If privileged account management is the number one cyber security priority, why are financial institutions still using manual processes?

The better the question. The better the answer.
The better the world works.

EY
Building a better working world

With an alarming series of cyber breaches being perpetrated using compromised privileged credentials, regulators now expect financial institutions to be able to demonstrate the effectiveness of their privileged account management (PAM) controls. But few institutions are currently following PAM best practice. EY teams are helping the region's banks, insurers and asset managers to help implement new PAM solutions that streamline compliance, reduce risk and lower the cost of auditing and monitoring.

Why organizations should be concerned about privileged accounts

'Privileged accounts' give people full access to and control over your organization's most valuable and confidential information: customer identities, financial information, strategic information and personal data.

If privileged accounts are not managed with appropriate controls, they can be compromised by external, malicious actors (e.g., a cyber-criminal) or internal actors (e.g., a rogue administrator). Both can lead to destructive damage unless they are spotted and stopped quickly.

Not surprisingly, the passwords, tokens, keys and certificates that come with privileged access are prime targets of cyber criminals. And, unfortunately, these accounts are often protected by weak passwords that can be changed manually and easily shared with colleagues and teams.

Forrester estimates that at least 80% of data breaches have a connection to compromised privileged credentials.[1] One of them was the SingHealth breach, which affected more than 1.5 million Singaporeans, including Prime Minister Lee Hsien Loong.

In today's increasingly complex IT environment, PAM is arguably a financial institution's most critical cyber security control – more important than standard identity and access management. Businesses that are not securing and managing these high-value targets have an increased risk of insider threat and fraudulent employee activity. Considering the potential magnitude of a breach, for two years in a row, Gartner has nominated PAM as the first security project CISOs should focus on as part of its Top 10 Security Projects.

[1] The Forrester Wave™: Privileged Identity Management, Q4 2018

Who has a privileged account in your institution?

Privileged accounts can be used by a human (DBAs, SysOps, network administrators, ITSecAdmins, helpdesk operators, data center technicians, change managers, release managers, website administrators, bloggers, brand ambassadors, and outsourced teams) or by software applications with high privileges (application accounts, service accounts or accounts embedded in a script or code).

New regulatory focus on privileged access management

In the past five years, financial services regulators have started focusing on privileged access management. Already, the region's institutions need to be mindful of:

- MAS TRM Guidelines, Singapore
- NIST Special Publication 800-53A Rev 4, US
- HIPAA, PCI DSS, FISMA and SOX compliance regulations, global
- GDPR Privacy by Design Intention, Europe
- Mandatory Data Breach Notification Laws, Australia
- APRA's CPS234 prudential Standard, Australia

The regulations expect institutions to:

- **Group the privileged accounts in a secure, centralized vault** – to manage and protect such high-value accounts. This includes establishing dual controls to closely monitor privileged access sessions to highly sensitive IT assets.
- **Monitor and trace all privileged actions and key strokes** – so they can be reviewed later and reconciled against origination requests to see if access was used for its intended purpose.
- **Limit privileged accounts usage based on time and location** – ensuring privileged accounts are only available for a specific time period and special levels of approvals are in place if usage is exceeded. This significantly reduces the risk of privileged account abuse or compromise.
- **Have a formal review and approval process for new privileged account creation** – making new accounts subject to specific reviews and approvals by peers or supervisors. Privileged sessions must be available for the full range of audits, including forensic audits.
- **Minimize revealing credentials in plaintext** – especially when granting remote access to IT systems.

Are you at risk?

- Do you have visibility of how privileged accounts are managed, created and decommissioned?
- Do you monitor the actions of privileged accounts?
- Do your admins have continuous access to privilege accounts?
- How are you controlling privilege application accounts, service accounts and accounts with "password never expire"?
- Are people sharing passwords of privileged accounts?
- Do you have approval mechanisms or expiry set for shared accounts to ensure accountability?

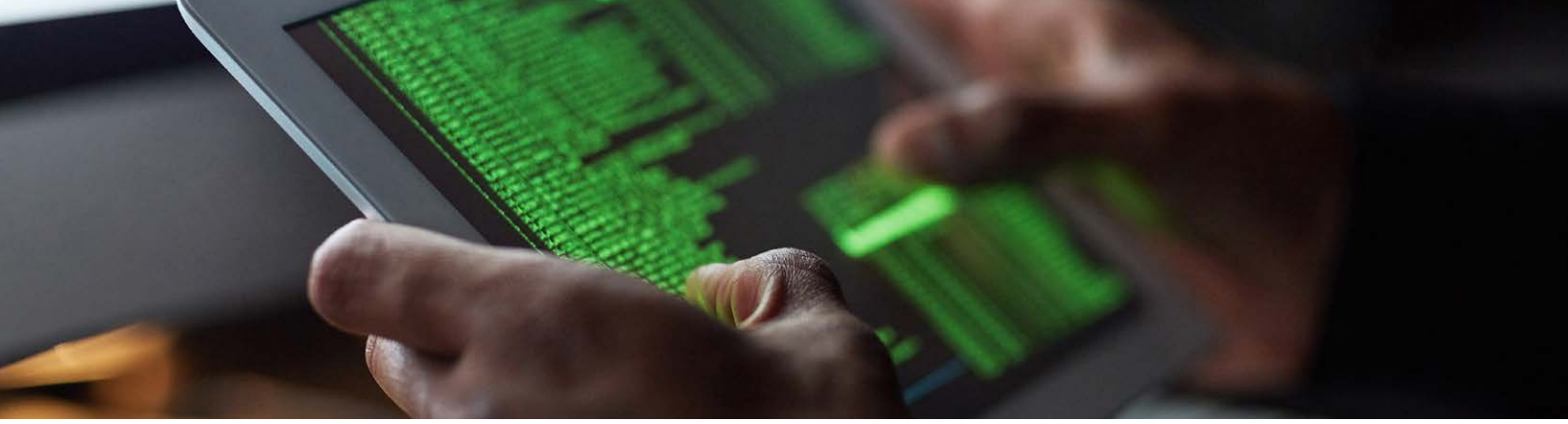
How can you strengthen PAM controls?

Deploying a PAM solution is a highly complex process, which requires appropriate planning, execution and appropriate product. To remain compliant and avoid catastrophic breaches, institutions need to start now.

To manage privileged accounts effectively, you need PAM controls that align within an integrated IAM process and technology framework. The starting point for identifying and moving towards a compliant target state requires:

People

- **PAM is not an IT-only initiative,** especially when it addresses regulatory/audit concerns. Appoint executive-level sponsors empowered to make decisions as required, supported by committed stakeholders.
- **Align your PAM plans** with auditors and compliance managers early and often. Plan early for ongoing support by designating an experienced operational manager as the Service Owner.
- **Hire experienced staff.** It can take a long time to become skilled in PAM tools, control implementation and process reengineering.
- **Change management** is key. Engage the business early and gain their buy in.



Process

- **Streamline PAM processes** – Review existing PAM processes to confirm that the process aligns to industry standards and regulations. For example, remove unnecessary and unused privileged accounts, and ensure all privileged access accounts have both an assigned and a secondary owner. Also, maintain an asset inventory of human and non-human application or service accounts in the IT infrastructure. Business processes will likely need to change to segregate duties requirements and PAM tools.
- **Use proactive communication and training** – to ensure the business adopts these new processes.
- **Setup discovery scans** – to identify the privileged accounts in the IT infrastructure.
- **Automate PAM-related processes** – such as discovery scans and account onboarding.

Technology

- **Adopt a common PAM solution** that will help you to:
  - **Standardize access request processes to improve efficiency**
  - **Restrict existing privileges** – Restrict access rights for users and accounts to all devices that privileged accounts can be used for. By centrally managing role-based permissions for privileged access, PAM helps create a less complex and audit-friendly network environment for HIPAA, PCI DSS, FISMA, and SOX compliance regulations.
  - **Record and audit privileged activity** – Record sessions and identify those with suspicious activities and correlate the information using solutions such as: SIEM, which analyses system and user activity; PAM session recording; File Integrity Monitoring; and Database Monitoring and Leakage.
  - **Monitor new privileged accounts** – Run periodic discovery to identify new or unauthorized privileged accounts. Flag inactive privilege accounts for periodic recertification.
  - **Align PAM-supported applications** – Consider how your applications work in a privileged enabled environment. These include tools such as remote access, patch management and vulnerability scanning. There should be a single solution that covers all environments.
- **Clean up data** – Discovering a privileged account does not mean it should be automatically onboarded. Best practice dictates to clean up accounts prior to onboarding. This may be time consuming, but it is essential.
- **Create an asset inventory** – Multiple privileged accounts or orphan accounts are often created and forgotten about. Creating an asset inventory of all the existing privileged accounts will decrease the attack vector.
- **Set up least privilege** – Deploy policies to control permissions of privileged users and integrate with User Behavior Analytical solutions to improve security.

Governance

- **Select an integrator** well versed in both PAM processes and technology. A strong delivery framework and deep skills in the areas of change management are essential. Your integrator should have strong alliances with appropriate vendors and understand all the relevant regulations.
- **Take a holistic approach.** It's vital to be able to account for what every privileged account has access to. Use a standard access matrix based on the account nature and industry policies, with on demand or just in time access. Set up tools, such as SIEM, Multi Factor Authentication, User Behavior Analytics and endpoint manager, to control and restrict access of privileged users.

What are the benefits of implementing a tailored PAM solution?

Financial institutions that take up the latest PAM tools will quickly start to:

Reduce risk – PAM tools secure access to sensitive systems and ensure business systems cannot be manipulated to defraud the institution or its customers or to misuse, steal or compromise data.

Improve compliance – By defining and enforcing controls that make privacy by design work. For example, any workflow where an employee has access to personal data should be subject to a control that prevents unauthorized sharing of that data. A PAM solution should give IT managers precise knowledge of who has the privilege of modifying that control.

Lower costs – PAM tools improve productivity and create savings by reducing cyber fatigue and simplifying the process of rotating and generating new complex passwords. They also remove the cost of sifting through thousands of logs to find evidence of unusual behavior as it happens.

Improve user experience – Institutions receive a complete record of who, when and why people have privileged accounts, as well as who approved those accounts and why. When this information is overlaid with provisioning details, IT administrators can easily define how long passwords will be valid before they must be changed. This way, auditors can quickly and easily see how well the business adheres to compliance.

Find out how to reduce risk and improve compliance with PAM.

As privileged accounts continue to be targeted and compromised, we expect regulators to increase control requirements. PAM is not a short journey. To ease transformation fatigue, it's best to start early. EY has been involved in numerous PAM transformations and has a team of dedicated resources based in Asia with hands on, strategy and implementation experience ready to help you.

To find out more, contact EY now.

Contact

Australia

Anthony Robinson
EY Oceania Financial Services Cyber Security Leader
Anthony.Robinson@au.ey.com
+61 2 9248 5975

Greater China

Wilson Feng
EY China Financial Services Cyber Security Leader
Wilson.Z.Feng@cn.ey.com
+86 21 2228 6855

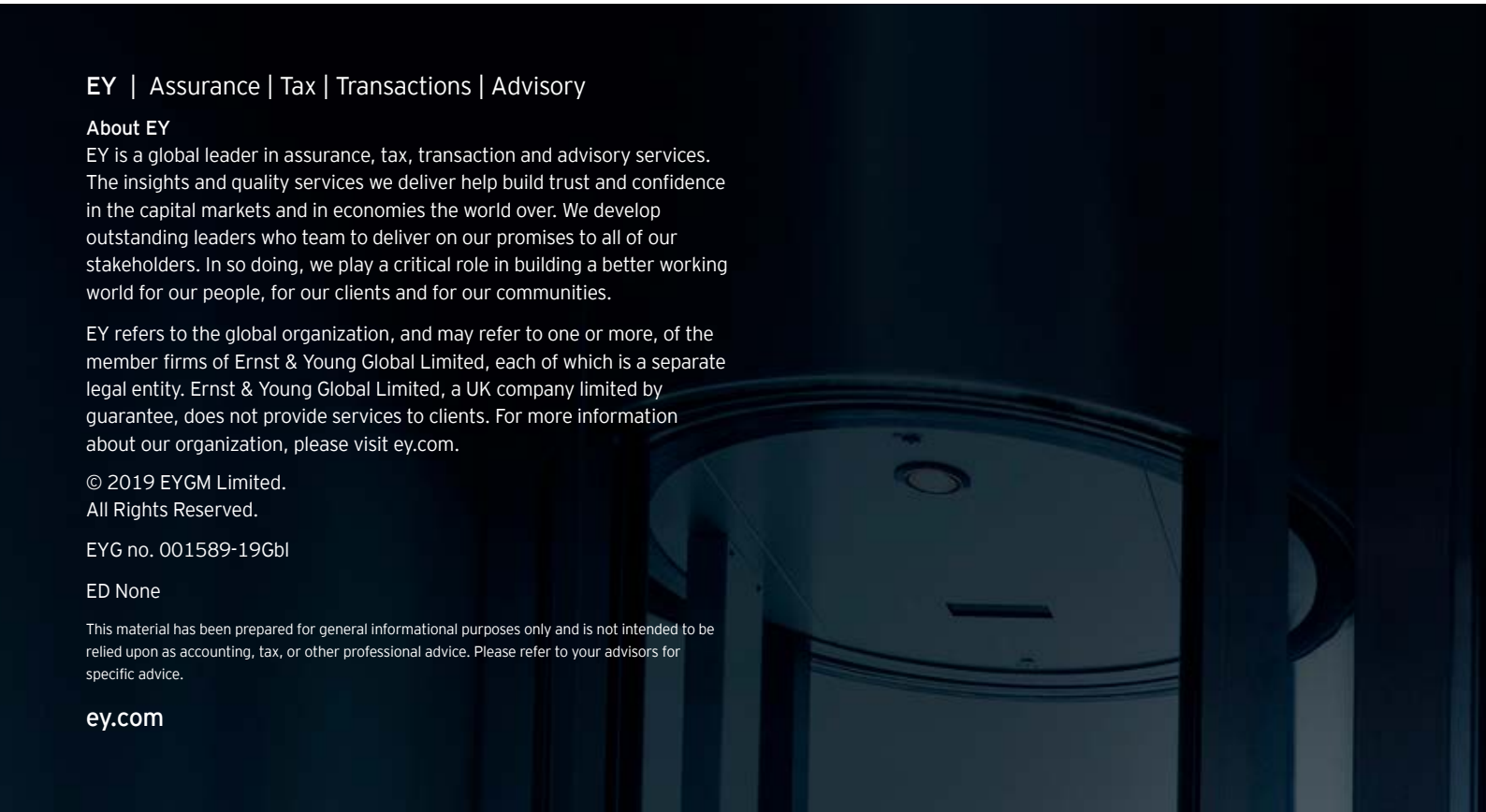
Hong Kong

Jeremy Pizzala
EY Asia-Pacific Cyber Security Leader
Jeremy.Pizzala@hk.ey.com
+852 2846 9085

Simon Chandran
EY Hong Kong Cyber Security Leader
Simon.Chandran@hk.ey.com
+852 2846 9888

Singapore

Sean Gunasekera
EY ASEAN Cyber Security Leader
Sean.Gunasekera@sg.ey.com
+65 6718 1162



EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no. 001589-19Gbl

ED None

ey.com