Identity and Access Management risks

Presented by Nermen Mostafa Kamal

- Introduction
- IAM Risks
- Weak Authentication and Authorization Procedures
- Inadequate Access Control
- Human Error
- Malicious Actors
- External Threats
- The Impact of IAM Risks
- Conclusion

INTRODUCTION TO IDENTITY AND ACCESS MANAGEMENT

- Critical component of any organization's security posture.
- Process of controlling who can access what resources, and how they can access them.
- Source of risk if not managed properly.
- Risks associated with IAM can range from weak authentication and authorization procedures to inadequate access control.

IAM RISKS

01

Technical risks

- Weak Authentication and Authorization Procedures.
- Lack of encryption.
- Inadequate authentication.

02

Human risks

- User behavior and include unauthorized access.
- Misuse of data.
- Malicious attacks.

01 Technical risks

Weak Authentication and Authorization Procedures

- Weak passwords.
- Lack of multi-factor authentication.
- Security vulnerabilities.

Inadequate Access Control

- Access control measures are not properly implemented, users may be able to access resources that they are not authorized to access.
- This can lead to data breaches, malicious activity, and other security risks.

Solution:

- Ensure that access control measures are in place and that they are enforced.
- Creating user accounts with appropriate access levels, logging user activity, and monitoring user access.
- Regularly review access control measures to ensure that they are up-to-date.

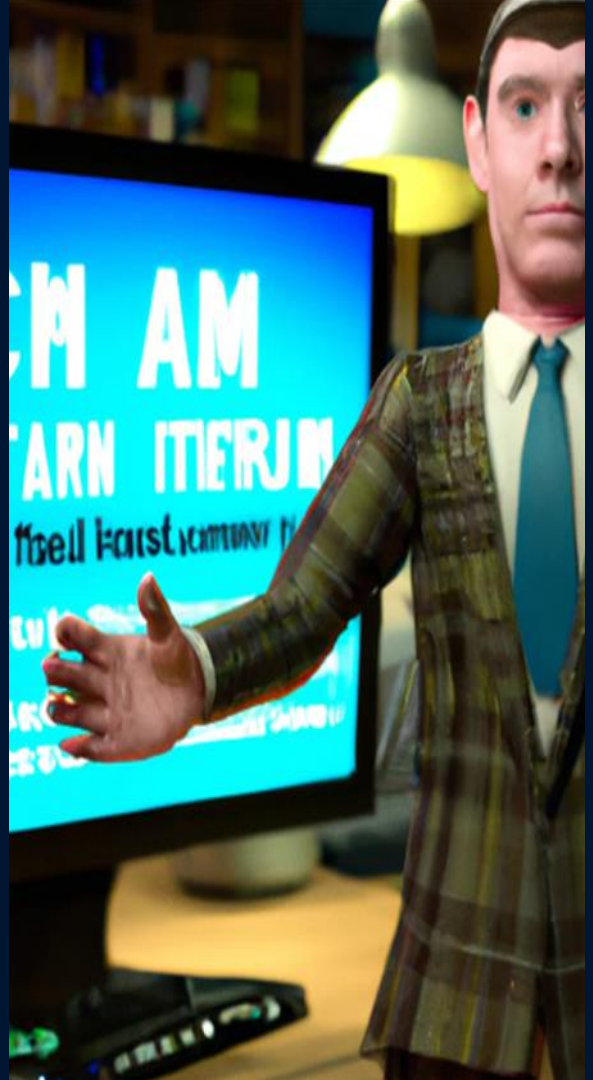
02 Human Error

Human Error

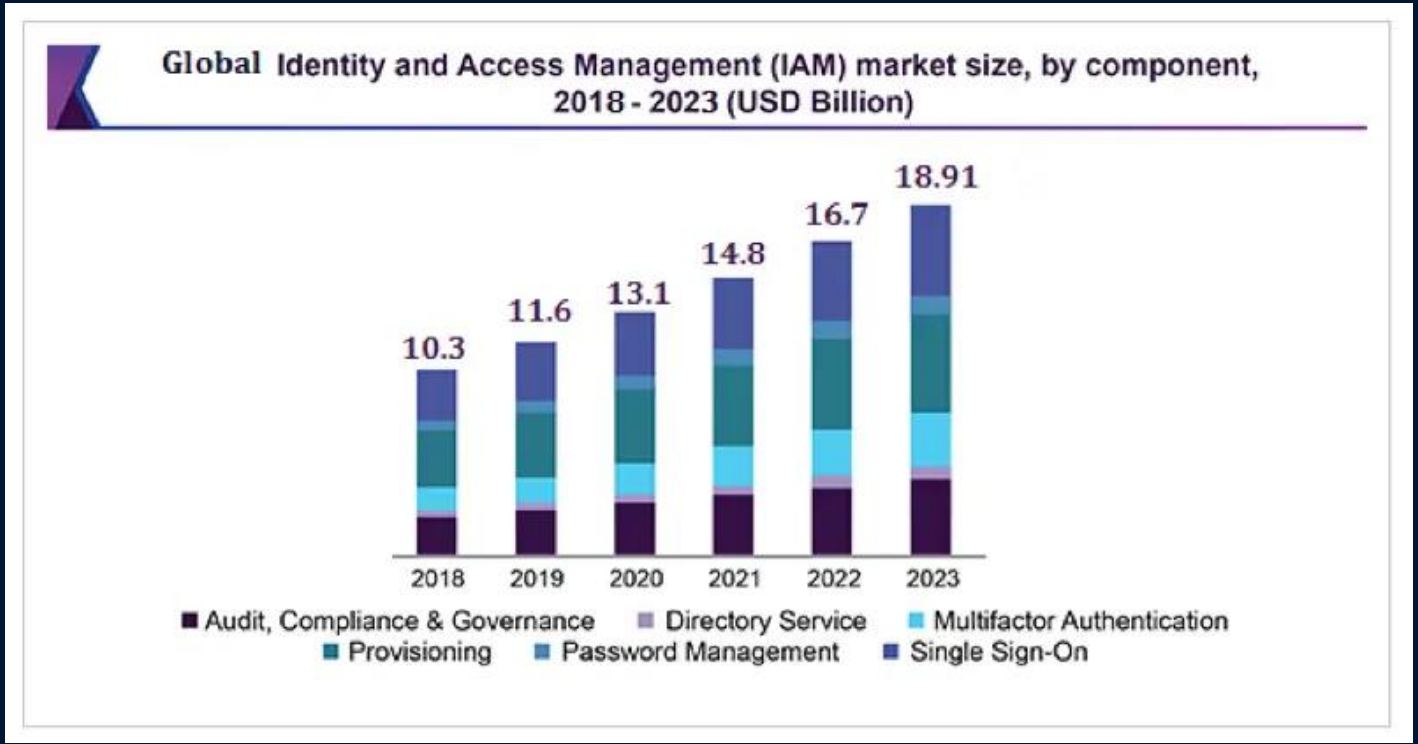
- Weak passwords.
- Sharing credentials.
- Granting unauthorized access.

Solution:

- Authentication and biometric authentication.



THIS IS A GRAPH!



Malicious Actors

- Gain access to resources, such as social engineering, phishing, and malware.

Solution:

- Strong authentication and authorization procedures.
- Access control, and user education.

External Threats

- Come from hackers, malware, or other malicious actors.

Solution:

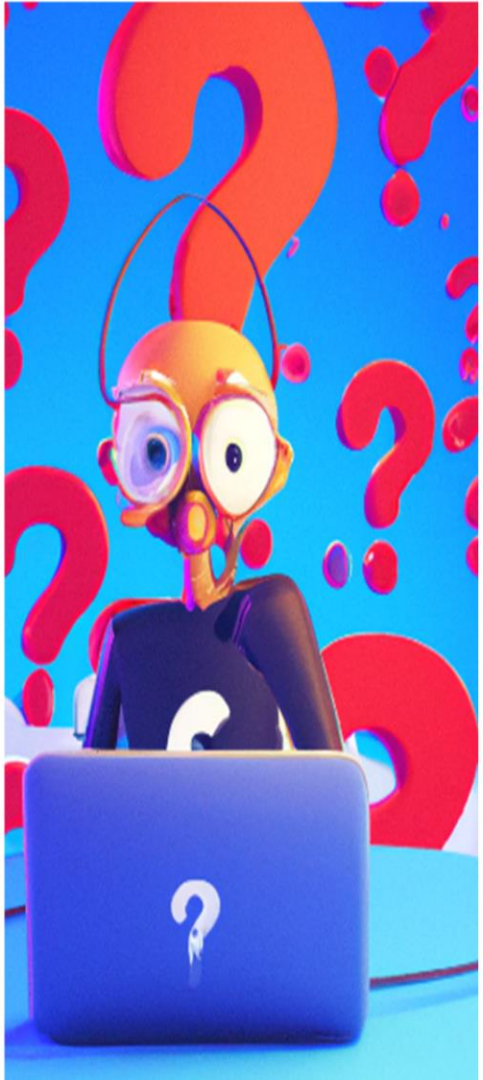
- Strong authentication and authorization procedures.
- Access control, and user education.

The Impact of IAM Risks

- Data breaches
- Identity theft
- Malicious attacks

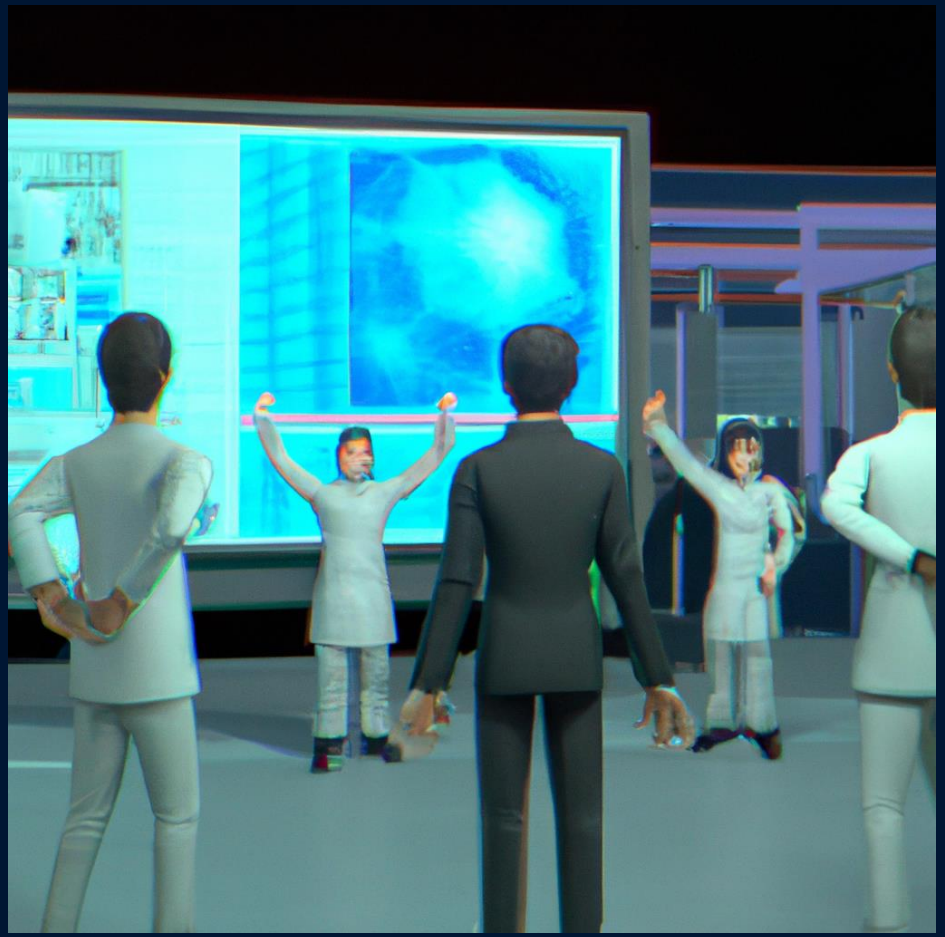
Result :

- Financial losses
- Reputational damage
- Regulatory penalties
- It is therefore important for organizations to take steps to mitigate IAM risks.



Conclusion

- Identity and Access Management (IAM) is an important for organizations to protect their networks and data from unauthorized access.
- IAM can also be a source of risk.
- Organizations should implement best practices to ensure the security of their IAM systems and regularly audit and monitor user activity.



THANKS!

Nermen Mostafa Kamal
Head of Identity and Access management (IAM) consultant.