International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Fortifying the Mobile Frontier: An Adaptive Framework for Proactive Vulnerability Management in the Era of BYOD

Chika Lilian Onyagu [1,*] and Izunna Lucky Chibuike [2]

[1] *Department of Cybersecurity, Faculty of Computing, Delta State University, Abraka.*
[2] *Department of Cybersecurity, School of Physics, Engineering and Computer Science, University of Hertfordshire, College Lane Campus, UK.*

International Journal of Science and Research Archive, 2025, 16(02), 965-970

Publication history: Received on 07 July 2025; revised on 15 August; accepted on 18 August 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.2.2392

Abstract

Mobile devices are now central to personal and corporate digital ecosystems, yet traditional security strategies often fail to address their unique vulnerabilities. This study introduces the Adaptive Mobile Vulnerability Management Framework (AMVMF), a sector-tested model that integrates Mobile Device Management (MDM), real-time threat intelligence, and context-aware risk scoring into a continuous defense cycle. Using a mixed-methods approach, including a systematic literature review, multi-sector case studies (healthcare, finance, education), and expert validation via the Delphi method, we identified and mitigated both technical and human-centric risks. Results demonstrate notable improvements, including reduced vulnerability remediation times, increased patch adoption rates, and fewer security incidents such as mobile phishing. The AMVMF's layered approach bridges the gap between policy and execution, providing a scalable solution for securing mobile endpoints in both BYOD and corporate settings. By uniting automation, proactive monitoring, and context-driven prioritisation, this framework advances mobile cybersecurity resilience while maintaining operational flexibility.

Keywords: Mobile security; Vulnerability management; Mobile Device Management (MDM); BYOD security; Adaptive cybersecurity; Threat mitigation; Endpoint protection

1. Introduction

In just over a decade, mobile devices have transformed from convenient gadgets into the central hubs of our digital lives. Smartphones, tablets, and wearables are no longer just for communication; they are our banks, our offices, and our access points to critical services. With over 7.7 billion active mobile connections globally, these devices now drive corporate operations, handle sensitive financial transactions, and store a treasure trove of personal and professional data [1]. While this mobile revolution has unlocked incredible productivity, it has also created a formidable new frontline in the battle for cybersecurity.

The very features that make mobile devices so useful, their portability, constant connectivity, and integration of diverse applications, also make them inherently vulnerable. They operate on a patchwork of trusted and untrusted networks, blurring the lines between personal and corporate security, especially within "Bring Your Device" (BYOD) environments. This has created a dynamic and challenging threat landscape where cybercriminals deploy sophisticated attacks, from malicious apps and phishing schemes to firmware exploits and zero-day vulnerabilities [2]. In this new paradigm, simply reacting to threats is no longer a viable strategy; a proactive and continuous approach to managing vulnerabilities has become essential.

* Corresponding author: Chika Lilian Onyagu

Despite this clear and present danger, a significant gap exists. This strategy aims to bridge that gap. We critically examine the principles, processes, and technologies of vulnerability management as they apply specifically to mobile devices. Our work extends beyond theory to provide a practical and refined framework designed for real-world implementation. This paper will:

- Analyze the modern mobile threat landscape and its direct impact on vulnerability management.
- Assess the shortcomings of existing security models when applied to mobile contexts.
- Propose and validate an adaptive framework for identifying, assessing, mitigating, and monitoring mobile vulnerabilities effectively.

By synthesising insights from academic research, industry best practices, and real-world case studies, this paper offers actionable guidance for enhancing the resilience of our most ubiquitous digital tools.

2. Related Work

The conversation around mobile security is not new, but it has often been fragmented. Research typically falls into several key areas. Firstly, studies have focused on cataloguing the types of vulnerabilities affecting mobile devices. These are broadly categorised into hardware-level weaknesses, such as insecure chipsets [4]; software flaws, including unpatched operating system (OS) bugs or overly permissive applications [5]; and user-centric risks, like weak passwords or susceptibility to social engineering [2]. Reports consistently highlight that mobile endpoints are implicated in a majority of enterprise cyber incidents, cementing their status as a critical attack surface [1].

Secondly, the discipline of Vulnerability Management (VM) itself is well-established, defined by governing bodies like NIST as the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities [6]. Foundational standards such as the NIST Cybersecurity Framework and ISO/IEC 27001 provide excellent high-level guidance for creating information security management systems [6, 7]. However, their recommendations are often too general to be directly applied to the mobile world without significant adaptation. The unique challenges of mobile VM—such as fragmented OS update cycles (especially on Android), limited device resources, and user reluctance to apply patches-are frequently underexplored in these broader frameworks.

This points to a clear research gap, which this study directly addresses. Most prior work either zooms in on a single problem, like mobile malware detection, or applies a one-size-fits-all endpoint security model that ignores mobile-specific constraints like battery life, bandwidth, and user autonomy. There is a notable scarcity of empirical research evaluating holistic VM frameworks in live organizational settings. Our study seeks to close this gap by developing and testing a multi-layered, adaptive VM framework designed specifically for the complexities of corporate and high-risk mobile environments.

3. The Adaptive Mobile Vulnerability Management Framework (AMVMF)

To address the shortcomings of existing models, we developed the Adaptive Mobile Vulnerability Management Framework (AMVMF). This framework is not a static checklist but a dynamic, five-stage cycle designed to be integrated into an organization's existing security operations. It combines technological automation with procedural intelligence to create a resilient defence system.

3.1. Framework Overview

The AMVMF is built on a foundation of real-time intelligence and contextual awareness. At its core, the framework integrates Threat Intelligence Feeds from security vendors and open-source communities to stay ahead of emerging threats. This intelligence fuels Automated Vulnerability Scanning, which is woven directly into Mobile Device Management (MDM) platforms for continuous, non-disruptive endpoint assessment. A key innovation is its Context-Aware Risk Prioritization, an engine that scores vulnerabilities not just by their technical severity but by the context of the device, its user, and the data it accesses. Finally, Continuous Compliance Monitoring ensures all activities align with regulatory standards like GDPR, HIPAA, and PCI DSS.

3.2. Framework Components

- Stage 1. Discovery & Asset Inventory: effective security begins with complete visibility. You cannot protect what you cannot see. The AMVMF automates the discovery and cataloguing of every mobile endpoint connected to the network, including personal devices in a BYOD setup. This creates a living inventory that details each

device's type, OS version, installed apps, and firmware, eliminating the risk of "shadow IT." This granular map is the foundation for all subsequent security actions.

- Stage 2. Vulnerability Assessment: Once inventoried, devices undergo a comprehensive, two-pronged assessment. This combines static analysis (reviewing configurations, code, and permissions) with dynamic analysis (monitoring the device's behaviour in real-time) to detect both latent weaknesses and active signs of compromise. These assessments are scheduled automatically and triggered by events like major OS updates to minimize the exposure time for new flaws.
- Stage 3. Risk Scoring and Prioritisation: Not all vulnerabilities are created equal. The framework enhances the standard Common Vulnerability Scoring System (CVSS) [9] with business-specific context. For example, a medium-severity vulnerability on a C-suite executive's phone or a device used for financial processing would be elevated to a critical priority. This intelligent scoring allows security teams to focus their finite resources on the threats that pose the greatest actual risk to the organisation.
- Stage 4. Remediation Workflow: The framework employs a blended remediation strategy. High-risk, critical vulnerabilities trigger automated patch deployment via the MDM platform for immediate resolution. Lower-priority issues enter a managed workflow, allowing for review to prevent operational conflicts. If a patch cannot be immediately applied, the framework recommends or applies compensating controls, such as disabling a vulnerable service, to mitigate risk until a permanent fix is possible.
- Stage 5. Verification & Reporting: The cycle concludes but never truly ends. After remediation, automated scans verify that the patch was successful and the vulnerability is closed. This data feeds into dynamic dashboards, providing security teams and leadership with a real-time view of the organisation's security posture and compliance status. This continuous feedback loop ensures the VM process remains agile and responsive to the ever-changing threat landscape.

4. Materials and Methods

To develop and validate the AMVMF, we employed a mixed-methods research design to ensure both theoretical rigour and practical relevance.

- Research Design: Our approach consisted of three main components. First, we conducted a systematic literature review of 52 peer-reviewed articles, industry security reports, and conference proceedings published between 2019 and 2025. This provided a comprehensive understanding of the current state of mobile security. Second, we performed a multiple case study analysis of three organisations in distinct sectors: healthcare, finance, and education. These sectors were chosen for their diverse risk profiles and regulatory demands. Finally, the framework underwent model validation through a series of structured interviews with cybersecurity experts, who provided critical feedback on its design and applicability.
- Data Collection: Data were gathered through three parallel streams. For the literature review, we sourced materials from leading academic databases (Scopus, IEEE Xplore, ACM Digital Library) and trusted industry publications (e.g., Verizon, Gartner) to get a balanced view. For the case studies, we conducted semi-structured interviews with Chief Information Security Officers (CISOs) and IT managers to gain deep, contextual insights into their real-world challenges and successes. To validate the framework, we utilised the Delphi method with a panel of 10 senior security professionals, allowing for iterative refinement of the model based on expert consensus.
- Data Analysis: We analyzed the collected data using a combination of qualitative and quantitative techniques. Interview transcripts and literature findings were subjected to thematic analysis to identify recurring patterns, challenges, and best practices. On the quantitative side, we used the CVSS v3.1 scoring system to objectively rate vulnerabilities and measure the impact of remediation efforts. Finally, we performed a comparative analysis, mapping our framework's features against established models like the NIST Cybersecurity Framework and CIS Controls to highlight its unique contributions (as shown in Table 1).

Table 1 Comparative Analysis of AMVMF with Existing Vulnerability Management Models

Criteria	NIST Cybersecurity Framework (CSF)	CIS Controls	ISO/IEC 27001	Proposed AMVMF
Primary Focus	Broad cybersecurity risk management	Technical controls for IT security	Information security management systems (ISMS)	Mobile device vulnerability management with adaptive threat intelligence
Coverage of Mobile Devices	Limited, general guidance only	Partial, with mobile-specific controls	General mobile policy framework	Full integration of mobile OS, app, network, and user-behaviour vulnerabilities
Adaptability to Emerging Threats	Medium – relies on periodic updates	Medium – updated annually	Low–medium – requires formal revision cycle	High – AI-driven adaptive intelligence updates in near real time
Integration with MDM	Not directly specified	Suggested via device control policies	Possible via Annex A controls	Direct integration for automated device monitoring and patch deployment
Threat Intelligence Utilization	General recommendations	Minimal	Minimal	Embedded threat intelligence feeds with automated analysis
Scalability Across Device Types	High for enterprise IT, moderate for BYOD	Moderate	High	High – optimized for both enterprise and BYOD environments

5. Results

The application of the AMVMF in our case studies yielded significant, measurable improvements in security posture across all three sectors.

5.1. Case Study Findings

Healthcare: In the hospital environment, where mobile devices are critical for accessing patient records and coordinating care, the framework's impact was immediate. The average time to remediate a critical vulnerability plummeted from 14 days to just five. This drastic reduction in exposure time was primarily achieved through the automated vulnerability scanning and prioritized patch deployment, ensuring compliance with strict HIPAA regulations without disrupting clinical workflows.

Finance: The participating financial institution saw a 30% reduction in successful mobile phishing incidents. This was attributed to the framework's real-time threat intelligence feeds, which powered on-device security alerts. Employees were proactively warned of suspicious links and malicious app behaviours before they could compromise sensitive data. The centralized monitoring also allowed the security team to identify and neutralize coordinated phishing campaigns within hours.

Education: In the university setting, notorious for its sprawling and diverse IT environment, the framework produced a 45% improvement in patch adoption rates among faculty devices. The combination of automated reminders, simplified one-click update processes, and clear communication explaining the risks of non-compliance successfully overcame common user resistance. This strengthened the institution's defense against exploits targeting outdated software.

6. Discussion

The results from our case studies offer several powerful insights into what makes a vulnerability management program successful in a mobile-first world. They also highlight persistent challenges that technology alone cannot solve.

A key takeaway is that mobile-specific prioritization is paramount. Generic, severity-only scoring is inefficient. By adding business context, such as the user's role or the device's function, organizations were able to direct their efforts

far more effectively. This context-aware approach ensured that the highest-risk vulnerabilities were fixed first, delivering the greatest security return on investment.

However, the findings also underscored that the human element remains the weakest link. Technology can patch a software flaw, but it cannot fix a user who repeatedly ignores update prompts or grants excessive permissions to a questionable application. This confirms that even the most advanced technical framework must be paired with continuous, targeted user education. Training must evolve beyond annual cybersecurity slideshows and focus on mobile-specific threats and behaviours.

Furthermore, the study overwhelmingly validated the importance of automated patch deployment. The "attack window", the dangerous gap between when a vulnerability is disclosed and when it is patched, was dramatically shrunk through automation. Where manual patching was slow and inconsistent, automated deployment ensured swift and uniform protection across the entire mobile fleet, establishing a robust security baseline.

Despite these successes, implementing a framework like the AMVMF is not without its hurdles. BYOD policies introduce a thorny mix of security and privacy concerns. Organisations must navigate a legal and ethical tightrope when scanning personal devices, often requiring containerization solutions that separate work and personal data. This adds complexity and may not eliminate risk. Resource constraints are another major barrier, particularly for smaller organisations that may lack the budget or specialised staff to deploy and manage enterprise-grade MDM and security tools. Finally, OS fragmentation, especially within the Android ecosystem, remains a chronic challenge. The long and unpredictable delays between when Google releases a patch and when it reaches an end user's device create an unavoidable period of vulnerability that organisations must work to mitigate through other controls.

7. Conclusions

The digital landscape has become irreversibly mobile, and our security strategies must adapt or risk becoming obsolete. This study introduced and validated the Adaptive Mobile Vulnerability Management Framework (AMVMF), a holistic system designed to secure mobile endpoints against a dynamic threat landscape. Through real-world case studies, we demonstrated that an integrated approach, combining automated technical controls, real-time threat intelligence, and context-aware risk prioritisation, yields significant improvements in security posture. Our framework proved effective at reducing remediation times, lowering incident rates, and improving security compliance across diverse industries.

Ultimately, this work advocates for a fundamental shift in how we approach mobile security: from a reactive, fragmented posture to a proactive, continuous, and adaptive strategy. The challenges of BYOD, user resistance, and OS fragmentation are substantial, but they can be managed with a well-designed framework that balances security, privacy, and usability.

Future research should build on these findings by exploring the integration of predictive, AI-driven models for forecasting vulnerabilities and automating patch-testing. Expanding the framework's validation across a wider range of international regulatory environments and incorporating principles from zero-trust architecture would further enhance its robustness and applicability in an increasingly borderless digital world.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Verizon. (2024). *Mobile Security Index Report*. Verizon Enterprise Solutions.

[2] European Union Agency for Cybersecurity (ENISA). (2023). *Mobile Security: Threat Landscape*. ENISA Publications.

[3] Ali, M., Khan, S., & Hussain, R. (2022). Mobile device patch management challenges. *Journal of Cybersecurity Research, 8*(2), 45–59.

[4] Shah, P., & Kumar, R. (2023). Hardware security in mobile computing. *IEEE Access, 11*, 20456–20468.

[5] Zhou, Y., & Jiang, X. (2019). Dissecting Android Malware: Characterization and Evolution. *Proceedings of the IEEE Symposium on Security and Privacy*.

[6] National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*. NIST.

[7] International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection*. ISO.

[8] Gartner. (2024). *Global mobile device market analysis*. Gartner Research.

[9] Mell, P., & Scarfone, K. (2021). *The Common Vulnerability Scoring System (CVSS) v3.1*. FIRST.org.

[10] Dalkey, N., & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. *Management Science, 9*(3), 458–467.