In an increasingly digital world, companies keep many trade secrets and intellectual property in an electronic form. They therefore face an increased risk of breach from external hackers, as well as current or former employees, who may have incentives to misappropriate company property. While many companies have put in place frameworks to obviate external attacks on their data, they are largely unprepared to counter the threat from within their own rank and file.

The resultant impact on a company’s competitive edge can be fairly substantial, and regulations, such as the General Data Protection Regulation, add another layer of complexity should the breach involve loss of personal data. It is crucial that organizations, from large corporations to small and medium-sized enterprises, know immediate steps to be taken if a data breach is identified at their firm.

The first session of this program, “Employee Investigations in Data/IP Theft Situation: Dos and Don’ts in the Early Days of GDPR,” focused on not only investigating data or IP thefts but also best practices to adopt to ensure compliance with the GDPR.

The second session, “Forensics to Prevent, Detect, and Investigate Senior Management Misconduct,” considered the broader aspect of employee misconduct, especially involving senior management. Industry experts and participants identified proactive and reactive measures to protect a company’s best interests if certain members of management run afoul of their mandate.

Abhijit Yadav contributed welcome remarks, and Stuart Witchell provided concluding remarks.

View the full agenda.