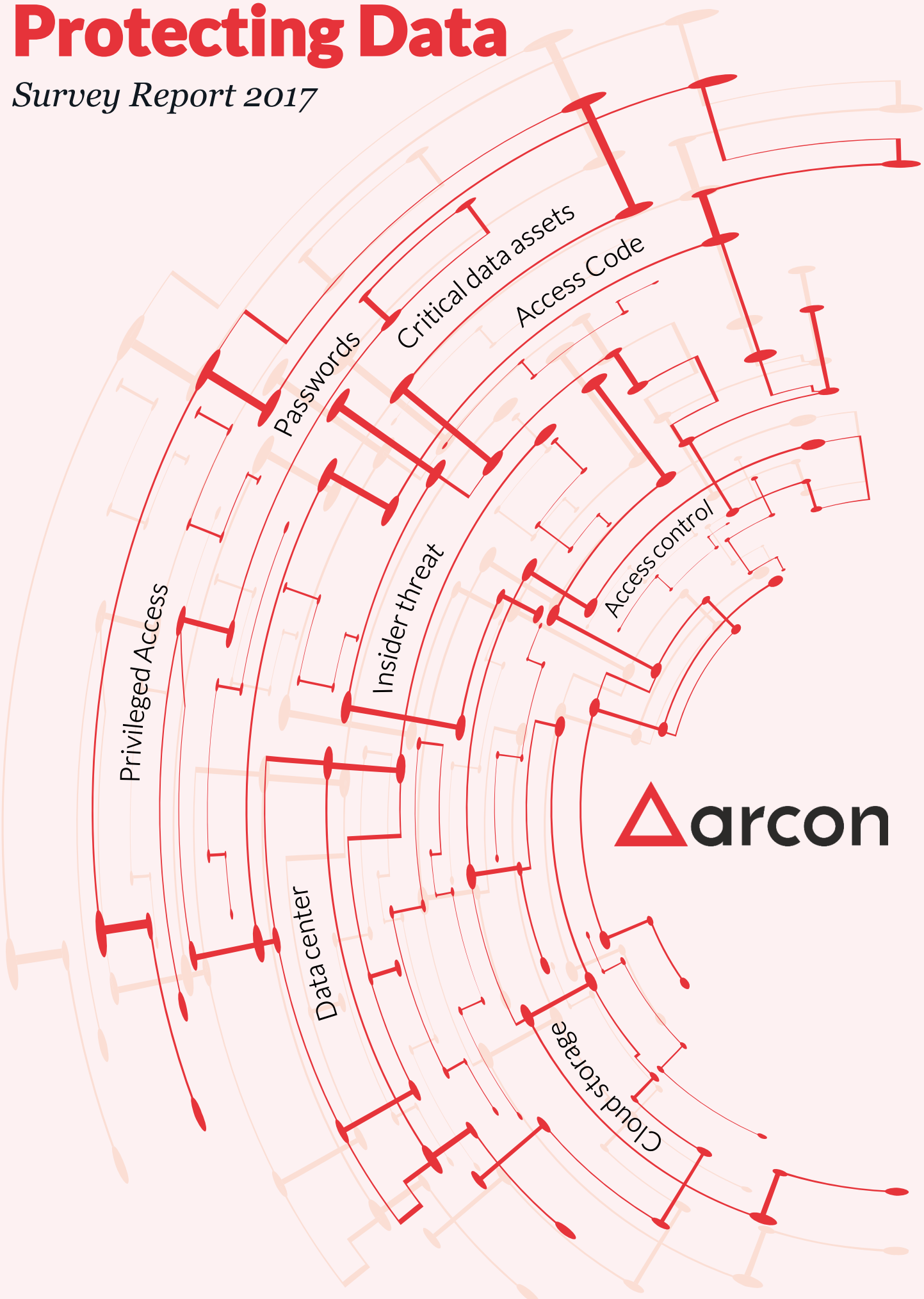
Protecting Data

Survey Report 2017



arcon

Every year, billions of dollars are spent on cyber security, yet extraordinarily organized and highly adept cyber crooks find ways to inflict heavy damage on global organizations by breaching critical digital assets.

They succeed in incising companies' reputation, brand value and steal a colossal amount of data because organizations often fail or pay scant attention to address data security gaps in their IT ecosystem. This report examines to what extent organizations are equipped to monitor and prevent unusual activity related to privileged access—one of the key risks to critical data.

Contents

Introduction

We are pleased to present our first ever report on data security. “The best preparation for tomorrow is doing your best today”... this famous quote by H. Jackson Brown, Jr., a famous American author known for his inspirational books inspired us to grind hard and find out why organizations remain increasingly vulnerable to data breaches as we yearn to become the thought leaders in our sphere of risk control.

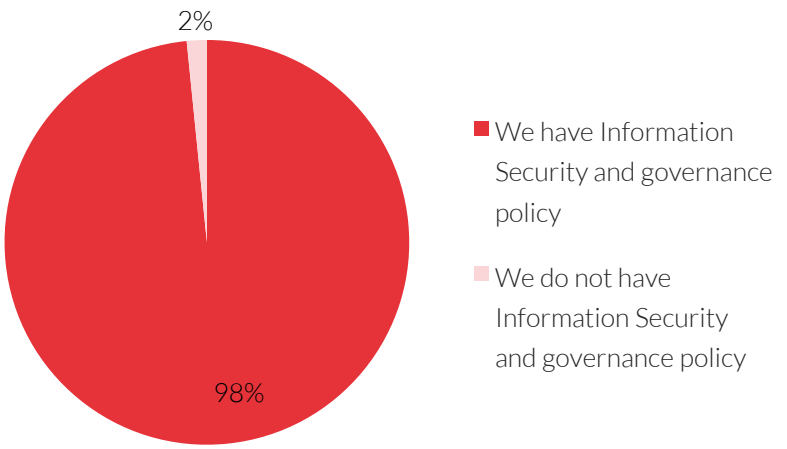
It took about six months for our dedicated teams to collate information as we met, discussed, and gathered opinion from Information Security professionals on a range of cyber vulnerability issues.

This report is based on responses from 188 Information Security professionals, comprising CIOs, CISOs and CTOs from various industries such as Banking Financial Services and Insurance (BFSI), Healthcare/Pharmaceutical, Retail, Manufacturing etc. across Asia, Africa, Europe, Middle East and North America.

Organizations are paying more heed to Information Security and governance

Question: Does your company follow Information Security and governance policy?

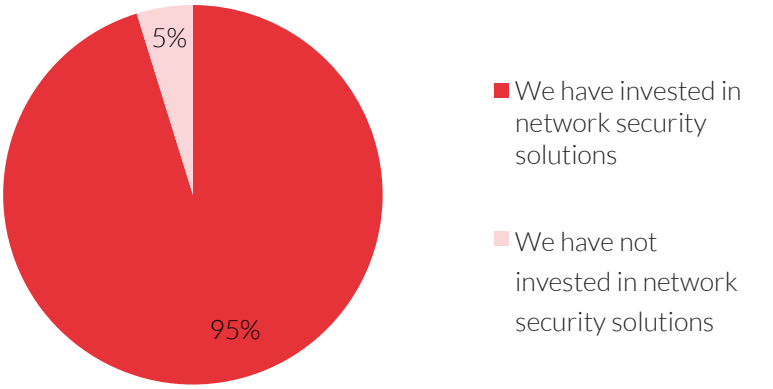
Result: Amid rising cybercrime, organizations have well-defined Information Security and governance policies. 98% of the organizations surveyed have Information Security and governance policies in place.



Analysis: Protecting critical business information assets is a recurrent subject in corporate boardroom discussions as the cost of cyber-attack becomes unfathomable even as the legal framework supporting Information Security gets more stringent. Therefore, it is absolutely vital for boards, the management, and compliance officers to remain on the same page for implementing Information Security and compliance policies. Ambiguity in this regard could leave an organization underprepared to prevent cyber-attacks.

Question: Have you invested in network security?

Result: 95% of the organizations have deployed network security solutions.

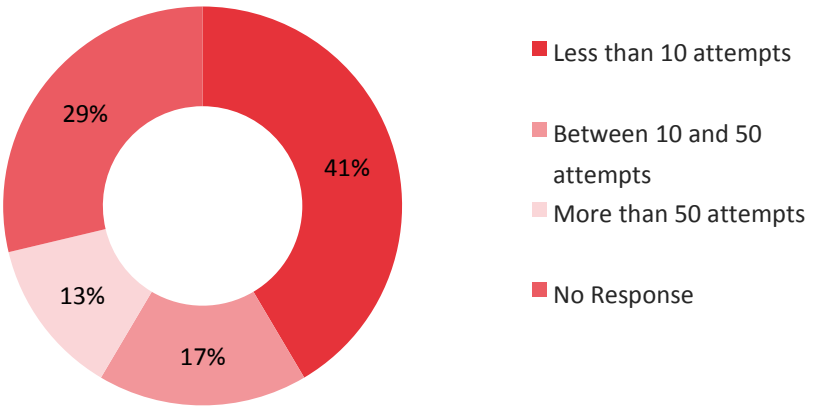


Analysis : As a part of broader cyber security policy, organizations are enhancing their network security by deploying network security solutions such as firewalls, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Virtual Private Network (VPN) etc.

Impact of compromised privileged access

Question: How many cases of unusual activity/ data breach attempts did you witness this year?

Result: 71% of the organizations surveyed suffered unusual activity or data breach attempts.



Analysis: Essentially, to prevent a data breach, organizations need to implement comprehensive mapping of their IT environment. Information Security staff should assess which endpoints in a given IT ecosystem malicious actor/s can exploit by targeting compromised identity and access control management.

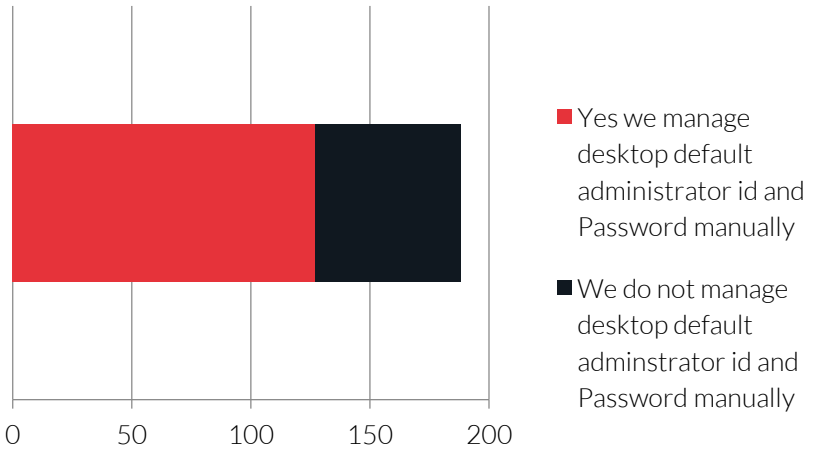
If those vulnerable endpoints get identified and patched at a right time, a serious threat such as data breach can be averted. While organizations have invested for strong information systems security in other domain, there is a clear lack of controls around endpoints in the IT ecosystem.

Most of the recent data breach incidents, involving many well-known organizations point out that compromised privileged access was a major security gap, causing unauthorized access to critical data assets.

Manually managing/changing passwords compromises IT systems

Question: Desktops' default administrator user id and Password: Do you currently manage manually?

Result: Nearly 70% of the surveyed organizations manually manage (change) desktop default administrator id and Password.



Analysis: A majority of organizations currently manage (change) desktop default administrator id and password manually, which is a cause for concern. The risk being from compromised insiders posing the biggest threat to an organizations' critical data.

The number of endpoints in a typical enterprise comprises of 100 to 1000 privileged accounts (more than 10,000 in case of a large organization). As these accounts enjoy elevated permission to access highly sensitive data, any rogue element can wreak havoc by misuse.

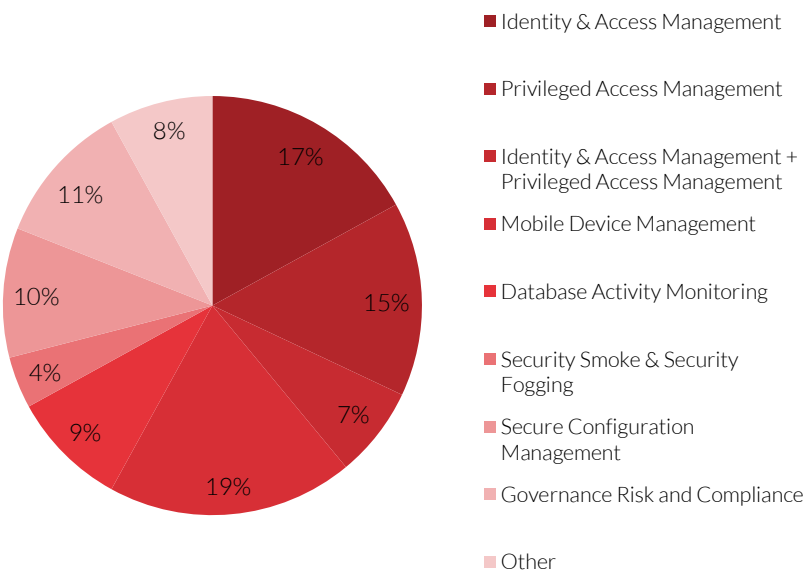
Most organizations currently lack Privileged Access Management, a highly effective solution that helps in monitoring and controlling activity around privileged access and passwords.

The solution also provides password vaulting features that ensures compliance with strength and frequency of change requirements demanded by regulators in a seamless manner. If done manually, such an exercise would be extremely challenging and hence the high occurrence of compromised systems in environments where privileged account credentials are managed manually.

Not surprising data security is the foremost concern for global Information Security professionals

Question: Where do you foresee firms spending the most for data security in times to come?

Result: About 40% of the respondents felt that organizations will spend the most in strengthening identity and access controls. The responses identified the following areas for spend:

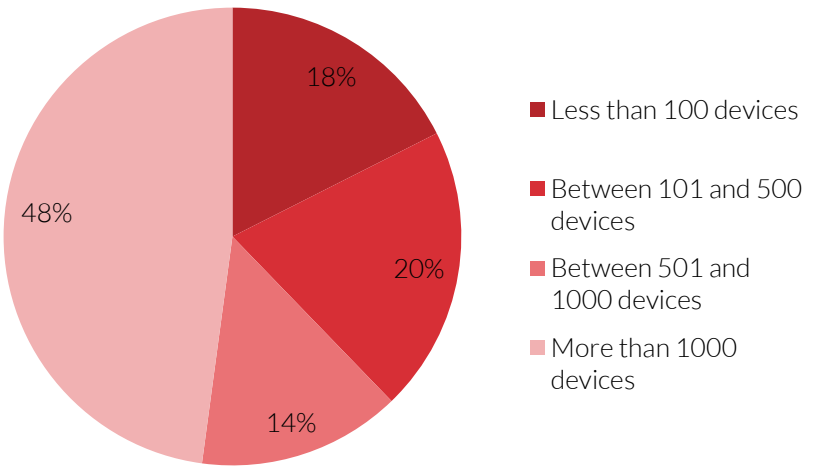


Analysis: As identity theft and data breach incidents rise amidst commercialization of cybercrime, organizations across the world are likely to spend more on securing critical data assets by reinforcing the Identity and Access Control management.

Why privileged access is vulnerable to misuse?

Question: How many devices does your company have?

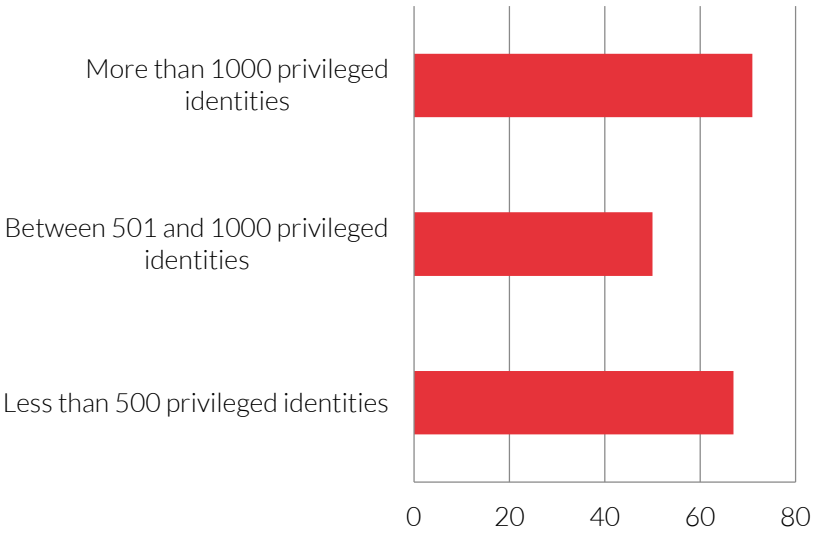
Result: About 60% of the surveyed companies have more than 500 devices.



Analysis : As data center devices proliferate, the number of privileged identities/accounts also multiplies. It is a huge challenge for organizations to monitor and control the activities of these large number of privileged accounts. Hence, in an uncontrolled/unmonitored environment privileged access is vulnerable to misuse.

Question: How many privileged identities does your organization have?

Result: About two third of the surveyed organizations have more than 500 privileged identities.



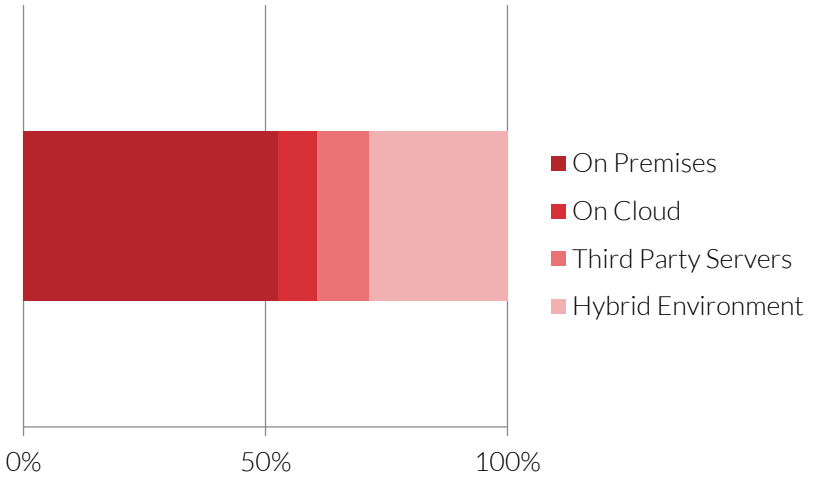
Analysis: The most important thing to keep in mind is that all identities are not alike. While many of those are administered by 'regular users', a growing number of identities have elevated permission to access highly classified information stored in computers, database servers, and applications. These identities with elevated permission to access critical data are called as privileged accounts or privileged identities.

In many cases, organizations fail to keep a check on to the number of privileged identities that exist within IT ecosystem. If organizations fail to control and monitor the growing number of privileged identities, malicious insiders can exploit the security gaps and steal data by gaining unauthorized access to network devices and data stores.

The threat level will only rise as firms shift data centers to cloud and hybrid environment

Question: How is your data center managed?

Result: 47% of the organizations store data on cloud, third-party servers or hybrid environment.



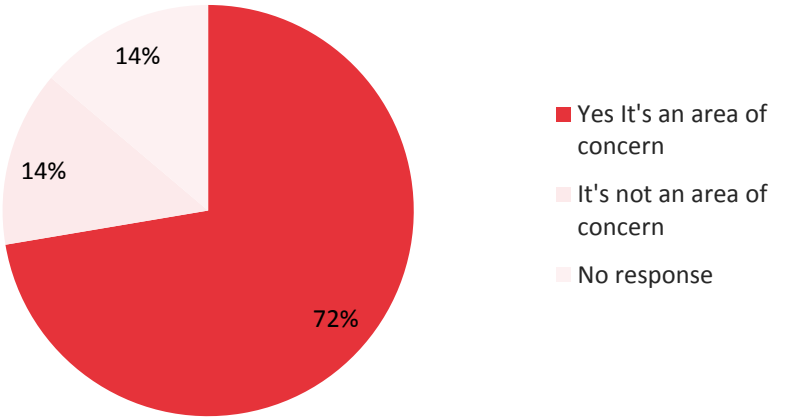
Analysis: Cloud computing is fast gaining acceptance among global organizations. Migrating and sharing data on cloud servers boosts operational efficiency. With several big technology companies providing cloud computing and storage services, it is believed that organizations will migrate data either completely on cloud or manage in a hybrid environment (on premises and cloud), in the coming years.

Cloud storage is not completely secure though. Shifting data to cloud essentially means storage location is beyond organization's premises. It brings shared vulnerabilities. A poor data back-up policy or lack of security and access control at cloud service provider's premises can compromise organization's critical data assets.

Protect data center like a fort but also be vigilant within your empire

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

Result: Almost three quarters of the total respondents agreed that that Privileged Access Management is an area of concern for their organizations.

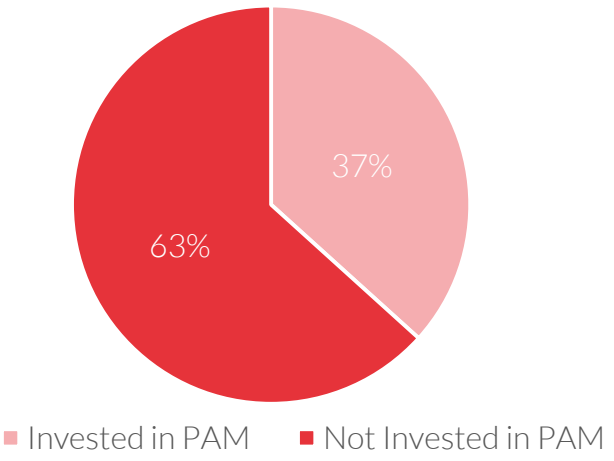


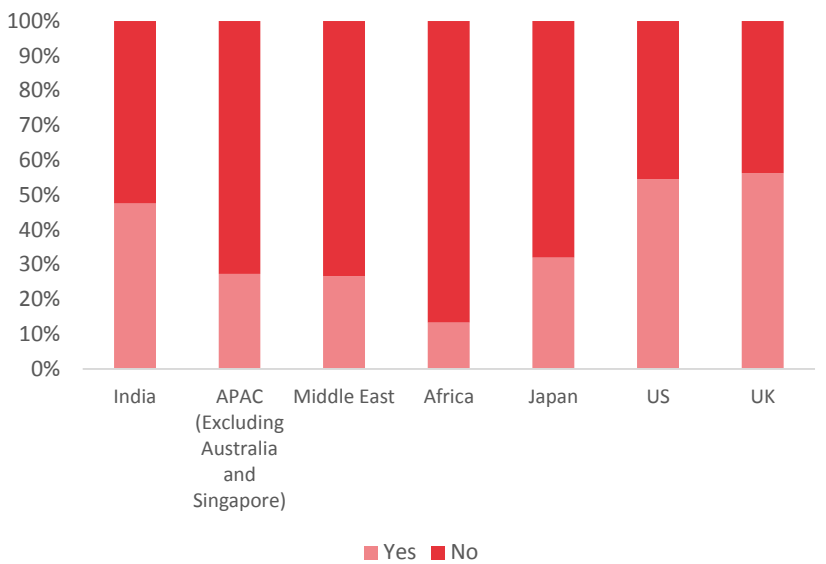
Analysis: Ever wondered why ancient empires such as Roman, Persian, and Greek etc. flourished? Their sheer might decimated the enemies; but more importantly, these empires maintained strong forts that played a crucial part in defending home territories. An organization is like an empire – always vulnerable to attacks from all quarters. That's why organizations should protect their data center like a fort. Accordingly, Information Security staff deploys expensive security solutions to protect information assets from external threats.

Organizations like empires could crumble if the focus remains only on external threats while missing out on insider threats… the enemies within. Not surprising, privileged access management is an area of concern for global organizations and requires due attention.

Question: Has your organization invested in Privileged Access Management solution (PAM)?

Result: More than 60% of the organizations surveyed have not deployed Privileged Access Management solution.

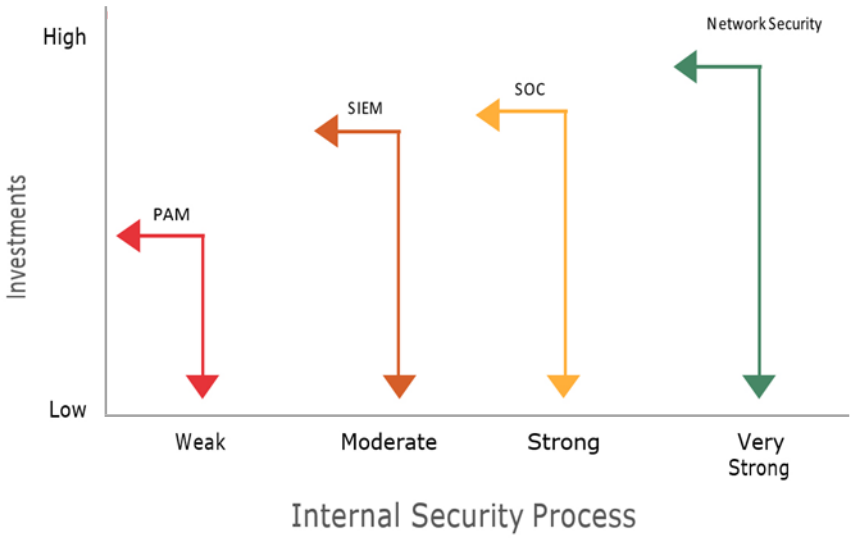




Analysis: While most organizations agreed that Privileged Access Management (PAM) is an area of concern, the level of preparedness is not up to the mark. Organizations in India, US and UK showed relatively higher PAM adoption rate; however, APAC, Japan, Middle East and Africa lag in implementation of Privileged Access Management solution.

Conclusion

In the Information Security domain, Privileged Access Management is an area where global organizations are least prepared. Investments made on network security solutions are high but security spending on monitoring and controlling privileged accounts remains inadequately low. Therefore to provide a balanced protection, organizations must consider deploying a Privileged Access Management (PAM) solution.



Recommendations

- Secure, manage and monitor privileged accounts
- Record all the privileged user activities and plan for a regular audit
- Keep a detailed account of all critical IT assets and privileged accounts.
- Outline a policy regarding privileged access to IT systems (time-bound access, dual control authorization etc.)

About ARCON

ARCON is 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 out of 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