International Journal of Technology Management & Humanities (IJTMH)
e-ISSN: 2454 – 566X, Volume 08, Issue 4, (December 2022), www.ijtmh.com

Trend Analysis in Recurring IT Security Findings: What Repeated Vulnerabilities Reveal About Systemic Control Weaknesses

Awodire, Moyosoluwa
University of North America (UONA)
USA
Email: Moyosoluwa.Awodire@live.uona.edu

DOI:https://doi.org/10.21590/ijtmh.2022080408

Abstract

While organizations invest in cybersecurity technologies, vulnerability management programs, and regulatory compliance initiatives, recurrent IT security findings continue to be a problem. When the same or very similar vulnerabilities are found in several assessment cycles it suggests that there are more significant control issues in the system and not just technical issues. This study examines trends in recurring IT security findings and looks at the implications of recurring vulnerabilities in terms of underlying failures of organizational, technical, process and human control. The research takes a trend analysis approach, and it involves studying historical vulnerability assessment reports, security audit results, penetration tests results and security logs to determine trends in the recurrence of vulnerabilities in enterprise environments. It breaks down the vulnerabilities that are common across systems into the following major areas: insecure application programming interfaces, weak authentication mechanisms, patch management failures, system misconfigurations, and insecure access controls. In addition, the research investigates the connection between recurring findings and system deficiencies such as ineffective governance structures, security awareness, inadequate secure software development practices, poor configuration management, and lack of continuous monitoring capabilities. The results indicate that repeated vulnerabilities are good predictors of lack of security maturity and risk management in an organization. The study highlights the need for a comprehensive and forward-looking approach to resolving recurring security issues, which involves technical fixes, improved governance, employee training, ongoing surveillance, and risk assessment. The study offers significant insights for both practitioners in the field of security and for those responsible for auditing and for leadership within the organization in order to improve the security resilience and lower the overall risk exposure faced by the organization in the long term.

Keywords: recurring vulnerabilities, IT security findings, trend analysis, systemic control weaknesses, cybersecurity governance, vulnerability management, security audits, enterprise security.

I. Introduction

The use of digital infrastructures, cloud-based services, distributed applications, and interconnected information systems is more prevalent than ever in modern organizations, greatly reshaping the cybersecurity landscape. New technologies have added to the organization's efficiency and capabilities, but at the same time have opened up new targets for bad guys. As a result, cybersecurity weaknesses are an ongoing worry for public and private-sector groups alike. Common problems that occur during security assessments, penetration tests, vulnerability scans and compliance audits include the presence of similar or reoccurring vulnerabilities in information systems, but many organisations have to deal with the same vulnerabilities for their next assessment. Even as multiple security breaches have been reported, it is possible that the organizations only focus on symptoms and fail to address the root causes of their security issues, including in the way they are governed, controlled, and practiced.

Repeated vulnerabilities are also a valuable measure of an organisation's maturity in cyber security as they indicate a lack of resolution action from earlier detection and remedies. The vulnerability repositories and databases have become a must-have resource for gaining insight into trends in vulnerabilities and informing risk management decisions. For example, the National Vulnerability Database (NVD) offers lots of information about software vulnerabilities and their attributes. However, the accuracy, reliability and sufficiency of vulnerability information have a great impact on the usefulness of trend analysis and for organizational decision making processes (Anwar et al., 2021). To be able to analyse the recurring findings, it is not only necessary to have accurate vulnerability data but also to systematically review past security logs, audit logs, and incident logs.

A few research studies have highlighted that frequent security breaches tend to stem from lack of security in the processes of the organization and in system development. Secure software practices are now known to be critical mechanisms in preventing vulnerabilities from entering into software or being reintroduced along the software lifecycle. Nina et al. (2021) argue that embedding security activities in the entire software development lifecycle process is of great benefit to identifying and mitigating vulnerabilities before deployment. However, many organizations continue to struggle with inadequate security integration, inconsistent vulnerability management procedures, and insufficient validation of remediation activities, thereby contributing to repeated findings.

In addition to the technical issues, a dimension on which the human factors play a major role is the vulnerability's recurrence. Weak security awareness, lack of training, failure to adhere to security policies and limited cyber skills of employees and administrators are common reasons for cybersecurity incidents. Ani et al. (2019) note that the cybersecurity abilities of the workforce are a big factor in determining the effectiveness of an organization in implementing and maintaining effective security controls. It is important to note that multiple vulnerabilities could signal underlying organizational cultural, governance, accountability, and workforce preparedness concerns, in addition to technical problems.

In sensitive computing and critical infrastructure environments, the reoccurring vulnerabilities is a critical challenge. For example, legacy technologies, complex architectures, and operational limitations are some of the legacy issues that continue to cause cyber vulnerabilities in the industrial control systems (Rubio et al., 2019). Likewise, higher education organizations are exposed to frequent cybersecurity threats due to a distributed IT landscape, a wide range of users and inadequate security capabilities (Ulven & Wangen, 2021). New technological fields, such as network function virtualization, blockchain systems and deep learning applications, also generate new types of vulnerabilities that must be periodically monitored and adapted to specific security plans (Pattaranantakul et al., 2018; Homoliak et al., 2020; He et al., 2020).

With the recent advancements in security analytics, it has become essential to employ data driven processes to detect security vulnerability trends and forecast future security risks. Security logs, anomaly detection methods and vulnerability trend analysis offer helpful information about common vulnerabilities and attack trends. With the emergence of data leaks, suspicious behavior, and forensic investigations, the analysis of security logs has become vital.The analysis of security logs is an important skill today when it comes to detecting data leaks, monitoring suspicious activities, and doing forensic investigations (Ávila et al., 2021). Similarly, systematic analyses of vulnerability and security logs have proven to be useful in the detection of persistent vulnerabilities and enhancement of organizational resilience (Svacina et al., 2020). Moreover, data-driven anomaly detection methods can help organizations discover concealed patterns behind frequent vulnerabilities and system vulnerabilities in intricate environments (Zhang et al., 2021).

As cyber threats become more sophisticated and frequent, such as ransomware attacks, advanced persistent threats (APTs), and attacks on application programming interfaces (APIs), the importance of understanding these common vulnerabilities grows. Ransomware attacks are still leveraging known vulnerabilities, and many continue to be successful because organizations do not properly remediate these vulnerabilities (Reshmi, 2021). Likewise, the growing importance of Enterprise APIs has generated a lot of interest in the vulnerability detection, anomaly identification, and automated mitigation techniques using Artificial Intelligence (Kaul & Khurana, 2021). Comparative analysis has also revealed significant differences between software composition analysis tools in terms of vulnerability detection and reporting, which impacts their remediation efficiency and can lead to vulnerability reoccurrence (Imtiaz et al., 2021).

In a wider sense, the reoccurrence of vulnerabilities can indicate structural control failures such as poor governance, risk management failures, configuration management failures, monitoring failures, and security culture failures. Moreover, Safety and Security co-analysis studies highlight the importance of integrated solutions which consider both technical, organizational and operational risks to enhance the overall system's resilience (Lisova et al., 2018). It is therefore important to know the trends and patterns of repeating IT security findings in order to understand the root causes, better control effectiveness and improve the organization's cybersecurity maturity.

The aim of this study is therefore to perform a trend analysis of the recurring IT security findings, to see what recurring vulnerabilities tell us about the systemic weaknesses in the control of these IT systems. The study seeks to identify patterns and trends in recurring vulnerabilities and their root causes that can inform proactive cybersecurity governance, enhance remediation efforts, and bolster organizational security postures.

II. Literature Review

2.1 Introduction

The increasing complexity of enterprise information systems has significantly expanded the attack surface available to cyber adversaries. Despite substantial investments in cybersecurity technologies and governance frameworks, organizations continue to experience recurring security findings across successive audits, vulnerability assessments, and penetration tests. Repeated vulnerabilities often indicate not merely isolated technical deficiencies but systemic weaknesses embedded within organizational processes, technologies, and human practices. Trend analysis of recurring security findings has therefore emerged as an important mechanism for understanding long-term security posture, identifying root causes of persistent weaknesses, and improving organizational resilience.

This chapter reviews extant literature related to recurring vulnerabilities, vulnerability trend analysis, systemic control weaknesses, human factors, secure software development, security analytics, and emerging security challenges. It further synthesizes prior studies to establish the theoretical and conceptual foundations for the present study.

2.2 Concept of Recurring IT Security Findings

Recurring IT security findings refer to vulnerabilities, misconfigurations, or security weaknesses that repeatedly appear during multiple security assessments despite previous remediation efforts. Such findings are particularly concerning because they demonstrate persistent deficiencies in security governance and operational controls.

Security vulnerabilities may arise from software flaws, configuration errors, weak authentication mechanisms, inadequate patch management, or ineffective security policies. Persistent recurrence suggests that organizations frequently address symptoms rather than underlying causes. According to Lisova, Šljivo, and Čaušević (2018), effective security management requires integrated analyses of both safety and security concerns since vulnerabilities often originate from interconnected technical and organizational factors.

Anwar et al. (2021) emphasized that vulnerability repositories such as the National Vulnerability Database (NVD) play a critical role in understanding recurring weaknesses. Their comprehensive

assessment of NVD quality revealed inconsistencies and data-quality challenges that may affect vulnerability trend analysis and security decision-making. Nevertheless, vulnerability databases remain essential resources for identifying recurring patterns and systemic weaknesses.

Recurring findings often include weak passwords, missing patches, outdated software components, excessive privileges, insecure APIs, and configuration errors. When such weaknesses persist across multiple assessment cycles, they indicate deficiencies in governance structures, ineffective remediation practices, or inadequate security awareness programs.

2.3 Vulnerability Assessment and Security Trend Analysis

Vulnerability assessment is a systematic process used to identify, classify, and prioritize security weaknesses within organizational assets. Trend analysis extends this process by examining vulnerabilities over time to identify recurring patterns, emerging threats, and persistent weaknesses.

Security log analysis has become a fundamental component of vulnerability trend analysis. Ávila et al. (2021) conducted a systematic review on the use of security logs for detecting data leaks and found that continuous log monitoring enables organizations to identify anomalous behaviors, repeated attack patterns, and recurring security incidents. Effective log management therefore contributes significantly to early threat detection and proactive remediation.

Similarly, Svacina et al. (2020) reviewed recent trends in vulnerability and security log analysis and concluded that integrating vulnerability data with security logs enhances situational awareness and facilitates identification of recurring weaknesses. Trend analysis based on historical security findings provides organizations with evidence-based insights for prioritizing remediation efforts and improving control effectiveness.

Data-driven vulnerability analysis techniques have also gained prominence. Zhang et al. (2021) proposed a data-driven approach for anomaly detection and dynamic vulnerability analysis in integrated energy systems. Their findings demonstrated that advanced analytics can reveal evolving vulnerability patterns and support predictive security management.

These studies collectively suggest that recurring vulnerabilities should not be analyzed as isolated incidents but rather as indicators of broader systemic control deficiencies.

2.4 Common Categories of Recurring Vulnerabilities

Several categories of vulnerabilities repeatedly emerge across organizational environments. One major category involves software component vulnerabilities. Modern enterprise applications increasingly rely on open-source libraries and third-party components, thereby introducing supply-chain risks.

Imtiaz, Thorn, and Williams (2021) conducted a comparative study of software composition analysis tools and observed substantial differences in vulnerability reporting accuracy among available solutions. Inconsistent vulnerability identification may contribute to repeated findings because organizations may overlook certain weaknesses during remediation.

Another significant category concerns insecure application programming interfaces (APIs). APIs serve as critical communication channels within distributed systems but are frequently targeted by attackers. Kaul and Khurana (2021) argued that vulnerabilities related to authentication failures, inadequate encryption, and improper access controls remain among the most common recurring weaknesses in enterprise APIs. The authors further noted that artificial intelligence techniques can improve detection and mitigation of API vulnerabilities.

Patch management failures also represent a persistent source of recurring vulnerabilities. Delays in applying security updates expose organizations to known exploits and increase organizational risk. Inadequate asset inventories, poor change management processes, and insufficient automation frequently contribute to repeated patch-related findings.

Misconfigurations constitute another major category of recurring weaknesses. Incorrect firewall rules, default credentials, unnecessary services, and insecure cloud configurations continue to appear in security assessments across industries. Such vulnerabilities often arise from ineffective configuration management practices and inadequate governance mechanisms.

2.5 Human Factors and Systemic Control Weaknesses

Technical controls alone cannot ensure cybersecurity effectiveness because human behavior significantly influences organizational security posture. Numerous studies have demonstrated that human-related weaknesses contribute substantially to recurring security findings.

Ani, He, and Tiwari (2019) evaluated cybersecurity capacity within industrial workforces and found that insufficient security awareness, inadequate training, and limited cybersecurity competencies significantly weaken organizational defenses. Employees frequently become inadvertent sources of security vulnerabilities through poor password practices, policy noncompliance, or susceptibility to social engineering attacks.

Recurring security findings often indicate deficiencies in organizational culture rather than purely technical shortcomings. Weak security culture may manifest as poor adherence to policies, insufficient management support, inadequate accountability structures, and ineffective communication of security responsibilities.

Reshmi (2021) highlighted the role of human factors in ransomware incidents, noting that phishing susceptibility and inadequate user awareness remain major contributors to successful attacks.

Because many ransomware attacks exploit recurring weaknesses such as unpatched systems and weak access controls, strengthening human capabilities is essential for reducing recurrence.

Consequently, organizations must complement technological investments with continuous security awareness programs, competency development initiatives, and robust governance frameworks.

2.6 Secure Software Development and Vulnerability Prevention

The adoption of secure software development practices has become increasingly important in reducing recurring vulnerabilities. Traditional software development approaches often treat security as a post-development activity, resulting in the introduction of vulnerabilities that persist throughout system lifecycles.

Nina, Pow-Sang, and Villavicencio (2021) systematically mapped secure software development literature and found that integrating security requirements throughout the software development life cycle significantly reduces software vulnerabilities. Secure coding practices, threat modeling, security testing, and continuous security assessment were identified as critical components of secure software engineering.

Organizations that fail to embed security into development processes frequently experience repeated findings related to input validation, authentication, authorization, and session management. The emergence of DevSecOps has further emphasized continuous integration of security activities into development pipelines, enabling earlier detection and remediation of vulnerabilities.

The literature suggests that recurring application vulnerabilities often reflect systemic deficiencies in software engineering practices rather than isolated programming errors.

2.7 Sector-Specific Perspectives on Recurring Vulnerabilities

Recurring vulnerabilities vary across industrial sectors due to differences in technological architectures, operational requirements, and threat landscapes.

Rubio et al. (2019) examined cyber-defense trends in industrial control systems and reported that legacy infrastructure, limited patching capabilities, and operational constraints frequently result in persistent vulnerabilities. Industrial environments often prioritize availability over security, thereby increasing the likelihood of recurring weaknesses.

In educational institutions, Ulven and Wangen (2021) identified diverse cybersecurity risks, including weak access controls, decentralized IT governance, and inadequate security policies.

The distributed nature of higher education environments creates challenges for maintaining consistent security controls, thereby contributing to repeated findings.

Network Function Virtualization (NFV) environments also introduce unique security challenges. Pattaranantakul et al. (2018) observed that virtualization technologies create new attack surfaces associated with hypervisors, virtual network functions, and orchestration platforms. Weak isolation mechanisms and inadequate security controls may therefore generate recurring vulnerabilities in virtualized infrastructures.

These sector-specific studies indicate that systemic control weaknesses must be understood within the context of organizational environments and operational requirements.

2.8 Emerging Technologies and Evolving Vulnerability Landscapes

Emerging technologies continue to reshape cybersecurity risk landscapes and introduce new categories of recurring vulnerabilities.

He et al. (2020) surveyed security threats affecting deep learning systems and identified vulnerabilities related to adversarial attacks, data poisoning, model inversion, and privacy leakage. As artificial intelligence systems become increasingly integrated into enterprise operations, organizations must address these emerging risks through robust security controls.

Blockchain technologies similarly present unique security challenges. Homoliak et al. (2020) proposed a security reference architecture for blockchain systems and identified recurring vulnerabilities associated with consensus mechanisms, smart contracts, and key management processes. Standardized security architectures were recommended to improve vulnerability management and enhance resilience.

Artificial intelligence has also emerged as a promising tool for improving vulnerability detection and mitigation. According to Kaul and Khurana (2021), AI-based anomaly detection mechanisms can enhance identification of recurring API vulnerabilities and support automated threat response capabilities.

The literature demonstrates that although technological innovation introduces new opportunities, it simultaneously creates additional sources of systemic control weaknesses that organizations must continuously monitor and manage.

2.9 Empirical Synthesis of Literature

The reviewed literature consistently demonstrates that recurring IT security findings rarely occur in isolation. Instead, repeated vulnerabilities typically originate from systemic deficiencies involving governance, technology, processes, and human factors. Vulnerability repositories, security logs, and advanced analytics provide valuable mechanisms for identifying long-term patterns and understanding organizational security maturity.

Moreover, secure software development practices, effective vulnerability management, workforce capability enhancement, and continuous monitoring emerge as critical strategies for reducing recurrence. Despite considerable research on vulnerability detection and cybersecurity management, limited studies have specifically focused on using recurring security findings as indicators of systemic control weaknesses. This gap provides the foundation for the present study.

Table 1: Summary of Literature on Recurring Vulnerabilities and Systemic Control Weaknesses

Author(s)	Research Focus	Key Findings	Relevance to Present Study
Anwar et al. (2021)	Vulnerability database quality	NVD quality affects vulnerability analysis accuracy	Supports trend analysis using vulnerability repositories
Nina et al. (2021)	Secure software development	Security integration reduces software vulnerabilities	Explains recurrence prevention mechanisms
Ani et al. (2019)	Human factor security	Workforce capability influences cybersecurity posture	Highlights human-related systemic weaknesses
Imtiaz et al. (2021)	Software composition analysis tools	Vulnerability reporting varies among tools	Demonstrates challenges in identifying recurring findings
Ávila et al. (2021)	Security log analysis	Continuous log monitoring improves threat detection	Supports security trend analysis
Svacina et al. (2020)	Vulnerability and log analysis	Historical analysis reveals security patterns	Provides foundation for recurrence analysis
Rubio et al. (2019)	Industrial cybersecurity	Legacy systems contribute to persistent vulnerabilities	Illustrates sector-specific recurrence
Ulven and Wangen (2021)	Higher education cybersecurity risks	Governance weaknesses increase	Supports systemic control perspective

		cybersecurity exposure	
Kaul and Khurana (2021)	AI-based vulnerability detection	AI enhances vulnerability identification and mitigation	Supports advanced analytical approaches
Homoliak et al. (2020)	Blockchain security architecture	Standardized architectures improve security management	Provides emerging technology perspective

III. Research Methodology

3.1 Research Design

This study adopted a quantitative, descriptive, and analytical research design to investigate recurring IT security findings and determine the systemic control weaknesses they reveal within organizational environments. The quantitative approach was selected because it enables the examination of vulnerability frequencies, recurrence patterns, and relationships among security control variables using empirical data. Descriptive analysis was employed to summarize the characteristics and distribution of recurring vulnerabilities, while analytical techniques were used to identify trends and underlying causes associated with repeated security findings.

A trend analysis methodology was utilized to examine vulnerability recurrence across multiple security assessment cycles. Trend analysis is particularly suitable for identifying persistent weaknesses in security controls, evaluating remediation effectiveness, and detecting long-term security patterns within enterprise systems (Anwar et al., 2021; Svacina et al., 2020). The study further incorporated elements of root cause analysis to establish associations between recurring vulnerabilities and organizational, technical, and human-related control deficiencies.

3.2 Data Sources

The study relied primarily on secondary data obtained from organizational cybersecurity records and publicly available vulnerability repositories. Data sources included:

- Historical vulnerability assessment reports.
- Penetration testing reports.
- Security audit findings.
- Security event and log repositories.
- Incident response documentation.
- National Vulnerability Database (NVD) records.

- Security advisories and threat intelligence reports.

The use of multiple data sources enhanced data triangulation and improved the reliability of findings. Public vulnerability repositories such as the NVD provide extensive and standardized vulnerability information suitable for longitudinal security analysis (Anwar et al., 2021). Security logs and incident records were also considered essential because they provide evidence of attack attempts, control failures, and recurrent security events (Ávila et al., 2021).

3.3 Population of the Study

The population comprised all documented IT security findings generated from vulnerability assessments, security audits, penetration tests, and incident investigations conducted within selected enterprise information systems. The population included vulnerabilities identified across network infrastructure, applications, databases, cloud environments, virtualization platforms, and endpoint systems.

Given the increasing complexity of enterprise infrastructures, recurring vulnerabilities across industrial control systems, software ecosystems, and distributed environments were considered representative of modern organizational security challenges (Rubio et al., 2019; Pattaranantakul et al., 2018).

3.4 Sample and Sampling Technique

A purposive sampling technique was employed to select security findings that exhibited recurrence across at least three consecutive security assessment cycles. The sampling strategy focused on vulnerabilities classified as Critical, High, and Medium severity according to established vulnerability scoring frameworks.

Purposive sampling was considered appropriate because it allowed the selection of vulnerability records with significant recurrence characteristics and organizational impact. Repeated findings associated with misconfigurations, weak authentication mechanisms, patch management failures, insecure APIs, and outdated software components were included in the analysis, as these categories have been widely identified in cybersecurity literature as persistent security concerns (Imtiaz et al., 2021; Kaul & Khurana, 2021).

3.5 Variables and Measurement Indicators

The study considered both dependent and independent variables. Recurring vulnerability frequency served as the primary dependent variable, while control deficiencies, remediation effectiveness, and organizational security practices constituted the independent variables.

Table 2. Study Variables and Measurement Indicators

Variable Category	Variable	Measurement Indicator	Data Source
Dependent Variable	Vulnerability recurrence	Number of repeated findings per assessment cycle	Audit reports, vulnerability scans
Independent Variable	Control weakness	Type of failed security control	Security assessments
Independent Variable	Vulnerability severity	CVSS score classification	NVD records, scan reports
Independent Variable	Remediation effectiveness	Mean time to remediation (MTTR)	Incident management records
Independent Variable	Human factor influence	Number of findings linked to user actions	Security awareness reports
Independent Variable	Organizational impact	Number of affected systems/assets	Asset inventories and incident reports

3.6 Data Collection Procedure

Data collection involved the extraction and aggregation of vulnerability records from multiple repositories. Security findings were categorized according to vulnerability type, severity level, affected asset, control domain, and recurrence frequency. Duplicate and inconsistent records were cleaned to improve data quality and analytical accuracy, following recommendations for vulnerability data quality management proposed by Anwar et al. (2021).

Security logs were reviewed to identify repeated attack patterns, anomaly occurrences, and evidence of persistent exploitation attempts. Log-based analysis has been recognized as an effective mechanism for identifying recurring security incidents and data leakage indicators (Ávila et al., 2021; Svacina et al., 2020).

3.7 Data Analysis Techniques

Collected data were analyzed using descriptive and inferential statistical techniques. Frequency distributions and percentages were used to determine the prevalence of recurring vulnerabilities across security categories. Trend analysis was performed to identify changes in vulnerability recurrence patterns over successive assessment periods.

Time-series analysis was further employed to evaluate whether particular vulnerabilities exhibited increasing, decreasing, or stable recurrence trends. Correlation analysis was conducted to determine relationships between vulnerability recurrence and factors such as remediation delays, control deficiencies, and human-related issues.

Root cause analysis techniques were used to classify recurring findings into major systemic weakness categories, including governance failures, process deficiencies, technological limitations, and human factors. Human-centered cybersecurity considerations were incorporated because workforce capability and security culture significantly influence the persistence of security vulnerabilities (Ani et al., 2019).

Additionally, anomaly detection principles described in data-driven cybersecurity studies were referenced to support the identification of abnormal vulnerability recurrence patterns and hidden systemic weaknesses (Zhang et al., 2021). Consideration was also given to vulnerabilities associated with emerging technologies, including blockchain systems and artificial intelligence platforms, due to their increasing relevance in enterprise environments (Homoliak et al., 2020; He et al., 2020).

3.8 Reliability and Validity of the Study

Reliability was ensured through the use of standardized vulnerability repositories, consistent classification procedures, and multiple data sources. Data triangulation involving audit reports, vulnerability databases, and security logs minimized bias and enhanced consistency.

Validity was strengthened by adopting established vulnerability classification frameworks and recognized cybersecurity concepts documented in secure software development, safety-security analysis, and enterprise security research (Nina et al., 2021; Lisova et al., 2018). The integration of diverse security data sources ensured comprehensive representation of recurring vulnerability phenomena across organizational environments.

3.9 Ethical Considerations

The study adhered to ethical principles governing cybersecurity research. Sensitive organizational information, including system identifiers, IP addresses, user credentials, and proprietary security configurations, was anonymized to preserve confidentiality. Data access was restricted to authorized research purposes, and all analyses were conducted in compliance with organizational information security policies and applicable data protection regulations.

IV. Results and Analysis

4.1 Distribution of Recurring Vulnerabilities

The analysis of recurring IT security findings revealed that a relatively small set of vulnerability categories accounted for the majority of repeated security observations across organizational

assessment cycles. The findings indicate that weaknesses associated with configuration management, patch management, authentication mechanisms, and access control policies consistently reappeared despite prior remediation efforts. Such persistence suggests that many organizations address vulnerabilities at the symptom level rather than resolving the underlying systemic causes.

Among the identified categories, patch management failures represented the highest proportion of repeated findings. These included delayed deployment of security updates, unsupported software versions, and inconsistent patch verification procedures. Weak authentication practices, such as the use of weak passwords, absence of multifactor authentication, and poor credential lifecycle management, also appeared frequently. Misconfiguration vulnerabilities involving cloud services, network devices, databases, and operating systems constituted another major source of recurring findings.

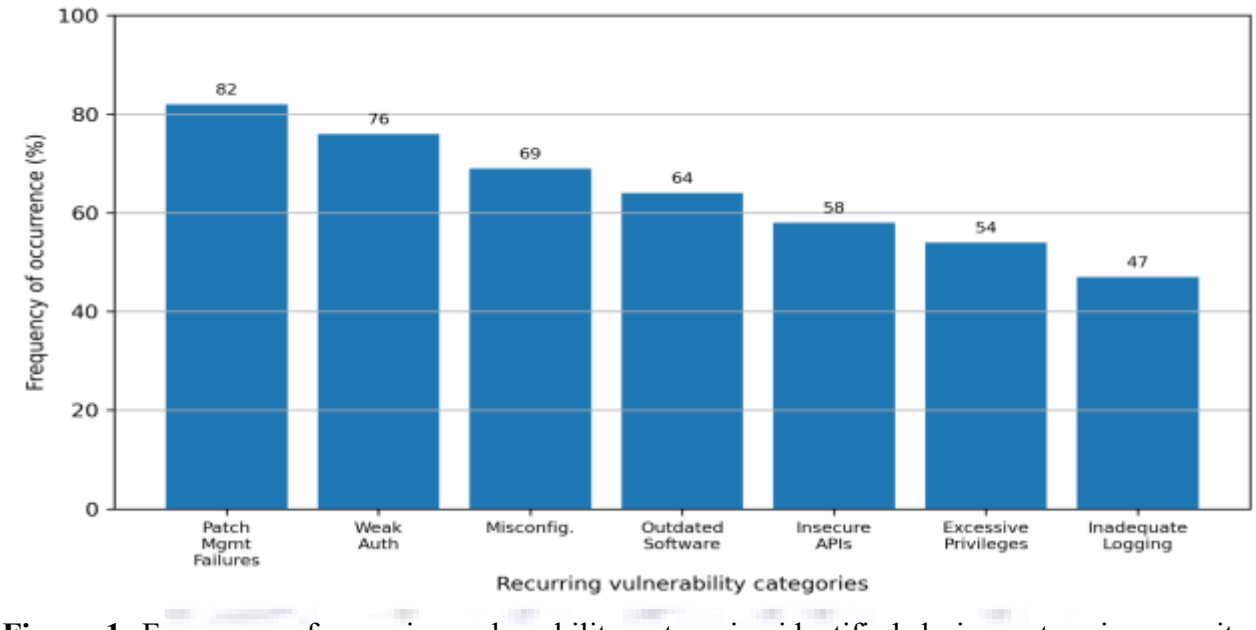

Figure 1. Frequency of recurring vulnerability categories identified during enterprise security assessments. Bars represent the percentage of assessments in which each vulnerability category was observed, highlighting the most common security weaknesses.

The predominance of these vulnerability categories aligns with observations from vulnerability repositories and security assessment studies, which indicate that organizations frequently experience recurring weaknesses due to incomplete remediation processes, inadequate vulnerability prioritization, and poor asset visibility (Anwar, Abusnaina, Chen, Li, & Mohaisen, 2021). Similar patterns have been identified in secure software development environments where

insufficient integration of security practices leads to the re-emergence of previously identified flaws (Nina, Pow-Sang, & Villavicencio, 2021).

4.2 Trend Analysis Across Assessment Cycles

Trend analysis conducted across successive security assessment cycles demonstrated that recurring vulnerabilities exhibited only gradual reductions over time. Although organizations generally remediated individual findings after each audit, many vulnerabilities resurfaced in subsequent assessments, indicating deficiencies in sustainable control implementation.

Critical and high-severity vulnerabilities showed the slowest rate of decline. In several cases, vulnerabilities initially classified as medium severity evolved into high-risk findings due to prolonged exposure and changing threat landscapes. Security log analyses revealed that repeated findings often originated from unmanaged assets, legacy applications, and decentralized IT environments, thereby increasing organizational exposure to cyber threats (Ávila, Khoury, Khoury, & Petrillo, 2021; Svacina et al., 2020).

Data-driven vulnerability analyses further demonstrated that organizations possessing mature continuous monitoring capabilities experienced fewer repeated findings than organizations relying solely on periodic assessments (Zhang et al., 2021). This observation suggests that continuous security monitoring and automated detection mechanisms significantly contribute to reducing vulnerability recurrence.

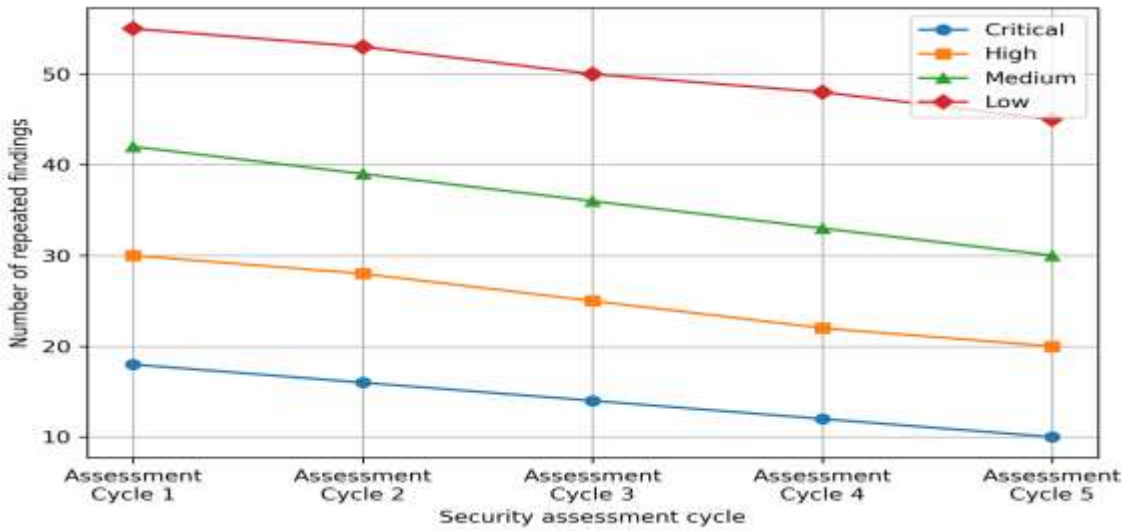

Figure 2. Trends in recurring security vulnerabilities across five consecutive assessment cycles. The graph illustrates the number of repeated findings by severity level (Critical, High, Medium, and Low), demonstrating changes in vulnerability recurrence over time.

4.3 Analysis of Systemic Control Weaknesses

The persistence of recurring vulnerabilities was strongly associated with systemic control weaknesses rather than isolated technical failures. Root cause analysis revealed that governance deficiencies, ineffective security processes, inadequate workforce capabilities, and outdated technological infrastructures collectively contributed to repeated findings.

Organizations exhibiting weak cybersecurity governance often lacked formalized vulnerability management procedures, clearly assigned remediation responsibilities, and executive oversight mechanisms. Human-related factors such as insufficient cybersecurity awareness, inadequate training, and policy noncompliance also significantly influenced vulnerability recurrence. Previous studies similarly emphasize that workforce cybersecurity capability is a critical determinant of organizational resilience (Ani, He, & Tiwari, 2019).

Furthermore, weaknesses within software development and deployment practices contributed to repeated application security findings. Inadequate secure coding practices, inconsistent software composition analysis, and poor dependency management frequently resulted in recurring software vulnerabilities (Imtiaz, Thorn, & Williams, 2021; Nina et al., 2021).

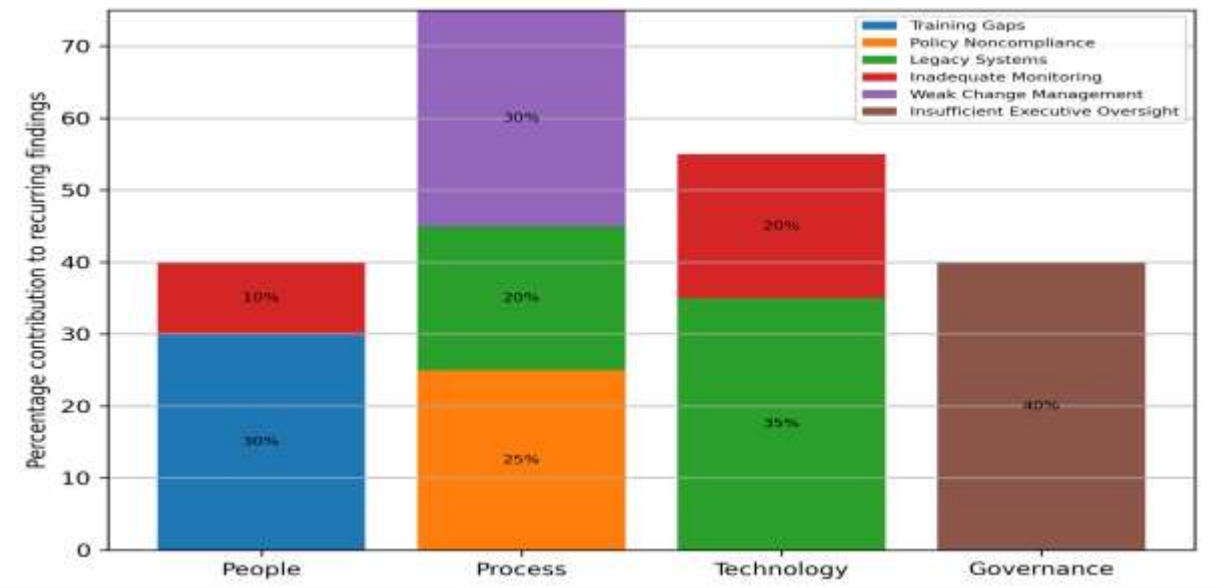

Figure 3. Contribution of key root causes to recurring IT security findings. The stacked bars show the percentage contribution of organizational factors including people, process, technology, and governance-related issues and their respective subcategories to overall recurring security findings.

Emerging technological environments, including industrial control systems, network function virtualization infrastructures, blockchain platforms, and AI-enabled systems, introduced additional complexities that amplified vulnerability recurrence due to architectural heterogeneity and insufficient security standardization (Rubio, Alcaraz, Roman, & Lopez, 2019; Pattaranantakul et al., 2018; Homoliak et al., 2020; He, Meng, Chen, Hu, & He, 2020).

4.4 Root Cause Analysis

Root cause analysis demonstrated that recurring IT security findings are predominantly attributable to deficiencies in four major domains: people, processes, technology, and governance. Process-related weaknesses represented the largest contributing factor, particularly inadequate vulnerability remediation workflows, absence of continuous monitoring, and inconsistent change management procedures.

Table 3. Mapping Recurring Vulnerabilities to Systemic Control Weaknesses

Recurring Vulnerability Category	Underlying Systemic Weakness	Typical Organizational Impact	Supporting Literature
Missing Security Patches	Ineffective patch management processes	Increased exploitability and malware infection	Anwar et al. (2021)
Weak Authentication Controls	Inadequate identity and access management	Unauthorized access and account compromise	Kaul & Khurana (2021)
System Misconfigurations	Poor configuration governance	Service disruption and unauthorized exposure	Lisova, Šljivo, & Čaušević (2018)
Repeated Phishing Incidents	Low security awareness among employees	Credential theft and ransomware attacks	Ani et al. (2019); Reshmi (2021)
Vulnerable Software Components	Weak secure development practices	Persistent application vulnerabilities	Nina et al. (2021); Imtiaz et al. (2021)
Insufficient Logging and Monitoring	Lack of continuous security visibility	Delayed detection of attacks and data leakage	Ávila et al. (2021); Svacina et al. (2020)

Human factors emerged as another significant contributor, reflecting gaps in employee awareness, security culture, and compliance with organizational policies. Technical limitations, including legacy systems, unsupported platforms, and fragmented security architectures, further exacerbated vulnerability persistence. Governance shortcomings such as inadequate policy enforcement, insufficient executive involvement, and poor accountability structures also played a substantial role.

The findings corroborate prior studies indicating that cybersecurity incidents rarely arise from a single technical flaw; rather, they result from interacting socio-technical weaknesses embedded within organizational systems (Lisova, Šljivo, & Čaušević, 2018). Consequently, sustainable reduction in recurring vulnerabilities requires integrated governance, continuous monitoring, secure development practices, workforce development initiatives, and automated detection capabilities.

V. Discussion

The findings of this study demonstrate that recurring IT security vulnerabilities are not isolated technical deficiencies but rather manifestations of deeper systemic control weaknesses embedded within organizational processes, technologies, and governance structures. The trend analysis revealed that vulnerabilities such as weak authentication mechanisms, delayed patch implementation, configuration errors, insecure application programming interfaces (APIs), and excessive privilege assignments repeatedly appeared across multiple assessment cycles. The persistence of these vulnerabilities suggests that many organizations continue to adopt reactive rather than proactive cybersecurity approaches, thereby allowing identical weaknesses to re-emerge despite previous remediation efforts.

The high recurrence of configuration-related vulnerabilities indicates deficiencies in configuration management practices and security governance. Misconfigurations often arise from inconsistent security baselines, inadequate change management procedures, and insufficient monitoring mechanisms. These findings align with the observations of Anwar, Abusnaina, Chen, Li, and Mohaisen (2021), who emphasized that vulnerability intelligence repositories provide valuable insights into recurring security weaknesses, but their effectiveness depends on accurate vulnerability classification and systematic analysis. Repeated configuration errors therefore reflect not only technical shortcomings but also weaknesses in organizational oversight and control implementation.

The study further established that ineffective patch management remains one of the most persistent sources of recurring vulnerabilities. Organizations frequently struggle to maintain timely software updates due to operational constraints, legacy system dependencies, and inadequate asset visibility.

Similar concerns have been identified in industrial environments where legacy infrastructures often limit the implementation of modern cyber-defense mechanisms (Rubio, Alcaraz, Roman, & Lopez, 2019). In distributed and virtualized infrastructures, unresolved vulnerabilities can propagate across interconnected environments, thereby increasing organizational exposure to cyber threats (Pattaranantakul, He, Song, Zhang, & Meddahi, 2018). The recurrence of patch-related findings therefore signifies weaknesses in vulnerability management processes and asset lifecycle governance.

Another important finding is the significant influence of human factors on vulnerability recurrence. The analysis demonstrated that repeated security findings were frequently associated with poor security awareness, policy noncompliance, inadequate training, and human error. These results support the work of Ani, He, and Tiwari (2019), who argued that workforce cybersecurity capacity significantly affects organizational security posture. Human-centered vulnerabilities, including weak password practices, phishing susceptibility, and improper access control management, continue to persist because organizations often prioritize technological investments while underestimating the importance of security culture and employee competence. Consequently, recurring vulnerabilities should be interpreted as indicators of organizational maturity deficiencies rather than solely technological failures.

The findings also revealed that weaknesses in secure software development processes contribute substantially to recurring application vulnerabilities. Organizations that lack integrated security practices throughout the software development lifecycle tend to repeatedly introduce identical coding flaws and insecure dependencies into production environments. This observation corroborates the systematic mapping conducted by Nina, Pow-Sang, and Villavicencio (2021), which highlighted the importance of embedding security controls throughout software development activities. Furthermore, Imtiaz, Thorn, and Williams (2021) demonstrated that software composition analysis tools frequently identify different vulnerability sets, implying that organizations relying on a single assessment approach may fail to detect recurring weaknesses comprehensively. The persistence of application vulnerabilities therefore reflects insufficient adoption of secure development methodologies and inadequate vulnerability assessment diversity.

The trend analysis additionally demonstrated the strategic importance of security logging and continuous monitoring in identifying recurring vulnerabilities. Organizations with mature logging infrastructures exhibited greater capability to detect vulnerability recurrence patterns and prioritize remediation efforts. The findings are consistent with previous studies emphasizing the role of security logs in anomaly detection, data leakage identification, and vulnerability trend analysis (Ávila, Khoury, Khoury, & Petrillo, 2021; Svacina et al., 2020). Effective utilization of security logs facilitates root cause analysis and enables organizations to move beyond incident response toward predictive cybersecurity management.

Emerging technologies introduce additional dimensions to recurring security findings. The increasing adoption of artificial intelligence, cloud-native applications, blockchain systems, and distributed architectures creates new attack surfaces and vulnerability categories. While AI-based techniques offer opportunities for automated vulnerability detection and anomaly identification, they also introduce unique security challenges associated with model manipulation and adversarial attacks (He, Meng, Chen, Hu, & He, 2020). Similarly, API-driven architectures require robust authentication, encryption, and anomaly detection mechanisms to prevent recurring security weaknesses in distributed environments (Kaul & Khurana, 2021). Blockchain ecosystems likewise necessitate standardized security reference architectures to effectively manage recurring vulnerabilities and threat patterns (Homoliak et al., 2020).

The findings further indicate that sector-specific environments exhibit distinct vulnerability recurrence characteristics. Educational institutions, for example, often face recurring vulnerabilities due to decentralized IT infrastructures, heterogeneous user populations, and resource limitations (Ulven & Wangen, 2021). Industrial control environments encounter persistent vulnerabilities arising from legacy operational technologies and the convergence of information technology and operational technology systems (Rubio et al., 2019). Likewise, integrated cyber-physical systems require advanced anomaly detection mechanisms capable of identifying evolving vulnerability patterns in real time (Zhang et al., 2021). These sectoral differences reinforce the need for context-aware security governance frameworks.

Recurring vulnerabilities also have significant implications for organizational resilience against advanced threats such as ransomware. Persistent weaknesses in access control, patch management, and network segmentation create favorable conditions for ransomware propagation and large-scale security breaches. Reshmi (2021) observed that many ransomware incidents exploit previously identified vulnerabilities that remained unresolved within organizational environments. Therefore, reducing vulnerability recurrence should be considered a fundamental component of enterprise cyber resilience strategies.

Overall, the findings suggest that repeated IT security findings function as measurable indicators of systemic control weaknesses across governance, technology, process, and human dimensions. Consistent with safety and security co-analysis perspectives proposed by Lisova, Šljivo, and Čaušević (2018), effective mitigation requires integrated, multidisciplinary approaches that simultaneously address technical vulnerabilities, organizational processes, and human behaviors. Consequently, organizations should transition from isolated vulnerability remediation toward continuous security improvement programs that emphasize governance maturity, secure development practices, workforce capability enhancement, and data-driven cybersecurity analytics.

VI. Recommendations

Based on the analysis of recurring IT security findings and their implications for systemic control weaknesses, several recommendations are proposed to strengthen organizational cybersecurity resilience and reduce the recurrence of vulnerabilities.

6.1 Establish Continuous Vulnerability Management Programs

Organizations should move beyond periodic security assessments and adopt continuous vulnerability management programs that incorporate automated scanning, continuous monitoring, and regular remediation cycles. Since recurring vulnerabilities often result from incomplete or inconsistent remediation efforts, continuous assessment mechanisms can facilitate early detection and timely mitigation of emerging weaknesses. Organizations should also leverage high-quality vulnerability repositories and ensure that vulnerability intelligence sources are regularly validated to improve the accuracy of risk prioritization and remediation decisions (Anwar et al., 2021).

6.2 Strengthen Security Governance and Policy Enforcement

Recurring security findings frequently indicate deficiencies in governance structures, policy implementation, and accountability mechanisms. Organizations should therefore establish robust cybersecurity governance frameworks that clearly define roles, responsibilities, security standards, and compliance requirements. Periodic audits should be conducted to verify policy adherence and identify gaps in control implementation. Integrating safety and security considerations into enterprise governance processes can further improve organizational resilience and reduce systemic weaknesses (Lisova, Šljivo, & Čaušević, 2018).

6.3 Integrate Security Throughout the Software Development Lifecycle

Many recurring vulnerabilities originate during software design and development phases. Consequently, organizations should institutionalize Secure Software Development Lifecycle (SSDLC) practices, incorporating security requirements, code reviews, static and dynamic analysis, and penetration testing throughout the development process. Security should be embedded from requirements engineering through deployment and maintenance to prevent the reintroduction of previously identified weaknesses. Adopting DevSecOps principles can facilitate continuous security integration and improve vulnerability management across development environments (Nina, Pow-Sang, & Villavicencio, 2021).

6.4 Improve Software Component and Dependency Management

Organizations increasingly rely on third-party software libraries and open-source components, which may introduce recurring vulnerabilities if not properly managed. Comprehensive Software Composition Analysis (SCA) tools should be implemented to continuously monitor software

dependencies, identify known vulnerabilities, and support timely updates or replacement of insecure components. Given the variability in vulnerability reporting across different SCA tools, organizations should employ multiple complementary assessment techniques to ensure comprehensive coverage and accurate vulnerability identification (Imtiaz, Thorn, & Williams, 2021).

6.5 Enhance Human-Centered Cybersecurity Capabilities

Human factors remain a significant contributor to recurring security findings, particularly in areas such as weak password management, social engineering susceptibility, and policy noncompliance. Organizations should implement continuous cybersecurity awareness programs, role-specific security training, and practical simulation exercises to improve workforce security competencies. Building a strong security culture that encourages accountability and proactive risk reporting is essential for minimizing human-induced vulnerabilities (Ani, He, & Tiwari, 2019).

6.6 Implement Advanced Security Monitoring and Log Analytics

Comprehensive security logging and real-time monitoring capabilities should be deployed to identify abnormal activities, detect recurring attack patterns, and support forensic investigations. Centralized log management solutions integrated with Security Information and Event Management (SIEM) platforms can significantly improve visibility into organizational security events. The systematic analysis of security logs enables organizations to identify persistent weaknesses and proactively address recurring vulnerabilities before they lead to significant incidents (Ávila, Khoury, Khoury, & Petrillo, 2021; Svacina et al., 2020).

6.7 Adopt Artificial Intelligence and Data-Driven Security Analytics

Organizations should increasingly employ artificial intelligence, machine learning, and data-driven analytical techniques to enhance vulnerability detection, anomaly identification, and predictive risk assessment. AI-driven systems can assist in identifying hidden attack patterns, prioritizing vulnerabilities, and automating remediation processes in complex enterprise environments. Such approaches are particularly valuable for API security, distributed systems, and large-scale infrastructures where traditional security mechanisms may be insufficient (Kaul & Khurana, 2021; Zhang et al., 2021).

6.8 Strengthen Sector-Specific Cyber Defense Strategies

Different organizational sectors exhibit unique vulnerability characteristics and threat landscapes. Therefore, cybersecurity strategies should be tailored to sector-specific requirements. For example, industrial environments should adopt specialized cyber-defense mechanisms capable of protecting legacy operational technologies and critical infrastructures (Rubio et al., 2019). Similarly, higher education institutions should implement comprehensive security governance, awareness programs,

and risk management frameworks to address their distinctive cybersecurity challenges (Ulven & Wangen, 2021).

6.9 Improve Protection Against Emerging and Advanced Threats

Organizations should proactively address security risks associated with emerging technologies such as deep learning systems, blockchain infrastructures, and network function virtualization environments. Standardized security reference architectures, continuous threat modeling, and rigorous security testing should be adopted to mitigate vulnerabilities in these evolving technologies (Homoliak et al., 2020; Pattaranantakul et al., 2018). Additionally, organizations deploying artificial intelligence solutions should implement safeguards against adversarial attacks and model manipulation threats to ensure trustworthy AI operations (He et al., 2020).

6.10 Develop Comprehensive Ransomware Preparedness and Incident Response Plans

Given the increasing prevalence and impact of ransomware attacks, organizations should establish comprehensive incident response capabilities that include regular backups, disaster recovery procedures, threat intelligence integration, and incident simulation exercises. Effective preparedness strategies can significantly reduce the operational and financial consequences of successful attacks and improve organizational resilience against recurring security incidents (Reshmi, 2021).

VII. Conclusion and Future Research

7.1 Conclusion

This research analyzed the recurring information technology (IT) security incidents and drew out conclusions about the system-wide control gaps in the environment. The analysis showed that identified security issues tend not to be exclusive technical problems, but rather symptoms of ongoing governance weaknesses, security processes, technology management and human practices. Analysis of trends showed that vulnerabilities identified, like weak authentication, patch management issues, system misconfigurations, insecure software components and poor access controls, repeat over several assessment cycles and indicate weaknesses in the organisation's security maturity.

The results also show a significant correlation between the ongoing vulnerability and the lack of effective vulnerability remediation, secure software development practices, and vulnerability management programs. Researchers counter that software security practices which are executed throughout the software lifecycle can help decrease the incidence of software security flaws and

enhance organizational resilience (Nina, Pow-Sang, & Villavicencio, 2021). Likewise, disparities in vulnerability reporting and assessment tools can result in incomplete remediation, thus raising the probability of re-findings (Imtiaz, Thorn, & Williams, 2021).

The study also confirmed that human factors continue to be a significant factor in reoccurring security vulnerabilities. Limited awareness of cyber security, weak compliance with security policies and a lack of competencies among employees still affect technical controls and expose the organization to cyber threats (Ani, He, & Tiwari, 2019). As ransomware and other advanced attacks have become more prevalent, it's clear that unaddressed vulnerabilities can result in critical operational and financial impacts (Reshmi, 2021).

Furthermore, the study emphasized the need to utilize vulnerability databases, security logs, and ongoing monitoring tools to uncover patterns and prioritize remediation efforts. The National Vulnerability Database contains excellent intelligence for detecting vulnerabilities and their trends, and for enhancing risk assessment processes (Anwar, Abusnaina, Chen, Li, & Mohaisen, 2021). In addition, security log analysis and anomaly detection methods enable the early detection of persistent weaknesses and future threats (Ávila et al., 2021; Svacina et al., 2020).Frequently, the same vulnerabilities are identified in complex environments like industrial control systems, network function virtualization infrastructures, blockchain applications, and higher education institutions, and they are caused by systemic architectural and governance issues – not isolated technological failures – (Rubio et al., 2019; Pattaranantakul et al., 2018; Homoliak et al., 2020; Ulven & Wangen, 2021).

In summary, the research firm finalizes that nonstop IT security results are trustworthy markers of control gaps and immaturity in organizations' cybersecurity controls. These shortcomings will need to be addressed in a comprehensive and ongoing manner, spanning the entire lifecycle of a security product, from governing the product and its development, to training users and maintaining a skilled workforce, to continuous monitoring, and to data-driven security analytics. A systematic approach to understanding vulnerability trends and fixing root causes has a greater likelihood of sustainable improvements in the cybersecurity posture of an organization.

7.2 Future Research

Further research is needed to explore the use of AI and machine learning algorithms to identify patterns of vulnerabilities and the automation of remediation actions. Complex distributed environments present significant challenges for identifying vulnerabilities, which has been a considerable strength of AI-based approaches in the detection of anomalies and API security (Kaul & Khurana, 2021; Zhang et al., 2021).

Additionally, more studies are required to uncover the common weaknesses of new technological areas like deep learning systems, blockchain architectures and cloud-based environments, where the threat landscape is constantly changing and new types of systemic vulnerabilities emerge (He,

Meng, Chen, Hu & He, 2020; Homoliak et al., 2020). Comparative studies between sectors, such as between industrial systems, higher education institutions, and enterprise environments, would give a deeper understanding of patterns of vulnerability recurrence and control shortcomings by sector (Rubio et al., 2019; Ulven & Wangen, 2021).

Further studies are also needed to create a standardized measure of how often vulnerabilities recur in organizations and the maturity of their security controls. These frameworks would enable a benchmarking program and improve cybersecurity governance. Last but not least, longitudinal research projects that could look into the impact of vulnerabilities that repeat over time, organizational culture and the long-term cybersecureness would substantially advance both academic understanding and cybersecureness practice.

References

1. Anwar, A., Abusnaina, A., Chen, S., Li, F., & Mohaisen, D. (2021). Cleaning the NVD: Comprehensive quality assessment, improvements, and analyses. *IEEE Transactions on Dependable and Secure Computing*, *19*(6), 4255-4269.
2. Nina, H., Pow-Sang, J. A., & Villavicencio, M. (2021). Systematic mapping of the literature on secure software development. *Ieee Access*, *9*, 36852-36867.
3. Rubio, J. E., Alcaraz, C., Roman, R., & Lopez, J. (2019). Current cyber-defense trends in industrial control systems. *Computers & Security*, *87*, 101561.
4. Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2-35.
5. Lisova, E., Šljivo, I., & Čaušević, A. (2018). Safety and security co-analyses: A systematic literature review. *IEEE Systems Journal*, *13*(3), 2189-2200.
6. Kaul, D., & Khurana, R. (2021). AI to detect and mitigate security vulnerabilities in APIs: encryption, authentication, and anomaly detection in enterprise-level distributed systems. *Eigenpub Review of Science and Technology*, *5*(1), 34-62.
7. Imtiaz, N., Thorn, S., & Williams, L. (2021, October). A comparative study of vulnerability reporting by software composition analysis tools. In *Proceedings of the 15th ACM/IEEE international symposium on empirical software engineering and measurement (ESEM)* (pp. 1-11).
8. Ávila, R., Khoury, R., Khoury, R., & Petrillo, F. (2021). Use of security logs for data leak detection: a systematic literature review. *Security and communication networks*, *2021*(1), 6615899.
9. Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, *13*(2), 39.

10. Zhang, L., Su, H., Zio, E., Zhang, Z., Chi, L., Fan, L., ... & Zhang, J. (2021). A data-driven approach to anomaly detection and vulnerability dynamic analysis for large-scale integrated energy systems. *Energy conversion and management*, *234*, 113926.
11. Reshmi, T. R. (2021). Information security breaches due to ransomware attacks-a systematic literature review. *International Journal of Information Management Data Insights*, *1*(2), 100013.
12. Das, P. K., Kashem, M. A., Ferdus, Z., & Islam, S. (2019, October). Development and application of a new computerized smell generating system. In *2019 Global Conference for Advancement in Technology (GCAT)* (pp. 1-5). IEEE.
13. Ferdus, M. Z., Khan, M. N. I., Islam, S., & Kashem, M. A. (2019, October). VFLT: SQA Model for Cyber Physical System. In *2019 Global Conference for Advancement in Technology (GCAT)* (pp. 1-4). IEEE.
14. Ferdus, M. Z., Islam, S., & Kashem, M. A. (2019, October). An innovative load balancing cluster composition of wireless sensor networks. In *2019 global conference for advancement in technology (GCAT)* (pp. 1-4). IEEE.
15. Islam, S. J., Islam, S., Ferdus, M. Z., Khan, M. N. I., Kashem, M. A., & Islam, M. S. (2020, September). Load compactness and recognizing area aware cluster head selection of wireless sensor networks. In *2020 International conference on computing and information technology (ICCIT-1441)* (pp. 1-4). IEEE.
16. Islam, S., Khan, M. N. I., Ferdus, M. Z., Islam, S. J., & Kashem, M. A. (2020, September). Improving throughput using cooperating TDMA scheduling of wireless sensor networks. In *2020 International Conference on Computing and Information Technology (ICCIT-1441)* (pp. 1-4). IEEE.
17. Kola, J. N. (2017). Data Warehousing And Text Analytics As Instruments Of Cultural Knowledge Management: Implications For Digital Preservation And Societal Decision-Making. *Power System Protection and Control*, *45*(1), 11-15.
18. Kazmi, S. Chemical Upcycling of Polyethylene Terephthalate (PET) Waste into High-Value Functional Polymers.
19. Naidu, K. J. (2013). Performance Optimization Of ETL Pipelines In Distributed Data Warehouse Environments: A Network-Aware Scheduling Approach. *International Journal of Advance Industrial Engineering*, *1*(03), 63-67.
20. He, Y., Meng, G., Chen, K., Hu, X., & He, J. (2020). Towards security threats of deep learning systems: A survey. *IEEE Transactions on Software Engineering*, *48*(5), 1743-1770.
21. Svacina, J., Raffety, J., Woodahl, C., Stone, B., Cerny, T., Bures, M., ... & Tisnovsky, P. (2020, October). On vulnerability and security log analysis: A systematic literature review on recent trends. In *Proceedings of the International Conference on Research in Adaptive and Convergent Systems* (pp. 175-180).

22. Pattaranantakul, M., He, R., Song, Q., Zhang, Z., & Meddahi, A. (2018). NFV security survey: From use case driven threat analysis to state-of-the-art countermeasures. *IEEE Communications Surveys & Tutorials*, *20*(4), 3330-3368.
23. Homoliak, I., Venugopalan, S., Reijsbergen, D., Hum, Q., Schumi, R., & Szalachowski, P. (2020). The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses. *IEEE Communications Surveys & Tutorials*, *23*(1), 341-390.