COMPLY OR DIE

2018 GLOBAL STATE OF PRIVILEGED ACCESS MANAGEMENT (PAM) RISK & COMPLIANCE

thycotic

2018 GLOBAL STATE OF PRIVILEGED ACCESS MANAGEMENT (PAM) RISK & COMPLIANCE

WHY THIS REPORT IS A MUST READ:

URGENT CHALLENGES:

Protecting access to privileged credentials---the preferred target of cybercriminals and malicious insiders---is rapidly evolving as a must have compliance requirement.

LIKELY CONSEQUENCES:

Millions of dollars in regulatory fines, business operations at higher risk of severe compromise or even shutdown.

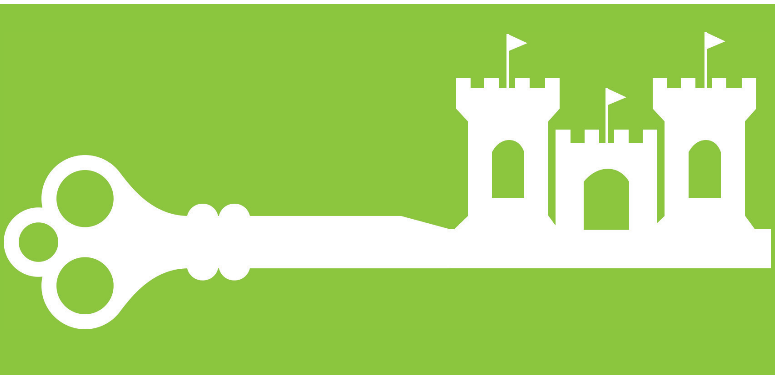
DISTURBING SURVEY RESULTS:

While more than 60% of organizations must satisfy regulatory compliance requirements around privilege credential access, a staggering 70% would Fail an Access Controls audit!

RECOMMENDED ACTIONS:

Develop a Privilege Access Management lifecycle security program to secure access and meet compliance mandates. Privilege Access Management is not a simple checkbox but an important continuous process.

Nearly three out of four organizations would fail an Access Controls audit, putting their privileged credentials (the keys to the kingdom) at high risk.



INTRODUCTION

COMPLY OR DIE: THE PRIVILEGED ACCESS MANAGEMENT (PAM) SECURITY IMPERATIVE

Most organizations only begin to implement Privileged Access Management after a failed audit or major cybersecurity attack that can cost millions of dollars and cause reputational damage.

This report describes the results from a groundbreaking global study by Thycotic that reveals major risk and compliance gaps in how organizations manage and secure their privileged accounts and access to sensitive systems, infrastructure and data. The 2018 Global State of Privileged Access Management (PAM) Risk & Compliance report highlights where many organizations are failing to fully put security controls in place to protect their most critical information assets.

"Privileged Access" encompasses access to computers, networks and network devices, software applications, digital documents, and other digital assets that upper management, IT administrators, and service account users work with daily. Access to privileged accounts allows more rights and permissions than those given to standard business users.

Privileged account access is the prize most frequently targeted by cybercriminals and malicious insiders because this access (often undetected) leads to highly valuable and confidential information, such as company IP, customer identities, financial information, and personal data.

80% of organizations Consider Privileged Account Management (PAM) security a high priority

While most organizations acknowledge the important role privileged credential access plays in their cybersecurity posture, most are failing to act on protecting and securing their privileged accounts. This report helps explain where and why.

PART 1

ASSESSMENT SURVEY RESULTS SHOW MOST ORGANIZATIONS FALL SHORT ON PAM POLICIES, PROCESSES AND CONTROLS

60% OF ORGANIZATIONS

indicate that PAM security is required to demonstrate compliance with government regulations

MANY ORGANIZATIONS WORLDWIDE ARE AT HIGH RISK OF PRIVILEGED ACCOUNT COMPROMISE AND FAILING TO MEET COMPLIANCE REQUIREMENTS

Among organizations surveyed, more than half of the respondents indicated that privileged account management is a required or regulated compliance issue within their organization or industry. While PAM security adoption is being driven by regulatory requirements, it also appears that many organizations are adopting privileged account security measures to reduce the risk of the growing cyber threats and to protect against both external and internal attacks.

Thus, establishing privileged account access controls is a growing priority driven by auditors, controllers, and greater awareness of threats targeting privileged accounts. In fact, cybercriminals are targeting employees at a higher rate than ever before.

Despite acknowledging the importance of PAM security, organizations do not follow through where it counts...

INADEQUATE POLICIES

Recent updates to compliance and regulatory standards require organizations to publish and distribute access control policies that cover privileged accounts and passwords in detail, so that they can limit access to information and systems. Yet the clear majority of respondents to the Risk Assessment still fail to ensure access control policies include privileged accounts and passwords.

This puts privileged accounts at risk of compromise as well as failing to meet compliance standards such as Access Control Policy part of ISO/IEC 27002:2013 & PCI Requirement 8.4. These require asset owners to determine appropriate access control rules, access rights and restrictions for specific user roles. The strictness of the access rules must reflect the associated information security risks.

POORLY EXECUTED PROCESSES

For employees to handle privileged accounts and passwords securely, organizations must develop consistent processes when providing users with access. This ensures they not only gain access but do so with additional security controls that harden the protection and security of privileged accounts.

Failing to implement processes on access control means a much higher risk of rogue access, inconsistent results, higher costs, failed audits and ultimately cyber breaches that could easily go undetected. It is important to have consistent, repeatable processes for Privileged Accounts. To ensure security and conserve resources, automating processes will reduce mundane tasks such as rotating passwords, enabling and revoking access, as well as making it easier to create risk and compliance reports. Ultimately implementing a solid Privilege Access Management solution can also save a company money to invest in other areas of the business.

You cannot secure and manage what you do not know you have. Today's complex IT environments, organizations may contain more than double the number of privileged accounts that are assumed to be in place. That's because undiscovered accounts can occur very easily in virtual environments by cloning and copying virtual machines, or even when restoring snapshots. Employees today can also easily install rogue software not approved by IT, and it is likely these applications come with default credentials or service accounts that expose them to a much higher risk of compromise.

Some of the survey's findings in process failures include:

- 62% of organizations fail at provisioning processes for privileged access
- 51% fail to use a secure logon process for privileged accounts
- 73% fail to audit and remove test or modify default accounts before moving applications to production
- 70% of organizations fail to fully discover privileged accounts---and 40% do nothing at all to discover these accounts
- 55% fail to revoke access after an employee is terminated

50% OF ORGANIZATIONS

of organizations are unable to properly execute effective PAM processes

64% OF ORGANIZATIONS

fail to include privileged accounts and passwords in Access Control Policies

INSUFFICIENT CONTROLS

All critical systems in any organization should have full audit logs to track log-ins and activities. Systems should be configured to issue a log entry and alert when an account is added to, or removed from a domain administrators group, or when a new local administrator account is added on a system. The audit logs need to be regularly checked for integrity or monitored with change detection, and access to audit logs restricted. Without auditing and tracking, you have no accountability for who is using these accounts and no way to properly analyze an incident and mitigate its damage.

Most concerning about the Risk Assessment survey results is the high percentage of companies that have not established a privileged account discovery process

Third party contractors are mostly treated like internal employees when it comes to access controls. However, organizations should ensure that security access controls for vendors or contractors are much more rigorous since they do not have full control over the security behaviors of third parties. Many recent high-profile data breaches resulted from third-party contractors, supply chains, partners and consultants. Often suppliers do not have rigorous security practices in place, putting the entire work environment at risk. Your security is only as good as the security controls that 3rd party contractors have in place when you are not managing and securing privileged access.

See where you face the greatest PAM risks

To see how well your organization meets current standards and best practices associated with Privilege Access Management be sure to the take the free PAM Risk Assessment Tool at https://thycotic.com/solutions/free-pam-risk-assessment-tool/ . You'll receive a Risk score along with a PDF report that reviews your survey answers and suggests ways to reduce your risks.

Control Deficiencies identified in the survey include:

- 73% of organizations fail to require multi-factor authentication with privileged accounts
- 63% do not track and alert on failed logon attempts for privileged accounts
- 78% fail to use a dedicated system for all administrative tasks
- 70% fail to limit third-party access to privileged accounts

PART 2

RECOMMENDATIONS: ESTABLISH A LIFE CYCLE APPROACH TO PRIVILEGED ACCESS MANAGEMENT

When planning, implementing, or expanding a more secure approach to Privileged Access Management leading analysts and practitioners emphasize building out a program that encompasses the complete Privilege Account Management (PAM) lifecycle. That means

1. Understanding the need for Privilege Access Management among exec and IT staff

2. Identifying privileged accounts across all systems

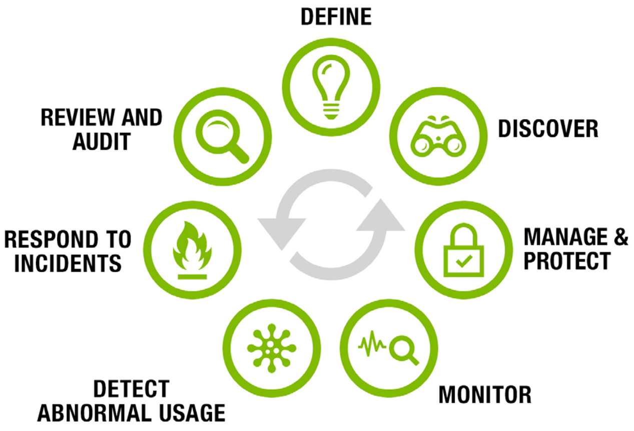
3. Managing and Protecting access to privileged accounts and restricting their use

4. Monitoring privileged account use on a continuous basis

5. Detecting anomalies in privileged account use indicating potential fraudulent activities

6. Responding to privileged account suspected compromise immediately and with targeted actions

7. Review and report to continuously improve your Privilege Access Management access controls



Like any IT security measure designed to help protect critical information assets, managing and protecting privileged account access requires both a plan and an ongoing program. You must identify which privileged accounts should be a priority in your organization, as well as ensuring that those who are using these privileged accounts are clear on their acceptable use and responsibilities. This report briefly describes a PAM lifecycle model which provides a high-level roadmap that global organizations can use to establish their own Privileged Access Management program.

64% OF ORGANIZATIONS

fail to fully audit privileged accounts

DEFINE:

Define and classify privileged accounts. Every organization is different, so you need to map out what important business functions rely on data, systems, and access. One approach is to reuse a disaster recovery plan that typically classifies important systems and specifies which need to be recovered first. Make sure to align your privileged accounts to your business risk and operations.

Develop IT security policies that explicitly cover privileged accounts. Many organizations still lack acceptable use and responsibilities for privileged accounts. Treat privileged accounts separately by clearly defining a privileged account and detailing acceptable use policies. Gain a working understanding of who has privileged account access, and when those accounts are used.

DISCOVER:

Discover your privileged accounts. Use an automated PAM software to identify your privileged accounts. and implement continuous discovery to curb privileged account sprawl, identify potential insider abuse, and reveal external threats. This helps ensure full, on-going visibility of your privileged account landscape crucial to combatting cybersecurity threats.

MANAGE & PROTECT:

Protect your privileged account passwords. Proactively manage, monitor, and control privileged account access with password protection software. Your solution should automatically discover and store privileged accounts; schedule password rotation; audit, analyze, and manage individual privileged session activity; and monitor password accounts to quickly detect and respond to malicious activity.

Limit IT admin access to systems. Develop a least-privilege strategy so that privileges are only granted when required and approved. Enforce least privilege on endpoints by keeping end-users configured to a standard user profile and automatically elevating their privileges to run only approved and trusted applications. For IT administrator privileged account users, you should control access and implement super user privilege management for Windows and UNIX systems to prevent attackers from running malicious applications, remote access tools, and commands. Least-privilege and application control solutions enable seamless elevation of approved, trusted, and whitelisted applications while minimizing the risk of running unauthorized applications.

MONITOR:

Monitor and record sessions for privileged account activity. Your PAM solution should be able to monitor and record privileged account activity. This will help enforce proper behavior and avoid mistakes by employees and other IT users because they know their activities are being monitored. If a breach does occur, monitoring privileged account use also helps digital forensics identify the root cause and identify critical controls that can be improved to reduce your risk of future cybersecurity threats.

DETECT ABNORMAL USAGE:

Track and alert on user behavior. With up to 80% of breaches involving a compromised user or privileged account, gaining insights into privileged account access and user behavior is a top priority. Ensuring visibility into the access and activity of your privileged accounts in real time will help spot suspected account compromise and potential user abuse. Behavioral analytics focuses on key data points to establish individual user baselines, including user activity, password access, similar user behavior, and time of access to identify and alert on unusual or abnormal activity.

RESPOND TO INCIDENTS:

Prepare an incident response plan in case a privileged account is compromised. When an account is breached, simply changing privileged account passwords or disabling the privileged account is not acceptable. If compromised by an outside attacker, hackers can install malware and even create their own privileged accounts. If a domain administrator account gets compromised, for example, you should assume that your entire Active Directory is vulnerable. That means restoring your entire Active Directory, so the attacker cannot easily return.

REVIEW AND AUDIT:

Audit and analyze privilege account activity. Continuously observing how privileged accounts are being used through audits and reports will help identify unusual behaviors that may indicate a breach or misuse. These automated reports also help track the cause of security incidents, as well as demonstrate compliance with policies and regulations. Auditing of privileged accounts will also give you cybersecurity metrics that provide executives with vital information to make more informed business decisions.

BOTTOM LINE

Bottom Line: The key to improving cybersecurity around Privileged Access Management stems from an understanding and implementation of a PAM lifecycle approach. Only a comprehensive solution can ensure that your “keys to the kingdom” are properly protected from hackers and malicious insider threats. And that your access controls meet the regulatory requirements for compliance mandates in your industry.

PART 3

PAM RISK ASSESSMENT & COMPLIANCE SURVEY METHODOLOGY

Launched in late 2017, the Thycotic Privileged Account Management Risk Assessment survey has engaged nearly 500 global IT security professionals. The survey poses 20 questions to participants according to a matrix scoring system. For each survey question, points are assigned for the Risk Value (the probability the threat will occur), along with additional points for the Impact Value (the severity of an event if it should occur).

REGULATORY STANDARDS INCORPORATED INTO THE RISK ASSESSMENT TOOL

The Thycotic PAM Risk Assessment online tool encompasses questions based on a combination of several regulatory standards that include:

ISO - ISO/IEC 27002 is the information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC) https://www.iso.org/standard/54533.html

EU GDPR - The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

NIST - The National Institute of Standards and Technology (NIST) is a measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce. http://csrc.nist.gov/projects/iden_ac.html.

PCI - The Payment Card Industry Data Security Standard (PCI-DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes.

CIS CSC - The Center for Internet Security Critical Security Controls for Effective Cyber Defense is a publication of best practice guidelines for computer security.

PART 4

NEXT STEPS – HOW THYCOTIC CAN HELP

As a global leader in Privileged Access Management and Least Privilege Management, Thycotic is unique in offering an end-to-end solution that encompasses least privilege management on endpoints with application control, along with protecting privileged account passwords across the entire IT infrastructure.

Thycotic provides free tools and software solutions for the key components that enable you to build out a Privileged Access Management program from privileged access training and account discovery to incident response for a compromised account.

To learn more, visit these Thycotic online resources:

- Get Free PAM security tools at thycotic.com/free-tools/
- Find Free Privileged Account Password protection trial software at thycotic.com/secret-server/
- Get Free Least Privilege Management trial software at thycotic.com/privilege-manager/
- Learn more about PAM compliance solutions at thycotic.com/solutions

ABOUT THYCOTIC

Thycotic, a global leader in IT security, is the fastest growing provider of Privilege Management solutions that protect an organization's most valuable assets from cyber-attacks and insider threats. Thycotic secures privileged account access for more than 7,500 organizations worldwide, including Fortune 500 enterprises. Thycotic's award winning Privilege Management Security solutions minimize privileged credential risk, limits user privileges and controls applications on endpoints and servers. Thycotic was founded in 1996 with corporate headquarters in Washington, D.C. and global offices in the U.K. and Australia. For more information, please visit www.thycotic.com.