Puleng Insights

Breakthrough

Guidelines for CISOs to create a cybersecurity aware organisation

Prepared by Puleng Technologies

FOREWORD

A quick conversation with almost anyone in the corridors of companies today will reveal a level of concern over their privacy, phishing attacks, data breaches, malware, misuse of personal credentials, identity theft and much more.

McAffee estimated that the damages associated with cybercrime now stands at over $400 billion, up from $250 billion two years ago.

> "There are only two type of companies, those that have been hacked and those that will be." – Robert Mueller, Former FBI Director

Universally there is an acknowledgement that a higher level of maturity of protection currently on offer is needed.

Last year alone Gartner reported that $114bn was spent on cybersecurity solutions in the private sector. Highly specialised categories such as Privileged Account Management (PAM) alone is seeing a 23% YOY growth rate.

Yet the successful management of these threats remains concerningly low.

A fact certainly not lost on the majority of CISOs who have to deal with a multitude of moving parts within an organisation such as people, culture, legacy systems, access management, privileges, politics, transactions, stakeholders. The list goes on. Even though the CISOs of today are more empowered than ever to keep the organisation "safe", their success is only as good as the level of awareness and buy-in from the rest of the organisation, from board level to the admin person on the ground floor.

BREAKTHROUGH attempts to provide guidelines for CISOs to *break through* some of the internal barriers to cybersecurity awareness and adoption at all levels of an organisation.

This report outlines the importance we place on our deep interactions with our customers and our employees; smart work leads to successful projects, long term reward, personal growth and potential industry-wide respect. But never rest on your laurels, as tomorrow's changes can bring even bigger challenges and with a potentially even greater opportunity.

Steve James
Executive Director, Puleng Technologies

Spotlight on Privileged Account Management

197 days. On average, that's how long it takes an organisation to realise they've been breached. A significant amount of damage can be done in 197 days.

Employees, vendors, and other insiders have unnecessary access or excessive access to systems and data. Passwords are created and shared, but are not audited, monitored nor managed with discipline and accountability. Desktops, laptops, servers and applications communicate and open paths to sensitive assets and data - to name a few - creating complexity and opening gaps, exposing your organisation.

Through Privilege Account Management, abuse can be prevented with a complete, integrated solution that unifies Enterprise Password Security, Endpoint Least Privilege, and Secure Remote Access for comprehensive visibility and control, both within your organisation and externally.

The goal: to move from a reactive security approach to a proactive one. **Don't let day 1 turn into day 197.**

BeyondTrust®

EMPOWERED PRIVILEGED ACCESS.

We defend against threats related to stolen credentials, misused privileges, and unwanted remote access, while empowering people.

Contact BeyondTrust

www.beyondtrust.com
sales@beyondtrust.com

A foundational story

Creating a narrative that the whole organisation can adopt

It is said that stories are memory aids, instruction manuals and moral compasses.

One of the biggest barriers to cybersecurity adoption is the paralysis caused by “too much, too fast”.

It is estimated that the average CISO of a large company has between 50-80 security vendors to manage. Whilst this may be less for smaller companies, securing data may be as critical as there is a plethora of cybersecurity functions.

It is no wonder that the Forbes Technology Council highlighted ‘Vision Setting’ & ‘Storytelling’ as the top skills in 2018 of future CISOs – to thread together the context and value of cybersecurity investment for their organisation.

It is true that it is near impossible to predict the future, but an organisation should be able to tell a story of itself including an ideal ending. The same holds true for the organisations relationship with cybersecurity.

A well articulated narritive provides a concise and impactful way to cut through the jargon and complexities associated with stradelling advanced technologies and complex organisational culture.

> “CISOs should make ‘storytelling’ part of it’s integrated strategy definition process”

No technical specifications. Not even case stories (for now). A simple, vivid picture with key principles that people can easily relate to and share with others. If cybersecurity Skills Shortage is a risk in your plan, then tell the story of skills development within your company. In order to set the Foundation for the tangible actions that will inevetiably be part of a cybersecurity solutions road map, a consistently told story gives the 1s-and-0s of technology, some colour, context and relevancy. Essential ingredients to get buy-in from the rest of your organisation and provide momentum for a change management process.

Cognitive science research in the last decade tells us that human beings make sub-conscious often irrational decisions on one side of the brain and then justify that decision logically and rationally on the other side of their brain, after the fact.

So we think we've made great rational decisions, when in fact we've made decisions driven by emotional sub-conscious reasons.
So if you want to influence peoples decisions or behaviours you need to influence them emotionally. Numbers and data do not do this, but storytelling does.

Mike Perk
CEO, WWC | Future Fit Leadership

Emerging leadership

Communicate the evolution to an enabling CISO leadership

In an anonymous survey conducted among Puleng customers, the majority of CISOs indicated a reluctance to engage with the “politics and emotions” of their organisation.

Yet, data science specialist, Datalere released a report last year indicating that companies expect 17 out of 20 of the skills expected from their CISO to be ‘relational’ skills such as the ability to engage across organisational silos and translate technology into ‘plain’ language.

A disconnect that is further supported by low representation of CISOs in executive management roles.

> “2 out of 10 CISOS are members of a board.” – Kaspersky, 2018

The internal perceptions of the organisation towards those responsible for protecting it’s assets is a major stumbling block towards a mature approach to managing cybersecurity. It is concerning that only a third of CISOs indicate that they do not report data breaches to their board.

The CISO must pro-actively identify methods for positioning his or her role as a trusted technology partner to the business.

This can be done at many levels, including promoting the profiles, skills and experiences of the team and individuals involved in cybersecurity.

A endorsement by your CEO of the importance of cybersecurity and the trust put into you, the CISO, by your CEO is a critical component in building an ongoing relationship with the executive as well as the rest of the organisation.

The CISO and his or her team need to emerge as being on the front-line of leading the company’s technology and digital ambitions into the future. An outcome that requires CISOs to take the initiative to engage with all stakeholders in the organisation.

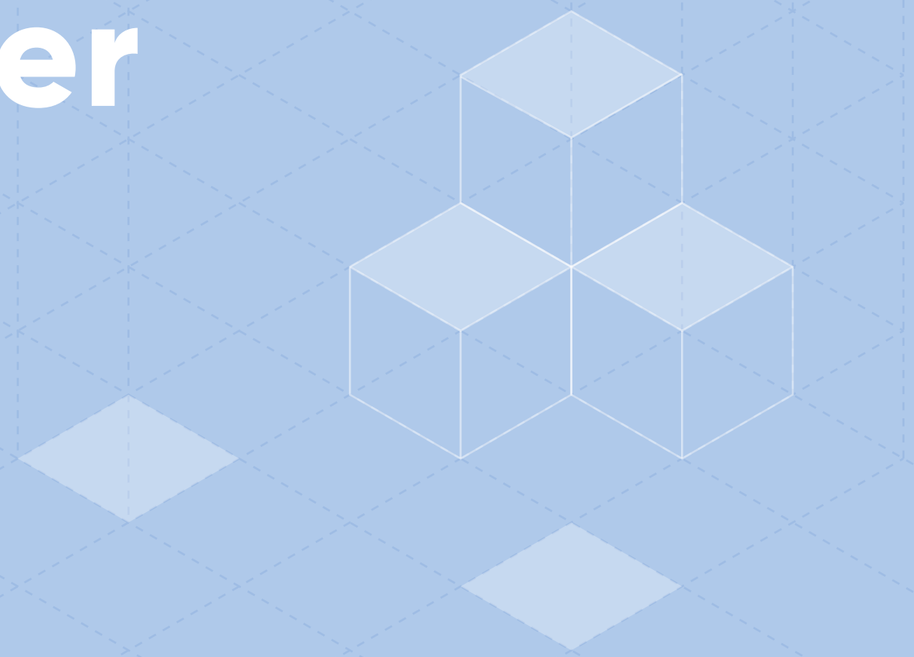
Leading what essentially amounts to a volunteer workforce – line of business, IT support, development, security operations and even risk and audit - does not only require that a shared vision is established, but also that collective agreement is reached on where essential resources must be applied first, for what purpose, and to what extent.

This alignment is foundational to establishing Group-wide support for, and confidence in, your Cyber Security Strategy. The second essential component lies in your ability to demonstrate the progress that this collective effort is making – not as a set of project milestones – but as a measure of your confidence in the security of the organisation at any point in time.

Kris Budnik
First Rand Group, CISO

Capable together

Take back control by
getting others involved



It is not uncommon for CISOs to report a high level of cybersecurity investment, yet still the majority of the breaches reported are due to internal, end-user behaviours.

As the rest of the organisation often displays an aloof-attitude towards cybersecurity, it is no surprise that the typical CISO is increasingly looking to enforce more systems and rules to take back control. Paradoxically, this leads to a further lack of personal responsibiliy from the end-user, creating a perpetual cycle of threats.

> "52% of organisations report that when breaches happen as a result of next-generation technologies such as IoT or the cloud, it's due to users having excessive privileges."

Advances in areas such as Privileged Access Management is providing CISOs with more control over the flow of data than ever before. In fact, 8 out of 10 Puleng customers reported that they have a centralised workflow-based option for managing access.

However, the need to get the end-user onboard is critical. The promotion of a shared-sense of solving the challenge will go a long way to increase the overall internal awareness of cybersecurity.

World renowned legal and security expert, Steven Chabinsky said: "Thinking of cybersecurity solely as an IT issue is like believing that an entire workforce, from the CEO down, is just one big HR issue."

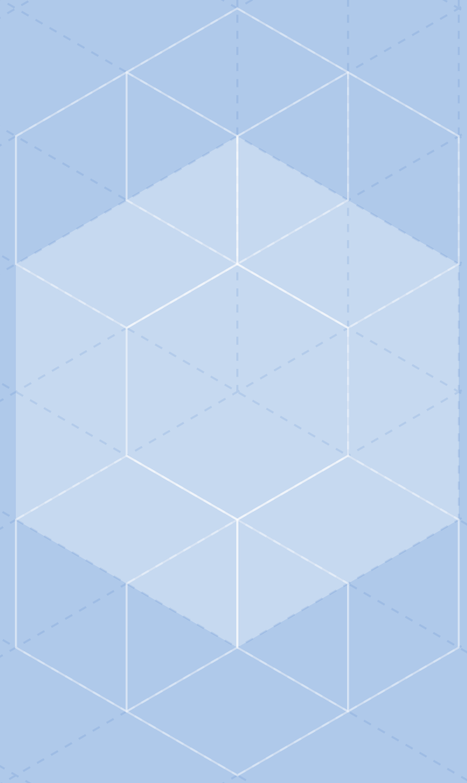
The willingness and capability of the end-user to behave in a more responsible manner as it relates to their account use and protection of data can be dramatically increased by the identification of individuals internally and outside the IT department, to champion your cause. Whether its a person within each department or someone at an executive level, these champions need to be empowered to speak on your behalf. Arming these champions with case stories specific to their department gives them the necessary empirical and anecdotal evidence that they can share in a relatable way to their colleagues.

Ensure end-users have access to the right information at the right time will enhance the user experience and protect the business.

Muhammed Mayet
IT Security Executive

Enhance ability

Provide access to support to create a perpetual cycle of organisational self-improvement



A major frustration for CISOs is the quality and availability of end-user training from the vendors they engage with.

Their need is two-fold in that they require support to empower themselves, but also, and equally important, is support to further educate others. London-based consultancy Willis Towers Watson said that 90% of all cyber claims stemmed from some type of unintended human error or behavior.

> "The creation and distribution of cybersecurity education content is the final and arguably most important part of creating a cybersecurity aware organisation."

Whether through an internal education series using online video or forums, enewsletter, or internal events, there is a need to push and pull people to dedicated areas where they can learn more about cybersecurity, fostering a belief that security belongs to everyone.

Uber invested millions of dollars into it's internal education programmes, says Samantha Davison, Security Programme Manager: "We are trying to change our employees' security stories, by creating programs catered to region, department, and role, our people understand that security is part of their story and our culture."

As the sophistication of breaches and attacks grow, so the role of CISOs will increasingly involve educating the organisation's end-users internally.

Your ability to create a system of ongoing internal education will provide CISOs with the dual-benefit of freeing up their time to control potential breaches as well as get the rest of the organisation in the habit of investing in their digital abilities.

The relevance and quality of cyber security training is a major concern for CISOs. The training should be relevant to the organizations vertical market, technology they have implemented, and the personas at risk within the organization.

Without relevant training, users are not being educated on the risks and threats that are truly preventable by basic cyber security education.

Morey Haber
Chief Technology Officer |
Chief Information Security Officer, BeyondTrust.

FOR YOUR CONSIDERATION

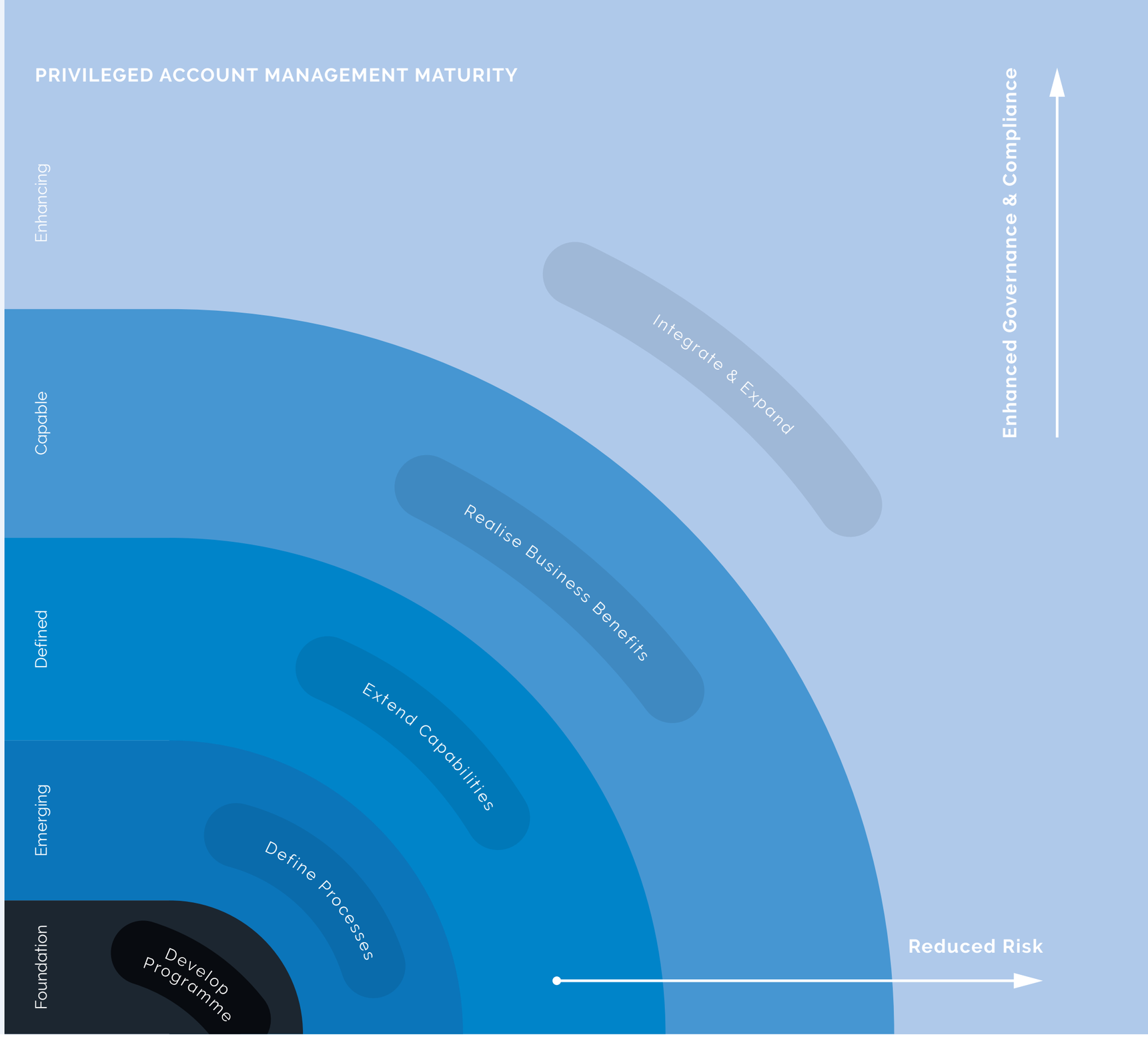
CISOs have more than their fair share of challenges to deal with and by extension a full menu of cybersecurity solutions to pick from. However, the ability to control threats is directly related to the level of maturity of the rest of your organisation and the vendor partners that can support you.

Below is a summary of BREAKTHROUGH guidelines to create a cybersecurity aware organisation.

CHALLENGE	INSIGHT	SOLUTION
Lack of organisational understanding.	Storytelling as means to speak to the head and heart.	A Foundational Story.
Lack of organisational trust.	Pro-active and enabling CISOs and team.	Emerging Leaders.
Lack of end-user responsibility.	Collaboration with internal champions.	Capable. Together.
Lack of organisation-wide support.	Access to always-on learning to promote security as a culture.	Enhance-Ability.

OUR JOURNEY WITH YOU

Our maturity model helps identify a starting point for Medium and Enterprise organisations who are focused on reducing risk and improving Governance and Compliance in their organisations, relative to the privileges and access their people have to their business.



PULENG
TECHNOLOGIES

Puleng Technologies (PTY) Ltd, is a fifteen-year-old, proudly South African ICT company with our roots firmly planted around building local expertise and providing our customers with “Project Success” linked to the solutions we design and support.

The Puleng Blueprint provides our customers with a client-centric strategy to manage and secure the two most valuable assets an organisation has: its data and users while facilitating IT and business with a platform to build an efficient, collaborative and integrated cybersecurity program

To further enhance our strategy, we provide our customers with Data Center infrastructure platforms, which allows us to leverage our core strengths across our Compute, Storage, Virtualisation and Management teams.

Puleng technologies (Pty) Ltd
Block A, River Park
Cnr Janadel & Bekker Roads
Halway Gardens
Midrand
1685

T. 011 205 4300

Governance, Risk and Compliance Platform

Security and Cyber Intelligence

Development and Integration Services

Consulting and Professional Services

Cloud Security

Data

- Cloud Access Security Broker
- Data Loss Prevention
- Data Audit and Protection
- Data Access Governance
- Data Classification

People

- Cloud Identity and SSO
- Access Management
- Identity Management
- Privileged Access Management
- Access Governance

Service Orientated Infrastructure

- Backup and Recovery
- Storage Infrastructure
- Converged
- Virtualisation
- Cost Efficiency and Waste

pu-leng

n.

[Tswana, *rain (used as greeting for good fortune)*.]

A Tswana word that means a place of rain and a symbol of knowledge and wealth.