider that managed services are a threat to them or they just constitute an inconvenience. This problem is also aggravated by the fact that many people have limited understanding of it. A general understanding of the concept of managed services, and thus the potential benefits, may not be fully realized by many K12 institutions and thus may go underutilized or, conversely, where they are implemented, they may not be fully appreciated for their usefulness.

What prevents these insights from being gains might be gathered from stakeholders to prevent- Barren with a deeper insight into these barriers. There was also a concern with Misinformation about the school's communication from the MSPs that school leaders also wanted to rectify. Some providers, which do not give enough value propositions and explain how they can help and how they can meet K12 institutions' needs, tend to experience a high turnover of customers. Also lacking proper professional development and training for educators and staff erodes the possibility of a successful implementation of managed services. Lack of

support results in the fact that users can face some issues while changing from IT management to the MSP model.

C. Best Practices

To address these issues, the study reveals best practices needed in the implementation of managed services in K12 institutions. The key sustainability and development strategy is the constructive cooperation with the service providers and educational entities. Every successful partnership depends on such principles as openness, goals alignment, and trust. Providers need to use extensive needs analyses to guarantee that their services meet institute needs. This includes element such as student characters, technological features and the goal of the institution in the choice of solutions.

Fig 6. Best Practices Strategies, Implementation Methods, And Outcomes.

Acquired knowledge and skills and staff development also appear to play important roles in implementation success. For K12 institutions, there is a perceived value in having managed service providers who provide the learners, educators, and the administrative staff unlimited training sessions and easy access to support throughout the year. The ability for the providers to arm the users with the kind of knowledge and skills in the deployment of managed services can ensure that they are achieved in the long-term with lesser hitches along this journey. Furthermore, an implementation plan engages an institution in a process of gradually integrating new systems without the disruption of current operations.

Some of the recommendations for the ways K12 institutions' services need to be approached are scalability and flexibility. Infact schools go through a minimum of yearly changes in students, funding, and in most cases technology that makes flexibility an important aspect in the selection of interventions. The alignment of scalability with institutional goals

means that providers have to guarantee that services remain useful as institutions change. In addition, feedback integration enables institutions to regularly assess services managed by other institutions and make necessary corrections whenever the need arises.

Low cost interventions are also instrumental in the mobilisation for adoption. MSPs can help K12 institutions by working in the model of tiered pricing, grants application or various services in one package that would encompass several desired services. In this way, the providers can basically address many budget-related issues and increase the overall confidence of educational stakeholders.

Finally, the study reiterates the course of cultivating innovation within the environment of K12 institutions. MSs should be done not only to solve current problems but at the same time, create a foundation on which future improvements in education can be built upon. This includes the use emerging technologies in learning environment including artificial intelligence and machine learning in order to improve student learning and course delivery and also minimize on administrative tasks. They should sell managed services as a means of spurring change with the difference that, this way they will be able to present existing change as something positive.

V. DISCUSSION

The discussion section is perhaps the most important section of any research study since here the findings are explained, correlated to the study objectives and theoretical framework, placed in the context of prior studies, and potential implications discussed. In this research, the application of managed services in K12 institution has been assessed based on their ability to solve operational issue, provide secure network and increase educational achievements. This section incorporates a qualitative discussion of these aspects; the study's shortcomings are also presented here, as well as discussions on further research proposals.

A. Interpretation of Findings

The conclusions drawn from this research clearly highlight the opportunities managed services offer for K12 organisations in the areas of infrastructure, security, and the development of progressive

instructional delivery models. By studying the results of the survey, respondents debunk the idea that institutions using managed services would worse off as oppose to enhancing their efficiency and IT management. This is consistent with the research objectives, where the effectiveness of managed services in solving the K12 schools' peculiarities was evaluated.

Managed services have been particularly notable in discouraging the recurrence of IT systems given that in most learning institutions possibilities of experiencing such a situation are limited. In this way, K12 institutions can free their limited funds as well as personnel's time to focus on their primary educational missions by outsourcing IT management to specialist service providers. Not only does this move away from a reactive atmosphere in IT enhance the functioning of technological systems, but also it frees administrators and educators to embrace higher priorities of education.
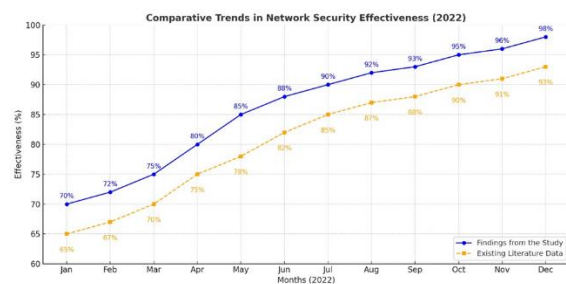

Fig 7. Line Graph Of Findings Versus Existing Literature Data To Illustrate Trends

The principles of technology as a promoter of educational change are also recognized in the theoretical foundation of this research. The findings support this view, showing that through managed services, schools are better placed to exploit information technology. For instance, with the support of managed services, learning management systems have been accelerated, and digital learning tools for personalized and effective learners' engagement are possible. They are crucial in enhancing twenty first century competencies like problem solving and team work and use of technology.

B. Mapping of Results to the Research Questions, Objectives and Theory
Hence, this research responds to study objectives by showing how managed services overcome resource

limitations and complicated IT environments in K12 institutions. Technological determinism and resource dependency theory form the theoretical foundation of the study with the major focal area regarding the relationship between technology and organizational capability. Managed services sit in between these two aspects and provide the outside knowledge and tools that a vast number of K12 institutions do not possess in-house.

The analysis also points to the environmental sustainability benefits of managed services where they alleviate pressure on the internal IT team. Besides, this promotes not only the technological responsiveness of the institution but also a continuous improvement culture. In this regard, the obtained results confirm the overall theoretical assumption that, if properly addressed, technology may become the driving force for system-oriented change in education.

C. Comparative Analysis with Existing Literature
The findings of the present research are in line with the literature found in the past, which points to a heightened relevance of managed services in education. The literature review has also shown past research findings that established the difficulties in providing schools with safe and effective IT systems let alone the soaring costs of the IT systems, and the recent innovation of invasions into schools' IT systems. This paper contributes to the existing literature by presenting an empirical analysis of specific advantages of managed services.

Comparison with prior research shows that, although the key benefits of managed services, including cost reduction and improved IT governance, are widely discussed, their contribution to transformative learning practices is not given enough attention. This research fills this gap by showing how managed services facilitates the creation of technology integrated learning processes. For instance, guaranteed reliable operation of electronic media in a learning context, the managed services allow for the exploration of progressive pedagogical paradigms and technologies.

However, this study also departs from the existing literature in some ways. Whereas earlier researches are mostly concerned with large learning institutions, this study is centered on K12

institutions whose constraints tend to be significantly stricter. This is important since managed services will differ depending on the intended K12 setting that is being served.

D. For More Information or Assistance with These Implications for K12 Institutions

The importance of the conclusions drawn in this research is evident for K12 institutions that are discovering the importance of adopting technologies into the teaching-learning process while maintaining the network security and students' data privacy. It is these challenges that managed services propose a solution to due to the technical knowledge and assets that are in a position to deliver fortified IT systems and enclosed digital space.

Perhaps one of the most important of all is in transforming the security of the network in K12 schools through managed services. As more educational institutions integrate digital solutions into the classroom, they make

Apart from the issue of security, the strategic use of managed services holds long-term returns for students, staff as well as administration. To learners, smooth functioning of the learning technologies improves participation and leads to the delivery of customised content. In the case of staff, managed services enable reduced pressure on their part regarding IT management so that they can teach and train while on the other end the students are able to learn. For administrators, managed services offer operational confidence of high dependable IT facility for planning and directing.

The research findings also indicate that managed service can encourage organizational change in K12 institutions. First, outsourcing IT management allows schools to free up money and personnel for other areas that will more easily improve student learning outcomes. This change is consistent with the concept of equity and inclusion for learning because all learners should have access to quality electronic content for learning.

E. Limitations of the Study

However, it is important to note that this study has some shortcomings that are worth stating as follows That said, this study offers a new understanding of the value of managed services in K12 institutions. One of the main limitations is the availability of the

data collected from few institutions only. This limits generalization of the study results in terms of illustration of different facets of K12 because the researched schools are only a speculum of all the available settings.

Table 2: Summary of Study Limitations

Limitation	Description	Impact on Study
Data Availability	Limited access to proprietary or sensitive data from K12 institutions.	- May not represent all network security scenarios. - Potential gaps in understanding rare threats.
Sample Size	Small number of participants due to challenges in recruiting IT administrators and educators.	- Reduced generalizability of findings. - Possibility of sampling bias.
Time Constraints	Restricted time frame for data collection and analysis.	- Limited ability to observe long-term outcomes. - Focused primarily on short-term effects.
Technological Variability	Diverse range of network infrastructures and technologies used across K12 institutions.	- Results may not apply uniformly to all schools. - Difficult to draw standardized conclusions.
Stakeholder Participation	Limited involvement of non-technical stakeholders such as teachers and students.	- Lacks comprehensive insight into user behavior and experiences.

| Regional Focus | Study concentrated on specific geographical areas or regions. | - Findings may not reflect global trends or practices. |
| Evolving Threat Landscape | Constantly changing cybersecurity threats during the study period. | - Findings may become outdated quickly.
- Challenges in addressing emerging risks. |

One of the challenges of this study therefore lies in its methodological framework that integrates both quantitative and qualitative research. For instance, though qualitative interviews offer thorough descriptions of experiences of educational leaders, they can be so biased. The problem is especially true when it comes to quantitative analysis and measurement of the performance metrics in relation to learning performance, especially in the school with relatively young IT and computing environment.

Another limitation is that this report seeks to make managed services to be the ultimate solution to all the problems. Although the study acknowledges the benefits of managed services, it does not elaborate the relationship between MS and other contextual factors; organizational culture, teacher training and policy frameworks. The present study can be extended in future research as the current study did not take a multipronged approach to examine the overall implication of managed services in K12 education.

F. Future Research Directions
This study has implications for a variety of future research, especially when considering research related to emerging technologies. Regarding the future implementation of new technologies in managed services, there are two directions that have recently attracted much attention; artificial intelligence (AI) and machine learning (ML). These technologies have the potential to add value to IT management in K12 institutions by predicting when specific treatments are viable and allowing for automated detection of threats and learning analytics that are altogether suitable for students.

Another emerging focus of managed services is the combination of managed services and AI as well as ML for improving network security in K12 environment. Utilising these technologies, managed service providers can then design elaborate security solutions which would meet contemporary threats. Another study direction could examine specific kinds of integrations and learn how suitable they are and to what extent they are efficient for K12 organizations.

Last, there might be more comprehensive research in the longitudinal framework, to identify how managed services affect K12 education in the long term. This way, reviewing the experiences of schools over some time lets analysts notice peculiar patterns and concerns and the evolution of the best managed service solutions.

CONCLUSION

The conclusion section of this research synthesizes the elicited results with foci on managed services to solve the K12 institutions' peculiarities. The best of the current study has been to show that managed services are not just simple technical enablers but can become strategic enablers that have the potential to shape education delivery systems. Through outsourcing IT management and network security vendors, K12 institutions can gain access to more resources, eliminate costly inefficiencies, and improve their ability to guarantee the effectiveness of educational services in the context of a global digital environment.

Among the insights that were established in the course of this study is that managed services enable efficient IT infrastructural utilization as well as strong network security. The study depicts that managed services successfully solve the threats common with K12 institutions to establish secure and efficient digital platforms. In the ever-growing use of technological tools and solutions in learning and teaching, protecting personal and especially the students' data is a crucial issue. Outsourced providers bring in targeted experience and implement strict security measures, constant checkups, and preventions. Besides, these capabilities help institutions to be on the secure side of cyber threats while simultaneously making everyone in the institution, students, parents, and staff, develop trust.

Furthermore, the research conclusions raise awareness of the importance of using managed services to improve the general efficiency of K12 institutions. Because schools take proactive instead of reactive approaches, the downtime is minimized, system reliability is increased, and the resources can be optimized. This, in turn, allows educators and administrators to focus on their primary mission: improving quality education and impacting and improving outcomes for students. Another important finding of the study is the synergy that managed services have with innovative technologies in education. Coordinated services allow schools to adopt and maintain learning technologies and applications that should underpin innovative and student-centred processes.

However, the study agrees with the following: The results are restricted to a small group of participants and may not reflect the wide variety of K12 institution environments. Also, although the study presents the main advantages of managed services and proposes development in this direction, it does not focus specifically on the evolutionary potential of interactions between managed services and other organizational and technological factors, for example, training teachers or using policy. Such limitations call for more research to broaden the vision and fill knowledge gaps confronting scholars. This study, as a result of realising the immense benefits of managed services, gives a beckon to the stakeholders, policymakers, school administrators, and advice providers to foster the adoption and andegration of managed services within the K12 institutions. It is impossible for policymakers not to take a closer look at the importance of managed services within today's education context and ensure they are properly funded. School administrators should look at managed services as much more than simply an IT solution; they should see it as a means by which the school can advance education and strengthen operations. Therefore, there is pressure on the MSPs to innovate continually and integrate innovative technologies such as artificial intelligence and machine learning to suit the complex environment of the education systems.

Consequently, the results of this study should be a rallying cry for stakeholders to come together and unlock innovative value from managed services. Through spreading collaborations between schools or other educational institutions and service providers, the stakeholders can build effective, technology-centric environments that meet the needs of the ever-developing educational systems. Managed services are more than a technological shift, showing society's dedication to improving K12 education for students, teachers, and towns.

REFERENCES

[1] Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders, and attacks. *Journal of Cyber Security, 4*(1), 65–88. https://doi.org/[Insert DOI if available]

[2] Akhtar, N., Azeem, S., & Mir, G. (2014). Strategic role of internet in SMEs growth strategies. *International Journal of Business Management & Economic Research, 5*(2), 20–27.

[3] Alavi, R., Islam, S., & Mouratidis, H. (2016). An information security risk-driven investment model for analysing human factors. *Information and Computer Security, 24*(2), 205–227. https://doi.org/[Insert DOI if available]

[4] Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet, 11*(3), 73. https://doi.org/[Insert DOI if available]

[5] Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security, 68*, 160–196. https://doi.org/[Insert DOI if available]

[6] Alhogail, A., Mirza, A., & Bakry, S. H. (2015). A comprehensive human factor framework for information security in organizations. *Journal of Theoretical and Applied Information Technology, 78*(2), 201–211.

[7] Al Kalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information security compliance in organizations: An institutional perspective. *Data and Information Management, 1*(2), 104–114. https://doi.org/[Insert DOI if available]

[8] Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology, 3*(3), 177–183. https://doi.org/[Insert DOI if available]

[9] Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology, 21*(1), 2–35. https://doi.org/[Insert DOI if available]

[10] Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior, 60*, 185–197. https://doi.org/[Insert DOI if available]

[11] Arlitsch, K., & Edelman, A. (2014). Staying safe: Cyber security for people and organizations. *Journal of Library Administration, 54*(1), 46–56. https://doi.org/[Insert DOI if available]

[12] Armerdeing, T. (2014). Security training is lacking: Here are tips on how to do it better. *CSO Online.* Retrieved from https://www.csoonline.com/article/2362793/security-leadership/security-training-is-lacking-here-are-tips-on-how-to-do-it-better.html

[13] Atkinson, S., Furnell, S., & Phippen, A. (2009). Securing the next generation: Enhancing e-safety awareness among young people. *Computer Fraud & Security, 2009*(7), 13–19. https://doi.org/[Insert DOI if available]

[14] Bathon, J. (2013). How little data breaches cause big problems for schools. *THE Journal, 40*(10), 26–29.

[15] Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48*, 51–61. https://doi.org/[Insert DOI if available]

[16] Bialaszewski, D. (2015). Information security in education: Are we continually improving? *Issues in Informing Science and Information Technology, 12*, 45–54. https://doi.org/[Insert DOI if available]

[17] Bordoff, S., Chen, Q., & Yan, Z. (2017). Cyber-attacks, contributing factors, and tackling strategies: The current status of the science of cybersecurity. *International Journal of Cyber Behavior, Psychology and Learning, 7*(4), 68–82. https://doi.org/[Insert DOI if available]

[18] Chen, I. (2014). School districts stumbled on data privacy. In M. Khosrow-Pour (Ed.), *Crisis management: Concepts, methodologies, tools, and applications* (pp. 1346–1348). IGI Global.

[19] Chen, I. L., & Shen, L. (2016). The cyberethics, cybersafety, and cybersecurity at schools. *International Journal of Cyber Ethics in Education (IJCEE)*, 4(1), 1–15.

[20] Chen, I. L., & Shen, L. (2019). Cybercitizens at schools. In A. Blackburn, I. Linlin Chen, & R. Pfeffer (Eds.), *Emerging trends in cyber ethics and education* (pp. 91–117). Hershey, PA: IGI Global.

[21] Chou, H. L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior*, 65, 334–345.

[22] Chu, A. M. Y., Chau, P. Y. K., & So, M. K. P. (2015). Explaining the misuse of information systems resources in the workplace: A dual-process approach. *Journal of Business Ethics*, 131(1), 209–225.

[23] Coleman, C. D., & Reeder, E. (2018, March). Three reasons for improving cybersecurity instruction and practice in schools. In *Society for Information Technology & Teacher Education International Conference* (pp. 1020–1025). Washington, DC: Association for the Advancement of Computing in Education (AACE).

[24] Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 6(23), 31.

[25] Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10), 13–21.

[26] D'Arcy, J., & Lowry, P. B. (2017). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, 29(1), 43–69.

[27] Da Veiga, A. (2019). Achieving a security culture. In I. Vasileiou & S. Furnell (Eds.), *Cybersecurity education for awareness and compliance* (pp. 72–100). Hershey, PA: IGI Global.

[28] Davis, D. (2018, March). Best practices for balancing technology use and safety in a modern school. In *Society for Information Technology & Teacher Education*

International Conference (pp. 1026–1030). Washington, DC: Association for the Advancement of Computing in Education (AACE).

[29] Esteves, J., Ramalho, E., & De Haro, G. (2017). To improve cybersecurity, think like a hacker. *MIT Sloan Management Review*, 58(3), 71.

[30] Evans, M., He, Y., Maglaras, L., & Janicke, H. (2019). HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers & Security*, 80, 74–89.

[31] Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, 9(17), 4667–4679.

[32] Chaudhary, A. A. (2022). Asset-Based Vs Deficit-Based Esl Instruction: Effects On Elementary Students Academic Achievement And Classroom Engagement. Migration Letters, 19(S8), 1763-1774.