BSP Circular 982

Are financial institutions in the Philippines geared up to secure critical information?

Table of Contents

Introduction

The data security framework needs to be robust for today's organizations as these entities continue to adopt digitization for streamlining IT operations. As data traverses through multiple devices, a large network of users and workloads are getting migrated to hosted environments, the regulators demand adequate security controls to mitigate risks of data theft or misuse.

Indeed, protecting data remains the topmost security concern for compliance and risk management officers as insider and third-party threats to confidential information is increasing every year at an alarming rate. It is extremely exigent for global organizations to delve deep not only into network security but also ensure comprehensive protection of their digital assets through real-time monitoring of users within the perimeter. And this security framework can only be strengthened when privileged identities are provided robust protection.

The BSP Circular 982 explicitly demands from Philippines's financial institutions to strengthen data security, which implies that these organizations will be required to carefully frame data access and control policies. In this whitepaper we will discuss what this circular mandates to secure information assets, which security vulnerabilities are faced by Philippines's financial institutions and what could be done to protect the data to comply with the BSP Circular 982. The whitepaper includes survey results from an exclusive IT summit wherein ARCON interviewed IT security pros from the Philippines.

BSP Circular 982: A mandate to secure information assets

The fast pace of digital transformation and subsequent evolving IT threats necessitated stringent compliance framework in the Philippines. The nation's central bank - Banko Sentral NG Pilipinas (BSP) issued a circular (982) in November 2017 that seeks to strengthen financial institutions' IT security blueprint. It seeks to enhance the cyber security policies among the organizations, especially from BFSI industry. The main objective of this circular was to make private and Government organizations from Philippines compliant to BSP Circular 982 and increase awareness to protect information assets from malicious actors and advanced cyber-threats. The digital information includes confidential business information, client/ customer details (personal details like name, email ID, contact no, etc.) or even corporate financial details among other types of sensitive data.

BSP Circular 982: A mandate to secure information assets

Sr. No.	Circular No.	BSP Circular 982 Mandates
1	**Section2 Subsections X177.3and 4177Q.3, 4196S.3, 4177P.3 and 4196N.3**	These subsections mandate securing: 1. IT Infrastructure and operations 2. Digital/ Electronic financial products & services 3. IT projects & initiatives 4. Outsourced services 5. IT infra from digital threats
2	**Section3 Subsections X177.5 and 4177.5, 4196S5, 4177P.5 and 4196N.5**	It underpins several IT security safeguards to comply with the security standards of MORB (Manual of Regulations for Bank) and MORBNBF (Manual of Regulations for Bank & Non-bank Financial Institutions). It includes: 1. APTs (Advanced Persistent Threats) 2. Cyber Threats 3. Cyber Security 4. Information Security Risk Management 5. Threat Intelligence
3	**Section 4. Item 3. A of Subsections X177.7 and 4177Q.7, 4196S.7, 4177P.7 and 4196N.7**	It underpins critical measures that demands complying with the amendments of MORB (Manual of Regulations for Bank) and MORBNBF (Manual of Regulations for Bank & Non-bank Financial Institutions) which deals with IT Risk Management System (ITRMS). It includes 1. Information Technology 2. Information Security Risk Management Framework (ISRM) 3. Cyber Threat Intelligence & Collaboration

What does the BSP Circular 982 imply?

Essentially, the BSP Circular 982 mandates financial institutions to shore up both network and IT infrastructure security. It requires security and compliance management teams to enhance their Information Risk Management framework by reinforcing the security around data assets spread across the IT network with the help of advanced threat detection capabilities.

Reinforcing security around Privileged Identities

Privileged identities are the most vulnerable IT assets for any organization. More than two thirds of data breach incidents occur due to compromise of privileged credentials, several research reports show.

Malicious actors -- compromised or disgruntled insiders, organized cyber-criminals, and malicious third-party IT users -- can cause serious damage if privileged identities, a gateway to critical systems and found across IT networks (databases, applications, cloud resources, hosted third-party environments such as MSP) are abused. The purpose of privileged identities abuse could be greed, personal animosity, corporate espionage or service disruption.

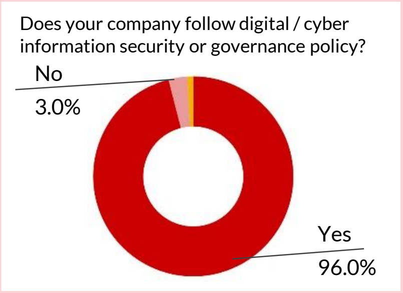
Enforcing security controls around privileged identities build the foundation for robust Information Risk Management framework. Data breach occurs, typically, when privileged accounts are not monitored, controlled and documented and access to critical systems does not have robust authentication mechanism or privileged passwords are not vaulted.

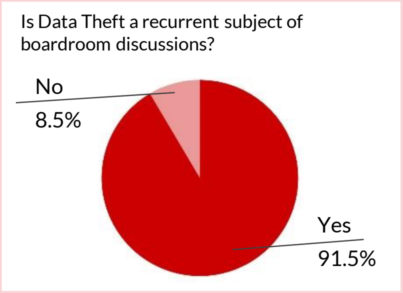
Are Philippines Organizations effectively implementing the BSP Circular 982?

ARCON recently participated in The Information Security Officers' Group Technical Barrier To (ISOG TBT) event in the Philippines on 28th June, 2019 and got the opportunity to conduct an exclusive survey among Information Security pros with a set of questions that helps in assessing cyber security preparedness in the region. Although ARCON do feel that organizations, especially financial institutions, are very agile in adapting to necessary security safeguards, the privileged access management is still not up to the mark. It's a huge concern because a robust privileged access management ensures rule and role based access to databases and applications, which minimizes the attack surface across the enterprise network.

The Survey Results

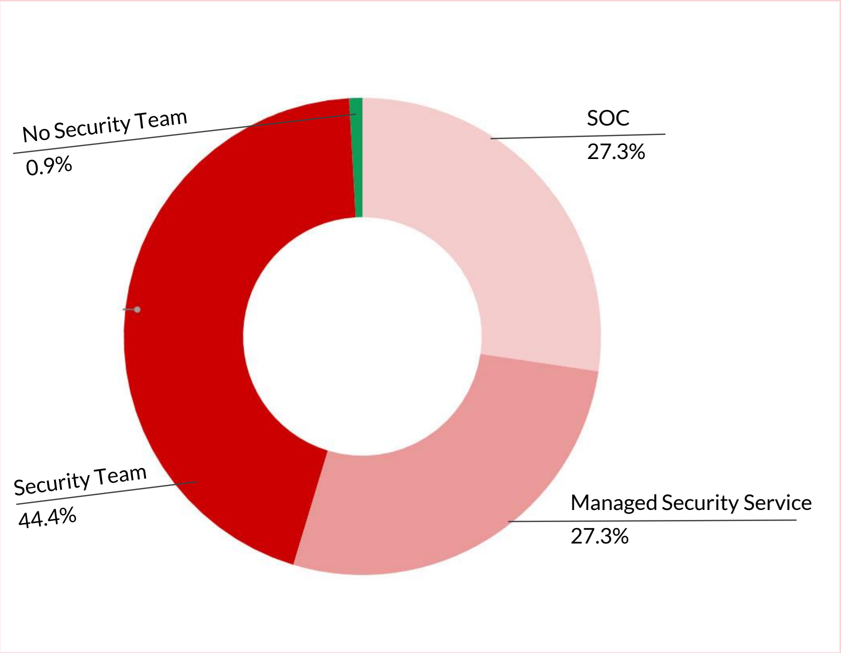
Let us analyze the situation based on the questions and the feedback received.





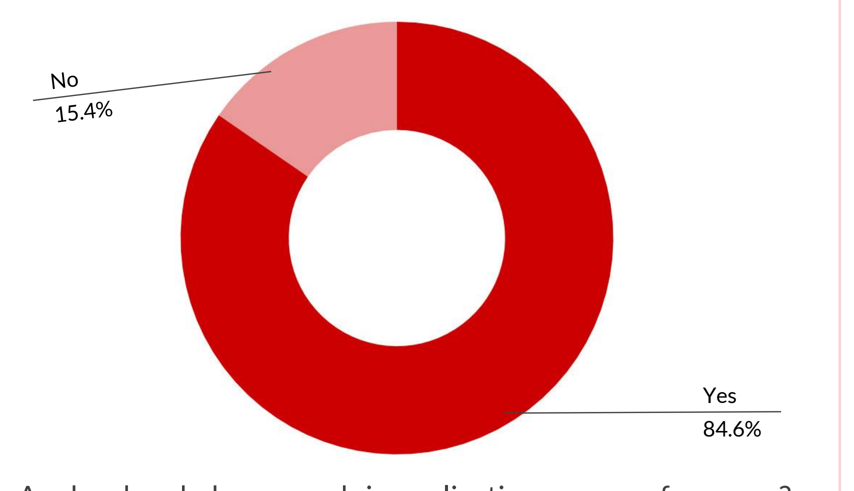
Analysis: Our survey shows that Philippines's organizations have a strong cyber-security framework. 96% of the respondents agreed to have information security and governance policies within their organizations. In addition, more than 90% organizations agreed to the fact that data theft is a subject of boardroom discussion which shows that the concern for data security is the topmost among risk and compliance officers due to increasing data theft incidents. Organizations agree that it's critical to have robust Information Security framework to protect enterprise digital assets, as mandated by the BSP Circular 982.

How do you monitor and respond to security incidents?



Analysis: Almost 50% of the respondents opined that their organization depends on the internal security team to respond to any security incidents. While it is good to learn that half of the organizations have dedicated their security teams to tackle cyber security concerns, at the same time we don't come to know whether those security teams are vigilant about the user activities in the organization. It is also important to note whether the organization is having any risk-assessment and real-time monitoring mechanism, which can protect the privileged accounts from misuse.

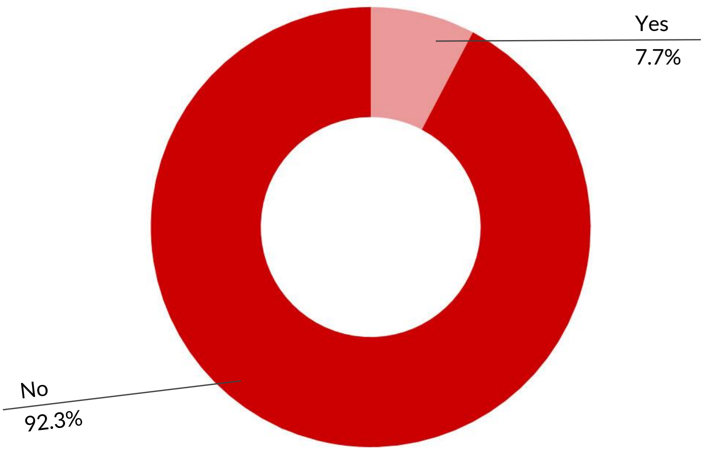
Are hard-coded passwords in application an area of concern and are you looking at automatically changing these passwords?



Are hard-coded passwords in application an area of concern?

Analysis: Almost 85% of the respondents believe that hard-coded passwords is an area of concern for securing enterprise data assets from malicious activities. Hard-coded passwords normally affect operational efficiency and hurt business process continuity. Hard-coded password management is tedious and manual and while there are benefits of hard-coded passwords like it can be encrypted, it does not offer the liberty of randomizing passwords (privileged password vaulting) -- so important to ensure authorized access and mitigate malicious activities centred around privileged identities.

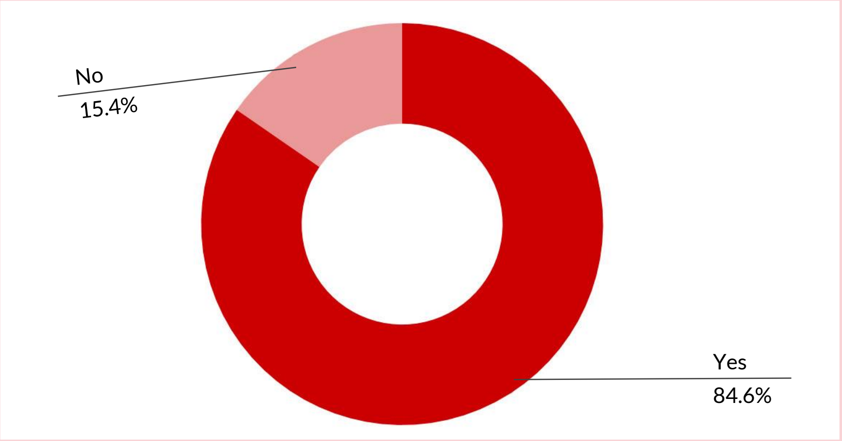
If your response is NO for the previous question, do you use an automated tool for a password change?



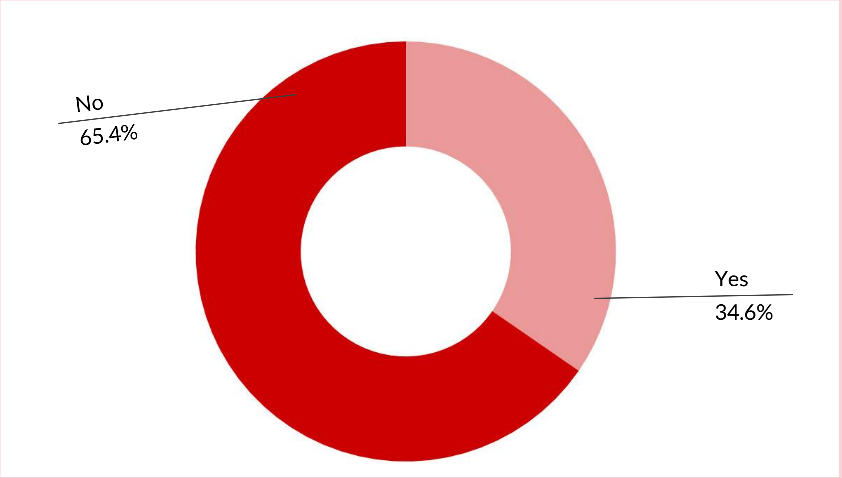
Do you use an automated tool for password change?

Analysis: This is a matter of grave concern that organizations are lacking automated tools for password management. As we discussed earlier, malicious actors snoop privileged credentials to steal data or launch attacks on critical business applications. If privileged passwords are stored in files and spreadsheets, it incentivises malefactors. Password Vaulting not only secures passwords, it automates the process by frequently randomising them as mandated by regulators.

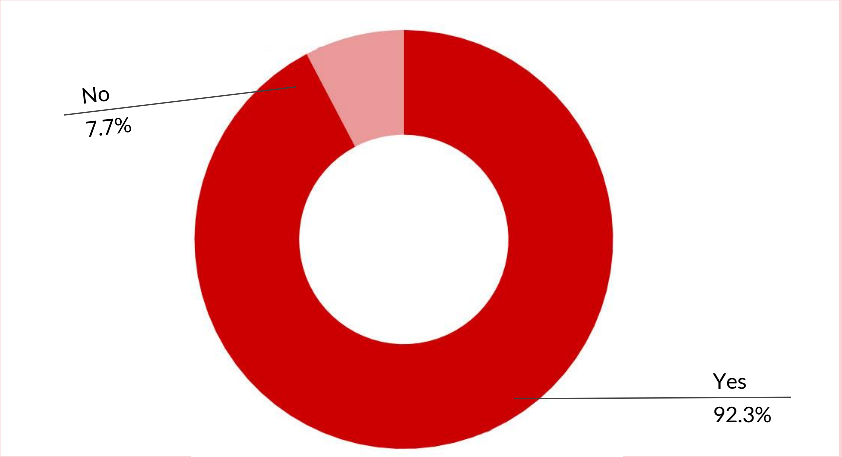
Is Privileged Access Management an area of concern for your Organization?



Has your organization invested in PAM?

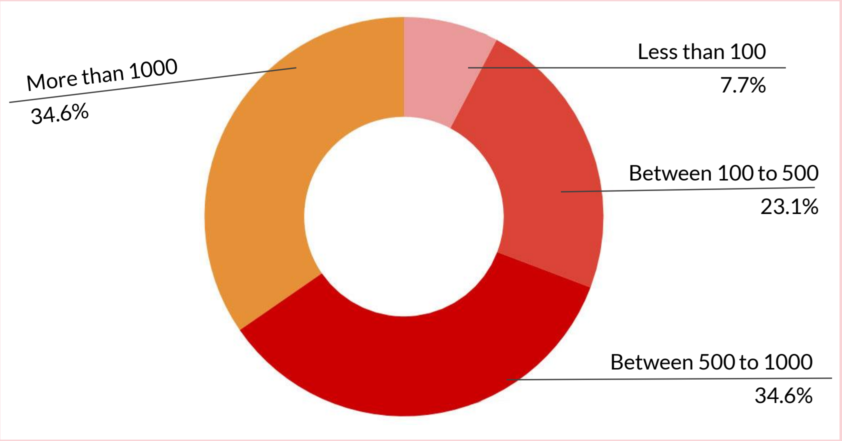


Do you think that a data breach occurs due to the compromise of privileged accounts?

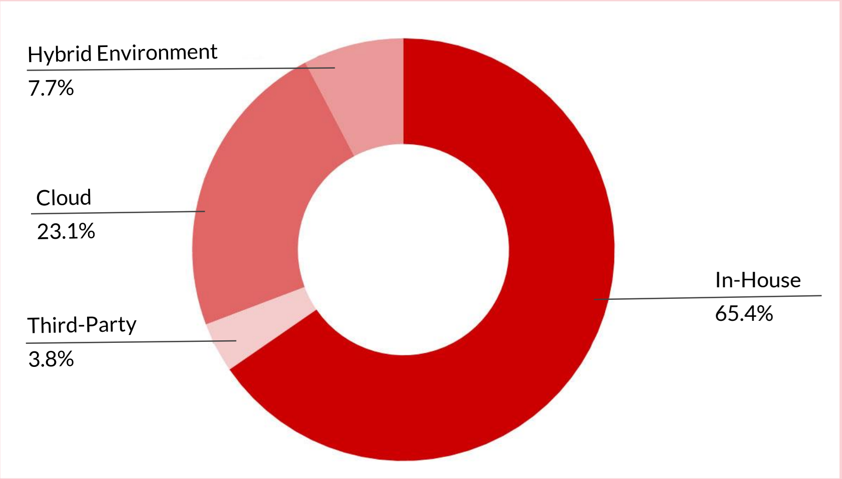


Analysis: Coming to Privileged Access Management (PAM) - the most crucial part of this survey, we do notice that almost 85% of the respondents surveyed believe that PAM is a big area of concern. The main reason behind this is almost 92% of the surveyed respondents believe that most of the data breaches happen due to compromise of privileged accounts. Inspite of this fact, we surprisingly notice that more than 65% of the organizations have not invested in Privileged Access Management technology. In order to effectively implement the BSP Circular 982, it is critical to protect privileged identities, the foundation of robust identity and access control management and Information Risk Management.

How many devices would your company have? (like server, database, security devices, network equipment etc.)



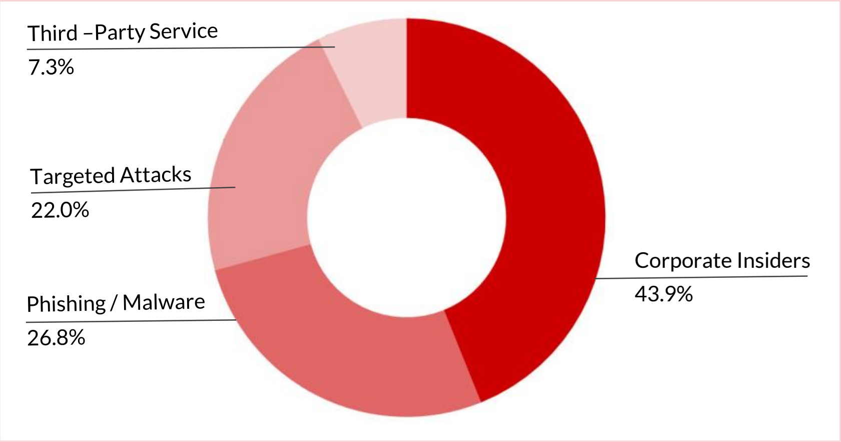
How your data center is managed?



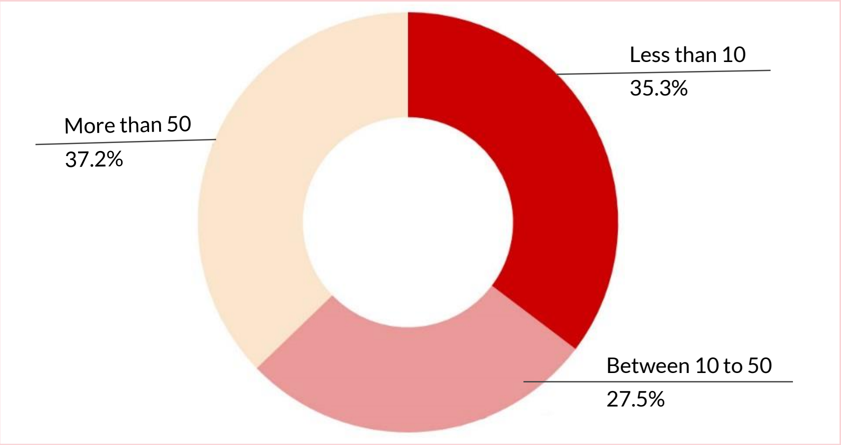
Analysis: We found that almost 35% of the organizations have more than 1000 devices. Higher the number of devices, the greater number of privileged identities-- and so the higher chance of possible misuse of privileged identities. Privileged Access Management offers an additional layer of security as every access to systems is authorized, authenticated and documented.

Likewise, 45% of the respondents mentioned that their data centers are managed by their in-house teams. It would be wrong to presume that data center managed by in-house team is inefficient or risky way (since the factor of human error is always there) to manage data assets but Privileged Access Management (PAM) automates data center activities.

Who do you fear the most?

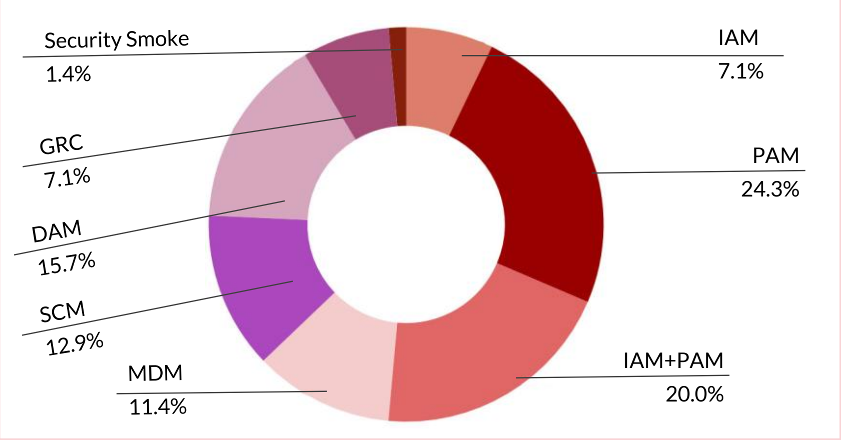


How many cases of data breach have you witnessed this year?



Analysis: This is another crucial part of the survey where almost 37% of the organizations have confirmed that they have witnessed more than 50 data breach incidents in the current year so far. This shows the amount of risks the organizations are bearing regarding securing their data assets by not deploying Privileged Access Management solution for their enterprise IT ecosystem. In addition, an almost 44% respondents have agreed to the fact that corporate insiders are most likely to inflict damage by compromising the trusted privileges.

What are the relevant digital / cyber / information security risk areas?



Abbreviations	Full Forms
*IAM	Identity Access Management
*PAM	Privileged Access Management
*SCM	Security Compliance Management
*MDM	Mobile Device Management
*GRC	Governance, Risk & Compliance
*DAM	Database Activity Monitoring
*SSSF	Security Smoke & Security Fogging

Analysis: To conclude the survey findings, ARCON found that almost 25% of the respondents voiced their opinion as uncontrolled and unmonitored privileged access to be the most feared Information Security related risk. It shows that IT security pros are aware of the benefits of PAM; however, when it comes to implementation, organizations are still lagging behind.

ARCON | Privileged Access Management: a Robust Tool to Secure Enterprise Data

Modern-day organizations, in spite of spending abundant resources in information technology, are failing to prevent attacks on one of the most valued resources—information assets. These incidents, often perpetrated by malicious insiders and sophisticated organized hackers, occur repeatedly because organizations behave reactively to decrease the damage done and not controlling it in the first place. There are no rule and role based privileged entitlements, lack of monitoring of IT users and weak authentication mechanism to access target systems.

It is imperative for this reason that organizations have an unambiguous policies and practices around data security. In the digital commerce age, highly advanced IT infrastructure will yield productivity gains; however, process improvements will get offset by weak internal identity and access security controls.

For this very reason, organizations need to relook at their security framework. Stopping advanced attacks is not possible; however, preventing such attacks by having a proactive approach towards systems security is in our hands.

Organizations will need to ensure that all privileged tasks both at on-prem data-centers and hosted environments are monitored whilst access control policies are well-defined through role-based privileged entitlements.

Risks and Compliance teams will need adopting to “Back-to-the-Basics” formula wherein organizations amend security framework by moving back to where it started; that is, safeguarding the ‘trusted identities’ through applying the “need-to-know” and “need-to-do” principles. It is the time to revisit and strengthen access controls.

ARCON | Privileged Access Management (PAM) suite enables any BFSI organization to overcome all the above mentioned challenges. Trusted by more than 300 enterprise customers across the globe, this highly scalable enterprise-class solution helps in integrating all the IT elements under a single centralized IT policy framework.

This robust solution complies with the BSP Circular 982 and reinforces every organization’s IT operations through real-time monitoring and controlling end user activities around privileged accounts.

ARCON | Privileged Access Management: a Robust Tool to Secure Enterprise Data

Some of the ARCON PAM benefits include:

- Implementation of a centralized access control policy
- Authorization of IT users having an elevated permission to access privileged accounts
- Securing privileged access with Multi-factor Authentication
- Implementing granular level control over privileged users
- Controlling escalation of privileged users by implementing the principle of least privilege
- Frequently randomization of privileged credentials
- Documenting of every privileged session; keep the audit trails

Conclusion

Despite widespread Information Security awareness and presence of strong regulatory landscape, we do find that organizations in the Philippines will need to reinforce their privileged access management policies to secure crucial corporate information.

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