corix partners

The board strikes back

Responding tactically to cyber threats is not sufficient. Boards now need to step up, argues **JC Gaillard**, managing director of Corix Partners

Recent data breaches have scared board members – in particular, the TalkTalk incident of October 2015, and the aggressive media coverage that surrounded it. Losses can easily run into the tens of millions and – more importantly – brand reputation and customer trust can be left irrecoverably damaged by cyberattacks.

Still, even in response to board-level demands, many large organisations continue to focus on IT point solutions, looking for some imaginary tactical silver bullet that would make the problem disappear. However, many recent breaches seem to relate to the absence of security controls that have been regarded as good practice for years and should have been in place. This is consistent with the low levels of cyber security maturity measured by many recent surveys.

In that sense, it is essential to look at the road to digital resilience from the right historical perspective. In spite of decades of spending in the information security space, many large organisations are still struggling today with problems going back to an era where security measures were seen as a necessary evil imposed by regulations – at odds with functionality and preventing innovation and agility.

Where problems are rooted in decades of neglect, underinvestment and adverse prioritisation, there can be no miracle solution, technical or otherwise. Avoiding cyber security breaches, or dealing with them, will require coherent action over time across the whole organisation.

It is also key to focus on driving tangible action, instead of open-ended risk discussions. On their road to digital resilience, large organisations have to accept first that this is no longer about "risks" – in other words, things that may or may not happen – and that security controls are therefore essential. But getting to that realisation after ten to 15 years of complacency, neglect or short-termist "tick-in-the-box" practices will not be simple. Only by identifying and removing the roadblocks that have prevented progress in the past will they establish a genuine and lasting transformation dynamic.

In our opinion, this is a problem deeply rooted in governance, organisational and cultural matters. It requires a fundamental rethinking and rewiring of information security practices, which can be articulated around three dimensions:

First, change must come from the top and, in that context, board involvement is essential, coupled with a true cross-silo corporate approach – looking beyond mere IT matters. The board must be prepared to look at the problem over the long term and be capable of sticking to a long-term plan. In such a sensitive area, changing approach every time a new board member comes in, or every time a serious breach happens elsewhere, is simply a recipe for confusion and failure. The board must also integrate cyber protection into the remuneration packages of key senior executives, alongside other factors such as delivering new products, increasing revenue or cutting costs.

Fundamental to success will be the personal gravitas, political acumen and management skills of the key transformation agent – the CISO in most large organisations. The CISO should not be just a technologist and must have the seniority and experience to make change happen. This means he or she must remain in charge over the necessary period to oversee real change, and they should be encouraged to consider their tenure over a five-to-seven-year horizon in many cases, instead of the more usual two to three years.

Finally, driving real change in that space will require a long-term transformative vision (supported and funded by the board), articulated into a strategic security road map and a sound security governance model – reaching across all corporate silos, major geographies and key partners across the supply chain. ●

Contact Corix Partners to find out more about developing a strong cyber security practice.

Corix Partners is a boutique management consultancy firm, focused on assisting C-level executives in resolving cyber security strategy, organisation and governance challenges