Should cybersecurity be linked to executive incentives, and how?

By Carmen Arico

Following major cyber-attacks, some large organisations around the world have started attaching cybersecurity assurance metrics to their executives' short-term incentive plans (STIPs).

According to Fortinet's 2024 Cybersecurity Skills Gap Report, approximately 50% of local companies have each experienced around four cyber-attacks in the last year alone, so should South African entities follow the same trend?

"Larger organisations in the US, including several Fortune 100 companies, have incorporated cybersecurity goals into the calculation of executives' short-term incentives. While we're not seeing this trend in South Africa yet, given the alarming growth in cybercrime, similar practices should be adopted urgently and remuneration committees and reward professionals need to stay abreast of these trends," says Carmen Arico, Chartered Reward Specialist, and spokesperson for the South African Reward Association (SARA).

Cybersecurity as a strategic consideration

With cyber-attacks escalating worldwide, so too have incidents of enterprises being caught completely off guard by them. Such breaches may result in massive data losses, possibly costing millions in lost revenue and potential fines to data regulators and other third parties. Crucially, senior executives are at risk of facing fines, jail time or loss of employment following a cyberattack.

"Cybersecurity has become an undeniable strategic imperative that should reflect in executive rewards as dedicated KPIs," says Arico. "Not including cybersecurity as a part of an overall risk and governance strategy places organisations at reputational or financial risk, among others."

But how should these KPIs be developed and attributed to remuneration?

Proactive, not punitive

Arico raises an important point - cybersecurity-linked KPIs should be proactive in nature and not punitive.

Rather than relying on reactive measures like penalties for breaches, a more effective approach is to proactively incentivise executives to focus on implementing robust security strategies and ensuring this mindset is cascaded through the entire organisation.

Imposing penalties after a breach is far less effective than providing incentives that encourage executives to prioritise organic systemwide protection in the first place.

Executives who maximise system resilience, develop rapid response protocols, prioritise data privacy and protection, assure business continuity and, most importantly, foster a cybersecurity-driven culture and

awareness across all functions in their enterprise are less likely to be breached, and will be able to pivot quicker in instances where a breach requires mitigation.

Those executives who will only be punished financially after an attack that might never happen will typically focus their attention on pressing concerns that impact the business - and their rewards - right now.

“Responsibility also can’t just be left to the CEO and CIO, but organisations must enlist other key players such as the Chief People Officer and Chief Financial Officer. Reinforcing a security mindset requires buy-in from all levels of leadership.” says Arico.

Cyber skills of the board and RemCo

If executive STIs should encompass rewards for resistance to cyber-attacks, who is qualified to develop them?

Cybersecurity awareness has become a top priority within organisations. However, board members and remuneration committees may lack the technical expertise to pinpoint specific cybersecurity priorities, so it’s essential they avoid setting vague or superficial goals for executive incentives.

Performance should be both meaningful and impactful in terms of staving off disaster, and that demands input from one or more subject matter experts.

This means that either someone with a cybersecurity background or expertise should be invited to act in an advisory capacity to the remuneration committee. It could be the CIO or a similarly qualified independent party.

“Either way, they must have a level of knowledge that contributes to the conversations around executive incentives, appropriate KPIs, and other elements of reward,” says Arico. “It is also critical that involvement of these experts should happen early on in the remuneration strategy development process.”

Additionally, reward consultants and practitioners should consider investing in cybersecurity training to expand their knowledge in this area, to allow for greater value to their clients and employers.

Carmen Arico is the Managing Director of Ignite Reward Consulting, and a SARA Chartered Reward Specialist.

RATE THIS ARTICLE