Speakers:

- Juan Rivera (JR) - Senior Managing Director, FTI Consulting
- Xavier Janer Serra (XJ) – Senior Marketing Manager, FTI Consulting

XJ Hello, and welcome to a new episode of our podcast. I am Xavi Janer (XJ), Marketing Manager for FTI Consulting in Spain, and today we have here with us Juan Rivera (JR), Senior Managing Director of the Strategic Communication segment (advisory on regulatory issues and public affairs) at FTI Consulting.

JR Hi. It's a pleasure to be here.

XJ Nowadays, more and more situations threaten the performance and reputation of companies. We are, for example, seeing and hearing about the importance of the ESG criteria, with a strong emphasis on the environmental factor. But in today's episode, we want to focus on the G for governance, as in good governance, but in relation to cybersecurity: that is, we will talk about cyber governance. Tell us, Juan, what's going on and why cybersecurity has become one of the key latent risks for businesses.

JR Companies are increasingly exposed to cybersecurity risks as teleworking is introduced and business digitalization grows. As a result governments, regulators and investors are exerting greater pressure on organizations to improve their cybersecurity measures, increase transparency around disclosures, and create corporate governance structures that demonstrate that managing cybersecurity risks is a priority issue.

One example is that the World Economic Forum has ranked cybersecurity among the top five global risks, and it has called on companies to incorporate cybersecurity protocols into their ESG risk management.

In terms of investment, we at FTI Consulting have conducted studies that have found investors now consider cybersecurity to be a key priority: a 2021 survey of 204 institutional investors showed that they placed the risk of cyberattacks among their biggest concerns regarding the companies in which they invest.

Large-fund managers are demanding more detailed information from companies, including past cyber incidents that may affect the current activities of running of the business. Therefore, how companies communicate their cyber risk governance is becoming increasingly important, as it has a direct impact on valuations and earnings prospects.

XJ We often imagine rogue hackers behind cyberattacks, but companies must not forget that you have to protect yourself from different types of profiles when it comes to cybersecurity. Who could be responsible for such threats?

JR In addition to cyberattacks by cyber criminals, threats also come from the so-called *hacktivists*, or activist hackers who target critical infrastructure and sectors and who are driven by ideological motives, and even from nation states, so one could speak of the current period as the beginning of a "cyber cold war." It should be remembered that a cybersecurity incident is still very costly for businesses; according to IBM, the average total cost of a ransomware breach in 2022 was $4.54 million. And this must be added to the reputational cost of the company attacked, which is forced to explain itself to its investors.

XJ With this context in mind, how can businesses prepare for these cybersecurity risks?

JR Our view is that companies should consider approaching cybersecurity in a manner similar to how they approach climate change/sustainability. Any approach should be built around four pillars, which would enable companies to acknowledge the risks of cybersecurity in a holistic manner: governance, strategy, risk management, and metrics and targets.

XJ There are many fronts to consider, and the complexity of coordinating the different areas of governance within an organization is challenging. What are some of the most common dangers in this regard (good governance)?

JR In recent years, a key executive position has emerged in this area, that of chief information security officer (CISO). Part of the role of the CISO is to communicate cyber risks and follow-up metrics in terms that resonate with the executive committee or the board. The CISO should also provide training to senior executive (C-suite) officials on how to take appropriate action in their decision-making processes in order to avoid cyber risks. At the same time, governance structures will be needed internally that give priority to the commitment of the CISO to identifying and resolving cyber risks. The role of the CISO is also critical when acting during a cyber crisis, where decisions need to be made and communicated quickly, both to protect the firm's reputation and to avoid sanctions from regulators. Finally, the CISO should define metrics to quantify the impact of cybersecurity in business and financial terms, considering it as an investment rather than an operational cost.

Let's look at some facts that reflect what the current situation is on the subject we are discussing. According to a recent survey of 165 CISOs in the United States, 58% admitted struggling to communicate with their companies' senior leadership. The survey also revealed that 53% of CISOs believe that cybersecurity priorities are not completely aligned with those of senior leadership.

XJ Understanding cybersecurity as a priority can be a good start, right?

JR That's true. But beyond that, given the increasing frequency of cyberattacks and their magnitude, having a cyber expert on the council has become increasingly important. The lack of technology expertise among board members creates a real and meaningful gap in the board's skillset: according to the survey cited earlier, in 2022, only 7.2% of FTSE 350 and ISEQ20 listed companies had directors deemed to have technology expertise.

In the end, the big challenge for organizations is to increase the technological knowledge of the members of the board of directors so that its cyber governance becomes more effective.

XJ That's what we are going to keep in mind then. Thanks a lot, Juan, for sharing your thoughts on this new episode of FTI Consulting Talks, and thanks to all of you who listen to us across the different platforms. Best regards.