Editorial

Do you need a wake-up call? A question often asked when you are travelling and forced to stay in a hotel. One of the "benefits" of having young kids is that you can get rid of your alarm clock. The risk though is that without them you won't wake up in time. But more figuratively speaking we can all use a wake-up call now and then. When my six year old daughter asked her little sister "Quick, can you see daddy's password for his iPad?" I had a sort of wake-up call. Am I still concerned about the security of my own devices? How does the current generation of children perceive data privacy and will this even be an issue in ten years' time?

Anno 2016 not many days pass without at least one news item on a "security breach", "cyber hack", "data privacy leak" or any other superlative. With all this media attention a lot of organizations have recognized the risk of data being compromised. Board members have woken up in the last years and increasingly accept their responsibility to effectively steer and allocate resources towards cyber security. They have even started to report on the measures taken against external and internal threats. However, this is to some extent prompted by regulators and supervisory committees that are also starting to open their eyes and require organizations to take the risks of cyber security seriously as it might impact the accuracy and completeness of financial statements. (Supervisory) board members have also "secured" liability insurance specifically aimed at Board members to limit their personal cyber risks.

Within organizations, staff is also waking up to the shift in risks related to cyber security. For example, procurement departments awake and notice that the change in procuring software from traditional applications to SaaS solutions requires a shift in addressing risks. HR and Legal staff open their eyes to the fact that European legislation on Data Privacy requires a step-up in the actions taken to safely process personal data.

However, there are still organizations that have not heard the alarm bells ringing and will only start to really invest in cyber security and data privacy when things have gone wrong. It is up to the security professionals to provide management with a clear and honest view, without resorting to the fud approach ("fear, uncertainty, doubt"). We need to beware of turning the alarm bell into a nightmare. With a report in our hands on the risks identified from a recent security test it is not too difficult to steer management towards panic mode. Security professionals should therefore always support the organization in addressing the (root causes of the) issues identified.

Some would argue that the cyber security "hype" is already declining and would even see a level of "cyber fatigue" arising at management level. This might be caused by the fact that board members have not seen the risk materializing within their organization or have other priorities. As the threat landscape is constantly evolving, we cannot afford to sit back and face the risk of being rocked to sleep.

Are you fully awake? Great, enjoy reading this edition of *Compact* on the ever-interesting topic of cyber security!

Pieter de Meijer

We've got you covered! On **page 42** you will find a webcam cover that helps you protect your privacy when not using your laptop camera. The webcam cover also serves as a reminder to regularly visit the KPMG Cyber Trends Index at **cyber.kpmg.nl**, the real-time overview of news, trends and threats in information security. Stay up-to-date with the latest cyber trends – online or via the app. You can read more about the Cyber Trends Index in this edition.