

تحليل طرق النسخ الاحتياطي المختلفة المستخدمة من قبل موظفي جامعة هرات (2024)

Analysis of Different Data Backup Methods Used at Herat University by Staff (2024)

- **Dr. Mohammad Hamed Amiry¹**,

Dean of Computer Science Faculty (Herat University– Afghanistan);

- **Dr. Mostafa Olumee²**,

Lecturer in Information System

Department of Computer Science Faculty

(Herat University– Afghanistan);

- **Dr. Noor Ali Mohmand³**

Lecturer in Veterinary Facult

(Herat University– Afghanistan).

- Received: 06/08/2025 Accepted: 11/10/2025 Published 15/11/2025

Abstract :

This study investigates data backup practices employed by staff at Herat University, highlighting current strategies, identifying challenges, and proposing practical solutions to enhance data security. The findings reveal significant inconsistencies in backup frequency and methods across departments, a heavy reliance on local storage solutions, and a lack of formal backup policies. A mixed-methods approach was used, combining quantitative data from 195 staff members with qualitative document analysis. The study identifies key challenges such as unstable power conditions, inadequate technical knowledge, and decentralized backup responsibilities. Most staff used full backups stored on hard disks, while cloud-based solutions were underutilized. The absence of standardized policies and regular backup evaluations further compromised data integrity. Based on these findings, the study recommends implementing a comprehensive university-wide backup policy, centralizing backup management within the IT department, promoting cloud storage, and conducting regular training and audits. These interventions aim to strengthen Herat University's data resilience and offer a model for other

¹- hamed.amir.2015@gmail.com

²- m.olumee@gmail.com

³- dnmpathology2010@yahoo.com

academic institutions facing similar challenges in data protection and continuity.

Keywords: *Data Backup, Data Security, Backup Policies, Cloud Storage, Herat University*

- ملخص:

تُحقق هذه الدراسة في ممارسات النسخ الاحتياطي للبيانات التي يعتمد عليها موظفو جامعة هرات، حيث تسلط الضوء على الاستراتيجيات الحالية، وتحدد التحديات، وتقدم حلولاً عملية لتعزيز أمان البيانات. تكشف النتائج عن وجود تفاوت كبير في وتيرة النسخ الاحتياطي وأسالبيه بين الأقسام المختلفة، واعتماد كبير على حلول التخزين المحلي، وغياب السياسات الرسمية الخاصة بالنسخ الاحتياطي. وقد استخدمت الدراسة منهجاً مختلطاً يجمع بين البيانات الكمية من 195 موظفاً وتحليل وثائق نوعي. وتحدد الدراسة التحديات الرئيسية مثل عدم استقرار التيار الكهربائي، وضعف المعرفة التقنية، وتشتت مسؤوليات النسخ الاحتياطي. أظهر معظم الموظفين استخدامهم لنسخ احتياطية كاملة تُخزَّن على الأقراص الصلبة، في حين لم يتم الاستفادة من الحلول السحابية بالشكل الكافي. كما أن غياب السياسات الموحدة وتقييمات النسخ الاحتياطي المنتظمة أدى إلى تقويض سلامة البيانات. واستناداً إلى هذه النتائج، توصي الدراسة بتطبيق سياسة نسخ احتياطي شاملة على مستوى الجامعة، ومركزة إدارة النسخ الاحتياطي ضمن قسم تقنية المعلومات، وتعزيز استخدام التخزين السحابي، وتنظيم دورات تدريبية منتظمة وعمليات تدقيق دورية. وتهدف هذه التدخلات إلى تعزيز مرونة البيانات في جامعة هرات وتقديم نموذج لمؤسسات أكاديمية أخرى تواجه تحديات مماثلة في حماية البيانات واستمرارية العمل.

- الكلمات المفتاحية: النسخ الاحتياطي للبيانات، أمن البيانات، سياسات النسخ الاحتياطي، التخزين السحابي، جامعة هرات

1. INTRODUCTION

Decision-making, management reporting, and transaction processing within organizations are becoming increasingly dependent on computer-based information systems. The majority of enterprises now store their data and information electronically on computer hard disks, tape drives, compact disks, and other storage devices due to increased computerization. Regardless of how well-designed they are, computer-based information systems frequently encounter issues like hardware malfunctions, software bugs, or user errors (Cashman et al., 2008). Data and information loss can occur from starting a computer, opening a file, adding new content to a hard drive, or performing a regular maintenance program (Ngemu, 2000). Since data and information loss

frequently leads to the unavailability of crucial information systems required for corporate operations, it can seriously disrupt an organization's operations. Businesses lose out on the money and labor required to restore lost data and information, as well as the damaged reputation of their company due to services and activities being interrupted. Therefore, it is important to protect an organization's data and information. However, as Doyle (2001) notes, maintaining an organization's hard drives is insufficient; instead, it should constantly maintain backup copies of its data.

According to Cashman et al. (2008), data backup transfers program files and data to ensure their preservation in case of equipment failure or another calamity. According to Doyle (2001), a backup file is a duplicate of a file that you can use if the original gets destroyed or corrupted. The most popular method for making sure that information and data can be readily restored in the event of a loss is to perform regular data backups (Heathcote, 2000). Restoration is the process of retrieving deleted files from a data backup.

Businesses adopt different backup plans and procedures to ensure preparedness against disasters resulting from data losses. In his case study, Mulhauser, G. (2010) discusses backup techniques based on the backup media used, which refers to the physical or virtual devices where the backup data is stored, the kind of backups, how often they are performed, where they are stored, and how the backup process is automated.

An organization's backup plans are chosen after considering various aspects, including the organization's needs for data confidentiality, cost, storage capacity, usability, and backup media reliability.

2. Research Objectives

2.1 Main Objective

The main objective of this study is to analyze the data backup methods employed by staff at Herat University, evaluating their effectiveness and alignment with recognized best practices, in order to identify areas for improvement in data security and backup management.

2.2 Sub-Objectives

1. Identify the types of backup methods employed by staff.
2. Assess the frequency, reliability, and consistency of backups.

3. *Examine staff adherence to data backup best practices.*
4. *Investigate challenges in implementing effective data backup strategies.*
5. *Propose recommendations for improving backup practices and data security*

3. Research Questions

3.1 Main Research Question

What are the different data backup methods employed by staff at Herat University, and how effective are they in safeguarding critical information?

3.2 Sub-Questions

1. *What data backup methods are employed by staff at Herat University, and to what extent are they effective in ensuring data security and recovery?*
2. *How frequently do staff members back up their data?*
3. *What challenges do the staff at Herat University face in their data backup processes?*
4. *What challenges do staff face in their backup processes?*
5. *Is there a standardized backup policy followed by the staff at Herat University?*
6. *What storage media are predominantly used by the staff at Herat University for data backups?*
7. *How well do current data backup practices align with best practices for data security and recovery?*

4. Literature Review

4.1 Introduction

Data backup is a cornerstone of data security and management, safeguarding against loss or corruption. It is especially crucial in academic institutions like Herat University, where digital assets encompass sensitive administrative records, research outputs, and teaching resources. This section reviews existing literature on data backup methods and backup media and the challenges associated with their implementation, providing a theoretical framework for analyzing Herat University's practices.

4.2 Importance of Data Backup

Data backup refers to duplicating data to ensure recoverability in case of loss, corruption, or disaster. According to Cashman et al. (2008), data loss can stem from multiple factors, including hardware failures, software errors, human mistakes, or cyberattacks. Doyle (2001) emphasizes that data backup is not just a technical necessity but a strategic imperative, particularly for institutions reliant on computer-based information systems. Adequate backups not only mitigate risks but also ensure continuity of operations.

The volume of data generated daily in educational institutions—from student records to academic research—makes the development of robust backup policies essential. Kisaulu (2010) highlights the role of systematic backup strategies in disaster recovery planning. Similarly, Nyambura (2005) notes that organizations with inadequate backup systems face operational disruptions, financial losses, and reputational damage.

4.3 Backup Methods and Media

Backup methods vary based on the organization's needs, technological infrastructure, and resources. The three primary types of backups are complete, incremental, and differential (Backup4All, 2009):

1. **Full Backup:** This involves duplicating all selected data to ensure a complete recovery point. While reliable, full backups are time-intensive and require significant storage capacity.
2. **Incremental Backup:** Only data modified since the last backup is saved. This method is faster and requires less storage but may complicate recovery, as multiple backups must be restored sequentially.
3. **Differential Backup:** This method saves all changes since the last full backup, balancing storage efficiency and recovery speed.

Backup media plays a critical role in data protection, with choices ranging from local storage solutions like hard disks and magnetic tapes to modern cloud-based systems. Hutchinson and Sawyer (1994) categorize backup media into magnetic disks, optical disks, and network-based storage solutions:

- **Magnetic Disks and Tapes:** Magnetic media were traditionally popular due to their affordability and high storage capacity. However, they are prone to physical degradation and are less secure compared to modern alternatives (Stevens, 2007).

- **Optical Disks:** CDs and DVDs are durable and resistant to magnetic fields but offer limited storage capacity, making them unsuitable for large-scale backups (French, 1996).
- **Network-attached storage (NAS) and Storage Area Networks (SAN):** These systems offer centralized data storage and support automated backups. NAS devices are easy to deploy, while SANs provide high-speed connections for large organizations (George & Stair, 2008).
- **Cloud Storage:** Cloud platforms like Google Drive, OneDrive, and Dropbox enable automatic offsite backups, offering scalability, accessibility, and enhanced security. Rubenking (2001) notes that cloud backups are ideal for institutions lacking robust IT infrastructure.

4.4 Factors Influencing Backup Strategy Selection

Organizations consider multiple factors when selecting backup strategies, including reliability, cost, usability, and data security (Reynolds & Stair, 2008):

- **Reliability:** Backup systems must ensure data integrity over extended periods. Kendall and Kendall (2007) argue that reliable systems should withstand hardware failures and maintain data consistency.
- **Cost:** The affordability of backup systems, including hardware, software, and operational costs, often dictates the choice of media. Cloud solutions, while initially costlier, provide long-term savings through reduced maintenance requirements (McNamara, 2002).
- **Ease of Use:** User-friendly interfaces and automated scheduling simplify backup processes, minimizing human error. Automation tools like NovaStor reduce the burden on end-users (American University of Beirut, 2009).
- **Security:** Confidentiality during data transmission and storage is critical, particularly for sensitive academic records. Encryption and access controls are essential features of secure backup systems (Stevens, 2007).

4.5 Challenges in Backup Implementation

Despite the availability of diverse backup solutions, organizations face significant challenges in implementing effective systems. Common issues include:

1. **Volume of Data:** Increasing data generation strains existing storage systems. As organizations expand, their backup solutions must scale accordingly (Nyambura, 2005).
2. **System Downtimes:** Backup operations often consume significant computing resources, reducing system performance and causing delays (Bitpipe, 2009).
3. **Multiple Data Locations:** Data stored across different devices and platforms complicates the backup process. ICT professionals often struggle to identify critical backup data (Regan, 2004).
4. **Power Instability:** Unstable power conditions disrupt backup processes, particularly in resource-constrained environments like Afghanistan. Richards (2001) highlights the need for reliable infrastructure to support consistent backups.
5. **Lack of Policies:** Organizations without formal backup policies are vulnerable to inconsistent practices. Clear guidelines are essential for defining roles, responsibilities, and procedures (Stafford, 2005).

4.6 Backup Policies in Educational Institutions

Educational institutions, as custodians of valuable intellectual property and student data, must adopt comprehensive backup policies. These policies should specify:

- Backup frequency and retention periods.
- Roles and responsibilities of IT staff and end-users.
- Guidelines for selecting appropriate backup media and methods.

Kisaulu (2010) underscores the importance of institutional oversight in ensuring compliance with backup policies. Without centralized control, departments may adopt disparate practices, increasing the risk of data loss.

5. Methodology

5.1 Research Design

This study employs a mixed-methods approach, integrating quantitative and qualitative methods. To gather quantitative data, a structured questionnaire was distributed among 195 staff members, including professors and administrative

personnel. Additionally, relevant documents, such as existing backup policies and training materials, were analyzed to provide qualitative insights.

5.2 Participants

Participants were selected using stratified random sampling to ensure representation from various university departments. The questionnaire covered backup methods, frequency, challenges, and policy adherence.

5.3 Findings

The findings of this study provide a comprehensive assessment of the data backup methods employed by staff at Herat University, highlighting significant inconsistencies, challenges, and areas for improvement. Based on data collected through surveys and document analysis, the following key findings were identified:

1. Inconsistent Backup Practices Across Departments

The study revealed significant inconsistencies in backup practices among university departments. While 59% of respondents reported performing backups regularly, 41% admitted they did not. The frequency of backups also varied widely:

Table 1: Frequency of Data Backups Among University Departments

Frequency of Backup	Frequency	Percentage
Hourly	3	1.5%
Daily	11	5.6%
Weekly	23	11.8%
Monthly	77	39.5%
Annually	1	0.5%
When Changing Computers	1	0.5%
Quarterly	1	0.5%
No Regular Backup (Missing)	78	40.0%
Total	195	100.0%

The infrequency of backups poses a serious risk of data loss, especially for departments that handle mission-critical information.

2. Predominance of Local Storage Solutions

47.2% of respondents reported using hard disks as the most common storage medium for data backups. Cloud storage, which provides enhanced security and accessibility, was used by only 29.7%.

Table 2: Table: Preferred Backup Storage Media Among University Departments

Backup Storage Medium	Frequency	Percentage
Hard Disk	92	47.2%
USB	15	7.7%
CD-ROM	10	5.1%
Cloud Storage	58	29.7%
No Backup	20	10.3%
Total	195	100.0%

The reliance on hard disks exposes backups to hardware failures, theft, and physical damage. Additionally, 26.2% of respondents reported experiencing accidental physical destruction of their backup data.

3. Lack of Formalized Backup Policies

The absence of a formal backup policy across departments emerged as a significant issue. Only 25.6% of respondents reported having a specific data backup policy in their department. This lack of standardization has led to inconsistent practices and vulnerabilities.

Table 3: Table: Existence of Formal Backup Policies in University Departments

Existence of a Backup Policy	Frequency	Percentage
Yes	50	25.6%
No	67	34.4%

No Answer (Missing)	78	40.0%
Total	195	100.0%

4. Limited Use of Advanced Backup Methods

The study found that full backups were the most commonly used method (44.1%), followed by incremental backups (11.3%) and differential backups (4.6%).

Table 4: Types of Backup Methods Used in University Departments

Backup Methods	Frequency	Percentage
Full Backup	86	44.1%
Incremental Backup	22	11.3%
Differential Backup	9	4.6%
No Backup Reported	78	40.0%
Total	195	100.0%

Advanced methods like incremental and differential backups, which are more efficient for large-scale data management, were underutilized.

5. Lack of Regular Backup Evaluation

Regular evaluation of backups is critical to ensuring their reliability. However, the study found that only 44.6% of respondents evaluated their backups for accuracy, and evaluations were often irregular.

Table 5: Frequency of Backup Evaluation Among University Departments

Backup Evaluation	Frequency	Percentage
Monthly	29	14.9%
Annually	12	6.2%
Irregularly	47	24.1%
No Evaluation Performed	107	54.9%

Total	195	100.0%
--------------	-----	--------

The irregular evaluation of backups raises concerns about their reliability and data recoverability.

6. Decentralized Responsibility for Backups

Data backup responsibility was highly decentralized, with 42.1% of respondents managing backups independently. Only 12.8% of respondents indicated that backups were managed by the IT department.

Table 6: Responsibility for Data Backups in University Departments

Responsibility for Backups	Frequency	Percentage
Managed by the IT Department	25	12.8%
Independently by Staff	82	42.1%
External Personnel	8	4.1%
General Management of Faculty	1	0.5%
No Answer (Missing)	79	40.5%
Total	195	100.0%

This decentralized approach has led to inconsistencies in backup practices, reducing the overall reliability of the university's data management framework.

7. Challenges in Data Backup Implementation

Respondents highlighted several challenges that impede the effectiveness of backup practices:

Table 7: Perceived Challenges in Implementing Data Backup Practices

Challenges	Very Important	Important	No Opinion	Less Important	Unimportant
Volume of Data to Back Up	48.2%	36.9%	10.8%	4.1%	0%
Unstable Power	50.3%	29.2%	13.8%	6.0%	0.5%

Conditions					
Inadequate Knowledge of Backup Methods	37.9%	32.8%	23.6%	4.6%	1.0%
Lack of Clear Backup Policies	35.9%	32.8%	20.5%	7.2%	3.6%
System Performance Degradation	33.3%	38.5%	22.1%	5.1%	1.0%

Key challenges included:

- Unstable power conditions (50.3% rated as very important).
- Inadequate knowledge of backup methods (37.9% rated as very important).
- System performance issues during backups, affecting productivity.

8. Factors Influencing Backup Media Selection

Respondents rated several factors influencing their choice of backup media:

Table 8: Factors Influencing Selection of Backup Media

Factors	Very Important	Important	No Opinion	Less Important	Unimportant
Reliability	64.1%	28.7%	6.2%	1.0%	0%
Security	61.5%	22.6%	12.8%	2.6%	0.5%
Ease of Use	39.0%	46.7%	11.8%	1.5%	1.0%
Storage Capacity	40.5%	40.0%	15.4%	4.1%	0%
Cost	34.9%	33.3%	23.6%	5.1%	3.1%

Reliability (64.1%) and security (61.5%) were the most critical considerations, reflecting a strong preference for robust and secure backup solutions.

Summary of Findings

1. *Significant inconsistencies in backup frequency and methods across departments.*
2. *Predominance of local storage solutions, with limited use of cloud platforms.*
3. *Lack of formalized backup policies leading to fragmented practices.*
4. *Minimal use of advanced backup methods, such as incremental and differential backups.*
5. *Irregular evaluation of backups, raising concerns about their reliability.*
6. *Decentralized backup responsibilities, reducing oversight and standardization.*
7. *Key challenges include infrastructure limitations, lack of training, and unstable power conditions.*

These findings emphasize the need for Herat University to address its data backup challenges through formalized policies, centralized management, and the adoption of secure, modern technologies like cloud storage.

6.CONCLUSION:

In the digital age, where data is the backbone of institutional operations, effective data backup practices are critical for ensuring resilience and continuity. This study evaluated the data backup methods used by staff at Herat University and identified significant gaps in their implementation. The findings revealed inconsistencies in backup frequency, a predominant reliance on local storage solutions, and a lack of formalized policies. These factors collectively expose the university to risks of data loss, corruption, and operational disruptions.

While specific departments demonstrated good practices, the absence of a university-wide policy and the decentralized nature of backup responsibilities has led to fragmented approaches. The reliance on traditional storage media such as hard disks—used by 47.2% of respondents—poses risks related to hardware failures, physical damage, and theft. Additionally, the underutilization of cloud storage, adopted by only 29.7% of respondents, limits the institution's ability to leverage secure, scalable, and accessible solutions.

Challenges such as unstable power conditions, inadequate technical

knowledge among staff, and irregular backup evaluation further hinder the effectiveness of the university's backup strategies. Without a centralized and standardized framework, the current practices fail to ensure data integrity and recoverability, which is essential for an institution like Herat University, which relies heavily on digital assets for its academic and administrative functions.

Despite these challenges, this study provides a roadmap for overcoming them through targeted interventions, improved policies, and capacity building. Implementing the proposed recommendations will significantly enhance the university's ability to manage its digital resources effectively, reduce vulnerabilities, and ensure institutional resilience.

7. Recommendations

To address the challenges identified in this study, the following recommendations are proposed:

7.1 Develop and Implement a Comprehensive Backup Policy

A formalized, university-wide data backup policy is essential to standardize department practices. The policy should be defined as:

- Roles and responsibilities of IT staff and department heads.
- The frequency and types of backups (e.g., complete, incremental, differential).
- Approved storage media, including cloud-based solutions for critical data.
- Guidelines for data retention, testing, and evaluation to ensure recoverability.

7.2 Centralize Backup Responsibilities

The IT department should oversee and manage all backup operations to ensure consistency, security, and adherence to best practices. This centralized approach will:

- Reduce redundancies and inconsistencies across departments.
- Ensure regular and automated backups for all critical data.
- Allow for more efficient resource allocation and monitoring.

7.3 Promote the Use of Cloud-Based Storage

Cloud storage offers a scalable, secure, and reliable alternative to traditional storage methods. Herat University should:

- Transition to cloud platforms such as Google Drive, OneDrive, or institutional-level solutions for data backups.
- Provide training for staff on how to use cloud platforms securely.
- Establish agreements with cloud service providers to access cost-effective and scalable storage.

7.4 Conduct Regular Training and Awareness Programs

Inadequate technical knowledge among staff was a significant barrier to effective backup practices. Regular workshops should be organized to:

- Train staff on backup procedures, including automated backups and cloud storage usage.
- Enhance awareness of data security best practices and the importance of regular evaluations.
- Build technical capacity to handle evolving data management challenges.

7.5 Regular Backup Testing and Auditing

To ensure the reliability and integrity of backups, regular testing and auditing should be mandated. The IT department should:

- Conduct periodic evaluations to verify the accuracy and completeness of backups.
- Automated tools are used to monitor backup health and resolve errors promptly.
- Implement audits to ensure compliance with the backup policy.

7.6 Address Infrastructure Challenges

Unstable power conditions were highlighted as a critical issue. The university should:

- Invest in backup power solutions, such as uninterruptible power supply (UPS) systems, to support backup processes during outages.
- Explore hybrid solutions that combine local and cloud storage to mitigate risks associated with infrastructure limitations.

7.7 Optimize Cost-Effective Storage Solutions

Balancing cost and reliability is essential for sustainable data management. The university should:

- Prioritize critical data for cloud storage while using local storage for less sensitive data.
- Evaluate and adopt hybrid storage models that offer both affordability and reliability.

Final Thoughts

Herat University stands at a pivotal juncture in its data management journey. By addressing the gaps identified in this study and implementing the proposed recommendations, the university can establish a robust data backup framework that aligns with global best practices. Such a framework will safeguard the institution's digital assets, ensure operational continuity, and enhance its resilience against data-related disruptions.

Moreover, this study serves as a case for other higher education institutions facing similar challenges. By prioritizing data security and adopting innovative solutions, universities can protect their intellectual assets and maintain educational and administrative functions in an increasingly digital world.

8. Acknowledgment

We sincerely thank our co-authors, **Mr. Mostafa Olumee** and **Dr. Noor Ali Mohmand**, for their invaluable contributions, collaboration, and support throughout this research. Their insights and dedication significantly enhanced the quality of this study.

We also express our deep appreciation to the staff of **Herat University** for their participation and cooperation. Their valuable input was essential to the successful completion of this work.

8. Bibliography List:

1. The American University of Beirut. (2009). Backup strategies and tools. Retrieved from <http://www.aub.edu.lb/info/data-backup.html>
2. Backup4All. (2009). Backup types explained. Retrieved from <http://www.backup4all.com>
3. Bitpipe. (2009). Challenges in data backup. Retrieved from <http://www.bitpipe.com>

4. Cashman, T. J., & Shelly, G. B. (2008). *System design and analysis*. Boston, MA: Thomson Course Technology.
5. Doyle, S. (2001). *Information systems for you*. United Kingdom: Nelson Thornes.
6. French, C. (1996). *Introduction to information systems*. Boston, MA: McGraw-Hill.
7. George, W. R., & Stair, R. M. (2008). *Principles of information systems*. Boston, MA: Course Technology.
8. Hutchinson, S., & Sawyer, S. (1994). *Computers and information systems*. Burr Ridge, IL: Richard D. Irwin Inc.
9. Kisaulu, P. (2010). *A survey of computer data backup strategies adopted by firms on the Nairobi Stock Exchange*. University of Nairobi.
10. McNamara, K. (2002). *Data backup methods*. RadioOnline Magazine. Retrieved from <http://radiomagonline.com>
11. Nyambura, A. (2005). *A survey of ICT aspects of disaster recovery among companies quoted in the Nairobi Stock Exchange*. University of Nairobi.
12. Rubenking, N. (2001). *Online backup services*. PC Magazine. Retrieved from <http://www.pcmag.com>
13. Stafford, G. (2005). *Best practices in backup management*. Datamation. Retrieved from <http://itmanagement.earthweb.com>
14. Stevens, A. (2007). *Backup methods for small businesses*. Personal Computer World. Retrieved from <http://www.emeraldinsight.com>