BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 5, No 3, April 2024 | Hal 252-259
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v5i3.520

Qualitative Analysis of Shadow IT Practices in Higher Education to Identify IT Security Needs

Ahmad Aunul Bari Hayiz*, Arif Wibisono

Department of Information Systems, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia
Email: 1,*6026231017@student.its.ac.id, 2wibisono@is.its.ac.id
Correspondence Author Email: 6026231017@student.its.ac.id

Abstract−The presence of Shadow IT in educational settings often stems from users' attempts to fulfill work needs that are not met by formal systems. These tools, typically accessed outside institutional infrastructure, are preferred due to their practical use in day-to-day activities. However, such informal practices have been observed to trigger a variety of technical and security-related issues that remain undocumented by institutional IT policies. These tools may also pose significant risks to information security and work system reliability. This research aims to examine recurring problems encountered by users and interpret how these issues relate to key components in the work systems such as participants, technologies, information, processes, and products/services. The study employed a qualitative case study and applied the Eisenhardt method (1989) approach involving 35 respondents through interviews and field observations. Data was analyzed using open coding to extract recurring problem patterns. The analysis revealed four primary categories of problems System Error, Slow System Response, Access Limitations and Data Loss. These findings indicate that Shadow IT disrupts the flow of information and affects both technological and human elements within the work system. The study contributes by mapping factual user difficulties to concrete IT security needs that extend beyond formal policies. It suggests that effective IT security must address not only technical safeguards but also user behavior, access reliability, and adaptive policies capable of integrating informal digital practices.

Keywords: Shadow IT; Work System Theory; Open Coding; Qualitative Case Study; Educational Organization

1. INTRODUCTION

The digital transformation has been making many organizations try to integrate information systems as part of work efficiency improvement. In other hand, user needs faster solutions, flexible for work contextually appropriate are often not met by formal systems provided by organizations [1], [2], [3]. When formal procedures are considered too slow, or incompatible with practical needs, there arises an option for users to use alternative technologies outside the oversight of the IT formal department [3], [4].This phenomenon is called Shadow IT, which is the use of software, services, or applications that do not have the official approval of the organization but are actively used to support work [5], [6], [7].

The problem arises when shadow IT practices were used without security mechanisms, potentially exposing organizations to various risks [8], [9], [10]. Shadow IT applications frequently operate without established data protection standards; they often rely on personal devices without proper encryption, while the associated workflows remain outside the scope of organizational oversight and governance mechanisms [2], [9], [11]. Within such a context, information security is placed at considerable risk [2], [11]. Managing incidents like data breaches, unauthorized access, loss of vital information, and exposure to malicious software becomes significantly more complex when such activities transpire outside the purview of sanctioned organizational systems and lack formal documentation or monitoring [8], [12].

This risk increases in organizations constrained by inadequate infrastructure or a shortage of skilled personnel. Many such organizations lack awareness of the applications their employees use informally, creating a grey area in data management and system security [13], [14], [15]. In such scenarios, strategic information may flow outside authorized systems without proper controls, and the division of security responsibilities between end-users and IT departments becomes unclear [1]. These conditions collectively present critical obstacles to ensuring robust and holistic information security management within the organization [11], [15].

In dealing with the issue of Shadow IT, this study does not offer a prohibition approach. Imposing restrictions on users deemed at risk may disrupt established workflows that have long relied on the flexibility offered by alternative technologies [16]. On the other hand, a more constructive strategy is to understand how shadow IT practices work, starting from identifying emerging problems, as well as formulating relevant information security needs based on user experience [8]. By adopting this approach, organizations can formulate security strategies that are more aligned with actual field conditions, reducing overreliance on centralized, top-down policies [4].

Several research such as Mallmann, G.L., & Maçada, A.C. (2021) [1], Rakovic et al. (2020) [2], Kapepo et al. (2021) [9], Huber, Melanie, et al. (2021) [3] have highlighted the rise of Shadow IT in organizational contexts. It often emerges when official systems fall short in meeting fast and specific work needs, as emphasized by Mörike, Frauke et al. (2024) [16], Kopper, Andreas et al. (2020) [7]. Employees are often motivated by the flexibility of unofficial tools, choosing to adopt them despite being aware of the potential risks involved, as demonstrated by, Ogedengbe, Fowokemi Alaba et al. (2023) [17]. Notably, some research such as that of Mallmann, G.L., & Maçada, A.C. (2021) [1] and de Vargas Pinto, Aline et al. (2023) [18] indicates that Shadow IT may contribute to organizational innovation, particularly in environments that encourage employees to experiment with new technologies on their own initiative. Ogedengbe, Fowokemi Alaba et al. (2023) [19] also reveals an ongoing conflict between the operational benefits of Shadow IT and its associated security vulnerabilities. Moreover, restrictive policy has shown limited effectiveness, emphasizing the need for greater user participation in shaping relevant IT policies [8], [9], [20], [21].

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 5, No 3, April 2024 | Hal 252-259
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v5i3.520

From some of the existing literature contributions, there are still gaps in studies that explicitly map security problems based on real user practices that occur [8], [16], [18], [19], [22]. Most of the research is still conceptual in nature and focuses on managerial perspectives [6], [16], [23]. In fact, understanding how users use Shadow IT, the types of problems they experience, and the impact on information security is essential to design contextual security needs. This is an important point in organizations with various levels of digital literacy, high work complexity and freedom in choosing work tools [1], [2], [24]. Research that does not focus on the user's perspective often results in security solutions that are unable to address the challenges faced by users, potentially leading to security issues within the organization. A lack of understanding of user behavior can result in the development of overly stringent policies that ultimately hinder productivity and fail to mitigate significant risks. Furthermore, if research is primarily oriented towards a managerial perspective without considering the experiences of users who frequently interact with Shadow IT systems, a misalignment may arise between the security policies implemented do not encompass the daily work context of the users, leading to a discrepancy between the existing systems and their needs in the field.

This research aims to address the identified gap by investigating the types of problems that arise from Shadow IT practices within organizational work systems. By focusing on these security-related challenges, the study contributes to a deeper understanding of how such practices affect the organization's overall information security posture, particularly from a user-centered perspective. Centering user experience using Work System Theory s as a critical lens, this study emphasizes the need to identify security requirements that are not only technically sound but also grounded in practical realities [25]. Using Eisenhardt's (1989) qualitative case study research method [26], which is designed to build theory from empirical evidence through iterative data collection and analysis. The method is particularly suitable for exploring complex, under researched phenomena such as Shadow IT, where user behaviors, organizational tasks, and digital tools interact in ways that are not yet fully understood. The interaction between users, organizational tasks and tools, as interpreted through Work System Theory [25]. The integration of these methodologies aims to produce security strategies that are both practical and responsive to real-world organizational conditions.

2. RESEARCH METHODOLOGY

2.1 Research Stages

The central focus of this research is to identify the types of problems arising from Shadow IT practices within organizational work systems. This research uses a qualitative approach through case studies research and applies the Eisenhardt method (1989) [26], [27]. This methodology was chosen because it is very suitable for developing theories of complex organizational phenomena, especially when the available knowledge is still limited or has not fully explained the dynamics that occur [28]. In this context, the practice of Shadow IT carried out informally by users in the organization is a phenomenon that is not easily observed through a quantitative approach [20], [29]. Therefore, the selection of the Eisenhardt method (1989) is considered relevant to explain in depth these practices and identify problems that arise from the user's point of view [27]. This study follows a five-stage research process, which is visually represented in Figure 1.

Figure 1. Research Stages

2.1.1 Identifying Research Questions

This study originates from a practical reality observed in many organizational settings: employees frequently resort to using digital applications or online platforms that have not been formally approved. This action usually came from the limitations of the official system, which does not correspond to the dynamic nature of daily work [11]. As a result, users seek alternative solutions that offer greater speed, adaptability, and ease of use, even if these tools fall outside institutional oversight. The research aims to examine these issues from the users' point of view, with a focus on understanding the kinds of problems that may compromise the security of organizational information systems based on Shadow IT practices.

2.1.2 Selecting Case Studies

This study uses a case study approach on one educational organization in Indonesia. The case was selected with careful consideration, as not all educational institutions demonstrate a wide range of practices involving the use of unregistered applications and services beyond the organization's formal system. The use of this application is carried out by non-IT employees to support daily administrative and operational tasks. The educational context was chosen because it reflects a work environment that often faces limitations in technological supervision but still requires fast and flexible digital solutions. This case study does not aim to represent the entire education sector, but to explore an in-depth understanding of the security issues that arise from the use of technology beyond the organization's control.

2.1.3 Collecting Data

Data collection is carried out through semi-structured interviews of users who are actively using digital applications or services outside of the organization's official IT system. in-person interviews are one of the main methods in case studies,

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 5, No 3, April 2024 | Hal 252-259
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v5i3.520

especially when researchers want to understand the complexity of phenomena involving many technical and operational aspects [25]. Field observations, on the other hand, provide researchers with the opportunity to see firsthand how Shadow IT is implemented and managed in the environment of educational organizations. This data collection focuses on the actions of employees who use Shadow IT to overcome problems they face in operational activities, especially related to WST aspects [25]. The interviewees were employees who actively used or were involved in the Shadow IT system in the organization. The total number of interviews at this data collection stage was 35 people.

2.1.4 Analyzing Data

This study employed open coding as the primary method for analyzing qualitative data [25], [30]. The process began by identifying meaningful units from the interview transcripts and field notes without altering the original statements. Each segment was preserved in its raw form as First Order data, then grouped based on similarity in meaning to form more general Second Order categories. To maintain consistency and avoid redundancy, these categories were carefully reviewed, merged when appropriate, and refined into more abstract classifications. These final groupings Third Order constructs were used to represent how users perceive and experience the presence of Shadow IT in their organizational work systems [25].

2.1.5 Developing Explanations

After the coding and categorization process was completed, the final step involved synthesizing the identified patterns into a structured classification of problems related to Shadow IT practices [25]. This synthesis was grounded in the empirical data and focused on how digital tools used outside the formal IT system contribute to emerging operational and security challenges within the organization. The resulting insights were interpreted within the context of the selected case, with emphasis on the specific interactions. The conclusions drawn from this stage were not intended to offer universal claims, but rather to reflect how risk perceptions and system vulnerabilities are shaped by the everyday practices of users operating beyond official digital infrastructures [25].

3. RESULT AND DISCUSSION

This study found that in educational organizations, the use of non-official digital tools has become a common part of the work routine. This practice comes naturally as staff seek practical solutions to meet their communication, automation and productivity needs. WhatsApp, Telegram, Zoom, and Email are commonly utilized as informal communication tools that facilitate faster information exchange, often taking precedence over the institution's formal communication systems. In addition, content creation platforms such as Canva, Microsoft Word and Google Docs are widely used to develop materials and documents without relying on official devices. Other practices involve automating administrative tasks through digital tools such as Google Forms that are used independently by staff to streamline processes such as data collection or attendance tracking without integration into formal IT. Moreover, file storage and sharing are often conducted using platforms like Google Drive, which operate outside the organization's regulated infrastructure. Quizizz, Duolingo, and Kahoot are often adopted by teachers as alternative tools to facilitate student evaluations in a more dynamic and flexible way, although these platforms are not officially part of the institution's core assessment framework. These various practices not only show the creativity and responsiveness of users to work needs but also become the starting point for the emergence of various information security problems that will be discussed in a structured manner in the following sections (see Table 1). Each identified practice and issue is analyzed not only from the perspective of tool functionality, but also in relation to how it illustrates the realities of daily work processes, the constraints posed by official systems, and the demand for security policies that are better aligned with organizational context.

Table 1. Coding Sample - Problem

No	Context	Transcript	1st Order	2nd Order	3rd Order
1	Informal communication and coordination	Yes, I made a lot of updates, not only on WhatsApp. I tend to act quickly, since delaying, I do update it often, because if I don't**, the app tends to error or freeze.** But honestly, sometimes those updates just make things more complicated.	Error	Error	System Error
2	Informal communication and coordination	So, I've also used an app for online meetings with Zoom that wasn't from work. **When there were more participants, the app just got super laggy.** Sometimes the audio was choppy the video would freeze and not move or suddenly I'd get kicked out of the meeting. It was annoying, especially since we were discussing important things and I ended up focusing more on the app than on the meeting.	Lags	Slow	Slow System Response

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 5, No 3, April 2024 | Hal 252-259
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v5i3.520

No	Context	Transcript	1st Order	2nd Order	3rd Order
3	Information access and dissemination	When **I try to upload something, it sometimes lags**. I've been trying to upload a file for two days and it still won't be sent even though my internet connection is fine. I tried switching to WiFi and then to mobile data, but it still didn't go through. Maybe it's because the update-uploading files have gotten slower. Honestly, I preferred the old version of Google Drive, before the update. Uploading large files used to be faster. And even when the upload finally works, sometimes the file doesn't open properly. For example, when I try to open a PDF, my phone often freezes-I can't do anything. I guess it's harder without a strong internet connection. Like, you really need a stable connection just to open the file.	Lags	Slow	Slow System Response
4	Information access and dissemination	Yeah, I've felt it, **it's hard to access** or really slow, especially when the internet connection is bad. It gets frustrating, you know... **especially when I can't access important files_**at crucial moments. I also had issues with storage space on my personal account. I had to choose which files to delete first, even though they all felt important. Well, that's the reality of being a free user.	Can't Access	Inaccessibility	Access Limitations
5	Informal learning assessment support	It really depends on the connection. Based on my experience, Kahoot needs a stable internet connection. When I'm running a live quiz and the network isn't stable, **everything slows down**, not just for me, but for everyone else too.	Slow	Slow	Slow System Response
6	Informal learning assessment support	Yeah, I've felt it. There was a time when Excel didn't show the data, the sheet just went blank. With Duolingo, the account sometimes logs out by itself, and **It's hard to log in using a username ,** I have to use email instead. Some of the kids also reported that their progress wasn't saved. Like, they had reached level 10, but it went back to level 9.	Hard to Log in	Inaccessibility	Access Limitations
7	Work process automation	At that time, I was pasting the questions one by one manually, and when I was done, I saved it. But when I opened it again, **all progress was lost.** I even checked through Chrome, but it still wasn't saved. I know it's a third-party app, so I don't entirely blame it, but I was really disappointed because I trusted the system from the beginning. I was also confused about where to find the "publish" button in the app. But using the website actually felt easier. That time, I tried to open a file I hadn't published yet, but I couldn't access it through the website, so I installed the app. Turns out, I couldn't find the publishing option in the app either.	Progress was lost	Unsaved Progress	Data Loss
8	Creation and delivery of work content	Login issues happen quite often, especially when I must log in again. Sometimes I get a message saying "Too many requests," It **blocks my access to the file** I need.	Access Block	Inaccessibility	Access Limitations
9	Creation and delivery of work content	I don't think I've ever experienced a data leak. But I have experienced messy data. I mean, back then I was using Excel to work on a project with my friends, we collaborated using one shared file via a link. But when I opened it on my device, the display looked different. It changed, you know? What I saw on my screen wasn't the same as what my friends saw. On their end, everything was neat, but on mine, the data was all jumbled, **like the data doesn't show up**	Data doesn't show up	Unsaved Progress	Data Loss

3.1 Informal Communication and Coordination

In the context of non-formal communication, Shadow IT is frequently adopted because of its ease of access and minimal procedural barriers [1]. Users often turn to these tools for their immediacy and adaptability, especially when formal systems are perceived as too rigid or time-consuming. While this approach offers practical advantages, operating outside the organization's official infrastructure also brings about significant risks, including potential disruptions to data security and overall system reliability. One respondent described their experienceas follows: "*I tend to act quickly, since delaying, I do update it often, because if I don't, the app tends to error or freeze.*" Another respondent described their experience as the following : "*So, I've also used an app for online meetings with Zoom that wasn't from work. When there were more*

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 5, No 3, April 2024 | Hal 252-259
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v5i3.520

participants, the app just got super laggy. Sometimes the audio was choppy the video would freeze and not move or suddenly I'd get kicked out of the meeting."

These two excerpts illustrate two major issues commonly found in informal communication and coordination practices involving Shadow IT: System Errors and Slow System Response. Both serve as indicators that the systems independently adopted by users may not necessarily be prepared to meet organizational needs. This is due to the fact that applications or services used outside of official systems are typically not designed with the complexities of workflows, security standards, or scalability required in an organizational context in mind. As a result, tools that function well for personal use may prove incompatible when integrated into broader organizational routines, potentially resulting in workflow disruptions, lack of coordination, and reduced overall efficiency.

As previously explained in the Research Methodology section, based on the voting process conducted during the analysis of interview data, System Errors and Slow System Response were frequently mentioned by participants. These two issues emerged as third order categories in the analysis because they were consistently identified across various responses. The frequent mention of these problems by different participants reflects their commonality and significance within the context of Shadow IT adoption in educational organizations. Within the framework of Work System Theory [25], such problems reflect pressure on the technology component, particularly when it operates outside the boundaries of formal control. When these tools fail to perform reliably, they can interrupt rather than enhance workflow processes, and in some cases, add further burdens to users rather than easing their tasks.

3.2 Information Access and Dissemination

In the practice of information access and dissemination, the use of Shadow IT often becomes a choice because it allows users to upload, store, and access documents quickly without relying on the official system infrastructure [8]. While this method provides convenience and faster access, it is not without the possibility of technical issues that may interfere with daily work processes. After going through the open coding phase, terms related to the problems experienced by users while using Shadow IT were extracted from the raw data and placed into the first order. Once the first order was organized, the second order was created by grouping categories that shared similar meanings, such as "*lags*" and "*slow*" which were then consolidated into the second order "*slow*". Based on the second order, a third order was derived through generalization of the user experiences, leading to the third order "*Slow System Response*", and same as the third order "*Access Limitations*".

One of the respondents shared the following experience: "*When I try to upload something, it sometimes lags. Uploading large files used to be faster. And even when the upload finally works, sometimes the file doesn't open properly.*" The statement indicates the presence of recurring and complex technical obstacles. Despite the network having been tested and been switched, barriers continue to arise, suggesting issues not only with connectivity but also with the stability of the applications in use. Technical interruptions are not limited to the uploading process; they often continue after the file has been stored, particularly when users attempt to reopen the file and encounter system freezes or unresponsive behavior. This situation renders the information distribution process unreliable, especially when conducted under time constraints.

Another respondent described their experience as the following : "*Yeah, I've felt it, it's hard to access or really slow, especially when the internet connection is bad. It gets frustrating, you know... especially when I can't access important files at crucial moments.*" This statement highlights the inconsistency users face when trying to access work-related files. The difficulties encountered are linked not only to unreliable internet access but also to the limited storage space provided by the digital services in use. As a result, users are often forced to remove essential files just to regain access or free up space when working under time pressure. This condition compels users to delete important files in order to regain access space, ultimately creating additional pressure, especially when those files are needed in urgent situations.

The two quotes highlight two main issues in the practice of accessing and disseminating information through Shadow IT, namely the Slow System Response and Access Limitations. These issues arise due to the unpredictable performance of user-adopted technologies and the inconsistent reliability of network connections, which are not always capable of supporting continuous access. Viewed through the lens of Work System Theory [25], such disruptions interfere with the information and technology components that are essential for maintaining effective and uninterrupted task execution. The practice of accessing and disseminating information through unregulated Shadow IT by unofficial departments can pose various serious security issues related to other practices. Delays in file access or system responsiveness hinder the flow of information, which in turn diminishes efficiency and may negatively affect overall productivity in the workplace.

3.3 Informal Learning Assessment Support

In interactive learning activities, Shadow IT is often used as a tool for quizzes, independent practice, or light evaluations outside of the official learning systems [31]. Quick and flexible access is the primary reason users rely on these platforms. However, its effectiveness is highly dependent on stable technical conditions during the process. After conducting open coding (see Table 1), expressions reflecting problems during the use of Shadow IT were extracted from the raw transcripts and categorized into the first order. For example, phrases such as "*everything slows down*" were coded as the first order "*slow*" and grouped under the second order category "*Slow*," while "*It's hard to log in using a username*" was coded as "*hard to log in*" and grouped under the second order category "*Inaccessibility*." These second order categories were then

BULLETIN OF COMPUTER SCIENCE RESEARCH
ISSN 2774-3659 (Media Online)
Vol 5, No 3, April 2024 | Hal 252-259
https://hostjournals.com/bulletincsr
DOI: 10.47065/bulletincsr.v5i3.520

generalized into the third order themes "*Slow System Response*" and "*Access Limitations*," which represent broader patterns of constraints that affect the reliability and continuity of learning processes supported by Shadow IT.

The two quotes illustrate two primary constraints in the practice of Informal Learning Assessment Support using Shadow IT, namely Slow System Response and Access Limitations. This problem highlights the weak technological support for non-formal learning processes that require stable connectivity and reliable storage. Applying the Work System Theory framework [25], this condition reveals strain on both the technological tools and the users themselves, where system instability hampers active participation and interrupts the flow of learning processes. When access is unreliable and user progress cannot be consistently saved, the role of Shadow IT as a tool for facilitating learning and assessment loses its credibility and effectiveness [8].

3.4 Work Process Automation

Shadow IT is often adopted as a tool for automating routine tasks in administrative workflows, including entering data, gathering responses, and saving records without manual input [32]. Many users perceive this approach as more practical and timesaving compared to formal systems provided by the organization. However, behind its efficiency, there are significant risks of data loss that cannot be ignored, particularly due to the uncertainty surrounding storage status and the lack of validation mechanisms in the systems employed. One respondent described their experience as follows: "*At that time, I was pasting the questions one by one manually, and when I was done, I saved it. But when I opened it again, all progress was lost. I even checked through Chrome, but it still wasn't saved.*"

This statement highlights the inability of the automation system in use to ensure secure and verifiable data storage. Despite adhering to standard steps like composing, saving, and reopening files, users may find that the system fails to register or retain the data as intended. When work progress disappears unexpectedly, it erodes users' confidence in the system's reliability. The situation becomes more difficult when interface differences between the web and mobile versions cause confusion, especially in locating key functions such as the "publish" feature that ideally should be intuitively placed. This case illustrates a data loss problem, which represents a critical issue in work automation practices involving Shadow IT. Interpreted through the framework of Work System Theory, this condition suggests a failure in how information is processed and maintains an essential requirement for sustaining daily operations. When the system falls short in preserving and retrieving input as expected, the role of automation shifts from being a solution to becoming a source of inefficiency within the work system. Instead of streamlining tasks, it imposes additional burdens and reduces the efficiency that technology is expected to enhance.

3.5 Creation and Delivery of Work Content

Shadow IT is often utilized in activities such as document preparation, visual content editing, and collaboration through online files that are not directly connected to the organization's official systems. Users are drawn to these tools mainly due to their adaptable nature, especially when tasks require seamless access across different types of devices. However, this ease of use is not always matched by system reliability issues related to consistent access and data accuracy often emerge during practical use. One respondent described their experience as follows: "*Login issues happen quite often, especially when I must log in again. Sometimes I get a message saying, "Too many requests," It blocks my access to the file I need.*" Another respondent's statement reinforces the issue related to data storage : "*But I have experienced messy data. But when I opened it on my device, the display looked different. It changed, you know? What I saw on my screen wasn't the same as what my friends saw. On their end, everything was neat, but on mine, the data was all jumbled, like the data doesn't show up*"

These two findings indicate that in the practice of content creation using Shadow IT, there are two main problems: Access Limitations and Data Loss. Both issues point to system shortcomings in maintaining consistency and dependability when multiple users engage in digital content creation. From the perspective of Work System Theory [25], these problems directly impact the elements of information and participants. When users are unable to access files smoothly or the compiled data appears incomplete, work productivity is not only disrupted but also carries the risk of producing inaccurate outputs [33]. If the practice of Creation and Delivery of Work Content is frequently carried out by users of Shadow IT in educational organizations, the impact will not only be felt by the organization itself but may also hinder the ongoing learning process. From this issue, it is evident that not all practices of using Shadow IT bring benefits, especially in the educational sector, but rather create various problems.

4. CONCLUSION

Using a qualitative approach through case studies research and applying the Eisenhardt method (1989), this study examines the types of difficulties encountered when staff members in educational institutions informally adopt digital tools outside official IT systems to support their tasks. The findings reveal that while Shadow IT offers ease of use, flexibility, and fast solutions for daily work activities, it also leads to several critical disruptions, such as System Error, Slow System Response, Access Limitations and Data Loss. These findings, which reveal an absence of structured

oversight, inconsistent system reliability, and limited built-in protections typically found in formally managed infrastructures, directly address the research objective of identifying system related issues emerging from the informal use of Shadow IT in educational institutions. By employing Work System Theory, the study connects each observed problem to specific components within the work system such as tools used, informational flow, and user roles illustrating how Shadow IT is intertwined with systemic shortcomings. Consequently, addressing IT security demands not only protecting sensitive information, but also ensuring stable access, responsive digital environments, and flexible policies capable of acknowledging and integrating informal technology use. Theoretically, this study contributes by extending the application of Work System Theory to the context of unofficial digital system usage by end-users in organizational settings. By mapping problems to the core elements of work systems, the study offers a conceptual lens that emphasizes how security risks stem not only from technical weaknesses, but also from user decisions to bypass formal systems due to efficiency, habit, or lack of suitable alternatives. This contribution reinforces the notion that understanding IT security requirements cannot be separated from the mapping of real-world problems and the informal structures that evolve outside official systems. Practically, the findings offer insights for institutions to revisit overly centralized system and information security designs, encouraging more adaptive approaches aligned with user realities. Institutions are encouraged to design systems that are not only technically robust but also aligned with actual user contexts, to reduce the reliance on unofficial and potentially vulnerable digital solutions. Nonetheless, this study is limited in that it does not yet measure the direct security consequences of Shadow IT. Future research could explore the relationship between types of problems and the levels of vulnerability they produce, or develop an evaluation framework that integrates technological, behavioral, and policy related factors.

REFERENCES

[1] G. L. Mallmann and A. C. G. Maçada, “The mediating role of social presence in the relationship between shadow IT usage and individual performance: a social presence theory perspective,” *Behav. Inf. Technol.*, vol. 40, no. 4, pp. 427–441, 2021, doi: 10.1080/0144929X.2019.1702100.

[2] L. Rakovic, T. A. Duc, and V. Vukovic, “Shadow it and ERP: Multiple case study in German and Serbian companies,” *J. East Eur. Manag. Stud.*, vol. 25, no. 4, pp. 730–752, 2020, doi: 10.5771/0949-6181-2020-4-730.

[3] M. Huber, C. Rentrop, S. Zimmermann, and C. Felden, “Decision Making to Integrate Shadow IT and Enterprise Systems,” in *Twenty-fifth Pacific Asia Conference on Information Systems*, 2021, pp. 1–14. [Online]. Available: https://aisel.aisnet.org/pacis2021/27

[4] D. J. Castanelli, J. M. Weller, E. Molloy, and M. Bearman, “Shadow systems in assessment: how supervisors make progress decisions in practice,” *Adv. Heal. Sci. Educ.*, vol. 25, no. 1, pp. 131–147, 2020, doi: 10.1007/s10459-019-09913-5.

[5] L. Raković, M. Sakal, P. Matković, and M. Marić, “Shadow IT – A systematic literature review,” *Inf. Technol. Control*, vol. 49, no. 1, pp. 144–160, 2020, doi: 10.5755/j01.itc.49.1.23801.

[6] G. L. Mallmann, A. de Vargas Pinto, and A. C. Gastaud Maçada, “Shedding light on shadow it: Definition, related concepts, and consequences.,” *Atas da Conf. da Assoc. Port. Sist. Inf.*, vol. 2018-October, 2018, [Online]. Available: https://aisel.aisnet.org/capsi2018/23

[7] A. Kopper, M. Westner, and S. Strahringer, “From Shadow IT to Business-managed IT: a qualitative comparative analysis to determine configurations for successful management of IT by business entities,” *Inf. Syst. E-Bus. Manag.*, vol. 18, no. 2, pp. 209–257, Jun. 2020, doi: 10.1007/s10257-020-00472-6.

[8] T. Nguyen, “Understanding Shadow IT usage intention: a view of the dual-factor model,” *Online Inf. Rev.*, vol. 48, no. 3, pp. 500–522, 2024, doi: 10.1108/OIR-04-2022-0243.

[9] M. I. Kapepo, J. P. Van Belle, and E. Weimann, “Towards a theoretical understanding of workarounds emerging from use of a referral mobile application: A developing country context,” *Procedia Comput. Sci.*, vol. 196, pp. 533–541, 2021, doi: 10.1016/j.procs.2021.12.046.

[10] S. Klotz, A. Kopper, M. Westner, and S. Strahringer, “Causing factors, outcomes, and governance of shadow IT and business-managed IT: A systematic literature review,” *Int. J. Inf. Syst. Proj. Manag.*, vol. 7, no. 1, pp. 15–43, 2019, doi: 10.12821/ijispm070102.

[11] D. Yılmaz Börekçi, S. Büyüksaatçı Kiriş, and S. Batmaca, “Analysis of enterprise resource planning (ERP) system workarounds with a resilience perspective,” *Contin. Resil. Rev.*, vol. 2, no. 2, pp. 131–148, 2020, doi: 10.1108/crr-06-2020-0022.

[12] A. Kopper and M. Westner, “Towards a taxonomy for Shadow IT,” in *AMCIS 2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems*, 2016, pp. 1–10. [Online]. Available: https://aisel.aisnet.org/amcis2016/EndUser/Presentations/3

[13] V. Chauhan, C. Arora, H. Khalajzadeh, and J. Grundy, “How do software practitioners perceive human-centric defects?,” *Inf. Softw. Technol.*, vol. 176, p. 107549, 2024, doi: https://doi.org/10.1016/j.infsof.2024.107549.

[14] D. Fürstenau, H. Rothe, and M. Sandner, “Leaving the Shadow: A Configurational Approach to Explain Post-identification Outcomes of Shadow IT Systems,” *Bus. Inf. Syst. Eng.*, vol. 63, no. 2, pp. 97–111, 2021, doi: 10.1007/s12599-020-00635-2.

[15] D. Fürstenau, M. Sandner, and D. Anapliotis, “Why do shadow systems fail? An expert study on determinants of discontinuation,” in *24th European Conference on Information Systems, ECIS 2016*, 2016, p. ResearchPaper157. [Online]. Available: https://aisel.aisnet.org/ecis2016_rp/157

[16] F. Mörike, H. L. Spiehl, and M. A. Feufel, “Workarounds in the Shadow System: An Ethnographic Study of Requirements for Documentation and Cooperation in a Clinical Advisory Center,” *Hum. Factors*, vol. 66, no. 3, pp. 636–646, 2024, doi: 10.1177/00187208221087013.

[17] M. Silic, D. Silic, and G. Oblakovic, “Influence of Shadow IT on Innovation in Organizations,” *Complex Syst. Informatics Model. Q.*, no. 8, pp. 68–80, 2016, doi: 10.7250/csimq.2016-8.06.

[18] A. de Vargas Pinto, I. Beerepoot, and A. C. G. Maçada, “Encourage autonomy to increase individual work performance: the impact of job characteristics on workaround behavior and shadow IT usage,” *Inf. Technol. Manag.*, vol. 24, no. 3, pp. 233–246,

2023, doi: 10.1007/s10799-022-00368-6.
[19] F. A. Ogedengbe, Y. Y. Abdul Talib, and F. H. Rusly, "Influence of structural factors on employee cloud shadow IT usage during COVID-19 lockdown: a strain theory perspective," *Cogn. Technol. Work*, vol. 26, no. 1, pp. 63–81, 2024, doi: 10.1007/s10111-023-00748-0.
[20] A. Györy, A. Cleven, F. Uebernickel, and W. Brenner, "Exploring the shadows: IT Governance approaches to user-driven innovation," *ECIS 2012 - Proc. 20th Eur. Conf. Inf. Syst.*, 2012, [Online]. Available: https://aisel.aisnet.org/ecis2012/222
[21] M. Silic, J. B. Barlow, and A. Back, "A new perspective on neutralization and deterrence: Predicting shadow IT usage," *Inf. Manag.*, vol. 54, no. 8, pp. 1023–1037, 2017, doi: 10.1016/j.im.2017.02.007.
[22] H. H. Huang and J. W. Lin, "Inconsistencies Between Information Security Policy Compliance and Shadow IT Usage," *J. Comput. Inf. Syst.*, vol. 64, no. 4, pp. 554–564, 2024, doi: 10.1080/08874417.2023.2234318.
[23] S. Haag, A. Eckhardt, and A. Schwarz, "The Acceptance of Justifications among Shadow IT Users and Nonusers – An Empirical Analysis," *Inf. Manag.*, vol. 56, no. 5, pp. 731–741, Jul. 2019, doi: 10.1016/j.im.2018.11.006.
[24] G. L. Mallmann, A. C. G. Maçada, and G. P. Z. Montesdioca, "The social side of shadow IT and its impacts: Investigating the relationship with social influence and social presence.," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2019-Janua, pp. 6460–6469, 2019, doi: 10.24251/hicss.2019.776.
[25] S. Alter, "Work system theory: Overview of core concepts, extensions, and challenges for the future," *J. Assoc. Inf. Syst.*, vol. 14, no. 2, pp. 72–121, 2013, doi: 10.17705/1jais.00323.
[26] K. M. Eisenhardt, "Building Theories from Case Study Research," *Acad. Manag. Rev.*, vol. 14, no. 4, pp. 532–550, 1989, doi: 10.5465/amr.1989.4308385.
[27] K. M. Eisenhardt, "What is the Eisenhardt Method, really?," *Strateg. Organ.*, vol. 19, no. 1, pp. 147–160, 2021, doi: 10.1177/1476127020982866.
[28] S. H. Appelbaum, "Socio-technical systems theory: an intervention strategy for organizational development," *Manag. Decis.*, vol. 35, no. 6, pp. 452–463, 1997, doi: 10.1108/00251749710173823.
[29] G. L. Mallmann, A. C. G. Maçada, and M. Oliveira, "The influence of shadow IT usage on knowledge sharing: An exploratory study with IT users," *Bus. Inf. Rev.*, vol. 35, no. 1, pp. 17–28, 2018, doi: 10.1177/0266382118760143.
[30] M. A. Cascio, E. Lee, N. Vaudrin, and D. A. Freedman, "A Team-based Approach to Open Coding: Considerations for Creating Intercoder Consensus," *Field methods*, vol. 31, no. 2, pp. 116–130, 2019, doi: 10.1177/1525822X19838237.
[31] M. Javaid, A. Haleem, R. P. Singh, R. Suman, and E. S. Gonzalez, "Understanding the adoption of Industry 4.0 technologies in improving environmental sustainability," *Sustain. Oper. Comput.*, vol. 3, no. January, pp. 203–217, 2022, doi: 10.1016/j.susoc.2022.01.008.
[32] M. Abbas and A. Alghail, "The impact of mobile shadow IT usage on knowledge protection: an exploratory study," *VINE J. Inf. Knowl. Manag. Syst.*, vol. 53, no. 4, pp. 830–848, 2023, doi: 10.1108/VJIKMS-08-2020-0155.
[33] S. Alter, "Theory of Workarounds," *Commun. Assoc. Inf. Syst.*, vol. 34, no. 55, pp. 1041–1066, 2014, doi: 10.17705/1CAIS.03455.