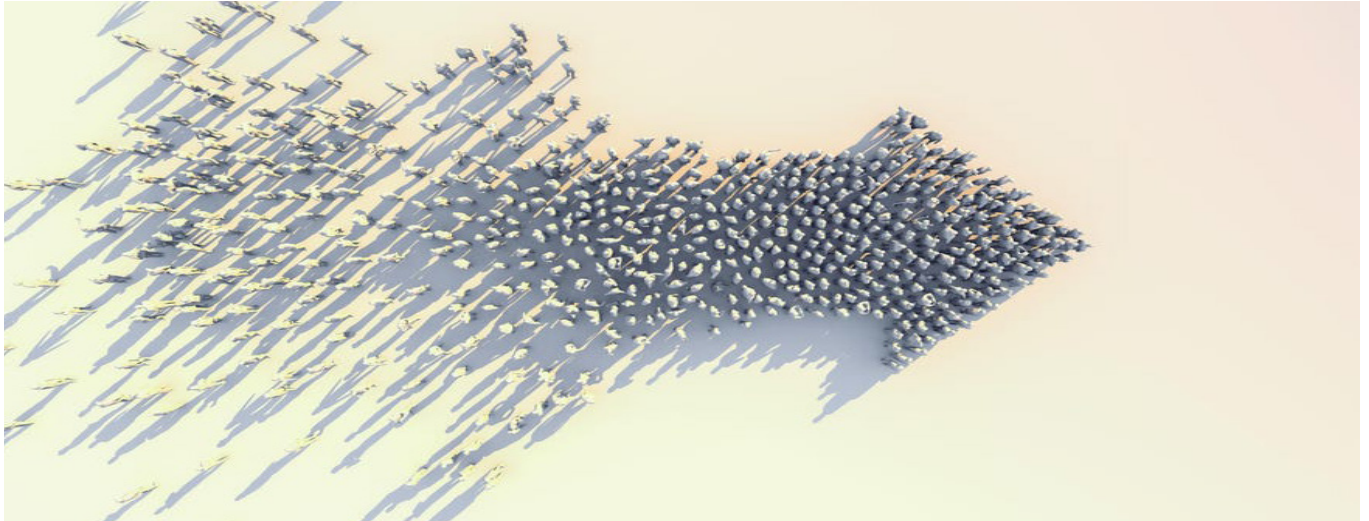


THE NEW CISO

ARE YOUR PERCEPTIONS ALIGNED? CISO REPORT



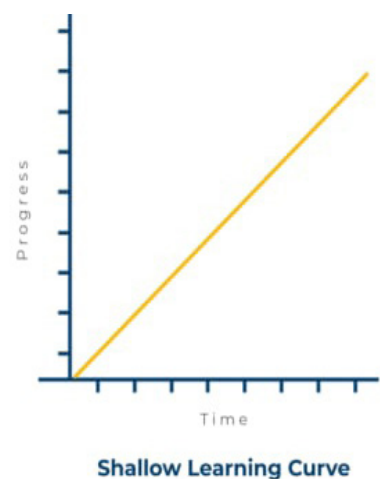
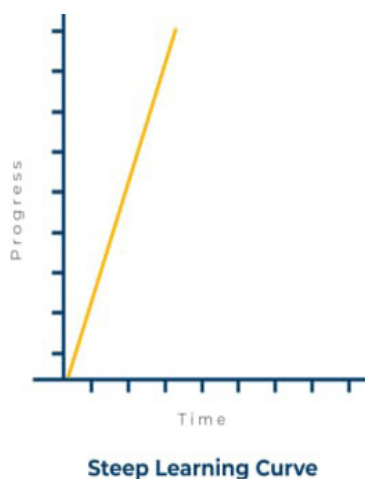
Chief Information Security Officers (CISO's) often get stuck in the operational aspects of their jobs due to talent shortages and fall short to expand their roles to play across multiple dimensions of the organization. This challenge is compounded by major talent shortages in the Cyber Security landscape that makes finding & keeping cyber specialists challenging, let alone grooming them into a future CISO. Reflecting the mirror back at the CISO, it is also worth appreciating that the demand that the organisation is placing on them is changing, moving from a more basement engagement (dealing technical issues) to where they are called on to support boardroom (strategic direction setting and execution) discussions.

These realities are not always well expressed by

organisations, and might contrast or conflict with individuals personal aspiration for growth and development of their respective careers. This reality was highlighted through survey results by a significant CISO sample pool, where, although more than 50% of CISO's who started their career in the Technology field, envision their future role to transition operating at an Executive or Board level role.

Only 12,5% of respondents believe that their current and future role will be similar. This data correlates with industry statistics, which indicate more than 50% of people are not happy with their careers, and 76% of people in companies are looking for growth opportunities.

This brings into sharp focus the urgency in which organisations will



have to build mechanisms to accelerate upskilling, certification and internal mobility to enable Cyber and Information Security (Cybersecurity) professionals to meet the future demands of their ever evolving roles. As the average global tenure for a CISO in a role is now 3.2 years, CISO's will need to not only leave a legacy but also a viable successor or two in the wings who have

been ramped up through a steep learning curve. With this backdrop, hardliners might feel that if people ship off to greener pastures you can just hire an alternative. The realities are however that globally there is a 3,5 million Cybersecurity Workforce shortage, with organisations on average expanding their Cybersecurity teams by 15%.

This sketches a picture, that even

if you wanted to, "outhiring" for skills shortage is not plausible. There are however options to tackle this situation, from being deliberate around career path development, focusing on closing skills gaps, grooming successors or running talent development pipelines. The process to leverage one or more of the options, rooted in a simple yet effective deliberately driven engagement comprising out of the following steps:

- Skills audit – understand if the existing skills in play are sufficient to meet current and future objectives.
- Skills gap – identify your teams technical bench strength to meet your technology and business strategy, and how the existing skills stack up against known industry benchmarks.
- Build customized learning paths leveraging of recognised learning platforms to support the individual in their learning journey.
- Change manage to drive outcomes – ensure that the development efforts are incorporated into the work effort, to ensure value from applying new found knowledge, through the aid of personal development plans.
- Skills at hand when you need it – incentivise staff to stay committed to the company as their skills grow to ensure that the skills are accessible to the organisation over the long-run.

The majority of respondents (78%) would suggest that that the largest impact on their career will be a result of personal and industry influences. Organizational influence is not seen as a majorly impactful factor in the life of a CISO. A reality that is collaborated by the fact that 74% of organisations have no formal knowledge transfer, and the average global tenure of a CISO is 26 months. This pressure cooker situation

is not stacked in favour of the organisation, especially if one appreciates that the future earning expectation of most responders in the survey are pegged in the R2m plus per annum salary bracket. Not an unrealistic number if compared to what can be obtained as a remote worker in this skillset.

Reflecting on the data, and the realities experienced in industry, there is a strategic imperative for each organization to enable and

speed their CISO's efforts and investment in growing and securing their successors. This would also allow current CISO's to pursue their own growth paths. The demands of the organisation on a CISO to know the business from basement to boardroom, and play across the technology to business continuum creates great opportunity, but if unsupported by the organisation in their growth aspirations, will most likely be supported by another organisation.