**EVALUATING CYBER THREAT IDENTIFICATION,VULNERABILITTY ASSESSMENT, AND MITIGATION STRATEGIES TO MINIMIZE BUSINESS IMPACT**

**BY**

**ODUWOLE EYINOJUOLUWA TAOFEEK**

**S121202009**

**A PROJECT SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE, COLLEGE OF INFORMATION AND COMMUNICATION TECHNOLOGY, CRESCENT UNIVERSITY ABEOKUTA**

**IN PARTIAL FUFILLMENT OF THE REQUIREMENT FOR THE AWARD OF BACHELOR OF SCIENCE (B.Sc) DEGREE IN COMPUTER SCIENCE**

**SECTION ONE**

**INTRODUCTION**

* 1. **Background to the study**

Risk management is a critical element in the governance of information systems (IS), enabling organizations to optimize costs by addressing potential incidents proactively rather than responding after they occur (McKeen & Smith, 2003; Anton & Afloarei Nucu, 2020). Nonetheless, the field of risk management remains challenging for both practitioners and academics, particularly due to the complexity of balancing organizational profitability with minimizing risk costs (Lei, 2011). Zhang (2009) emphasizes that the equilibrium between proactive risk management strategies and potential financial losses following risk realization highlights the necessity of implementing tailored risk management processes, adapted to the unique characteristics of each information system context.

The central objective of risk management in IS is fostering **resilience**, which involves systematically identifying threats, adopting preventive actions, and mitigating the negative effects of risk through structured and evidence-based strategies (Mahapatra et al., 2024). Recent systematic literature reviews underscore the growing importance of understanding **Enterprise Risk Management (ERM)** frameworks and their adoption across industries. Notably, the banking and insurance sectors are leading in ERM implementation, while the role of Small and Medium Enterprises (SMEs) in adopting these strategies for performance optimization and competitive positioning has also been emphasized (Blanco-Mesa et al., 2019; Anton & Afloarei Nucu, 2020).

The adoption of ERM can be broken down into four key research areas: **ERM adoption**, **determinants of its implementation**, **the effects of ERM strategies**, and **other organizational factors influencing strategic decision-making** (Anton & Afloarei Nucu, 2020). Among these, the relationship between the implementation of ERM and organizational performance continues to receive considerable attention. Additionally, environmental factors, institutional norms, and organizational culture are pivotal in determining how ERM strategies are adopted, executed, and evaluated across firms (Mahapatra et al., 2024).

The literature collectively suggests that risk management is essential for achieving organizational sustainability. It does so by not only addressing threats but also optimizing resource allocation and creating strategic opportunities that foster competitive advantages (Anton & Afloarei Nucu, 2020; Mahapatra et al., 2024). Future studies are expected to investigate the micro-level determinants influencing ERM adoption further and assess the operational effects of ERM implementation across different industries.

* 1. **Statement of the problem**

Organizations are increasingly reliant on digital technologies, making them vulnerable to a wide range of cyber threats. Despite implementing advanced security measures, many businesses face challenges in effectively identifying, assessing, and mitigating vulnerabilities due to the evolving complexity of cyber threats and the dynamic nature of technological advancements. The inability to accurately identify cyber threats, conduct comprehensive vulnerability assessments, and implement effective mitigation strategies often results in significant financial losses, reputational damage, operational disruptions, and compromised sensitive data.

Many organizations lack the necessary tools, expertise, or structured processes to prioritize risks, respond to breaches in a timely manner, or predict potential vulnerabilities. This gap in risk management and threat mitigation hinders the ability to minimize business impact during cyber incidents. Therefore, there is an urgent need to evaluate current methodologies for threat identification, vulnerability assessment, and mitigation to determine their effectiveness and ensure they align with modern cyber risk environments. Addressing these challenges is vital to building organizational resilience and safeguarding business continuity in the face of persistent and sophisticated cyber threats.

**1.3Aim of the study**

The primary aim of this study is to **evaluate cyber threat identification processes, vulnerability assessment methodologies, and mitigation strategies to minimize the business impact of cyber threats**. This research seeks to:

1. **Analyze the current methods and frameworks** used for identifying cyber threats, assessing vulnerabilities, and implementing mitigation strategies.
2. **Identify gaps in organizational preparedness** regarding the detection, assessment, and response to cyber risks.
3. **Examine the relationship between threat identification, vulnerability assessment, and mitigation strategies**, focusing on their collective role in reducing financial, operational, and reputational risks.
4. **Propose evidence-based strategies and recommendations** to strengthen organizations’ cybersecurity posture and response mechanisms.
5. **Explore the adoption and integration of threat intelligence and risk management tools**, emphasizing organizational culture, technology, and strategic leadership.

The study intends to contribute to the growing body of research on cyber risk management by providing insights into proactive and strategic approaches that businesses can employ to minimize their exposure to cyber threats, enhance resilience, and maintain operational stability in an increasingly connected digital landscape.

**1.3.1 Objective of the study**

The objectives of this study are to:

1. **Identify and analyze prevalent cyber threats** faced by organizations across industries.
2. **Assess existing vulnerability detection mechanisms** to determine their effectiveness in identifying security gaps.
3. **Evaluate mitigation strategies** currently implemented to counteract cyber risks and reduce business disruptions.
4. **Develop a framework or set of best practices** for integrating cyber threat identification, vulnerability assessment, and mitigation strategies into business operations.
5. **Examine the impact of effective cybersecurity practices** on minimizing financial, operational, and reputational damages.

**SECTION TWO**

**LITERATURE REVIEW**

**2.1 Cyber Threat Identification, Vulnerability Assessment, and Mitigation Strategies**

Cybersecurity efforts are fundamentally centered on identifying threats, assessing vulnerabilities, and implementing mitigation strategies to minimize risks. These processes are crucial for organizations seeking to maintain operational integrity and resilience in a rapidly evolving digital landscape. Cyber threat management can be categorized into three core areas: **identification**, **assessment**, and **mitigation**.

**2.1.1 Cyber Threat Identification**

Cyber threat identification involves recognizing potential threats that could exploit vulnerabilities within a system. Methods and tools for threat identification include:

1. **Threat Intelligence Platforms**

Threat intelligence platforms (TIPs) gather, analyze, and share information about potential threats. They leverage data from multiple sources, including dark web monitoring, malware analysis, and threat actor profiling (Ahmed et al., 2019).

1. **Anomaly Detection**

Anomaly detection systems identify unusual activity within networks or systems, which could indicate the presence of malicious activities. Machine learning algorithms are commonly employed to detect deviations from established baselines (Khan et al., 2021).

1. **Behavioral Analysis**

Analyzing user and entity behavior helps in detecting insider threats or compromised accounts. Behavioral analysis systems observe patterns such as access times, file usage, and geographic anomalies to identify suspicious activities (Isyanto et al., 2020).

**2.1.2 Vulnerability Assessment**

Vulnerability assessment is a systematic process aimed at identifying, analyzing, and evaluating weaknesses, flaws, or potential vulnerabilities within systems, networks, or applications that could be exploited by malicious actors or other threats. This process plays a critical role in enhancing an organization's overall security posture by proactively addressing risks before they are exploited. Key methods employed in vulnerability assessment include the following:

1. **Penetration Testing**

Penetration testing, often referred to as ethical hacking, is a structured and controlled process that simulates real-world cyberattacks on systems, networks, or applications to identify and exploit vulnerabilities. By replicating the techniques and methods used by malicious actors, penetration testing provides organizations with a clear understanding of their security posture. The process involves various stages, including reconnaissance, vulnerability scanning, exploitation, and reporting.

Through this approach, penetration testing offers actionable insights into system weaknesses, highlighting areas where security measures are inadequate or misconfigured. This enables organizations to prioritize corrective actions effectively, ensuring critical vulnerabilities are addressed promptly to minimize potential risks. Furthermore, it helps validate the efficacy of existing security controls, compliance with regulatory requirements, and overall resilience against potential threats (Porwik et al., 2021).

1. **Automated Scanning Tools**

Tools such as Nessus and OpenVAS play a pivotal role in automating the vulnerability scanning process, providing organizations with a comprehensive method to identify potential security issues across their IT environments. These tools specialize in detecting outdated software versions, identifying misconfigurations in system settings, and flagging known security flaws that could be exploited by threat actors.

By leveraging extensive databases of vulnerabilities and integrating seamlessly with enterprise systems, Nessus and OpenVAS enhance the efficiency and accuracy of the assessment process. They generate detailed reports outlining the severity of identified vulnerabilities, offering actionable recommendations for remediation. This automation significantly reduces the time and effort required for manual analysis, allowing security teams to focus on implementing mitigation measures and strengthening the organization's overall defense posture (Li et al., 2019).

1. **Risk Scoring Models**

Analyzing user and entity behavior helps in detecting insider threats or compromised accounts. Behavioral analysis systems observe patterns such as access times, file usage, and geographic anomalies to identify suspicious activities (Isyanto et al., 2020).

**2.1.3 Mitigation Strategies**

Mitigation strategies aim to reduce the likelihood or impact of cyber threats through proactive measures. Common approaches include:

**a. Network Segmentation**

Network segmentation isolates critical assets, limiting the spread of potential breaches. It is often combined with access control measures to ensure data protection (Kortli et al., 2020).

**b. Zero Trust Architecture**

Zero trust models enforce strict access policies based on identity verification and least privilege principles, enhancing security across systems (Ahmed, 2019).

**c. Incident Response Planning**

Incident response plans outline the procedures to be followed during security incident. They include roles and responsibilities, containment strategies, and recovery protocols(Dargan et al.,2020).

1. **Continuous Monitoring**

Continuous monitoring systems employ tools like security information and Event management (SIEM) to detect, report , and respond to threats in real-time(Mahapatra et al.,2024)

**2.2 Summary of Related works**

**SECTION THREE**

**METHODOLOGY**

The biometric based exam hall authentication is to assist in the examination malpractice and impersonation.Multi-biometrics system provides accuracy and can be established in much large scale biometric application.Fingerprint is one of the easily accessible parts of the user and requires minimum efforts on the part of the user. Face detection is also included as it is, yet another option for human identification and authentication technology is also included, due to its high precision, as they are unique to each individual.

Multimodal biometric authentication, which combines multiple biometric traits for identity verification, offers a more secure and reliable approach compared to single-modal authentication. Using both facial recognition and fingerprint recognition in examination verification is an effective way to reduce fraud, enhance security, and ensure accurate identity verification.

How it works:

1. **Facial Recognition**

**Capture**: During examination registration or entry, a live image of the examinee's face is captured using a camera.

**Processing:** The facial image is processed and compared to the stored facial data (previously registered during user on boarding).

**Verification:** The system checks the facial features like the distance between eyes, nose shape, and overall facial structure for a match.

1. **Fingerprint Recognition**

**Capture:** A fingerprint scanner is used to scan the user's fingerprints, usually at the time of entry or before starting an exam.

**Processing:** The scanned fingerprint is processed to extract unique features, such as ridge patterns, loops, and whorls.

**Verification:** The system compares the live fingerprint scan with the previously stored fingerprint template to confirm the examinee identity.

1. **Multi-modal Fusion**

**Authentication Process:** Both biometric traits (face and fingerprint) are combined for a higher level of security. The system checks for a match in both modalities, making it harder for unauthorized individuals to spoof or bypass the authentication process.

**Error Reduction:** In cases where one modality (e.g., facial recognition) may be less accurate due to poor lighting or positioning, the other modality (fingerprint recognition) serves as a reliable backup.

**Cross-validation:** The two systems work in parallel, enhancing the accuracy and reliability of the authentication process.

1. **Advantages for Examination Verification**

**Enhanced Security:** The combination of two biometric factors (something you are) reduces the likelihood of identity fraud, as it’s significantly harder to fake both a fingerprint and facial image.

**Non-intrusiveness:** Both methods are non-intrusive (no need for passwords or pins) and quick, ensuring minimal disruption to the exam process.

**Spoof Resistance:** Multi-modal systems are resistant to spoofing (e.g., using photographs or fake fingerprints) because a combination of features is required for successful authentication.

**Accuracy:** Combining the two modalities can improve overall accuracy, as errors from one biometric system can be cross-checked by the other.

**Online Exams:** For remote examination settings, students could use webcams for facial recognition and fingerprint scanners for secure log-ins.

**Physical Exams:** At exam centers, students can be verified at entry points with both facial and fingerprint scans.

**Proctoring:** During exams, biometric verification can prevent impersonation by verifying the student’s identity multiple times throughout the examination process.

**CHAPTER FOUR**

**CONCLUSION**

**Reference**

Saniya S. , Acharya P.P. , Sangeetha.A. , Sagarika.S. ., Priya.K. (2021) Multilevel Biometrics for Exam Hall Authentication.International Journal of Research in Engineering, Science and Management

Volume 4, Issue 5, May 2021 https://www.ijresm.com | ISSN (Online): 2581-5792

Bhuiyan.M.A., Samad.M.A., Hossain.M.S (2020) Biometric verification system using Facial Recognition.International journal of Computer Application(IJCA) Volume 176, Issue 1, September 2020 <https://ijcaonline.org> | ISSN(Online): 0975-8887

Tiwari.H.D., Tiwari.A.K., Kumar.V (2019) Iris Scanning Examination Verification System,International Journal of Computer Application Volume 178, Issue 1, July 2019 <https://ijcaonline.org> | ISSN(Online): 0975-8887

Singh.A.K., Shukla.K.K., Saha.S.C. (2020) Examination Verification Using Multimodal Biometrics,International Journal of Computer Applications Volume 176, Issue 4, August 2020 <https://ijcaonline.org> | ISSN(Online): 0975-8887

Singh.S.K., Yadav.A.K., Verma.R.K., (2019) Security and Privacy in Examination Verification System, International journal of Computer Application(IJCA) Volume 178, Issue 1, July 2019 <https://ijcaonline.org> | ISSN(Online): 0975-8887

Korolov, M, (2019) What is biometric? 10 physical and behavioural identifiers. CSO online. Retrieved 10 June 2020, from <https://www.csoonline.com/article/3339565/what>-is-biometrics-and-why-collecting-biometric-data-is-risky.HTML.

Ahmed, A.A. Future effects and impacts of biometrics integrations on everyday living. Al-Mustansiriyah J. Sci. 2019, 29, 139–144. [CrossRef]

Dargan, Shaveta, and Munish Kumar. "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities." Expert Systems with Applications 143 (2020): 113114.

Socheat, Sek, and Tianjiang Wang. "Fingerprint enhancement, minutiae extraction and matching techniques." Journal of Computer and Communications 8, no. 05 (2020): 55.

Kortli, Yassin, Maher Jridi, Ayman Al Falou, and Mohamed Atri. "Face recognition systems: A survey." Sensors 20, no. 2 (2020): 342.

Lee, Young Won, and Kang Ryoung Park. "Recent iris and ocular recognition methods in high-and lowresolution images: A survey." Mathematics 10, no. 12 (2022): 2063.

Bharathi, B., and P. Bindhu Shamily. "A review on iris recognition system for person

identification." International Journal of Computational Biology and Drug Design 13, no. 3 (2020): 316-331

Li, Xiaochang, and Mara Mills. "Vocal features: from voice identification to speech recognition by machine." Technology and culture 60, no. 2 (2019): S129-S160.

Wang, Chen, Yan Wang, Yingying Chen, Hongbo Liu, and Jian Liu. "User authentication on mobile devices: Approaches, threats and trends." Computer Networks 170 (2020): 107118

Porwik, Piotr, Rafal Doroz, and Tomasz Emanuel Wesolowski. "Dynamic keystroke pattern analysis and classifiers with competence for user recognition." Applied Soft Computing 99 (2021): 106902

Isyanto, Haris, Ajib Setyo Arifin, and Muhammad Suryanegara. "Performance of smart personal assistant applications based on speech recognition technology using IoT-based voice commands." In 2020

International conference on information and communication technology convergence (ICTC), pp. 640-645. IEEE, 2020

Khan, Simon, Charles Devlen, Michael Manno, and Daqing Hou. "Mouse dynamics behavioral biometrics: A survey." ACM Computing Surveys 56, no. 6 (2024): 1-33.

O. Sarjiyus, El Yakub M.B , Benjamin Ezra “Examination Verification System Using Biometric Authentication, International Journal of Integrative Sciences (IJIS) Vol.2, No.9, 2023: 1459-1478 (2023).

Rajesh N B, Subhiksha R, Oormila T S “BIOMETRIC EXAMHALL AUTHENTICATION” International Research Journal of Engineering and Technology (IRJET) Volume: 07 Issue: 04 | Apr 2020.

Jaimit Patel, Anubhav, Ayush Kumar Singh, Rachit Kumar Tiwari, Abhi Singh and

Bhupinder Kaur “Biometric Authentication System For Access Control” *School of Computer Science and Engineering , December 29-30, 2023.*

Meennapa Rukhiran , Sethapong Wong , and Paniti Netinant “IOT-BASED BIOMETRIC RECOGNITION SYSTEMS IN EDUCATION FOR IDENTITY VERIFICATION SERVICES: QUALITY ASSESSMENT APPROACH” College of Digital Information Technology, 9 March 2023.