Deloitte.

Cyber considerations for C-suite while addressing the board

Ready reckoner for security leaders to build an effective presentation for the board

The following questions act as a ready reckoner or checklist for the C-suite while presenting to the board:

- What is the background and experience of the attendees? Is our presentation customised (not quite technical) to answer their concerns and queries?
- What is the frequency of these presentations? Have we addressed the points raised in the previous meeting? Does our presentation cover and respond to topics the board wants more clarity on?
- Have we got a buy-in from influencers/sponsors before the presentation? Have we shared a narrative of the key points before the board meeting for their reference?
- Have we informed the board that we have categorised assets and focused our security resources to protect critical assets?
- Have we been able to demonstrate measurable business impact when presenting technical content to business leaders?
- Is our messaging restricted only to past events and statistics? Does it also chalk out future risk prospects, their impacts, and the resilience of the organisation?
- Are we giving the board relevant information on time that will help them understand their duties and responsibilities and allow them to make informed decisions?
- Have responses to audit points or external assessments been included in the board presentation?
- Does the presentation give enough information on return on security investments?
- When speaking about controls against key risks, do we have a bifurcation of 'must have', 'good to have,' and 'nice to have' controls?
- Have we communicated the purpose and intent of our key asks to the board?
- Have compliance and regulatory requirements been considered when making this presentation?
- Is the presentation giving enough insights on the strengths of information security programmes and more importantly key white spaces?
- Does the presentation talk about security as an enterprise-wide risk management issue? Have the risks that the organisation has decided to avoid, accept, mitigate, and transfer been communicated to the board?
- Does the presentation clarify the cyber skills present within the management? Does it consider succession planning for key information security roles?
- Through our presentation, will the board be able to identify where the organisation stands compared with its industry peers?
- Have insider risk and third-party risks exposures been covered in the presentation?
- Has the coverage of security awareness sessions and training given to the professionals of an organisation highlighted to the board?