Five questions audit committee chairs should be asking

by Professor Mark Rodbert, CEO of idax.

With a series of large data breaches occurring in the last year, cyber security has made its way onto the agenda of audit committees across the FTSE 500 and beyond. Tasked with ensuring effective audit and control, the traditional focus of these groups of non-exec directors has been to monitor the integrity of financial statements and performance. However, the growth of mobile and cloud technology has increased the threat to data and critical company information, transforming the risk landscape at a rapid pace. Audit committee chairs typically have a background in finance, and are unlikely to be experts on cyber security, so here are the five key questions they need to be asking their technology teams:

1. Could a TalkTalk happen here?

The TalkTalk breach was seen by many as a turning point. Seeing CEO Dido Harding sat on the This Morning sofa, defending her company's management of customer data encouraged many to examine their own security policies. Kantar Worldpanel estimates the breach has lost the company 4.4 percent of its home telecoms services market share, with its total down to a meagre nine percent.

I'm sure this question has already been asked by most committees, probably multiple times. But the response from in-house teams is likely to have focused on external threats, the hacking of websites, penetration testing and virus protection. This is all positive, but it is only part of the story. The majority of data breaches aren't caused by cyber criminals, but insiders, especially in financial services, with 72 percent of security incidents involving a current or former employee (Source: PWC Global State of Information Survey).

2. What is our vulnerability to insider threat?

Again a key question that is on the agenda of many boards. The challenge is how to interpret the response. Research by business consultancy EY warns that malicious insiders are the fastest growing threat to cyber security. With so many breaches occurring as the result of compromised staff credentials, audit committees need to look for reassurances that sufficient protection exists. The key phrase to look for is 'least privilege'. Every employee in any organisation, from directors to support staff should only have access to the things they need. Allowing employees access to confidential information that they don't need in their day-to-day roles is a big unnecessary risk.

3. How should we reflect cyber-crime in our Viability Statement?

Under the 2014 code directors are required to make a statement that takes into account the company’s principal risks, and should reflect the board’s responsibility for risk and ongoing monitoring. As part of this view on operational risk, how can boards get a clear view on whether staff, contractors and customers have access to data that could be compromising?

4. Do the new EU rules on cyber security impact us and our suppliers?

Recent rhetoric from the UK government and the EU reflects clear concern about both internal and external threats. The nature of some of the recent EU legislation and rulings, has not only put necessary focus on organisation's own policies, but those of suppliers and contractors. The safe-harbour ruling in the early Autumn and EU Network and Information Security Directive in December both put limitations on how companies manage and look after citizens data.

5. Are we measuring risk?

Having policies to manage processes and internal access is a great first step, but these must be fully enforced and risk properly evaluated. Our experience is that most companies are reasonable at managing processes, but poor at measuring risk. Technology departments must be able to tell auditors not just about policy and process but quantify exposure as well. Attacks will come, and understanding the potential impact of either an outsider breaching an account or an employee going rogue is critical to planning and assessing risk.

In today’s fast paced workplace environment, audit committees need to be able to challenge their organisations to measure and manage cyber threats, monthly, weekly and daily, not just when the chairman of the risk committee asks for it. There are tools available that can help to achieve this, enabling quick measurement and quantifying of risk repeatedly through the regular business cycle. As cyber security continues to move up the agenda, it is critical that audit committees respond appropriately and ask the right questions to keep their organisations safe and fully operational.