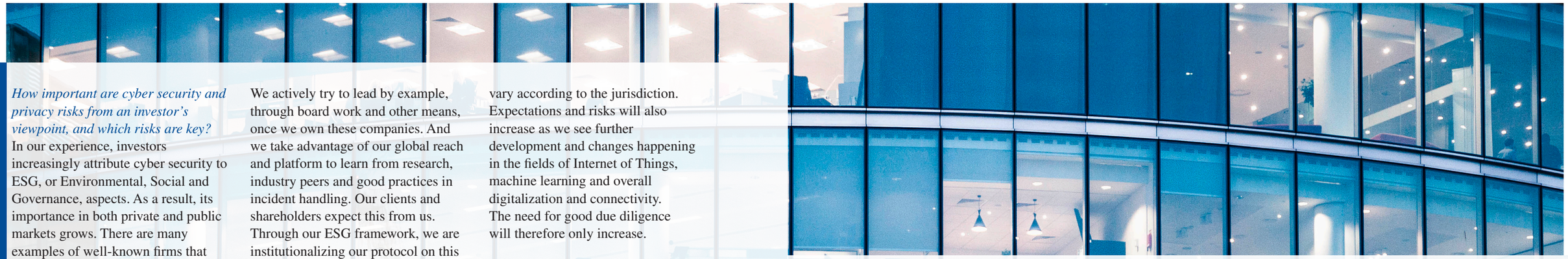
Know your target: how cyber due diligence feeds investment decisions

Christian Unger, Managing Director and Co-Head Industry Value Creation at Partners Group, shares his insights into how cyber due diligence is becoming an integral part of ESG frameworks, and its potential to protect investors and customers alike.

Christian Unger
Managing Director and Co-Head Industry Value Creation at Partners Group



How important are cyber security and privacy risks from an investor's viewpoint, and which risks are key?
In our experience, investors increasingly attribute cyber security to ESG, or Environmental, Social and Governance, aspects. As a result, its importance in both private and public markets grows. There are many examples of well-known firms that have seen their value diminish due to breaches related to cyber security and/or privacy. At Partners Group, cyber security and privacy is important to protect investors but ultimately also the customers of our portfolio companies. The topic of data and its privacy is also becoming more prominent in public discussions and through cross-border regulations and directives such as GDPR and NIS. The priority for Partners Group is to make a thorough assessment of each company we consider investing in, with cyber security as a standard item in our due diligence process.

We actively try to lead by example, through board work and other means, once we own these companies. And we take advantage of our global reach and platform to learn from research, industry peers and good practices in incident handling. Our clients and shareholders expect this from us. Through our ESG framework, we are institutionalizing our protocol on this topic to be a standard part of our investment processes.

We have not until recently seen many investors looking at cyber security or privacy risks as part of their due diligence. Do you expect this to change?
For Partners Group, cyber security and privacy risks are key items and discussion points in any due diligence process. We believe more and more investors and shareholders will expect companies to have a clear strategy in this area. As will regulators, even though specific expectations may vary according to the jurisdiction. Expectations and risks will also increase as we see further development and changes happening in the fields of Internet of Things, machine learning and overall digitalization and connectivity. The need for good due diligence will therefore only increase.

How do you balance the depth vs scope and duration of assessments of cyber security and privacy risks in target businesses?
This is a very interesting question. The non-binary outcome of a cyber security and privacy assessment often results in a decision to prioritize, for example, risk exposure related to the business's position in the supply chain (e.g. critical infrastructure) or handling of sensitive (personal) information. Covering all aspects would not only be time-consuming but also very costly and would not give 100% security. At Partners Group, we first carry out an initial analysis to highlight some of the major risks, from dark-web scanning to vulnerability testing. Based on this initial analysis, we decide where to focus going forward. We have also found that by simply asking the management team cyber security-related questions, we quickly gain a basic but good understanding of the company's cyber security and privacy health. We have also noted in these processes that management teams appreciate an investor who can give them some guidance in a field where they feel growing pressure and where they might lack deep functional expertise.

How do such findings influence your investment decision?
As with other elements in a due diligence process, it is a risk-reward offset. If a potential investment shows clear cyber security risks, we can decide to walk away from the opportunity or we can choose to reflect the risk in our valuation or offer. We have an industry value creation team that works closely with our portfolio companies to grow and develop their businesses. In the case that we choose to move forward with an investment in a company that needs improvement in the area of cyber security, our value creation team would work with management to solve critical issues as a near-term priority. This might include staff training, assessment of the company's culture, cyber response plans etc.

Do you believe investors use cyber due diligence it to its full potential?
Compared to other due diligence elements such as financial due diligence or management assessment, cyber is a relatively new topic. However, the overall understanding of technology and its associated risks is growing rapidly in the investor community. We will see this clearly develop further and become more sophisticated. This will be necessary as the threats and risks will become more difficult to judge. Companies will have to continue to train and develop staff and make sure they have in place the most relevant technical solutions and third party providers.

Looking forward, how do you expect cyber and privacy due diligence to develop?
As mentioned, the market is developing fast and we will see new challenges arise. As with many digital developments generally, it will be important to be agile. This is because remaining 'current' will be a key success criterion in this field. It will be about managing risk, but also sharing best practices between companies or within the investor community. In the future, cyber security and privacy processes and assessments will be included as standard in any ESG framework.

«The overall understanding of technology and its associated risks is growing rapidly in the investor community. We will see this clearly develop further and become more sophisticated.»