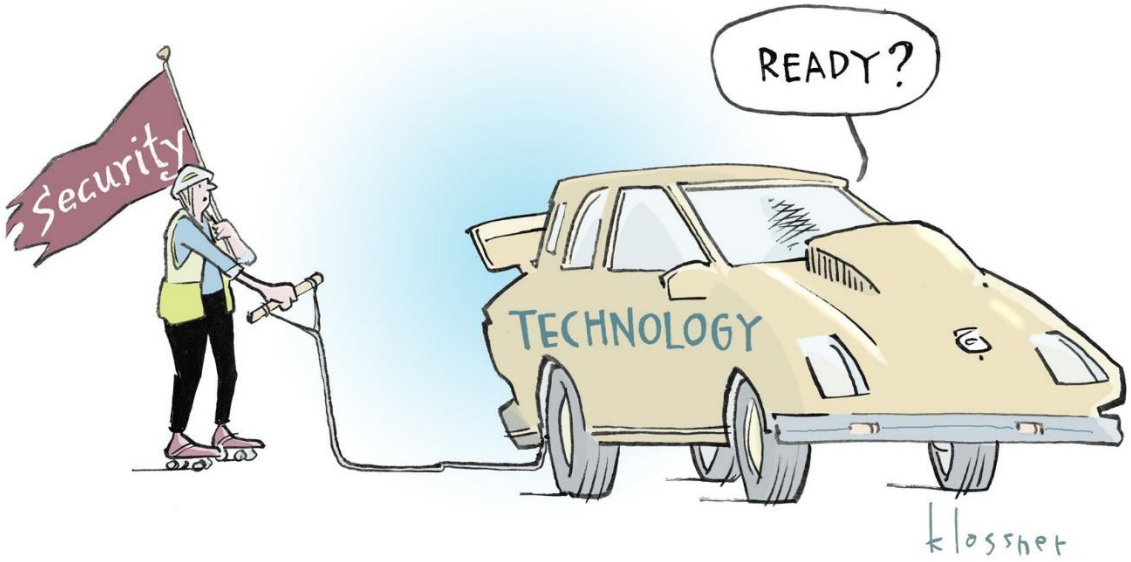

Amidst so much uncertainty and with so much being written about the uncertainty, it is clear only that we don't yet know how much life will change (or perhaps not) when COVID 19 is finally behind us. Amidst the chaos, however, there remains one topic upon which consensus seems to be steadily growing: ESG. Under the coronavirus spotlight, the immediate relevance and practical application of all three of its elements – environmental, social and governance – are being weighed and measured as never before.

In the context of ESG as part of investment, the CFA Institute published its manual *Environmental, Social, and Governance Factors at Listed Companies* as long ago as 2008. Subsequently *Environmental, Social, and Governance Issues in Investing* arrived in 2015, when a survey of charterholders suggested that "board accountability" was the single most important ESG factor in investment analysis and decision-making. There was, however, (surprisingly) no mention of one area, which sits in both Social and Governance areas, which is growing faster and which is now arguably more immediately important than any other: cybersecurity.

Published in January, *RBC Global Asset Management's "Responsible Investment Survey"* revealed that two-thirds of 800 institutional investors, in the United States, Canada, Europe and Asia, are more concerned about the impact of cybersecurity on their investments than anything else under an ESG heading. We should not be surprised. Cyber breaches rose by over 65% over five years (to 2019) and the total global cost of cybercrime between 2019 -2023 is estimated to be $5.2trn, according to *Accenture's "Ninth Annual Cost of Cybercrime"*. And, of course, that was *before* the world was forced to work from home. From the huge number of reports of surging cyber-attacks, it is particularly depressing to hear of the World Health Organisation having suffered a fivefold increase, while behind the scenes rival agencies cyber-spy in the race to find a vaccine.

There are many pieces of (free) advice and "thought leadership" on the subject and not least around boards' ability and willingness to take ownership of cybersecurity. Many adopt a similar tone, i.e. they assume a board's ignorance and suggest it be addressed periodically through bite-size education. The burden of educating now often falls on a Chief Information Security Officer, who rightly and rapidly is

growing in corporate status (*The role of the CISO, Leathwaite*). But if there's nobody within the company, boards "may also want to consider hiring outside experts to explain the latest technologies and best practices to help directors become more educated on cyber risk and preparedness" (*Cybersecurity, The Board's Role, Spencer Stuart, 2015*).

But the truth is that board ignorance remains largely unchanged. The Principles for Responsible Investment's recent *Stepping up Governance on Cybersecurity* is a snapshot of the *status quo*, noting that "nearly 60% of companies did not indicate that their board or board sub-committee was responsible for cyber security related issues". Furthermore "only 10% indicated that they actively appointed directors with cyber security skills and expertise". This is growing harder to reconcile with not only the institutional investors' and shareholders' concerns, but also those of stakeholders, who bear the brunt of (for example) a major data breach. There seems to ongoing denial that cybersecurity "is not just an IT issue, it is a board issue" (Clara Durodié, CEO, Cognitive Finance).

A cyber-attack (the defence against it and/or the response to it) is in fact one of the few potential wholesale catastrophes which can (should) be incorporated into company strategy. Of twenty two principal global risks listed in the biennial *Lloyd's City Risk Index*, only the threat of "Cyber-attack" (ranked 7th) is constant and in large part (relatively) known: less of a black swan perhaps, than grey. The rest (earthquakes, solar storms, war, etc.) are sporadic and unpredictable, beyond the control of any board and requisite of an insurance policy. As an aside, a Human Pandemic ranked 4th (and its cost seems somewhat underestimated) in the same Index.

Board composition and corporate governance have been and are subject both to academic and increasingly empirical investor scrutiny. There has been particular emphasis on the importance and benefits of ethnic and gender diversity. Scrutiny of competence, however, and *relevance* has been less intense, in large part because of an absence of data. In the context of ESG and specifically cybersecurity, this seems unsustainable. By way of (an admittedly simplistic) example of a dichotomy, the average age of a public company independent non-executive director is currently over 60 for FTSE companies; and over 63 on the Dow (*www.boardex.com*). Both are rising. By comparison, 73% of CISO's are under 45; and 42% of female CISO's are under 35 (*The CISO in 2020, Marlin Hawk*). It is not only the gap in knowledge that stands out.

The good news is that boards are at last being more than spoon-fed knowledge. For example, *Resilient Governance for Boards of Directors* (Center for Long-Term Cybersecurity at UC Berkeley) accepts that "currently, there is no stable and consensual playbook for board oversight of cyber", but it usefully sets out and offers guidance around the choices open to a board (including possibly having "specific board members who offer deep specialized knowledge of cyber").

One prominent investor, Warren Buffett, described cybersecurity as "the number one problem with mankind" (albeit he did so in 2017; it has recently, let's hope temporarily, been usurped). The point is that it is the investors – including CFA charterholders – who must shoulder the burden of driving change at board level. Stakeholders are in the public eye and the politicians too, who will take advantage (Elizabeth Warren et al.); but it is the larger shareholders, with a voice or even a seat at the table, who are most likely to have an immediate impact. As a first step, they need to ask for more detail and data around boards' ownership of ESG generally and cybersecurity in particular.

Today, more than ever, we individuals depend on technology. But many companies depend *totally* on technology. Dependency and vulnerability go hand in hand. Investors, over to you.

Rupert Mathieu is a Managing Partner of Sainty, Hird & Partners. He started working in executive search in 1999, having spent eight years at JP Morgan in London and Tokyo. He now runs the Asset & Wealth Management practice.