Factsheet - Board Briefings

A Business Strategy must have a coordinated cyber strategy as an integral part?

Our Board cyber briefings will explore how senior management teams and non-executive directors can bring their wealth of experience and judgement to developing a well-structured and robust cyber security strategy. The briefing will cover threat actors and their target/ motivation, the current and emerging cyber landscape as well as sector specific discussions. This will assist Boards in defining an appropriate and proportionate response.

What can you expect in our briefings?

The briefing will be presented in non-technical, business language and will address the concept of cyber risk strategy and how it can be made to align to, and therefore fully support, the business strategy. This will include a discussion about the executive duty (and accountability) of the Board members and to help them fully understand the compliance requirements of them. *Please note this is not designed to make people security professionals!*

This is designed for those not necessarily immediately connected to the cyber security area of the business but who need to ask the right questions about their own area of accountability regarding their people, processes and systems so that they can provide proper guidance to those under their remit.

This is a critical point that helps to ensure the business provides the right messages internally to all staff and shareholders as well as externally to the greater public which in turn, provides assurance about the company's stable cyber security posture.

How long will the briefing last?

Depending on the size of the audience, the briefing will last approximately 60-90 minutes and will be led by one of our industry experts with knowledge of the relevant sector. Company specific challenges will also be built into the discussions and our expert will allow plenty of time after for any forthcoming questions.

What do you cover?

Key areas to be covered are:

- What does 'Cyber' actually mean to them?
- Digitisation and infrastructure transformation
- Current and emerging threats
- Board level accountabilities
- Why is the company a target?
- The requirement for structured cyber education for all roles
- The breadth of possible government assistance
- Highlighting recent obvious mistakes
- How to build cultural change starting with leadership

This will allow the Board to move forward and devise its cyber strategy with the business objectives in mind that will build a robust and cyber-resilient organisation for the future.

Contact **info@sikercyber.com** for more details.