International Journal of Business Quantitative Economics and Applied Management Research
Volume-6, Issue-12, 2021 ISSN No: 2349-5677

THE ROLE OF PRIVILEGED ACCESS MANAGEMENT (PAM) IN PREVENTING INSIDER THREATS: HOW PAM CAN MITIGATE RISKS ASSOCIATED WITH INSIDER THREATS

Sri kanth Mandru
Mandrusrikanth9@gmail.com

Abstract

Privileged Access Management (PAM) is a security solution that helps businesses protects themselves against cyber threats by detecting unauthorized access to their systems. The solution works through technology, people, and processes to identify people with privileged access and what they are doing in their accounts. Limiting people with privileged access improves an organization's system security and reduces vulnerability to the IT infrastructure. The two primary uses of PAM are to ensure compliance with industry regulations and prevent credential theft. Insider threats are a common cyber security problem in organizations. It results in the loss of confidential data and affects the overall business operations of an organization. Additionally, insider threats could have significant financial implications if the organization is faced with lawsuits. Rebuilding the damaged reputation among customers, stakeholders, and investors can take time and effort. Companies may also experience loss of competitive edge due to insider threats. Digital assets are lost, and production secrets are shared with people who should never have access to them. A PAM solution can mitigate credential theft by ensuring just enough and just-in-time access and authentication for administrator accounts and identities. Privileges allow applications and users to access certain resources and perform specific operations. Insiders' potential for abuse or misuse of privilege presents businesses with a significant security threat. Breaches caused by insider threats cost organizations an average of $16.2 million annually. Unfortunately, organizations spend only $3.2 million yearly to fix security vulnerabilities.

Keywords: Insider threat, privilege, Access management, Information technology, Privileged access management, breaches

I. INTRODUCTION

Human beings resent a significant security risk to information technology (IT) risks. Privileged access management (PAM) comprises cyber security technologies and strategies to exert control over privileged permissions and access for accounts and users. It ensures staff members have limited access to IT systems that allow them to perform their jobs [6]. PAM allows businesses to condense their attack surface and reduce risks from insider and external attacks. Technologists and analysts consider these strategies one of the most important approaches for addressing compliance initiatives and reducing cyber security. PAM provides auditability, control, and visibility over all privileges and credentials. The zero trust policy is based on the principle that

all staff members pose significant vulnerability to the organization's IT systems. As a result, all digital items attempting to connect to the company's IT infrastructure must be verified to access data. The principle of least privilege allows companies to reduce the number of individuals in a company who can access certain data [17]. It plays an important role in preventing insider threats by ensuring only few people can access critical data. The approach averts cyber threats that can have devastating impacts on an organization's IT system and data.

II. PROBLEM STATEMENT

Insider threats present a dynamic and complex risk affecting private and public components of critical infrastructure. According to The Cyber security and Infrastructure Security Agency (CISA),"insider threat is the threat that an insider will use their authorized access, intentionally or unintentionally, to harm the department's mission, resources, personnel, facilities, information, equipment, networks, or systems [12]. Insider threats manifest in various ways: violence, espionage, sabotage, theft, and cyber acts"[1]. When they occur, insider threats significantly impact an organization's operations and survival.

Insider threats can lead to critical data loss, affecting an organization's operations. A malicious insider could delete or steal critical organization data using a flash disk [16]. From financial records to customer information, a legitimate user could leak or steal sensitive data essential for an organization's operations [11]. Additionally, firms may be forced to pay hefty fines for non-compliance with data laws and regulations. Moreover, insider threats may have considerable financial impacts. A company's trade secrets may be revealed when insiders steal confidential information. The company may experience massive financial loss if this information is revealed to outsiders through human error social engineering. The following graph shows cyber security threat costs.

Fig 1: Cybersecurity threat costs. Adapted from [2].

Malicious employee activity can have a considerable operational impact on an organization. Interference with IT systems can affect the organization's operation and lead to downtime. A cybersecurity activity injecting a virus into the IT infrastructure can jeopardize operations. Depending on the downtime, the company may experience a reduced production capacity [2]. Furthermore, insider threats can lead to legal implications. Legal and regulatory costs, including

litigation and fines, can impact the organization. An insider threat can introduce unexpected legal problems and costs for the organization by stealing user credentials and unauthorized access. Losing intellectual property requires improved security compliance and legal actions for many organizations.

Companies may also experience loss of competitive edge due to insider threats. Digital assets are lost, and production secrets are shared with people who should never have access to them. Rivals may use their strategic plan to beat them in the market. Organizations want to protect their reputation due to its impact on business operations. Insider threats can lead to lost trust among customers, business partners, and shareholders [10]. The management faces challenges in explaining insider threats because it is their responsibility to ensure system security.

III. SCOPE

Insider has become common in the United States, especially due to the increased use of artificial intelligence and cloud computing. In 2021, about 35% of US companies saved their workload in the cloud. Insider threats went from 3,200 in 2018 to 4,700 in 2020 [9]. These statistics indicate that insider threats, either due to human errors or malicious actors, are on an upward trajectory. Moreover, privileged users represent the greatest risk to an organization's IT systems. These privileges allow employees to access sensitive information that could significantly impact the organization when it lands in the wrong hands. Breaches caused by insider threats cost organizations an average of $16.2 million annually. Unfortunately, organizations spend only $3.2 million yearly to fix security vulnerabilities [13].

Apart from the financial implications, insider threats can negatively impact an organization's reputation. When trust has been broken, it can be difficult to regain it among stakeholders, investors, and customers. Additionally, insider threats can affect an organization's performance. Stolen data or deleted data can compromise an organization's ability to conduct its business. A company's trade secrets may be revealed when insiders steal confidential information [4]. The company may experience massive financial loss if this information is revealed to outsiders through human error. The following graph shows insider threat statistics for 2023.

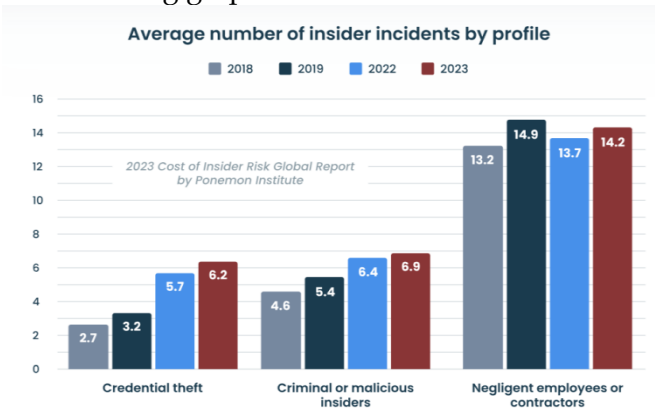

Fig 2: Insider threat statistics in 2023. Adapted from [15].

International Journal of Business Quantitative Economics and Applied Management Research
Volume-6, Issue-12, 2021 ISSN No: 2349-5677

IV. SOLUTION

PAM reduces an organization's vulnerability to insider threats. Privileges allow applications and users to access certain resources and perform specific operations. Insiders' potential for abuse or misuse of privilege presents businesses with a significant security threat. Nevertheless, PAM can reduce the risk of insider threats to an organization's IT infrastructure. The zero-trust methodology provides the basis for this solution [8]. It is a strategic data approach that suggests that businesses should not trust their network assets. As a result, they must develop multiple authentication and security protocols to grant access to accounts. The methodology controls access using different approaches, such as multi-factor authentication or centralized password management. The following image shows the PAM workflow.

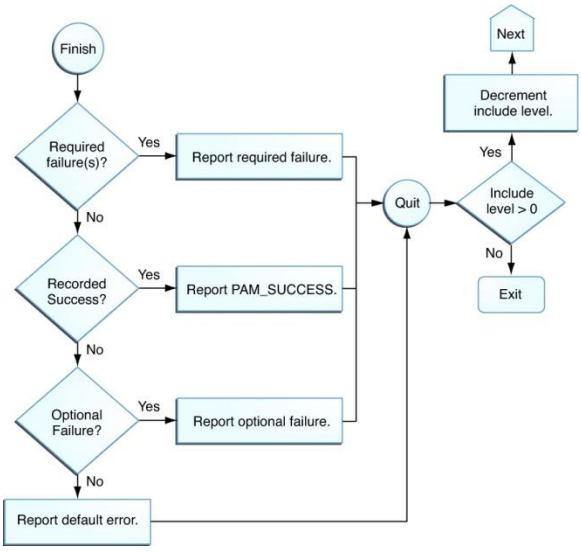

Fig 3: PAM workflow. Adapted from [5].

The Principle of Least Privilege (PoLP) is another strategy organizations use to reduce insider threats using privileged access management. The approach allows businesses to restrict access to company data. The principles offer a comprehensive data security approach that covers employees, third parties, and database services. "Least Privilege plays a significant role in identifying and preventing insider threats and is based on determining the users who will have privileged access to data and the access levels of such users" [7]. The principle allows organizations to create different accounts and define different authorization levels. As a result, the approach averts insider threats such as identity theft, rootkits, and malware. The following graph shows the PAM lifecycle.

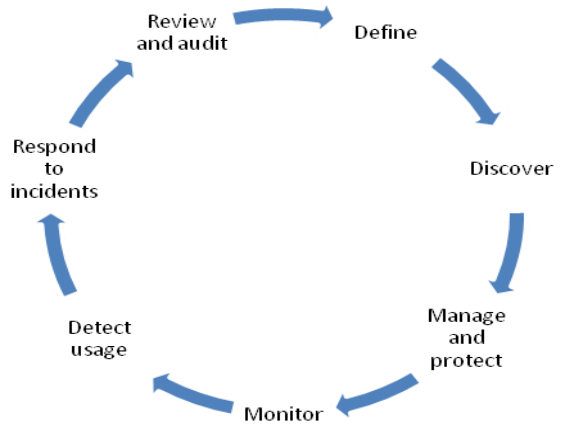

Fig 4: PAM lifecycle. Adapted from [6].

Organizations can also block access to cloud storage sites. These sites store significant corporate data that can be misused if accessed by unauthorized individuals. Sites not being used must be closed and only opened under management authorization. Organizations must also limit privileged access to a single individual. Responsibilities are spread across multiple privileged users. Each individual will have a specific area of focus to reduce threats. Additionally, organizations can encrypt sensitive data [14]. This approach ensures data can only be read by individuals with the decryption key. Access to the decryption key must also be protected effectively.

Data backup is crucial to ensure sensitive company information is not deleted or lost when a data breach occurs. Critical data should be backed up in multiple locations and systems. During insiderincidents, malicious individuals may want to delete certain information from the organization's systems. Backing up the data ensures that the information is not lost. The data security teams must control access to the backup system to avoid the double deletion of critical data. Well-developed procedures for backing up the data are crucial to avoid losing critical data. The following graph shows the 3-2-1 backup strategy.

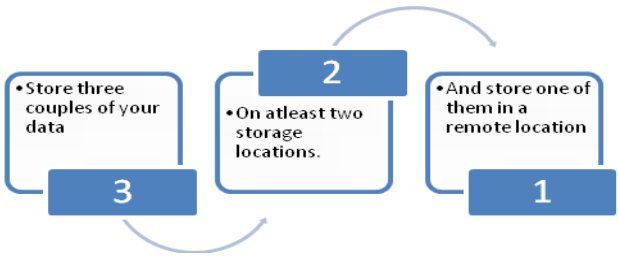

Fig 5: 3-2-1 backup strategy. Adapted from [8].

Effective policies for staff members on using information systems can reduce insider threats. Organizational policies are developed based on industry standards and regulations. Employees must be trained to understand the importance of compliance with organizational policies regardinginsider threats. Moreover, this problem can be addressed by implementing workflows to develop and control privileged accounts. Organizations must adopt best practices for insider threats to mitigate their impact on the organization [5]. Additionally, staff training on IT systems is crucial to reduce critical data loss through human error.

V. USES

A PAM solution identifies technology, people, and processes that require privileged access and provides the protocols that apply to them. The solution must have capabilities to support industry regulations and organizational policies. Furthermore, administrators must be able to create, delete, and amend accounts based on the organization's changing needs. The solution continuously monitors system operations to identify security gaps and generate reports in real-time [15]. The two primary uses of PAM are to ensure compliance with industry regulations and prevent credential theft. A PAM solution can mitigate credential theft by ensuring just enough and just-in-time access and authentication for administrator accounts and identities.

A least-privilege policy in an organization is necessary to protect critical data like personal health information and payment information. The PAM solution can generate an access report to determine who has access to what data and why they need it. Use cases may include securing remote access, recording privileged accounts, and automating the user lifecycle. IT administrators can also apply these solutions to DevOps projects, cloud environments, and devices. Nevertheless, misuse of privileged access can pose significant cyber security threats to an organization. System administrators must monitor privileged sessions to identify activities that may be jarful to the organization's data. They must also generate reports for privileged sessions for future review.

PAM provides enhanced visibility in an organization. It gives them real-time information about who has access to an organization's device network and servers. Additionally, it allows IT experts to set alerts and receive notifications when unauthorized individuals attempt to access the system. Organizations also use PAM to enhance compliance with industry standards and regulations. Adopting least privilege access principles allows organizations to prove compliance and reduce risk in an audit process.

VI. IMPACT

Malicious insiders can cause significant consequences for an organization due to their knowledge of where sensitive data exists. One of the impacts of insider threats is critical data loss. Many organizations have transitioned from paperwork to digital records containing sensitive organization information. A malicious insider could delete or steal critical organization data using a flash disk [6]. From financial records to customer information, a

legitimate user could leak or steal sensitive data essential for an organization's operations. The leaked information could lead to market value reduction. Many investors want to invest in an organization that can protect their reputation. Insider threats indicate that an organization's management cannot protect shareholders' data.

Insider threats can also result in intellectual property theft. One of the most valuable assets for an organization is its trade secrets. Intellectual property theft has a significant impact on an organization and can result in loss of business. This information could be shared with competitors, or an employee could leave with it to start a new business. The employee may patent the new product, and the original owner cannot sue them for the theft [4]. Additionally, insider threats lead to loss of reputation. Business partners, customers, and shareholders can lose trust in an organization when they receive news of insider threats. It is difficult to rebuild lost trust, and the organization may fail to attract new investors, affecting its growth.

The legal impact of insider threats can significantly impact an organization's performance. There are legal and regulatory costs beyond the costs of prosecuting the case. An insider threat creates unpredicted costs, such as attorney costs and fines associated with failure to comply with industry laws and standards. For example, a malicious employee may run a program that prohibits it in a country. The company is liable for its employee's actions and may be forced to pay hefty fines[4]. Unfortunately, employees may leave the organization once they commit malicious activities, forcing it to spend more money on hiring new staff members to replace them. The following graph shows the average cost of insider incidents by profile.

Insider threats can also lead to market value reduction. When the image of an organization is damaged, investors are less interested in investing in the business. It shows that critical investor data can be accessed by unauthorized individuals, increasing data risks. Failure of an organization to attract investors can affect its daily business operations, leading to low productivity.

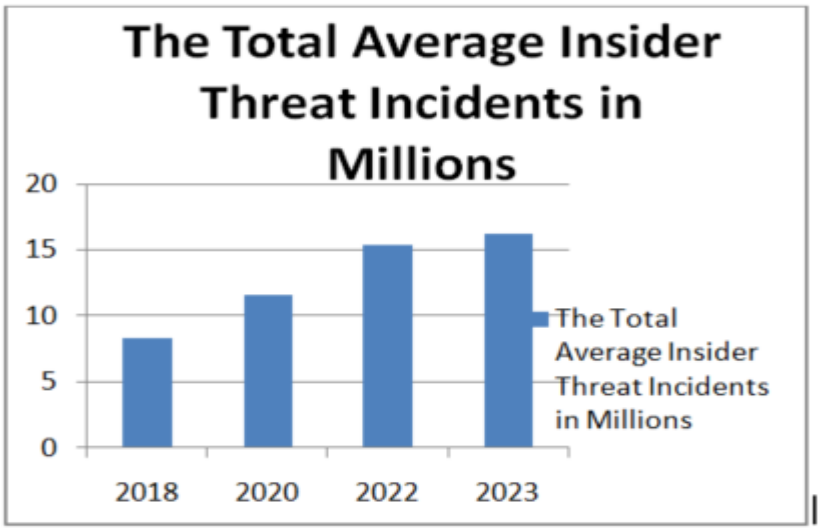

Fig 6: The average cost of insider incidents by profile. Adapted from [14].

The greatest impact of insider threat is operational interference. Malicious activities may interfere with critical infrastructure essential for company operations. For instance, an employee can introduce a virus in the It system, interfering with workflow. Glitches caused by the virus can also lead to defective products [3]. A sophisticated sleeper virus could affect an organization's operations, reducing its production capacity and lowering its product market capacity share. While many organizations have well-developed security procedures for using information systems, many employees do not adhere to them, leading to insider threats. Moreover, a lack of training for staff members exacerbates the problems, making it difficult for organizations to address them.

VII. CONCLUSION

- Insider threats present a dynamic and complex risk affecting private and public components of critical infrastructure.
- Insider threats can lead to critical data loss, affecting an organization's operations.
- A malicious insider could delete or steal critical organization data using a flash disk.
- The legal impact of insider threats can significantly impact an organization's performance.
- A PAM solution identifies technology, people, and processes that require privileged access and provides the protocols that apply to them.
- The solution must have capabilities to support industry regulations and organizational policies.
- A least-privilege policy in an organization is necessary to protect critical data like personal health information and payment information.
- Malicious insiders can cause significant consequences for an organization due to their knowledge of where sensitive data exists, including critical data loss, intellectual property theft, and loss of business.
- The zero-trust methodology provides the basis for this solution by encouraging organizations to develop multiple authentication and security protocols to grant account access.
- The Principle of Least Privilege (PoLP) is another strategy organizations use to reduce insider threats using privileged access management.
- An insider threat creates unpredicted costs, such as attorney costs and fines associated with failure to comply with industry laws and standards.

REFERENCES

1. Fang, Mei Lan, Sarah L. Canham, Lupin Battersby, Judith Sixsmith, Mineko Wada, and Andrew Sixsmith. "Exploring privilege in the digital divide: implications for theory, policy, and practice." The Gerontologist 59, no. 1 2019: e1-e15. https://doi.org/10.1093/geront/gny037
2. Syed, Toqeer Ali, Ali Alzahrani, Salman Jan, Muhammad Shoaib Siddiqui, Adnan Nadeem, and Turki Alghamdi. "A comparative analysis of blockchain architecture and its applications: Problems and recommendations." IEEE Access 7 (2019): 176838-176869.https://ieeexplore.ieee.org/abstract/document/8922632/
3. Harris, Clyde Device. Understanding Controls to Detect and Mitigate Malicious Privileged User Abuse. Diss. Capitol Technology University, 2020. https://www.proquest.com/openview/3879636d67ac0a70ec51fcddeb5b340a/1?pq-origsite=gscholar&cbl=44156
4. Jeong, Myeongki, and Hangjung Zo. "Preventing insider threats to enhance organizational security: The role of opportunity-reducing techniques." Telematics and Informatics 63. 2021: 101670. https://doi.org/10.1016/j.tele.2021.101670
5. El Mrabet, Zakaria, Naima Kaabouch, Hassan El Ghazi, and Hamid El Ghazi. "Cyber-security in smart grid: Survey and challenges." Computers & Electrical Engineering 67 (2018): 469-482.https://doi.org/10.1016/j.compeleceng.2018.01.015
6. Thomas, Jason. "Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks." Thomas, JE. 2018. Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International Journal of Business Management 12, no. 3 2018: 1-23. https://doi.org/10.5539/ijbm.v13n6p1
7. Safa, Nader Sohrabi, Carsten Maple, Steve Furnell, Muhammad Ajmal Azad, Charith Perera, Mohammad Dabbagh, and Mehdi Sookhak. "Deterrence and prevention-based model to mitigate information security insider threats in organizations." Future Generation Computer Systems 97. 2019: 587-597. https://doi.org/10.1016/j.future.2019.03.024
8. Ghaleb, Baraq, Ahmed Al-Dubai, Elias Ekonomou, Mamoun Qasem, Imed Romdhani, and Lewis Mackenzie. "Addressing the DAO insider attack in RPL's Internet of Things networks." IEEE Communications Letters 23, no. 1 (2018): 68-71. https://napier-repository.worktribe.com/preview/1319032/PID5634995.pdf
9. Uddin, Mumina, Shareeful Islam, and Ameer Al-Nemrat. "A dynamic access control model using authorizing workflow and task-role-based access control." Ieee Access 7 (2019): 166676-166689.https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8868170
10. Sindiren, Erhan, and Bünyamin Ciylan. "Application model for privileged account access control system in enterprise networks." Computers & Security 83 (2019): 52-67.https://doi.org/10.1016/j.cose.2019.01.008
11. Haber, Morey J., and Morey J. Haber. "Privileged access management." Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations 2020: 151-171. https://doi.org/10.1007/978-1-4842-5914-6_11
12. Cser, Andras, and BeyondTrustcyberArk. "The Forrester Wave™: Privileged Identity

Management, Q4 2018." Forrester Research, Inc. 2018. https://www.promero.com/wp-content/uploads/2019/02/forrester-wave-for-privilege-identity-management-2018.pdf
13. Paci, Federica, Anna Squicciarini, and Nicola Zannone. "Survey on access control for community-centred collaborative systems." ACM Computing Surveys (CSUR) 51, no. 1. 2018: 1-38. https://dl.acm.org/doi/pdf/10.1145/3146025
14. Liu, Liu, Olivier De Vel, Qing-Long Han, Jun Zhang, and Yang Xiang. "Detecting and preventing cyber insider threats: A survey." IEEE Communications Surveys & Tutorials 20, no. 2. 2018: 1397-1417.http://nsclab.org/nsclab/esi/comst_liu2018.pdf
15. Homoliak, Ivan, Flavio Toffalini, Juan Guarnizo, Yuval Elovici, and Martín Ochoa. "Insight into insiders and it: A survey of insider threat taxonomies, analysis, modelling, and countermeasures." ACM Computing Surveys (CSUR) 52, no. 2. 2019: 1-40.https://arxiv.org/pdf/1805.01612
16. The American's Cyber Defense Agency. Defining Insider Threats. Cybersecurity &Infrastracture Security Agency.https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats
17. Lacework. What is the principle of least privilege in cybersecurity?https://www.lacework.com/cloud-security-fundamentals/what-is-the-principle-of-least-privilege