The authors used three coding techniques: theory-based approach / program-driven evaluation, open-ended questioning, and axial coding for the qualitative assessment. The authors then used quantitative methods to assess the theoretical model derived from the qualitative observation, mainly to measure how security policies and control align with the business objectives and values and how users routinely contribute a business perspective to IT on managing security risks. The evidence observed by the qualitative and quantitative study indicates that promoting awareness of security risks and management to the more significant population of stakeholders in an organisation provides an advantage in improvement in both control development and performance. The study also benefited users (business stakeholders) in managing specific security risks within their business process as an alternative to user awareness training (Barki, 2010).

The participation by users in the security risk management (SRM) process leads to users better relating to the process. Participation by users in the SRM also improves aligning the security controls and the business processes. User participation may provide benefits of on the job training for the users. Information Technology(IT) practitioners benefit by better understanding the business processes by engaging with users when developing security control.

Adjusting the behaviour of users requires that IT practitioners evaluate users' understanding and knowledge of risk and security controls. Thus, the lack of users will negatively impact assessing how users understand the significance of security controls in protecting the business. The lack of users may lead to a design of controls that are misaligned with the business process and may interfere with the company's mission. The lack of users will impact the quality of the security controls and their effectiveness; for example, some control may need to be redesigned after they have affected the business process (Harkins, 2016).

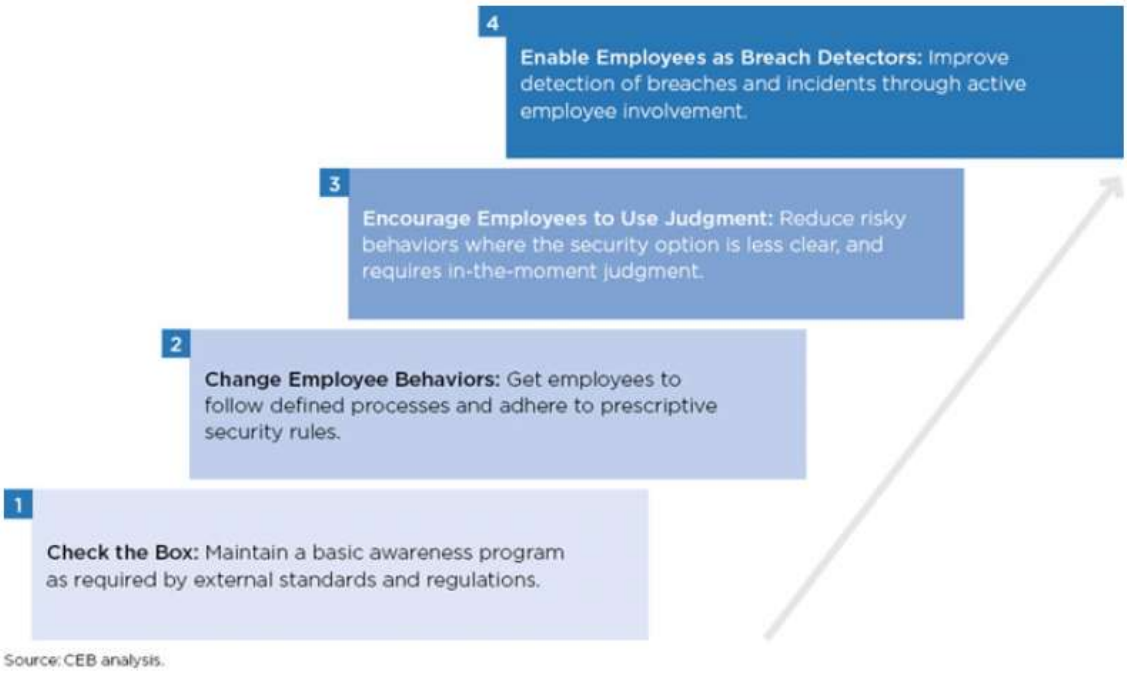

Figure 5-2. *A four-stage model for programs seeking to improve security awareness and behavior. Source: CEB Inc., 2015*

References :

Barki, H. (2010) 'Qa ' rteny', 34(3), pp. 503–522.

Harkins, M. W. (2016) *Managing Risk and Information Security*, *Managing Risk and Information Security*. doi: 10.1007/978-1-4842-1455-8.