JICN: Jurnal Intelek dan Cendikiawan Nusantara
https://jicnusantara.com/index.php/jicn
Vol : 3 No: 3, Juni - Juli 2026
E-ISSN : 3046-4560

Cybersecurity Challenges in Management Information Systems in the Hybrid Work Era

Tantangan Keamanan Siber dalam Sistem Informasi Manajemen di Era Kerja Hibrida

Rayyan Firdaus[1], Apni Gustiari Tanjung[2], Dea Lorenza[3]
Universitas Malikussaleh
Email: rayyan@unimal.ac.id[1] , apni.240420158@mhs.unimal.ac.id[2] , dea.240420143@mhs.unimal.ac.id[3]

Article Info

Article history :
Received : 18-07-2026
Revised : 20-07-2026
Accepted : 22-07-2026
Pulished : 24-07-2026

Abstrak

Penerapan model kerja hibrida memberikan fleksibilitas operasional yang tinggi bagi organisasi, tetapi di sisi lain, hal ini memperluas celah kerentanan dalam Sistem Informasi Manajemen (SIM). Studi ini bertujuan untuk mengidentifikasi tantangan keamanan siber utama yang dihadapi SIM di era kerja hibrida dan untuk merumuskan strategi mitigasi yang efektif. Dengan menggunakan pendekatan deskriptif kualitatif berdasarkan tinjauan pustaka, studi ini menemukan bahwa terkikisnya perimeter jaringan, penggunaan perangkat pribadi yang tidak aman (BYOD), dan meningkatnya serangan phishing merupakan ancaman siber yang paling dominan. Analisis menunjukkan bahwa model keamanan tradisional tidak lagi cukup untuk melindungi aset informasi perusahaan. Sebagai solusi, artikel ini merekomendasikan implementasi arsitektur Keamanan Zero Trust, aktivasi Otentikasi Multi-Faktor (MFA), enkripsi data ujung-ke-ujung, dan penguatan budaya sadar siber di antara karyawan. Implementasi strategi ini diharapkan dapat mempertahankan integritas SIM tanpa mengorbankan fleksibilitas kerja karyawan.

Kata kunci: Sistem Informasi Manajemen, Keamanan Siber, Kerja Hibrida

Abstract

The adoption of the hybrid work model provides high operational flexibility for organizations, but the other hand, it expands vulnerability gaps within Management Information Systems (MIS). This study aims to identify the main cybersecurity challenges faced by MIS in the hybrid work era and to formulate effective mitigation strategies. Using a qualitative descriptive approach based on a literature review, this study finds that the shattering of network perimeters, the insecure use of personal devices (BYOD), and the rise of phishing attacks are the most dominant cyber threats. The analysis indicates that traditional security models are no longer sufficient to protect corporate information assets. As a solution, this article recommends the implementation of a Zero Trust Security architecture, the activation of Multi-Factor Authentication (MFA), end-to-end data encryption, and the strengthening of a cyber-aware culture among employees. The implementation of these strategies is expected to maintain the integrity of MIS without sacrificing employee work flexibility.

Keywords: Management Information System, Cybersecurity, Hybrid Work

INTRODUCTION

The acceleration of digital transformation in the last two decades has transformed the Management Information System (SIM) from just an operational support tool to the main strategic instrument that determines the competitiveness of an organization. SIM serves as a driving force that integrates data from various lines of business, simplifies internal bureaucratic processes, and

provides a valid database for managers to make decisions quickly and accurately. However, the landscape of SIM utilization has undergone a very drastic paradigm shift after the COVID-19 pandemic, marked by the birth of the hybrid *work trend.*

The hybrid work model, which combines on-site and remote work, has now been massively adopted by various global corporations and government agencies in Indonesia. The flexibility offered has been proven to increase productivity, save operational costs, and improve employees' *work-life balance* . Nonetheless, this operational convenience holds a great latent risk from an information technology governance standpoint. When physical control over the network infrastructure is weakened, SIM security is in a very vulnerable position.

Before the hybrid era dominated, SIM security was relatively more predictable because it relied on a perimeter-based security approach. Company data is locked inside a local server or private cloud fenced by a firewall, where access is granted only to devices that are directly connected to the office's internal network. Currently, the perimeter boundary collapsed *(shattered perimeter).* Employees access the SIM through home Wi-Fi networks with minimal encryption, or even public networks in coffee shops that are prone to data interception. This phenomenon is exacerbated by the Bring Your Own Device (BYOD) policy, in which personal devices that do not have corporate standard protections are used to open confidential company documents.

This condition opens up a very wide exploitation gap for cybercrime perpetrators. Social engineering-based attacks such as phishing, malware infiltration, and ransomware threats that lock SIM databases are becoming more sophisticated and targeted. Based on the cyber threat landscape report, human *error* and weak access configurations are the main gateways for the majority of data leak incidents in remote work environments. The impact of this security system failure is not only in the form of financial losses due to operational shutdowns, but also damage to institutional reputations and potential lawsuits due to the leak of consumer data.

Given that SIM is the heart of the organization's information flow, maintaining the integrity, *availability*, and *confidentiality* of data in this hybrid era is no longer just a technical task for the IT team, but a strategic urgency for management. Various previous literature has extensively discussed cybersecurity in general or hybrid work flexibility separately. However, there is still a *research gap* on how the SIM architecture specifically should respond to vulnerabilities in this fragmented work environment.

Therefore, this article aims to in-depth dissect the cybersecurity challenges faced by SIM in the hybrid work era and formulate a mitigation strategy based on Zero Trust architecture to build a resilient and adaptive system.

RESEARCH METHODS

This study uses a qualitative descriptive approach with a literature review method. This approach was chosen to analyze, synthesize, and evaluate contemporary phenomena related to cybersecurity in Management Information Systems (SIM) in the hybrid work era, where the dynamics of threats and technology are changing very quickly.

The data collection process is carried out in a secondary manner through searching reputable scientific literature in journal databases such as Google Scholar, IEEE Xplore, ScienceDirect, and the national journal portal indexed SINTA. The keywords used in the search process include a

combination of terms: *"Management Information Systems", "Cybersecurity", "Hybrid Work", "Zero Trust Architecture",* and *"Management Information Systems Cybersecurity".*

To maintain the validity and relevance of the data, the literature inclusion criteria used are:

1. Journal articles, conference proceedings, or official industry reports published in the last five years (2021–2026).
2. The focus of the discussion centered on information technology vulnerabilities due to remote/hybrid work or information security architecture transformation.

The data analysis stage adopts an interactive analysis model, which includes four main steps:

1. Data Collection: Collect scientific articles and cyber research reports relevant to keywords.
2. Data Reduction: Selecting, filtering, and focusing raw data from the literature. Articles that only discuss hybrid work from the psychological side of employees or cyber hygiene in general without linking it to the SIM structure will be excluded.
3. Data Display: Organize the reduced data into a matrix of themes, such as challenge groups (perimeter, BYOD, phishing) and solution groups (MFA, Zero Trust, governance).
4. Draw Conclusions: Draw theoretical and practical conclusions regarding the best mitigation models that organizations can apply in securing their driver's licenses.

FINDINGS AND DISCUSSION

Based on the results of an analysis of various scientific literature and the latest cyber threat landscape reports, it was found that the transition to a hybrid work model radically changed the risk map in the organization's Management Information System (SIM). The discussion below dissects the findings into two main axes: the identification of critical vulnerability points and the formulation of an adaptive security architecture based on Zero Trust.

1. Deconstructing SIM Vulnerability Points in the Hybrid Work Era

   The integration of hybrid work forces driver's licenses to operate beyond the confines of traditional infrastructure. The results of the literature review show that there are three main challenge clusters that are most crucial:

   a. Collapse of Shattered Perimeter Protection

      In a conventional operating model, the SIM resides in an isolated environment protected by a strong physical and logical perimeter (firewall, intrusion detection system, and local access control). However, research shows that when access is opened from outside the office on a massive scale, this concept of "fortresses" collapses.

   b. The Complexity of the Bring Your Own Device (BYOD) Policy

      The use of personal devices to access SIM provides significant cost efficiencies for organizations, but creates a huge blind spot for information security administrators. In contrast to corporate-owned devices that can be monitored and configured centrally, personal devices (BYOD) generally:

2. Rarely do operating system updates (patching) periodically.
3. Lack of protection against advanced malware or ransomware.

4. Often shared by family members, increasing the risk of accidental data leaks.

When a laptop or personal phone that has been compromised by spyware enters the SIM network through a valid login session, hackers can perform an internal exploit (lateral movement) to infect the organization's main database.

c. Social Engineering and Human Error

No matter how powerful technology is, it still has a weak point in its loyal users. In a remote work environment, supervision weakens and communication between employees becomes fragmented. The psychological condition of employees who work in isolation is exploited by cybercriminals through highly targeted phishing attacks (spear-phishing).

Fake emails disguised as SIM system update notifications or urgent instructions from the board of directors often succeed in tricking employees into handing over their login credentials. Once a valid account belonging to an employee is successfully controlled (credential stuffing), the system cannot distinguish whether the data access activity is carried out by legitimate personnel or by an intruder.

5. MIS Security Architecture Mitigation and Reconstruction Strategy

To address the vulnerabilities inherent in hybrid work models, organizations can no longer simply update antivirus or renew firewall subscriptions. It is necessary to reposition the SIM security architecture towards a more proactive and dynamic model.

a. Implementation of Zero Trust Architecture (ZTA)

The main recommendation born from this analysis is the full adoption of the Zero Trust architecture as standardized by NIST SP 800-207. The fundamental principle of Zero Trust is to remove implicit trust based on geographic or network location.

Traditional Components	**Paradigma *Zero Trust***	**Impact on MIS**
Access Trust	Trust if you're in the office network.	Never believe, always verifying (anyone, anywhere)
Access Control	Once logged in, you are free to access any module.	Least *Privilege Access*
Device Validation	Only check usernames and passwords	Check the security posture of the device (whether the OS is up-to-date, malware-free)

Through Zero Trust, whenever a hybrid employee wants to open a payroll module or inventory data on a driver's license, the system will automatically verify the user's identity, check the security condition of the device, and limit access rights to only the data that is really needed to complete their task at the time juga.

b. Layered Authentication and Continuous Session Security

The use of conventional passwords should be upgraded to Multi-Factor Authentication (MFA), especially those based on dynamic or biometric tokens. If your

login credentials are leaked as a result of a phishing attack, the second layer of defense on MFA will block hackers' login attempts.

In addition, connection sessions from outside the office must be routed through a Virtual Private Network (VPN) corridor that implements end-to-end encryption, to ensure that the data flowing between the employee's device and the SIM server cannot be read by third parties.

c. Internalizing Cyber Aware Culture (Cyberpunctuation)

Technical mitigation must be in line with behavioral mitigation. Companies need to design regular cyber awareness training programs that are interactive, for example by simulating self-phishing attacks on hybrid employees. Education on the importance of securing home routers, recognizing anomalies in incoming emails, and quickly reporting incidents has been proven to drastically reduce the success rate of social engineering attacks.

CONCLUSION

The *hybrid work* paradigm has brought an inevitable transformation to modern organizational operations. On the one hand, this model provides high cost efficiency, scalability, and work flexibility for employees. But on the other hand, this flexibility brings logical consequences in the form of exponential security vulnerabilities in Management Information Systems (SIMs). The loss of traditional network perimeter boundaries, the rise of non-standardized use of personal devices (BYODs), and the increasing intensity of *social engineering attacks* such as *phishing* are clear evidence that conventional security models that rely on physical "fortresses" of the office are no longer relevant and adequate.

To deal with this dynamic threat landscape, organizations can no longer view cybersecurity as a technical cost *center,* but rather as a strategic investment pillar that determines business survival. The implementation of *the Zero Trust Security architecture* that carries the principle *of "never trust, always verify"* is an absolute solution. Through least privilege-based access control, the use of Multi-Factor Authentication (MFA), end-to-end data encryption, and real-time monitoring of network activity, organizations can build a resilient SIM ecosystem without sacrificing employee operational flexibility.

More than that, the success of this mitigation does not only rely on technological sophistication, but also on the synergy of three main elements: *people, process*, and *technology*. Companies are obliged to balance system updates with the continuous internalization of *cybersecurity awareness* for all elements of hybrid employees. Through a combination of adaptive technology infrastructure and human capital with good cybersecurity literacy, Management Information Systems will be able to transform into a digital foundation that is secure, trusted, and ready to face the complexity of cyber threats in the future.

REFERENCES

Dhillon, G., Smith, K., & D'Aubeterre, F. (2021). Information security governance in the cloud and hybrid work environments: Challenges and future directions. *Computers & Security*, 108, 102354.

Husein, M. F., & Wijaya, A. (2023). Tantangan Manajemen Keamanan Data pada Sistem Informasi Enterprise di Era Fleksibilitas Kerja. *Jurnal Tata Kelola Teknologi Informasi Nasional,* 5(2), 89-101.

Pratama, A. R., & Sutedja, I. (2021). Analisis Risiko Keamanan Informasi pada Tren Work From Home (WFH) Menggunakan Framework NIST SP 800-30. *Jurnal Sistem Informasi dan Teknologi Informasi,* 10(1), 45-56.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology.

Sari, W. P., & Utomo, R. B. (2022). Evaluasi Kesadaran Keamanan Siber Karyawan di Era Hybrid Working: Pendekatan Social Engineering. *Jurnal Manajemen Informasi,* 13(2), 112-125.