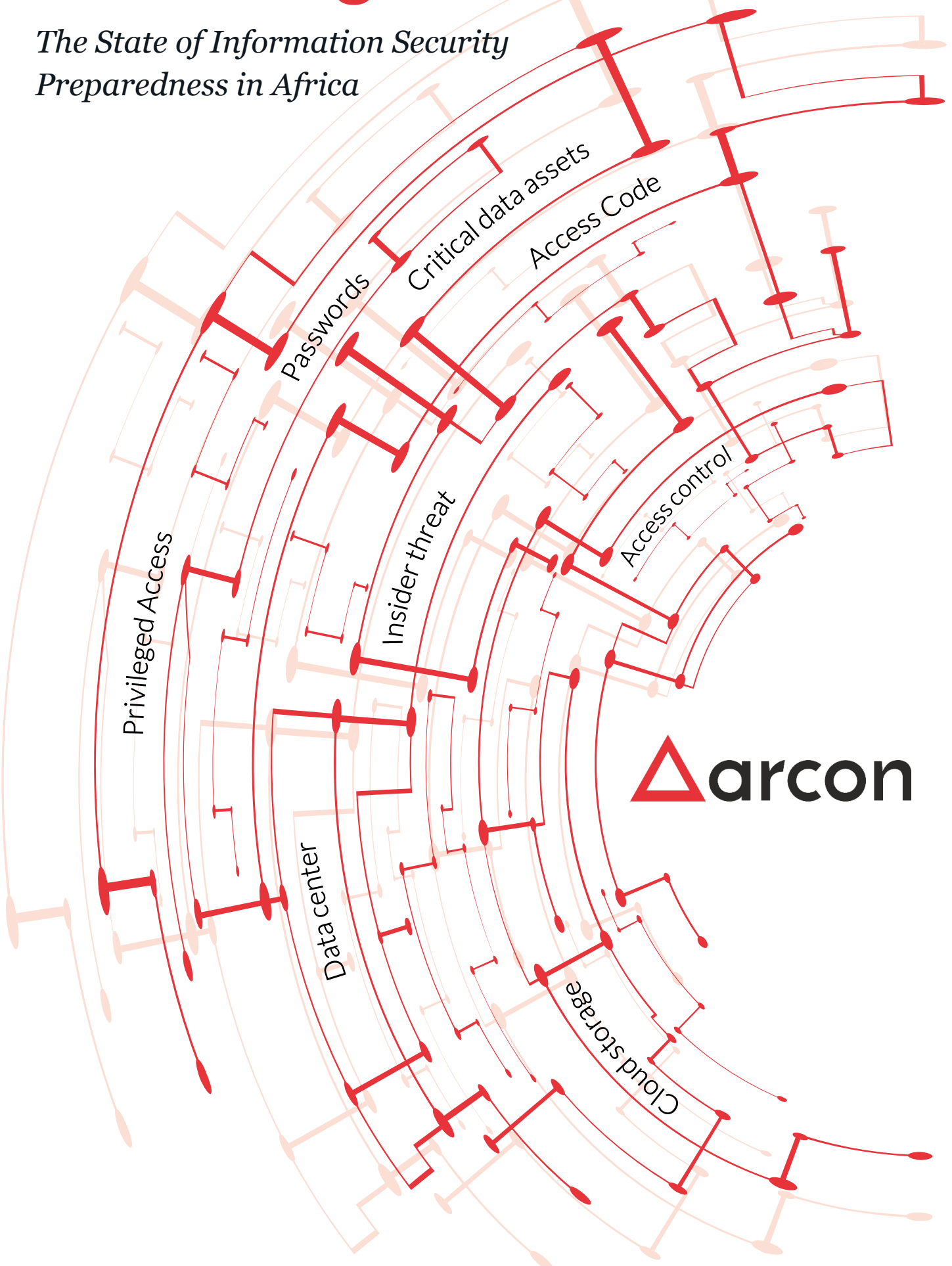
Protecting Data - 2019

The State of Information Security Preparedness in Africa



Darcon

Foreword

To stay afloat in the competition, organizations across Africa of all shapes and sizes are modernizing technology and IT operations. However, this IT-led business process transformation has increased security vulnerabilities. The nature of cyber risks are getting increasingly sophisticated in the expanding digital economy. Indeed, for a modern-day enterprise, protecting data remains a major challenge whether it is stored on-prem data centers, third-party servers, managed service environments, hybrid environments or cloud environments.

In this backdrop, a spate of major data breach incidents have jolted some of the biggest organizations in Africa. This report focuses to find out the state of data security preparedness in Africa.

Table of Contents

Introduction

After a successful release of our first exclusive Protecting Data survey report in 2017, we are pleased to publish our new report which is focused on the state of data security preparedness in Africa. Organizations from Africa remain increasingly vulnerable to data breaches. Being a thought leader in the Information Security space, ARCON decided to focus on this region to find out the root cause behind rising data breach incidents.

Renowned cybersecurity expert and ARCON Business Development consultant, Africa, Mr. Paresh Makwana decided to participate in several IT round-table conferences and summit, held across Kenya, Nigeria, South Africa and Ghana between 2018 and 2019 and met more than 100 IT professionals, CIOs, and CISOs from various industries such as Banking & Financial Services and Insurance (BFSI), Healthcare/ Pharmaceutical, Government, Retail, Manufacturing, Hospitality and Telecom to understand the state of IT and data security preparedness.

This survey report highlights some alarming statistics which might prompt the organizations to shore up their IT security policies and posture.

The Threat Landscape

Whether adaptation to cloud technologies or managed service environments, from global oil & gas majors to large banking institutions, enterprises spanning wide-ranging industries are shifting their workloads to distributed IT environments.

The transformation is bringing process improvements whilst enterprises cut operational expenses by diverting funds to other critical resources rather than spending money on legacy IT infrastructure present on-prem data centers.

However, controlling and monitoring IT users becomes a daunting task amid ever-expanding IT ecosystem. Securing corporate data is extremely important in this digital age. Who is accessing?; what is being accessed?; why was it accessed?; - are some of the important security measures that every enterprise should be able to keep a tab on.

Misuse of corporate confidential information often stems due to inadequate identity & access control management. Privileged accounts or Super Admin accounts that provide access to critical information are often accessed with shared credentials and without proper authorization and authentication mechanism. Malicious insiders or external malefactors such as third-party IT users could damage an organization by compromising “trusted privileges” to abuse confidential information.

Managing and securing privileged access remains one of the biggest pain-points for any organization. This enormous challenge arises due to a high level of complexity involved in managing a large number of privileged accounts that are present across IT ecosystem such as databases, critical business applications, CRMs, among several types of critical IT assets.

The Threat Landscape

Privileged Accounts typically get targeted due to the following reasons

Lack of stringent centralized access control policy

Shared accounts and shared privileged credentials

Absence of monitoring of privileged accounts

No password management policy

No reporting mechanism for privileged sessions

Privileged Access Management (PAM) can mitigate insider threats and third-party threats

Recently, there is a steep rise in the number of data breach incidents in Africa wherein most cases a highly elevated administrative accounts such as privileged accounts are targeted to steal or abuse sensitive business information. As we have already discussed the typical causes that expose these accounts, we do observe that malicious actors use social engineering, snoop credentials and misuse trusted privileges to target privileged accounts for accessing confidential business information.

The exclusive survey conducted by ARCON shows that 74% of the survey participants accepted that Privileged Access Management (PAM) is an area of concern for enterprise IT security.

Moreover, 79% of the survey participants have agreed to the fact that most of the data breach incidents happened in Africa are due to compromised privileged accounts. In addition, almost 50% of the participants in the survey agreed to the fact that absence of Privileged Access Management (PAM) is the major area of concern for information security.

To overcome these enormous IT pain-points and secure enterprise databases and critical business applications from malicious activities, enterprises need to adopt best privilege account management practices. Privileged Access Management offers the security team with a foundation to build a robust mechanism to manage, monitor and control privileged identities as every access to target systems is authorized, authenticated, and documented.

Paresh Makwana

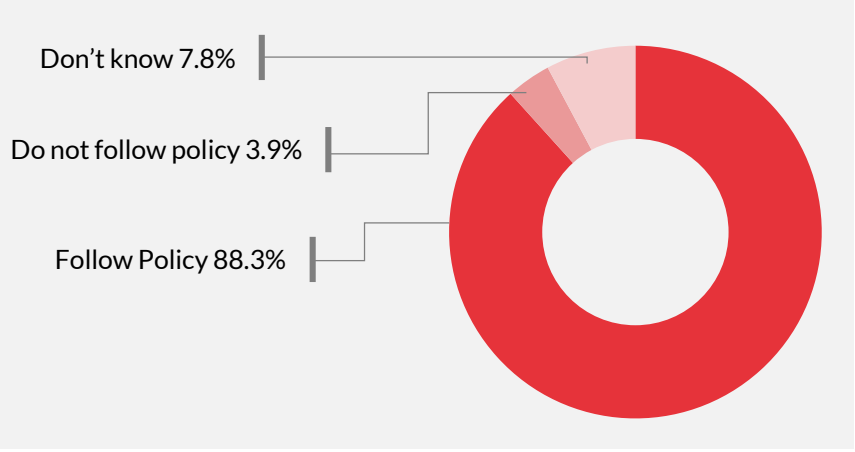
CISSP

Organizations' IT attack surface expands when adequate attention is not given to secure the access control mechanism. Typically administrative accounts are targeted by malicious insiders or compromised third-party users and sometimes organized cyber criminals. They are always on the lookout to steal or misuse information by making an unauthorized access to target systems. Privileged Access Management (PAM) practice helps an organization to establish a rule and role based centralized access control policy over users. Therefore, any malicious attempt to breach sensitive information is prevented and the IT administrator receives alert messages about the suspicious activities.

Survey Result

Question: Does your company follow digital/ cyber / information security and governance policy?

Answer: Yes: 88.3%; No: 3.89%; Don't know: 7.8%

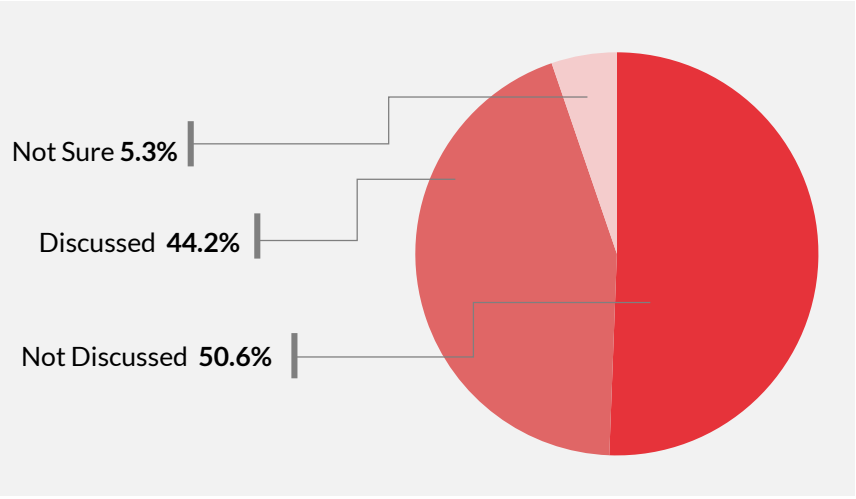


Analysis : Most of the respondents (88.3%) among all the participants in the survey acknowledged that they have information security and governance policies in their organizations. However, any of those policies hardly emphasize on the security of privileged accounts that are the gateways to crucial and confidential data. In fact, most of the organizations have confessed that they have not invested in Privileged Access Management (PAM) solution till date which is a matter of genuine concern.

Survey Result

Question: Is data theft a recurrent subject in boardroom discussions?

Answer: **Yes:** 44.2%; **No:** 50.6%; **Not Sure:** 5.3%

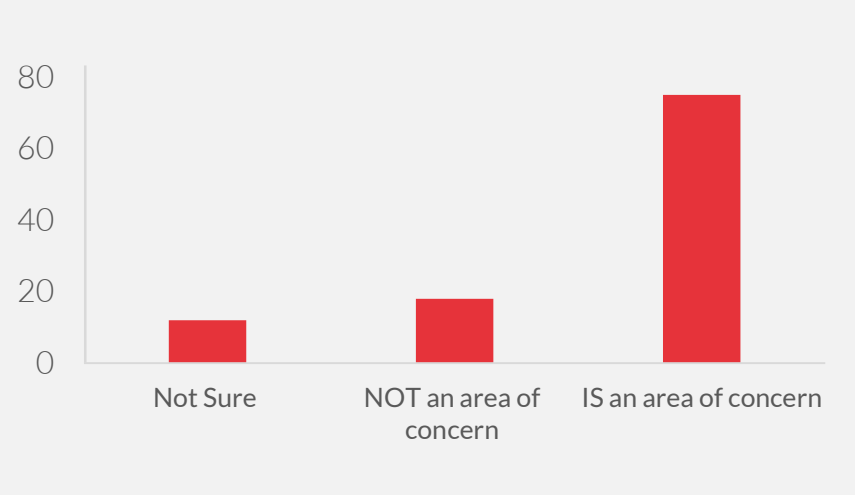


Analysis : Inspite of rampant data breach incidents hurting organizations; surprisingly, around 50.6% of respondents believe that data theft is not a recurrent subject of boardroom discussions. IT security personnel should make this matter more pronounced to the management and board so that everyone is on the same page regarding steps taken to mitigate data security threats.

Survey Result

Question: Is Privileged Access Management (PAM) an area of concern for your organization?

Answer: Yes: 74.02%; No: 16.88%; Not Sure: 8%

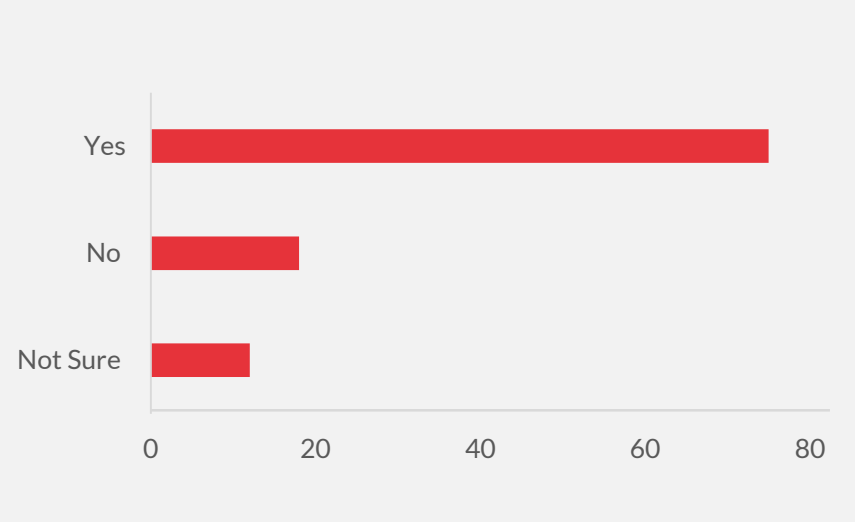


Analysis : 74% of the respondents agreed to the fact that PAM is a major area of concern for organizations today. With IT administrative accounts rising amidst ever growing layers of business applications and a host of IT devices, monitoring users in a controlled environment (role and rule based privileged entitlements) is critical to safeguard IT assets.

Survey Result

Question: Do you think that a data breach occurs due to the compromise of privileged accounts?

Answer: Yes: 79%; No: 12.98%; Not sure: 8%

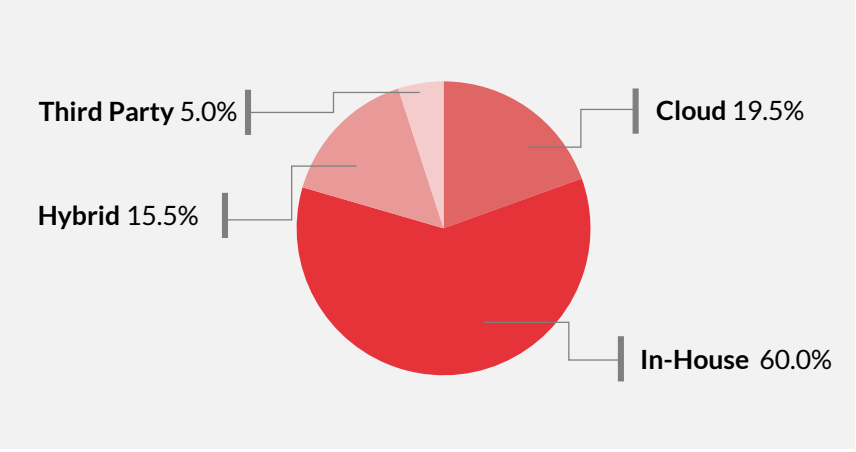


Analysis : The most important analysis comes from this statistics. More than 79% of the total respondents agreed that most data breach incidents happening today are due to compromise of privileged accounts. Unfortunately, the awareness alone is not enough to build up a secure IT environment. Implementing best privileged account management practices like access based on only "need-to-know" and "need-to-basis" and "principle of least privilege" along with frequent randomization of privileged credentials can make the IT security posture more robust.

Survey Result

Question: How is your data center managed?

Answer: In-House 60%; Cloud: 19.5%;
Hybrid Environment: 15.5%; Third-party: 5%

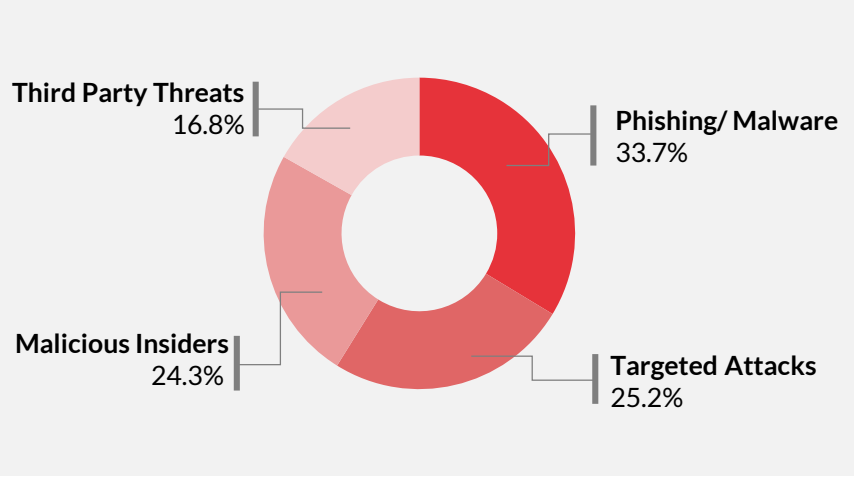


Analysis : While the survey shows that most organizations still manage and process data on-prem data centers, a substantial number of respondents said that they store data in hybrid or third-party environments. As migrating data in third-party environments involve an element of risk mainly associated with access control, an adequate security should be maintained to monitor and control privileged access to target systems.

Survey Result

Question: Who do you fear the most?

Answer:
Phishing/ Malware Threats: 33.7%
Targeted Attacks: 25.2%
Malicious Insiders: 24.3%
Third-party service: 16.8%



Analysis : While the statistics show that malware/ phishing remains as the topmost security threat, it is also observed that three quarters of security professionals surveyed fear third-party IT users, insiders and targeted attacks. It is important to note that the IT attack surface widens due to unmonitored privileged accounts. Malicious third-party IT users, disgruntled corporate insiders and organized cyber criminals snoop privileged credentials to target confidential information.

Survey Result

Question: Where do you foresee IT investments in the times to come?

Answer:

Privileged Access Management (PAM) : 48%

Database Activity Monitoring (DAM) : 41.55%

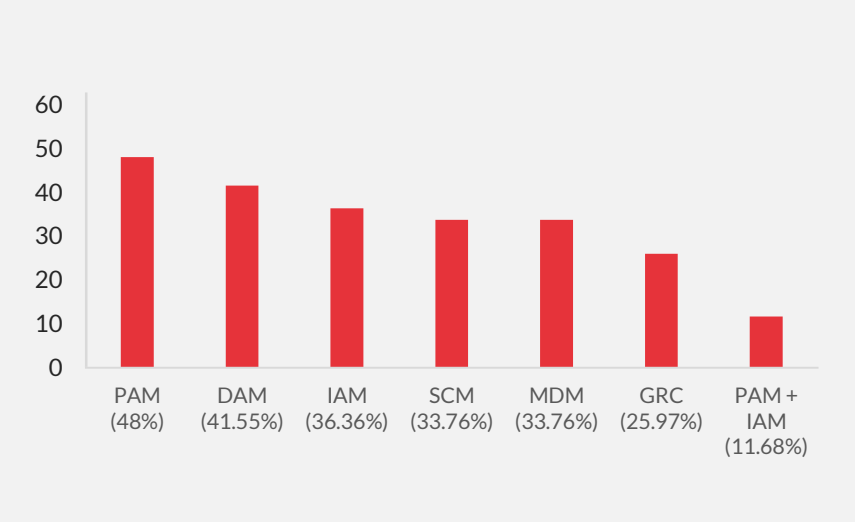
Identity Access Management (IAM) : 36.36%

Security Compliance Management (SCM): 33.76%

Mobile Device Management (MDM) : 33.76%

Governance, Risk and Compliance (GRC) : 25.97%

IAM + PAM : 11.68%



Analysis : Coming to the ultimate part of the survey, we did find that there are numerous information security risk areas that IT pros are concerned about in the times to come. 48% of the respondents felt that IT risk and security management team would like to invest in Privileged Access Management followed by Database Activity Monitoring (DAM) - almost 41.55% and Identity Access Management (IAM) - around 36.36%. In addition to these, 33.76% participants voiced their opinion for Security Compliance Management (SCM) and Mobile Device Management (MDM). Governance, Risk and Compliance (GRC) factor is also seen as a matter of concern because almost 25.97% respondents held that opinion; and finally, 11.68% respondents felt that both IAM & PAM technologies will be critical IT security investment areas.

Conclusion

The survey concludes that despite a high level of IT security awareness and robust corporate IT governance policies in Africa, the level of data security preparedness is still very low. Organizations will have to reinforce their privileged access to secure confidential and sensitive corporate data amid rising incidents of data breach.

Recommendations

- Implement a centralized access control policy
- Authorize IT users having an elevated permission to access privileged accounts
- Secure privileged access with Multi-factor Authentication
- Implement granular level control over privileged users
- Control escalation of privileged users by implementing the principle of least privilege
- Frequently randomize privileged credentials
- Document every privileged session; keep the audit trails

About ARCON

ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and continuous Risk Assessment solutions.

ARCON Privileged Access Management (PAM) is a leading global product and a robust solution that mitigates risks arising from privilege identity and access management.

Connect with at www.arconnet.com

Predict | Protect | Prevent


Critical data assets
passwords
Privileged Access
Cloud storage
Access Code
Access control
data center
Insider threat
Arcon