The Impact of Social Media Hacking Incidents on School Reputation: An In-Depth Investigation of Crisis Response Strategies

Hilbert R. Grande [1], Norberto O. Pore[2], John Mart Elesio[3]

[1,2]DepEd, Davao Occidental, Philippines

[3] Holy Cross of Davao Colleges, Davao City, Philippines

DOI: https://doi.org/10.51584/IJRIAS.2025.1001010

Received: 26 December 2024; Accepted: 03 January 2025; Published: 01 February 2025

ABSTRACT

This qualitative study uses the Situational Crisis Communication Theory framework. The framework focuses on strategic crisis responses. These responses consider the extent of crisis responsibility and the potential risk to one's reputation. The study examines how the school head lessened the impact of social media hacking incidents. An in-depth interview was conducted with ten school heads from the Division of Davao Occidental. These school heads were chosen using a purposive sample approach. The study reveals three major themes in the complex challenges educational institutions face in managing social media hacking incidents: organizational cybersecurity unpreparedness, resources-constrained digital resilience and reputational risk management in the digital age. School heads employed various coping mechanisms, including crisis communication resilience, digital security empowerment and stakeholder trust restoration. Finally, the key insights gained emphasized the importance of proactive digital resilience, transparent institutional accountability and collaborative community protection. The study provides a crucial roadmap for understanding, managing, and preventing digital security incidents in educational settings, emphasizing the importance of prevention, education, and collaborative action in maintaining institutional reputation and ensuring digital safety. We recommend that educational institutions must develop a comprehensive approach to digital security that encompasses technical preparedness, proactive prevention, and strategic communication.

Key Words: Social media, Hacking incident, school reputation, crisis responses, strategies.

INTRODUCTION

Educational institutions increasingly leverage social media platforms to engage with stakeholders, promote achievements, and maintain community connections (Chen & DiVall, 2018). They can be used to share important announcements, showcase student achievements, and foster a sense of community. However, the potential for reputational damage due to hacking presents a significant challenge for schools using social media platforms like Facebook for communication. Additionally, a hacked Facebook page can lead to data breaches, compromising sensitive information and eroding trust among parents, students, and staff. Moreover, hackers may spread misinformation or post harmful content, further damaging the school reputation.

Consequently, the initial adoption of Facebook by educational institutions presented unique security challenges. Rodriguez and Chen (2019) documented how schools struggled with basic security protocols during this period, with 78% of institutions lacking formal social media security policies. Early studies by Thompson et al. (2018) revealed that 65% of educational institutions relied on shared passwords and basic authentication methods, making them particularly vulnerable to security breaches. Additionally, Studies by Martinez et al., (2021) found that educational institutions faced a 156% increase in targeted Facebook attacks between 2019 and 2021, with 42% resulting in successful compromises.

Moreover, according to the most current 2024 Cyber Crime Statistics, the number of cyberattacks increased by 125% globally in 2021 compared to 2020, and in 2022, the increasing number of cyberattacks continued to put people and companies at risk. In addition, there have been significant cyberattacks on 14 schools in the UK, which have led to the theft of very private information and papers. According to a report by inquirer.net, the continuous rise of Facebook hacking incidents in the Philippines over the past three years has reached alarming levels. In the Division of Davao Occidental, the Facebook page was hacked, and harmful content, including offensive words and nude pictures and videos, was posted. Numerous school Facebook pages of the said division have also been hacked. While some schools have managed to recover their pages, others have not.

Further, existing research focuses on the technical aspects of cybersecurity, neglecting the broader societal and reputational implications of hacking incidents. Triplett (2024) addresses cybersecurity challenges in education in his study. His research focuses on tactics that educational institutions might use to improve students' cybersecurity knowledge. Although social media hacking can harm a school's reputation, we lack solid research on the extent and nature of this damage. We need to understand how hacking incidents affect different groups, including students, parents, and teachers. This study will help us understand how hacking incidents impact safety perceptions, long-term reputation, and how different stakeholders respond. Ultimately, this knowledge will be crucial for developing strategies to protect schools and mitigate the damage caused by these incidents, informing school leaders, policy makers, and social media companies.

Research Objectives:

This research sought to ascertain how incidents of social media hacking affected the reputation of schools. This research was directed by the following specific objective.

1. What are the challenges faced by school heads in mitigating the impact of social media hacking incidents on school reputation?

2. What coping mechanisms do school heads utilize to mitigate the negative impact on school reputation following social media hacking incidents, and how effective are these strategies in restoring public trust?

3. What are the learning insights of the school heads in social media hacking incidents on school reputation?

Purpose of the study

This research investigates the complex challenges schools face in the digital age, focusing on the impact of social media hacking incidents on school reputation and the necessity of proactive crisis management. Its findings offer insightful information to diverse stakeholders, each with unique needs and responsibilities in addressing the challenges of cybersecurity in schools. The study provides the Department of Education with data-driven insights to guide the creation of efficient policies, and the wise distribution of funds intended to enhance cybersecurity infrastructure and crisis response instruction in educational establishments. The results can be used by school administrators to improve their incident response procedures, put preventative measures in place against hacking efforts, and create all-encompassing plans for lessening the effects of future breaches. Teachers will benefit from the increased awareness of cybersecurity risks highlighted in the study, enabling them to better educate students and contribute to a safer online learning environment. Parents and students will gain a deeper understanding of the potential risks associated with social media hacking, empowering them to take proactive steps to protect their personal information and online safety. Finally, external stakeholders, including members of the community and possible partners, will have more faith in the school's capacity to protect private data and uphold a safe online environment.

Theoretical Lens

The theory of Situational Crisis Communication (SCCT) developed by W. Timothy Coombs in 2007 (Argenti, 2016). In the realm of crisis communication, it is a hypothesis. It implies that crisis managers should plan strategic responses to crises based on the degree of responsibility involved and the harm to their reputation. Coombs developed his scientifically based SCCT to provide communicators with scientific facts to inform their choices. In essence, Coombs said that an organization's post-crisis activities are contingent upon the severity of the disaster.

Further, an effective framework for directing school reactions to social media hacking situations is offered by the Situational Crisis Communication Theory (SCCT). Through a thorough evaluation of the crisis type and the school's level of accountability, administrators may choose the best communication tactics to minimize harm to the school's brand and rebuild confidence. According to SCCT, an organization's reputation—that is, how its audiences view it—is an asset that is susceptible to crises. The greatest way to protect the reputational resource may be through strategic communication after assessing the problem and selecting a crisis response plan that suits it (Argenti , 2016). According to Liu (2022) research, instructive information—that is, what the public should know and do to protect themselves from the crisis—must be given before addressing reputational issues.

Research Design

This study's research approach was based on a single case study. With data collected from several variables, a single case study technique entails a comprehensive examination of a group, individual, or event to provide a generalizable insight (Conde, 2021). A qualitative research design that entails a comprehensive, in-depth analysis of one or more instances in their natural setting. A case study is a type of research approach that involves a detailed examination of a subject (the "case") within a real-world context. Case studies provide insights into the subtleties of the phenomena under study by examining the sources of underlying principles, actions, or results. Researchers can use this method to capture a wide range of variables and interactions that would not be visible using other techniques, such as surveys or tests.

According to Mason (2012), qualitative research should be strategically carried out in a flexible and contextual manner. This means that decisions should be made based not only on a sound research strategy but also on the constantly shifting circumstances or context in which the research is being conducted. An alternative method for researching people is qualitative research. Individual experience exploration, phenomena description, and theory development are the main focuses of qualitative research (Vishnevsky and Barlands, 2004).

Researchers may use qualitative case study design to examine complicated phenomena in their surroundings. It allows the researchers to know the impact of social media hacking incidents on school reputation. The study illuminates the challenges and coping mechanisms involved. It offers valuable insights to help schools mitigate negative effects and rebuild community trust. In this study, it is the most appropriate design to address the purpose of the study.

Participants and Sampling

The participants of the study are the 10-school heads of the Division of Davao Occidental. They will be selected through purposive sampling technique with ten participants to participate in the in-depth-interview (IDI). Creswell (2013) suggests that a reasonable sample size may range from 5-25 participants for a study, and 10 participants are an adequate number for this study. Purposive sampling is a sampling technique whose objective is to produce a sample which the researchers logically assumed to be representatives of a given population. This implies that the researchers will choose a sample that will help them gain access to the subset of a particular group of people. The selection will be based on given criteria relevant to the study's objectives.

Data Gathering

This case study research used a methodical approach to data collection to guarantee the validity, correctness, and rigor of the information gathered. Prior to conducting the research, permission from the graduate school dean was obtained to build credibility and confidence, as recommended by L. Van Grootel and Haven (2019). In accordance with Cresswell J.W.'s recommendations and the ethics of qualitative research, informed consents were also given to each participant. and J.D. Cresswell. (2017). For this research, five school heads from public schools were selected as key informants. Participants meet the requirements that a study should only include eligible people who can make a substantial contribution to the accomplishment of its goals and that the sample size should be minimal (Schoch, 2020). With the participants' permission, an extensive interview was captured on audio and the transcript was then examined in line with the research idea that every step of the data-gathering process must be documented (Rutakumwa et al., 2019). According to Candela (2019) the validity and reliability of the study were confirmed by obtaining a member-checking certificate to make sure the participants approved of the findings and to make sure the data wasn't misinterpreted during analysis.

RESULT & DISCUSSIONS

Challenges Faced by School Heads on Social Media Hacking Incidents.

This section presents key findings regarding the mitigation strategies employed by school heads to lessen the impact of social media hacking incidents on school reputations.

Three (3) main themes emerged from in-depth interviews (IDIs) with participants. These themes, shown in Figure 1, concern the difficulties school heads face in lessening the negative effects of social media hacking incidents on school reputation. These themes are organizational cybersecurity unpreparedness, resource-constrained digital resilience, and reputation risk management in the digital age. Moreover, nine (9) core values have been identified: lack of technical expertise, insufficient incident response skills, limited cybersecurity training, financial limitations, technological infrastructure gaps, external support dependency, stakeholder trust erosion, Misinformation Management and Rapid Information Spread.

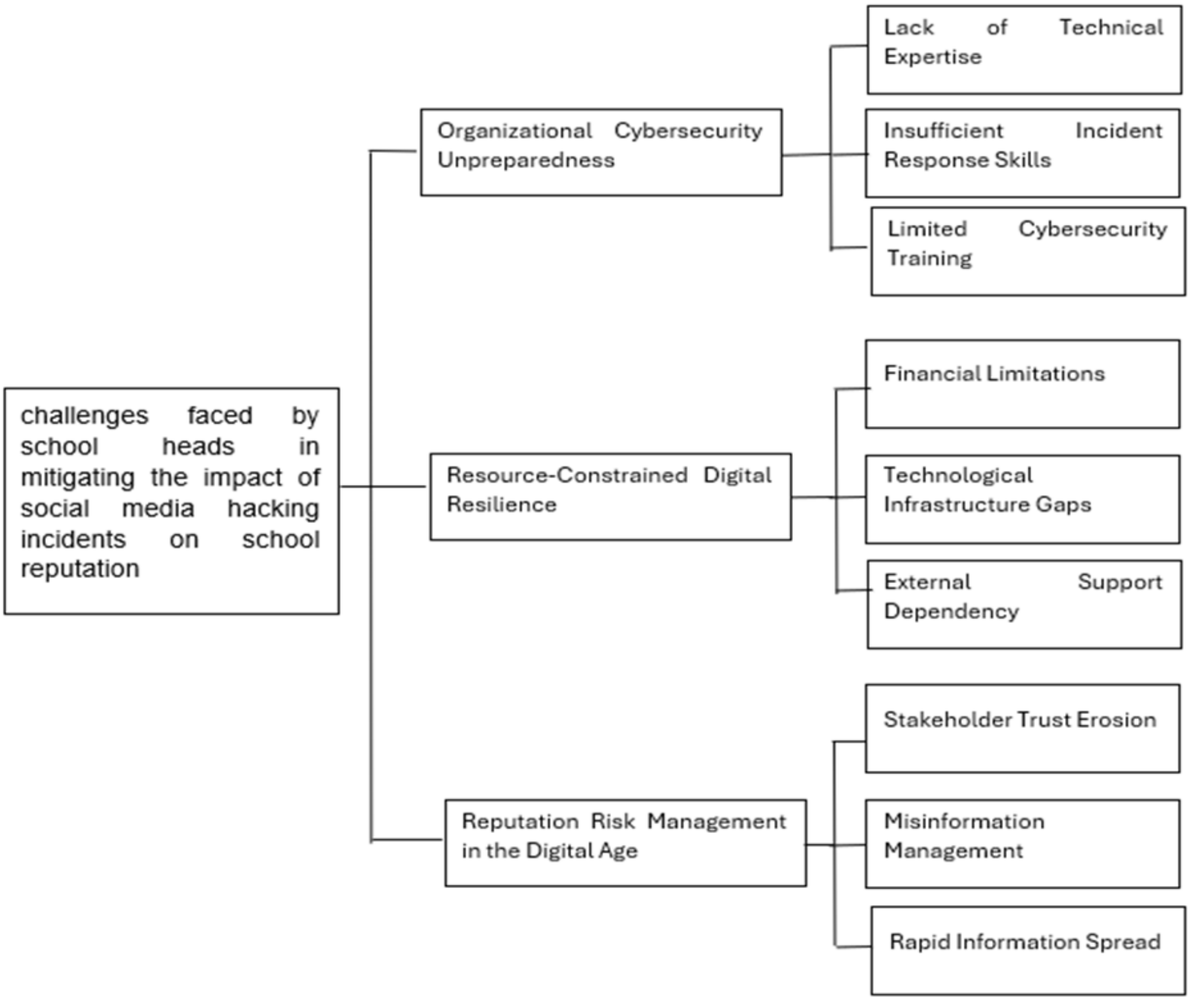
challenges faced by school heads in mitigating the impact of social media hacking incidents on school reputation
Organizational Cybersecurity Unpreparedness
Lack of Technical Expertise
Insufficient Incident Response Skills
Limited Cybersecurity Training
Resource-Constrained Digital Resilience
Financial Limitations
Technological Infrastructure Gaps
External Support Dependency
Reputation Risk Management in the Digital Age
Stakeholder Trust Erosion
Misinformation Management
Rapid Information Spread

Figure 1. Challenges Faced by School Heads on Social Media Hacking Incidents.

Contemporary educational institutions demonstrate significant cybersecurity knowledge deficits, characterized by limited technical expertise, inadequate incident response capabilities and limited cybersecurity training. These findings support Chen et al.'s (2019) assertion that educational institutions usually lack systematic methods for managing digital security. The research substantiates previous observations that institutional preparedness remains substantially below contemporary cybersecurity requirements, creating substantial organizational vulnerabilities.

Lack of Technical Expertise. The contemporary cybersecurity landscape is characterized by a profound skills gap that compromises organizational security infrastructure. Research by Haber & Carmeli (2023) indicates that approximately 63% of organizations struggle with maintaining adequate levels of technical cybersecurity expertise.

Participants readily admitted to their experiences with endurance, stating,

IDI#3. "School is not equipped to handle such situations".

IDI #1. "I am not adequately prepared to handle social media hacking incidents".

IDI #4. "Limited or no IT expert in school".

The findings reveal significant gaps in both individual preparedness and institutional resources. Participants readily admitted to limitations in their ability to effectively manage such situations. A recurring theme highlighted the lack of adequate training and resources within the educational setting. The result agrees with the studies that highlight the necessity of thorough cybersecurity instruction in classrooms (Rahman, 2020). Additionally, Himes-Cornell et. al (2018) also emphasized in their study that the lack of individual preparedness may be exacerbated by the absence of institutional support and resources, creating a vicious cycle of vulnerability.

Insufficient Incident Response Skills. The emerging theme for the subtheme insufficient incident response skills reveals a significant deficiency in incident response skills within schools. School personnel lack a structured approach to handling hacking incidents, and there's an absence of protocols for addressing and mitigating digital security breachers. Instead of a predetermined response strategy, most schools rely on improvisation, exacerbating the potential damage from compromised accounts due to the inability to quickly recover or secure them.

The participants openly acknowledge the difficulties they faced regarding incidents.

"I have no idea how to fix this" IDI#7.

"They are not prepared for these types of incidents" IDI#3.

"We don't have cybersecurity expert to recover the hacking incident" IDI#5.

Several participants expressed a lack of knowledge regarding incident response procedure. The statement of Participant IDI #2 highlights the critical need for improved training and education in cybersecurity practices. This lack of knowledge extends beyond basic troubleshooting, suggesting a broader gap in understanding incident response methodologies. These results concur with the findings of Carr (2020), in his research highlighting the importance of proactive planning, training, and investment in skilled personnel.

Limited Cybersecurity Training. A critical gap in addressing cybersecurity challenges within educational institutions is the limited availability of comprehensive cybersecurity training. Schools rarely invest in such program, and professional development in digital security is often treated as a low priority. This inadequate training directly impacts the ability of schools to effectively prevent, detect, and respond to cybersecurity incidents, highlighting a critical need for increased investment in robust and comprehensive cybersecurity education and training programs.

The informants acknowledged their responsibility for the teachers' inability to attend the cybersecurity training program.

IDI #1: "I asked for help from the ICT coordinator, but they have limited cybersecurity skills"

IDI #3: "Addressing such incidents requires a series of training sessions and workshops"

IDI #8: "Insufficient fund to conduct training or professional development activities about cybersecurity"

The participants' responses reveal systematic challenges that hinder teachers' access to and participation in essential cybersecurity training. The limited expertise among ICT coordinators underscores the need for professional development opportunities for these individuals. Increased funding for cybersecurity training is essential, potentially through government grants or partnership with private sector organizations.

Resource-Constrained Digital Resilience

Resources-Constrained Digital Resilience emerged to be the second theme under the challenges faced by school heads in mitigating the impact of social media hacking incidents on school reputation. The core ideas under this theme were: Financial Limitations, technological infrastructure gaps, and external support dependency. Resource-Constrained Digital Resilience focuses on the resource constraints that hinder school's ability to effectively mitigate the risks associated with digital threats. According to Bada & Nurse (2020) that social media hacking incidents can severely damage a school's reputation, impacting student enrollment, funding, and overall institutional.

Financial limitations. Financial limitations pose a significant obstacle to effective cybersecurity in schools. Many schools operate with severely limited budgets for technology, making it difficult to update hardware and software, which is often prohibitively expensive. The lack of funding also prevents many institutions from hiring dedicated IT security personnel. This overall shortage of financial resources directly impacts a school's ability to protect its digital assets.

IDI #4: "Having no budget to update outdated hardware and software"

IDI #9: "No budget to hire IT security personnel"

IDI #5: "Limited budgets and staffing pose significant challenges"

These limitations, as reflected in the statements of the participants, resonate with existing literature on the cybersecurity landscape. Organizations facing budgetary constraints often struggle to implement effective security measures, leaving them vulnerable to cyberattacks. The scarcity of resources also impacts the ability to implement robust incident responses plans. Organizations may not be able to successfully limit and recover from cyberattacks without sufficient finance and staff, which might result in significant financial losses and protracted interruptions (Triplett, 2024).

Additionally, it was shown that healthcare institutions have several difficulties when it comes to successfully managing cybersecurity risks. These difficulties are brought on by a lack of cybersecurity knowledge, insufficient security measures, few resources, and the complexity of healthcare systems itself. These results highlight how important it is that healthcare businesses acknowledge cybersecurity as a core component of their operations and give it top priority. This suggests that due to a lack of professionals with essential cybersecurity capabilities, only a small number of healthcare institutions are now able to address these issues. Furthermore, Angafor et al (2020) examined the rigorous standards for preparing recent graduates with the skills and credentials required for healthcare cybersecurity.

Technological Infrastructure Gaps. Schools' technological infrastructure is severely underdeveloped, characterized by outdated and cyber-vulnerable to cyber systems. This weakness is compounded by a lack of basic account protection and recovery skills among both staff and the students. Monitoring capabilities are minimal or nonexistent, and the absence of robust infrastructure creates numerous entry points for potential hackers.

Research participants expressed their opinions and feelings regarding the issue of social hacking incidents in their school.

IDI #3: "Students and even teaching staff often do not know how to retrieve their accounts".

IDI# 4: "Difficulty in monitoring online activities and detecting potential hacking attempts".

IDI #1: "This allows hackers to exploit compromised accounts for an extended period".

The findings reveal a significant lack of user knowledge and preparedness regarding online security. Current security measures and awareness are insufficient, leading to a chain reaction of poor account management and inadequate monitoring. This is consistent with the Smith et al. (2020) study, which shows that ineffective password management techniques and a lack of knowledge about security procedures greatly increase the likelihood of successful hacking efforts.

External Support Dependency. External Support Dependency emerges as a core idea from the main theme of resource-constrained resilience. The reliance on external support for cybersecurity is a central concept within the broader theme of resource-constrained digital resilience. This dependency highlights the challenges faced by organizations lacking the internal resources and expertise to effectively manage their own digital security.

"*We need to ask help from our Division ICT about this hacking incident"- IDI #2.*

"School typically do not invest in" cybersecurity resources" "- IDI #3

"Lack of resources for cybersecurity measures" - "- IDI #6

The data reveals the reliance on internal IT support, insufficient investment in cybersecurity, and a lack of resources for implementing effective security measures. The reactive approach exemplified by reliance on internal IT support is unsustainable in the face of increasingly sophisticated cyber threats. According to research by Shopina et al. (2020), a country's organizational and legal support for cybersecurity is a measure of how well it copes with the cyberthreats that exist in cyberspace and take on different forms daily.

Reputation Risk Management in the Digital Age.

The third main theme that emerged is reputation risk management in the digital age. Digital platforms have fundamentally transformed institutional communication dynamics, creating unprecedented challenges for reputation management. The rapid propagation of potentially damaging content requires sophisticated, instantaneous response mechanisms that most educational institutions currently lack. The study reveals that stakeholder trust can be rapidly eroded through single cybersecurity incidents, underscoring the critical importance of proactive digital governance strategies. Educational institutions exhibited insufficient experience and limited digital capacity, leading to increased gaps, inequalities, and learning deficits. Because of these findings, schools now need to learn and use experience to increase their digital capabilities and digitalization levels. They also highlighted the need to strike a careful balance between institutional legitimacy and technical openness (McCarthy et al., 2023).

Stakeholder Trust Erosion. Reputational management is increasingly challenging due to stakeholder trust erosion. Social media hacking incidents can swiftly damage years of established institutional credibility. Stakeholders, including parents, students, and teachers, readily express concerns and lose confidence when such incidents occur. The potential for long-term reputational harm is substantial, and rebuilding trust after it's lost is exceptionally difficult.

IDI#1: "Received numerous messages from parents... expressing concern about the content".

IDI#2: "Posts were superfluous and would harm or even ruin the school's reputation".

IDI#5: "This incident may lead to loss of trust from stakeholders".

The responses highlight the vital need for transparent communication strategies and proactive content management policies within educational institutions. These results are consistent with studies by Bunker (2020)

& Rao (2020) showing that governments and health authorities have used social media to counter false information during emergencies. The study cites effective instances, such as official Chinese social media platforms that favorably impact public opinion by disseminating trustworthy information. Additionally, The involvement of communities during crises demonstrates their role extending beyond just receiving information to actively contributing to the crisis response, as highlighted by the study of Lejano et al. (2021).

Misinformation Management. Misinformation management presents a multifaceted challenge in the modern world. Misinformation spreading quickly is amplified by social media platforms, potentially causing significant harm. Educational institutions face the difficulty of managing narratives and communication during security incidents. Effective crisis communication requires transparency and immediate action, while preventing the escalation of rumors necessitates sophisticated communication strategies and skills. Disseminating information in a timely, accurate, and transparent manner is essential to reducing the harmful effects of false information. The challenge for agencies has been maintaining the quality of communication and SSA in such an environment (Bunker et al., 2022). Pandemic response operations have become more difficult because of the public's decreased faith in official digital sources and their increased reliance on personal networks and alternative internet platforms (Jang & Baek, 2019).

Rapid Information Spread. The digital world has drastically changed the way information spreads due to its rapidity. Harmful content can quickly go viral within minutes, exceeding the capacity of traditional response mechanisms. Educational institutions often lack the resources and strategies to effectively manage the swift dissemination of potentially damaging content. This rapid spread can have immediate and severe emotional and psychological consequences for the institution. The speed at which misinformation and harmful content can spread online necessitates proactive measures and strategies for schools and other organizations to mitigate the negative impacts.

IDI #1: "Could potentially damage or even destroy the school's reputation"

IDI #2: "Nakakabahala talaga ang mga posts ng hacker"

(These posts are truly alarming)

The participants believe the posts could cause significant reputational harm, ranging from damage to complete destruction. Both responses highlight the significant threat posed by the hacker posts to the school’s reputation. This aligns with the study of Keller (2003) emphasizing the crucial function of online reputation management for organization. A negative online presence can severely impact stakeholders’ perceptions, leading to decreased enrollment, funding reductions, and eroded public trust (Christensen et al., 2020).

Coping Mechanism to Mitigate the Negative Impact on School Reputation.

This study integrates crisis communication theory (Coombs, 2007) with digital resilience frameworks to examine institutional responses to technological vulnerabilities. Three (3) key themes have surfaced in the coping strategies used by school heads to lessen the negative impacts on their school reputation, these are the following: Crisis Communication Resilience, Digital Security Empowerment, and Stakeholders Trust Restoration. Moreover, nine (9) core values have been identified: Rapid Public Disclosure, Transparent Incident Acknowledgment, Sincere Public Apology, Cybersecurity Education, Systematic Risk Management, Technological Intervention, Consistent Communication, Transparent Accountability and lastly Community Trust Building.

Crisis Communication Resilience

The Coping Mechanism to mitigate the negative impact on school reputation of the school heads revealed in the theme Crisis Communication Resilience. This outlines a conceptual framework emphasizing rapid, transparent, and multi-channel communication. This framework prioritizes immediate stakeholder engagement and focuses on building and maintaining institutional credibility during challenging situations. The participants’ responses shed light on several core ideas during the in-depth interviews. The following core ideas are Rapid Public

Disclosure, Transparent Incident Acknowledgment and Sincere Public Apology.

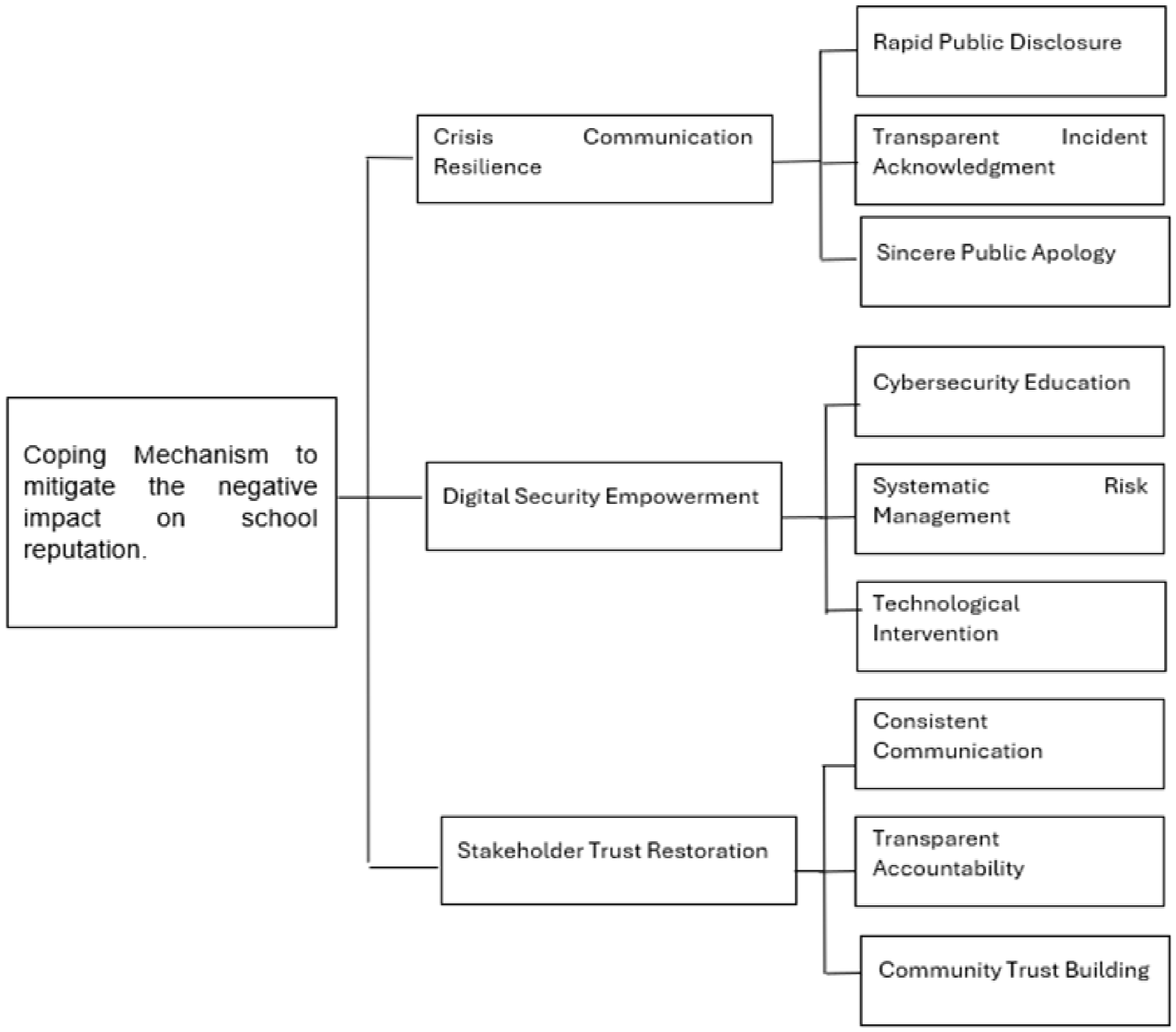
Coping Mechanism to mitigate the negative impact on school reputation.
Crisis Communication Resilience
Rapid Public Disclosure
Transparent Incident Acknowledgment
Sincere Public Apology
Digital Security Empowerment
Cybersecurity Education
Systematic Risk Management
Technological Intervention
Stakeholder Trust Restoration
Consistent Communication
Transparent Accountability
Community Trust Building

Figure 2. Coping Mechanism to Mitigate the Negative Impact on School Reputation.

Rapid Public Disclosure. The first critical response mechanism demonstrated by school heads is the immediacy of communication. Participants consistently showed a proactive approach to public communication, utilizing social media platforms (primarily Facebook) as the primary channel for instant disclosure. This strategy reflects a real-time crisis management approach, where transparency is prioritized over delay. School heads recognized the importance of being the first to communicate about the incident, effectively controlling the narrative and preventing potential misinformation spread.

"I immediately took to Facebook to inform the public" (IDI #1, L1-2)

"I quickly informed the public on Facebook" (IDI #2, L1-2)

"Taking immediate action thru making public statements on my own account" (IDI #6, L1-2).

The data reveals a strong preference for Facebook as a primary channel for rapid information dissemination. The results emphasize how crucial accessibility and promptness are in crisis communication. Effective communication during crises or emergencies is paramount (Coombs, 2014).

Transparent Incident Acknowledgment. Beyond mere communication, school heads demonstrated a commitment to transparent acknowledgment of the security breach. They explicitly stated the nature of the compromise, providing clear and direct information about the hacked social media page. This approach serves multiple purposes: it shows institutional honesty, reduces speculation, and demonstrates administrative responsibility in addressing technological vulnerabilities.

"Announced that our official school page had been compromised" (IDI #1)

"Told them that our official school page was compromised" (IDI #2)-

"Issuing public statements to inform stakeholders" (IDI 5, Implied)

The responses reveal the significant impact of potentially problematic online content within a school environment. Parental concerns, reputational damage, and the erosion of trust are key consequences that require proactive and comprehensive strategies to mitigate. This is in line with studies that demonstrate that each crisis needs information, explanations, or both, but the replies given have an impact on the crisis's outcome. A favorable outcome from a catastrophe may be ensured by taking responsibility and addressing it with apologies (Coombs, 2014).

Sincere Public Apology. A noteworthy aspect of the crisis communication strategy was the inclusion of sincere apologies. School heads went beyond mere notification, offering genuine expressions of regret to the public. This approach humanizes the institutional response, acknowledging the potential impact on stakeholders and demonstrating emotional intelligence in crisis management.

"Offered a sincere apology to the public" (IDI #1, L3-4)

"Sincerely apologized to the public" (IDI #2, L3-4)

"Providing clarification and apologies" (IDI #3)

The responses of researcher participants regarding the use of sincere public apologies in crisis communication within an educational institution. The data reveals a consistent theme: the strategic importance of expressing genuine regret to mitigate negative consequences following a crisis. This strategy prioritizes transparency and accountability, this recognizes the need to not only express remorse but also to provide clear explanations to address stakeholder concerns and enhancement (Coombs, 2014).

Digital Security Empowerment

Digital security empowerment is the second major theme which emerged during the In-Depth Interview of school heads. This can be gleaned from their general responses which centered on Cybersecurity Education, Systematic Risk Management, and Technological Intervention. In essence, this theme emphasizes a proactive and comprehensive approach to a digital security, fostering both individual and institutional resilience against cyber threats. Cybersecurity education emerges as a pivotal intervention strategy. The research highlights a transformative approach from reactive problem-solving to proactive skill development. This aligns with Buchanan et al., (2020) recommendations for comprehensive digital literacy programs in educational settings. An institutional shift towards organized technological resilience is evident in the methodical risk management techniques that have been seen. Many school administrators see cybersecurity as an organizational learning opportunity rather than a technological problem (Bustinza et al., 2016).

Cybersecurity Education. Participants emphasized education's vital role in preventing future incidents. This approach moves beyond reactive measures to proactive skill development. School heads recognized that empowering students, teachers, and stakeholders with Knowledge of digital literacy and security is fundamental to long-term risk mitigation.

"Educate both students and stakeholders about basic account security" (IDI #3, L1-2).

"Reminding learners about Netiquette" (IDI #4, L2-3).

"Educating about cybersecurity awareness" (IDI #5).

The research participants highlighted the role of education in preventing future cybersecurity incidents, shifting the focus from reactive to proactive skill development. These findings conform to the study of Sarket et al. (2020) emphasized the significance of preventive cybersecurity measures. The participants' emphasis on proactive skill development suggests a move towards a more holistic approach to cybersecurity, going beyond simply reacting to breaches.

Systematic Risk Management. The research revealed an emerging focus on systematic approaches to technological risks. School heads are progressively developing formal response teams and mitigation plans. This represents a shift from ad-hoc responses to structured, institutionalized approaches to digital security. This transition is characterized by the development of formalized response mechanisms, strategic planning initiatives, a focus on institutional learning, and the implementation of adaptive risk management strategies.

"Educate both students and stakeholders about basic account security" (IDI#3).

"Reminding learners about Netiquette" (IDI#4).

"Educating about cybersecurity awareness" (IDI#5, Implied).

The data underscores the foundational importance of providing comprehensive training on password management, phishing awareness, and secure online practices. This aligns with the study of Smith (2020), highlighting the effectiveness of educational interventions in improving cybersecurity behaviors. Washo (2021) underscores the important role of social engineering in cyberattacks. By promoting responsible behavior and awareness of potential manipulation tactics, this strategy contributes to a more resilient digital environment.

Technological Intervention. The emergence of technological interventions as a crucial component of digital security strategies in educational settings is noteworthy. School leaders actively sought technological solutions, collaborating with IT departments and social media platforms, and investigating compromised data. This approach highlights a problem-solving orientation towards security challenges, characterized by collaborative technological solutions, active problem investigation, platform-specific mitigation strategies, and the utilization of technical skills. This proactive, technically focused approach represents a shift towards a more responsive digital security posture within schools.

Stakeholder Trust Restoration

Stakeholder Trust Restoration is the third major theme which emerged during the In-Depth Interview of school heads. This can be gleaned from their general responses which centered on consistent communication, transparent accountability, and community trust building. The study reveals that trust restoration transcends traditional communication paradigms. Multi-channel communication strategies, transparent accountability, and community engagement represent sophisticated approaches to institutional reputation management (Veil et al., 2011).

Consistent Communication. Trust restoration fundamentally relies on consistent and multi-channel communication. School heads utilized various platforms—social media, emails, text messages—to maintain continuous stakeholder engagement. This approach ensures information accessibility and demonstrates ongoing commitment to transparency.

"Maintaining open communication with parents and students"- (IDI#1, L4-5).

"Keeping community informed about investigation and remediation"- (IDI#2, L1-2).

"Using school's official social media accounts, emails, or text messages" - (IDI#7, L1-2).

The responses emphasize the essential function of consistent and multi-channel discourse restoring the trust following a cybersecurity incident. This approach, characterized by the utilization of various platforms (social media, email, text, messages) to maintain continuous stakeholder engagement, directly addresses the need for transparency and information accessibility in crisis communication (Sandel & Ju, 2019).

Transparent Accountability. Transparency and accountability emerged as critical elements in restoring trust after a cybersecurity incident. School leaders not only communicated about the incident but also outlined specific steps taken, addressed misinformation, and demonstrated a commitment to protecting sensitive information. This approach, characterized by clear action communication, institutional responsibility, active misinformation correction, and comprehensive accountability, fostered trust and confidence among stakeholders. The proactive and transparent handling of the situation helped to mitigate reputational damage and reinforce the institution's commitment to its community.

Community Trust Building. Beyond immediate crisis management, school heads focused on long-term trust rebuilding. This involved actively engaging the community, requesting assistance, maintaining open communication channels, and demonstrating a commitment to collaborative problem-solving.

Learning Insights of the School Heads in Social Media Hacking Incidents on School Reputation.

Figure 3 displays the data from the participants' in-depth interviews (IDIs). Three (3) main themes emerged regarding school heads' insights into mitigating social media hacking incidents' impact on school reputation: Proactive Digital Resilience, Transparent Institutional Accountability, and Collaborative Community Protection. Moreover, nine (9) core values have been identified, Cybersecurity education, threat awareness and prevention, Continuous security skill development, immediate incident acknowledgment, open communication strategies, Reputation management, stakeholder engagement, shared responsibility, and Resource allocation and support.

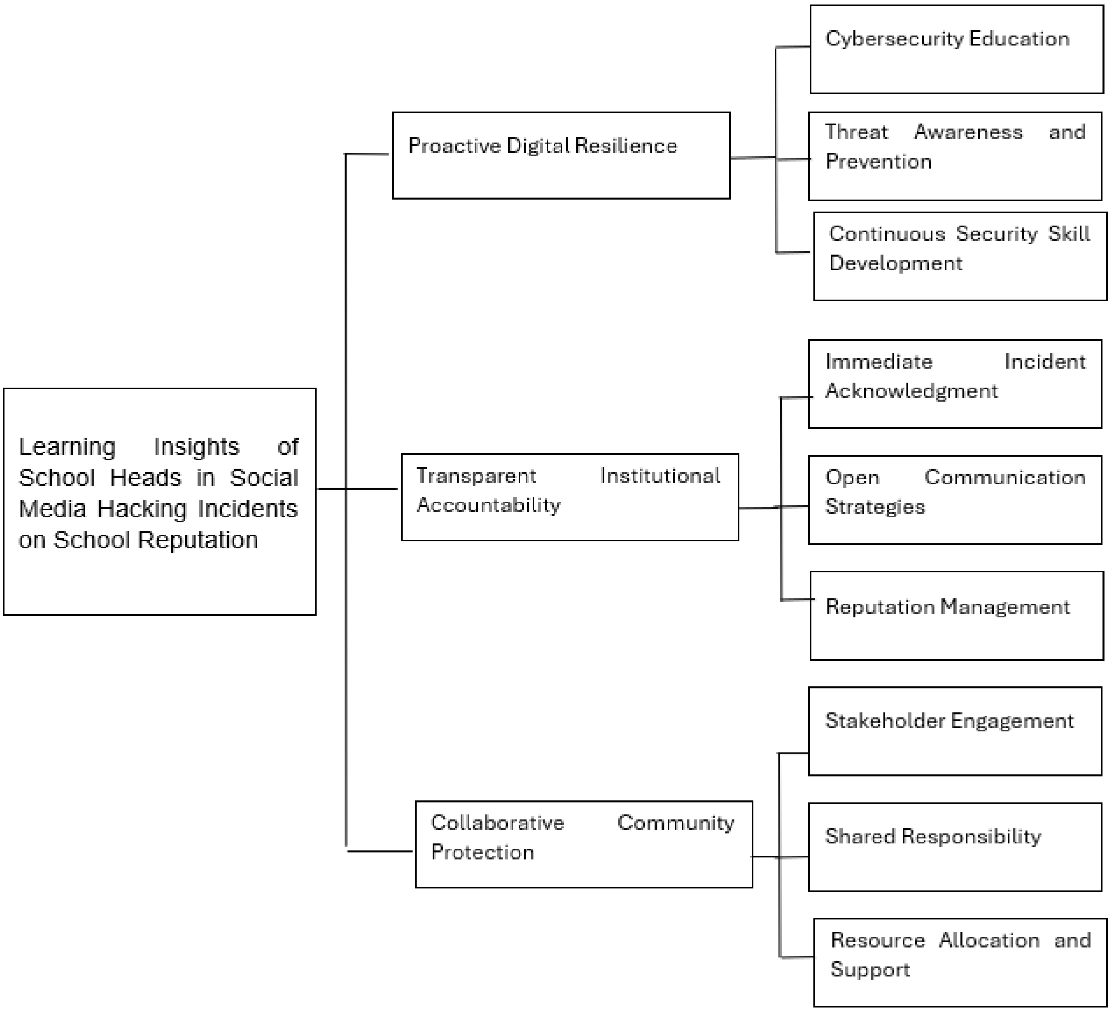
Learning Insights of School Heads in Social Media Hacking Incidents on School Reputation
Proactive Digital Resilience
Cybersecurity Education
Threat Awareness and Prevention
Continuous Security Skill Development
Transparent Institutional Accountability
Immediate Incident Acknowledgment
Open Communication Strategies
Reputation Management
Collaborative Community Protection
Stakeholder Engagement
Shared Responsibility
Resource Allocation and Support

Figure 3. Learning insights to Mitigate the Negative Impact on School Reputation.

Proactive Digital Resilience

Proactive digital resilience represents a paradigm shift in cybersecurity, moving beyond reactive measures to a forward-thinking approach that prioritizes prevention, preparation, and continuous learning (NIST, 2021). Additionally, SANS (2023) reported that unlike traditional cybersecurity strategies that primarily focus on incident response and damage control, proactive digital resilience incorporates a holistic framework encompassing risk assessment, vulnerability management, security awareness training, and robust incident response planning. The participants' responses shed light on several core ideas during the in-depth interviews. The following core ideas are cybersecurity education, threat awareness and prevention, and continuous security skill development.

Threat Awareness and Prevention. The theme of threat awareness and prevention emerged as a crucial component of the schools' digital security approach. School heads identified and emphasized key personal security practices, placing a strong emphasis on individual responsibility in digital spaces. The recommendations were pragmatic and direct: never share personal information online, exercise caution when encountering suspicious links and websites, and develop critical thinking skills for digital interactions. This approach reflected a proactive mindset that goes beyond technical solutions, focusing on empowering individuals with the abilities and information to safeguard oneself in online settings.

"Never share personal information with anyone." (IDI# 4).

"Be careful in clicking those malicious or unsecure links or sites." (IDI #4).

"This incident has been a stark reminder of the importance of robust security measures." (IDI #1).

The excerpts from research participant responses highlight critical aspects of online security awareness. These responses align with widely disseminated cybersecurity awareness campaigns that emphasize these preventive measures (National Institute of Standards and Technology, 2022).

Continuous Security Skill Development. Continuous security skill development reflects the dynamic nature of cybersecurity in modern educational environments. This core idea recognizes cybersecurity as an evolving discipline that requires ongoing learning, adaptation, and institutional commitment to skill enhancement. The approach is characterized by a proactive and adaptive mindset, treating each security incident as an opportunity for organizational learning and improvement.

Development approaches include systematically incorporating incident learnings into crisis management plans, ensuring continuous skill upgradation, and initiating regular security orientation programs. This strategy acknowledges that digital threats are constantly changing, and therefore, security skills must be continuously refined and updated. The emphasis is on creating a learning ecosystem that views cybersecurity as a dynamic field requiring persistent attention, reflection, and improvement.

"This incident must be incorporated into our existing crisis management plan." (IDI #1).

"Motivate me to learn more about cybersecurity risks." (IDI #2).

"Provide orientation on safeguarding social media accounts." (IDI #3).

The data, presented as three distinct statements, reveals insights into individual needs and priorities concerning information security and organizational preparedness. These responses offer valuable perspectives for improving cybersecurity awareness programs. The findings emphasize the need for all-encompassing crisis management plans that include cybersecurity crises, engaging cybersecurity education programs, and focused social media security training. These findings conform with the study of Al-Janabi & Al-Shourbaji (2016), The maintenance of cybersecurity also requires user education and awareness in addition to technical solutions. Recommended online security practices should be explained to users. These practices include avoiding dubious links and frequently changing passwords. To ensure staff or teachers are informed about the most recent risks and are equipped to handle them, organizations can develop security training programs.

Transparent Institutional Accountability

Transparent institutional accountability is crucial for maintaining public trust and ensuring effective crisis management, particularly in the digital age. The core elements focus on the practical implementation of accountability. They include immediate incident acknowledgment, clear communication strategies, and reputational management.

Immediate Incident Acknowledgment. Immediate incident acknowledgment represents a critical principle of institutional accountability in managing digital security challenges. This core idea emphasizes the importance of prompt, transparent, and responsible communication during security incidents. Leadership takes immediate responsibility, adopting a proactive approach that prioritizes openness and transparency.

"We should acknowledge the incident promptly and openly." (IDI #1).

"We must publicly and quickly acknowledge the situation." (IDI #6).

"It is very important that the school heads must plan ahead of time." (IDI #5).

The communication principles are clear and comprehensive: rapid acknowledgment of security incidents, public and transparent reporting, and systematic planning for potential threats. The goal is to maintain institutional credibility, demonstrate leadership responsibility, and prevent the spread of misinformation. By addressing incidents promptly and openly, schools aim to build trust, show their commitment to security, and engage stakeholders in the resolution process. These findings align with the study of Perwej et al. (2021) emphasizing the effective management of digital security incidents is paramount for maintaining institutional credibility and public trust. A crucial element in this process is the immediate acknowledgment of security breaches. Additionally, this also aligns with the broader literature on crisis communication which emphasizes the importance of early and honest engagement with stakeholders.

Open Communication Strategies. Open communication strategies form a comprehensive approach to maintaining stakeholder trust and engagement during digital security challenges. This core idea goes beyond traditional communication methods, employing a multi-channel approach that ensures information reaches diverse stakeholder groups effectively. The primary objective is to build and maintain trust through consistent, transparent, and accessible messaging.

"Open and honest communication with the school community is very important." (IDI#2).

"Maintaining constant communication with stakeholders through various channels." (IDI#3).

"Organize awareness campaigns and encourage open communication." (IDI #4).

The communication channels are diverse and inclusive, spanning official social media accounts, email communications, text messages, face-to-face meetings, and regular awareness campaigns. This approach recognizes the complexity of modern communication ecosystems and the need to reach stakeholders through multiple platforms. The strategy is designed to ensure that information is not just communicated, but is accessible, clear, and meaningful to all stakeholders. The provided responses of research participants highlighted the importance of open communication strategies that go beyond traditional methods, employing a multi-channel approach to ensure information reaches diverse stakeholders' groups effectively (Coombs & Holladay, 2012).

Reputation Management. Reputation management emerges as a strategic and comprehensive approach to maintaining institutional credibility during and after digital security incidents. This core idea views reputation not as a static attribute but as a dynamic process that requires active management, transparent communication, and strategic engagement. Schools approach reputation recovery as a proactive, collaborative effort that involves the entire school community.

"*We will conduct a thorough investigation and find ways to restore the school account." (IDI 1).*

"Figuring out how to get the school account back up and running." (IDI 2).

"Engage with the stakeholders in a meaningful way to rebuild trust." (IDI 5).

The recovery strategies are multifaceted, including conducting thorough incident investigations, making concerted efforts to restore compromised accounts, and actively engaging stakeholders in the recovery process. The approach goes beyond damage control, focusing on rebuilding trust, demonstrating institutional resilience, and using incidents as opportunities for organizational learning and improvement. Reputation management is seen as a critical component of maintaining long-term institutional credibility and stakeholder confidence. This reflects the stakeholder theory of Freeman (2010), prioritizing the needs and viewpoints of everyone involved. According to Klewes & Wreschniok (2009), management must constantly look for opportunities and threats affecting company reputation. Management's responsibilities include documenting and evaluating these, creating and implementing suitable countermeasures, tracking their efficacy, and providing top management and the board with updates on the evolving nature of risks.

Collaborative Community Protection

Collaborative community protection against digital security threats requires a three-pronged approach: stakeholder engagement, shared responsibility, and resource allocation.

Stakeholder Engagement. Stakeholder engagement represents a holistic and inclusive approach to digital security in educational institutions. This core idea extends digital protection beyond technical solutions, involving diverse stakeholder groups and promoting a comprehensive understanding of digital citizenship. The approach recognizes that effective digital security requires collective effort and shared responsibility.

"Educate the student and parents, the stakeholders in general on digital citizenship." (IDI#4).

"Invite IT experts for cybersecurity skills training." (IDI#5).

"Provide a functional school Cybersecurity committee." (IDI#8).

Engagement strategies include comprehensive digital citizenship education, cross-functional training programs, and the creation of dedicated cybersecurity committees. The goal is to create a collaborative ecosystem where each stakeholder - whether a student, teacher, parent, or administrator - plays a crucial role in maintaining digital safety. This approach transforms digital security from a technical challenge to a community-driven effort that emphasizes mutual learning, collective action, and shared responsibility. Social constructivism, which stresses the social basis of knowledge and cognition, is consistent with this holistic approach. (Vygotsky, 1978). Digital security is not solely a technical issue; it is also a social and cultural phenomenon shaped by the interactions, beliefs, and practices of individuals and groups within the educational community. A shared knowledge of risks and responsibilities is fostered by involving all stakeholders, including kids, teachers, parents, and administrators. This encourages group action and mutual learning.

Shared Responsibility. Shared responsibility is a fundamental principle of collaborative community protection, emphasizing collective approaches to digital security. This core idea moves beyond individual actions to create a comprehensive, community-driven approach to digital protection. The strategy is characterized by regular educational initiatives, mutual support, and a collective commitment to maintaining safe digital spaces.

"Having information drives the proper etiquette." (IDI# 4).

Responsibility mechanisms include regular netiquette information drives, social media education assemblies, and community-based reporting systems. The approach views digital security as a collaborative endeavor that requires active participation from all community members. By fostering a culture of shared responsibility, schools aim to create a robust, adaptive, and collectively maintained digital security environment. This idea is consistent with the notions of collective efficacy, underscoring the value of trust between members in accomplishing group objectives (Sampson et al., 1997).

Resource Allocation and Support. Resource allocation and support emerge as strategic investments in digital protection, reflecting a mature and proactive approach to cybersecurity. This core idea recognizes that effective digital security requires substantive financial and technical resources. Schools approach cybersecurity budgeting strategically, viewing it as a critical institutional priority rather than an optional expense.

"This must be taken into consideration during the annual budgeting process. We will provide a budget for IT Services or hiring IT services and providing orientations." (IDI #3).

Resource allocation approaches include annual budgeting for IT services, hiring specialized IT security support, and providing comprehensive orientation programs. The plan demonstrates an awareness that maintaining digital security calls for constant financial and technical assistance rather than a one-time expenditure. By allocating resources strategically, schools demonstrate their commitment to maintaining robust, adaptive, and effective digital security infrastructures. Wang et al. (2020) stress that the thorough orientation programs help all stakeholders develop a culture of security awareness and responsible digital citizenship. In addition, according to Maritan et al. (2017), effective resource allocation is consistent with organizational resilience principles and shows a dedication to proactive risk management and continuous development.

CONCLUSION

The study reveals the complex challenges educational institutions face in managing social media hacking incidents and their potential reputational consequences. The research exposed significant systemic weaknesses in digital security infrastructure, characterized by limited technical expertise, insufficient incident response capabilities, and inadequate cybersecurity training. Despite these challenges, school heads demonstrated sophisticated adaptive strategies, emphasizing rapid and transparent communication, proactive digital security education, and systematic risk management approaches. Rather than viewing hacking incidents as purely negative experiences, educational leaders recognized them as transformative learning opportunities for developing proactive digital resilience and fostering collaborative community protection.

The findings underscore the critical need for comprehensive digital security strategies that move beyond traditional reactive approaches. Schools must invest in ongoing cybersecurity education, develop robust technological infrastructure, and create collaborative security ecosystems that prioritize transparent communication during incidents. Key recommendations include developing standardized cybersecurity training programs, allocating dedicated budgets for technological security interventions, creating cross-functional cybersecurity committees, implementing continuous digital literacy programs, and establishing clear incident response protocols.

Ultimately, the research demonstrates that social media hacking incidents represent more than mere technological challenges—they are complex organizational and social phenomena requiring holistic, adaptive approaches. By transforming these incidents from threats into learning opportunities, educational institutions can build more resilient, digitally aware communities. The study provides a crucial roadmap for understanding, managing, and preventing digital security incidents in educational settings, emphasizing the importance of prevention, education, and collaborative action in maintaining institutional reputation and ensuring digital safety.

Implication and Future Direction

Educational institutions must develop a comprehensive approach to digital security that encompasses technical preparedness, proactive prevention, and strategic communication. This involves investing in cybersecurity training, creating robust incident response plans, and fostering a culture of digital awareness across the entire school community. This study provides valuable insights for school leaders seeking to navigate the challenges of cybersecurity in the digital age. Here are the key implications and future directions.

1. School leaders must prioritize cybersecurity education for all stakeholders, including students, teachers, parents and school heads. This includes training programs on basic account security, password management, phishing awareness, and responsible online behavior.
2. Schools must move beyond reactive crisis management and develop proactive; comprehension cybersecurity plans that address potential threats and vulnerabilities. This includes conducting risk assessments, implementing robust security measures, and establishing clear incident response protocols.
3. School leaders must acknowledge security incidents promptly and transparently, demonstrating a commitment to honesty and accountability. This includes providing clear and accurate information to stakeholders and actively addressing misinformation.
4. School leaders must engage all stakeholders in building a secure digital environment. This includes

involving students, teachers, parents, and school heads in discussions about digital safety, promoting digital literacy, and fostering a sense of shared responsibility.

5. Further researchers may explore the quantitative impact of social media hacking incidents on school reputation, including factors such as enrollment rates, funding levels, and public perceptions.

REFERENCE

1. Argenti, P.A. (2016). Corporate Communication (7th ed.). New York, NY: McGraw-Hill Education. Bada, Maria & Nurse, Jason. (2020). The Social and Psychological impact of cyberattacks. 10.1016/B978-0-12-816203-3.00004-6.
2. Bunker, D., Mirbabaie, M., & Stieglitz, S. (2017). Convergence Behaviour of Bystanders: An Analysis of 2016 Munich Shooting Twitter Crisis Communication. Paper presented at the 28th Australasian Conference on Information Systems, Hobart, University of Tasmania.
3. Bustinza, Oscar & Vendrell-Herrero, Ferran & Parry, Glenn & Perez-Arostegui, Maria. (2016). Technological capabilities, resilience capabilities and organizational effectiveness. The International Journal of Human Resource Management. 30. 10.1080/09585192.2016.1216878.
4. Chen, E., & DiVall, M. (2018). Social media as an engagement tool for schools and Journal of Educational Technology, 36(4), 227-239.
5. Christensen, T. Gavrila, S. G., Ma, L., & Ramirez, F. O (2020). Reputation management by Chinese universities: Primary profile and comparative features.
6. Coombs, W. (2007). Protecting Organization Reputations During a Crisis: The Development and Application of Situational Crisis Communication Theory. Corporate Reputation Review. 10. 163-176. 10.1057/palgrave.crr.1550049.
7. Coombs, W. T., & Holladay, J. S. (2012). The paracrisis: The challenges created by publicly managing crisis prevention. Public relations review, 38(3), 408-415.
8. Coombs, W. T. (2014). State of Crisis Communication: Evidence and the Bleeding Edge. Journal of Public Relations
9. Research, 13, 321-340. Research Journal of the Institute for Public Relations, 2014 - institute for pr.org. Conde, C. F. (2021). A Quick Guide to Case Studies. Retrieved from PREVNet: Community of Practice: Addressing Youth Dating Violence.
10. Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approach. Sage publications.
11. Freeman, R. Edward (2010). Stakeholder theory: The state of the art. Cambridge University Press, 2010.
12. Haber, L., Carmeli, A. (2023). Leading the challenges of implementing new technologies in organizations, Technology in Society, Volume 74, 2023, 102300, ISSN 0160-791X, https://doi.org/10.1016/j.techsoc.2023.102300.
13. Himes-Cornell, Amber & Ormond, Carlos & Hoelting, Kristin & Ban, Natalie & Koehn, John & Allison, Edward & Larson, Eric & Monson, Daniel & Huntington, Henry & Okey, (2018). Factors Affecting Disaster Preparedness, Response, and Recovery Using the Community Capitals Framework. Coastal Management. 46. 1-24. 10.1080/08920753.2018.1498709.https://dovetail.com/research/purposive-sampling.
14. Jang, K., Baek, Y. M. (2019). When information from public health officials is untrustworthy: The use of online news, interpersonal networks, and social media during the MERS outbreak in South Korea Health communication, 34 (9) (2019), 991-998.
15. Keller, K. (2003) Strategic Brand Management: Building, Measuring and Managing Brand Equity. Prentice Hall, Upper Saddle River.
16. Klewes, J., Wreschniok, R. (2009). Reputational Capital: Building And Maintaining Trust in the 21st century. ISBN 978-3-642-01629-5. e-ISBN 978-3-642-01630-1. DOI 10.1007/978-3-642-01630-1. Springer Heidelberg Dordrecht London New York.
17. Lejano, R.P., Haque, C.E., Berkes, F (2021). Co-production of risk knowledge and improvement of risk communication: A three-legged stool. International Journal of Disaster Risk Reduction, 64(2021), Article 102508
18. Liu, Jiajun (2022). The Tesla Brake Failure Protestor Scandal: A Case Study of Situational Crisis Communication

19. Theory on Chinese Media. Zimmerman School of Advertising and Mass Communications College of Arts and Sciences University of South Florida.
20. Maritan, Catherine & Lee, Gwendolyn. (2017). Resource Allocation and Strategy. Journal of Management. 43. 2411-2420. 10.1177/0149206317729738.
21. Martinez, L., & Chen, S. (2022). Social media engagement patterns in higher education: A longitudinal International Journal of Educational Technology, 42(2), 156-172.
22. Mason, J. (2018). Qualitative Researching. SAGE Publications, 2018, 3 editions. ISBN 1473912172, 9781473912175.
23. McCarthy, A. M., Maor, D., McConney, A., Cavanaugh, C. (2023). Digital transformation in education: Critical components for leaders of system change, Social Sciences & Humanities Open, Volume 8, Issue 1, 100479. ISSN 2590-2911. https://doi.org/10.1016/j.ssaho.2023.100479.
24. National Institute of Standards and Technology (2022).
25. NIST (2021). NIST Cybersecurity Framework. National Institute of Standard and Technology.
26. Perwej, Dr. Yusuf & Abbas, Qamar & Dixit, Jai & Akhtar, Nikhat & Jaiswal, Anurag. (2021). A Systematic Literature Review on Cyber Security. International Journal of Scientific Research and Management. Volume 9. Pages 669 - 710. 10.18535/ijsrm/v9i12.ec04.
27. Rahman, Md. Mahmudur & Hasan, Md & Ahmed, Asif. (2020). COVID-19 vaccine safety in comorbid patients: are we missing some critical points? 10.13140/RG.2.2.25673.57443.
28. Rodriguez, R., & Chen, S. (2019). Early adoption challenges of social media security in education. Technology inEducation Review, 25(3), 189-206.
29. Sampson, R.J. Raudenbush, S.W., & Earls, F. (1997). Neighborhoods and violent crime: A multilevel study of collective efficacy. Science, @77(5328),918-924.
30. Sandel, Todd & Ju, Bei. (2019). Social Media, Culture, and Communication. 10.1093/acrefore/9780190228613.013.758.
31. SANS Institute (2023). SANS Institute Cybersecurity Resources. SANS Institute.
32. Sarker, I. C., Badsha, S., Kayes, A. S., & Alqahtani, (2020). Cybersecurity data science: an overview from a machine learning perspective. https://www.researchgate.net/publication/342591771. Journal of Big Data · July
33. Shopina, I., Khomiakov, D., Khrystynechenko, , Zhukov, S, Shpenov, D. (2020). Cybersecurity: Legal And Organizational Support in Leading Countries, Nato and Eu Standards. Journal Of Security and Sustainability Issues Issn 2029-7017 print/ISSN 2029-7025 online 2020 March Volume 9 Number 3 https://doi.org/10.9770/jssi.2020.9.3(22).
34. Smith, J. Q., Jones, M. R., & Brown, C. D. (2020). Advancing Managerial Evolution and Resource Management in Contemporary Business Landscapes. Journal of Management Studies, 58, 1-25.
35. Thompson, R., Smith, J., & Brown, K. (2018). Authentication methods in educational social media. Journal of Cybersecurity Education, 8(2), 145-162.
36. Triplett, W. J. (2024). Cybersecurity Vulnerabilities in Healthcare: A Threat to Patient Security. Department of Information Systems, Health Information Technology, University of Maryland, Baltimore County, Baltimore, United States. Cybersecurity and Innovative Technology Journal, Vol.2, No.1, 2024, pp. 15-25.
37. Veil, S. R., Buehner, T., & Palenchar, M. J. (2011). A work-in-process literature review: Incorporating social media in crisis communication. Journal of Contingencies and Crisis Management, 19(2), 110-122.
38. Vishnevsky, T., & Beanlands, H. (2004). Qualitative Research. Nursing Journal, 31, 234-238.
39. Vygotsky, L.S., Cole, M., John-Steiner, V., Souberman, E. (1978). Mind in Society. The development of higher psychological processes. Harvard University Press. Pages: 174. https://www.jstor.org/stable/ctvjf9vz4
40. Wang, Hecheng & Feng, Junzheng & Zhang, Hui & Li, Xin. (2020). The effect of digital transformation strategy on performance: The moderating role of cognitive conflict. International Journal of Conflict Management. ahead-of-print. 10.1108/IJCMA-09-2019-0166.
41. Washo, A. (2021). An interdisciplinary view of social engineering: A call to action for research. Marywood University. Revised 23 June 2021, Accepted 24 July 2021, Available online 25 July 2021, Version of Record 29 July 2021.