ComputerWeekly.com.com

Growing board focus on cyber risk challenges current thinking

By Marcus Alldrick

I recently had the pleasure of chairing a unique discussion between a panel of active board directors and a room full of cyber risk and information security leaders.

It was a discussion that the security community has long worked to achieve as they battle to have our growing dependence on technology and the associated risks well appreciated at the highest level. It was also very timely as we move into an era of increasing transparency for cyber risks, including at board level.

While this transparency is helping companies better acknowledge the threats we face, our discussion demonstrated that it is also challenging a few perceptions widely held within security communities.

The argument from many chief information security officers (CISOs) for a reporting line that sits outside of the IT department, for example, was soundly challenged by our panel of board directors.

Security managers often pursue such an ideal to assure security autonomy and protect budgets. However, the experience shared in the room demonstrated that IT, more often than not, implements the strategy and can present a barrier if not sufficiently engaged in it.

The discussion, held under the Chatham House Rule by Pulse Conferences at its inaugural CISO 360 Talk to the Board event, encouraged a very open debate, with 70 delegates able to freely share their experience with the promise that they could not be associated with their comments outside of the room.

The four board directors included people serving as non-executive and management board directors in four sectors: advertising and public relations, publishing, retail hospitality, and aerospace.

Delivering desired outcomes

In discussing reporting lines, one of our panellists insisted that his security team stay within IT and that his technical professionals spend time working in frontline business units so they can better understand their role in delivering company outcomes. All the board directors pointed out that they ask their security leaders for credible and provable support around the CISO's ability to deliver their strategy.

Case studies shared in the room demonstrated the need for middle management buy-in and recognition of varied business drivers for the disparate organisations that exist within the businesses – commonality may be found around threats, but the likelihood and impact of the threat coming to fruition will be different across the business. Overall, the conclusion was that the CISO's reporting line is no guarantee of the authority needed.

All of our board panellists confirmed that their businesses' digital transformation, driven by globalisation or disruptive competition and underpinned by new technical platforms, is serving to focus their attention around the inherent cyber risks. They confirmed that the track record of experience in the board room is early in its development.

Establishing credibility, therefore, requires an understanding of who they are and their level of existing appreciation for cyber risk. This should be steeped in an appreciation of the board agenda rather than generic demands for them to become more aware of the issues. They wanted real context from their business and emphasised that this did not mean everything must be expressed in terms of a return on investment.

Managing cyber crises

Our panellists also reassured the room that they are very receptive to being told there is uncertainty, and that, in fact, they are used to it.

When asked if they knew what to do when something happens, it became very obvious that the board members on the panel were well-versed in managing crises. They weren't convinced that they needed to be trained in how to handle a cyber crisis in particular.

We must expect digital transformation to underpin ongoing change in the business and risk landscape and work to develop this conversation.

Perhaps the point that really resonated for me on the day came from a board director who expressed genuine relief that he was now getting to grips with the issues likely to affect his business as he said: "We are now much better informed on the risks and rewards of our initiatives, the costs… The debate continues to this day and aspects change every month. The main thing is the debate is happening."

Read more about cyber risk

- Boards of many of the UK's biggest firms must do more to be cyber aware, according to a government report.
- Keep people at the centre of risk management, says consultant.
- Every organisation must consider the cyber risks it faces and the impact an attack might have.
- Few organisations are managing cyber risk, survey shows.

19 Mar 2019