The Cybersecurity Law Report Features Partner Alysa Hutnik on FTC Expectations Regarding Reasonable Security

November 2, 2016

Partner Alysa Hutnik was featured in *The Cybersecurity Law Report* article "Demystifying the FTC's Reasonableness Requirement in the Context of the NIST Cybersecurity Framework (Part Two of Two)." In this article on the FTC's data security expectations in the context of the NIST Cybersecurity Framework, in-house and outside counsel discuss how the Framework's core functions -- Identify, Protect, Detect, Respond and Recover – align with the FTC's requirements. Ms. Hutnik discuses each of these core functions and how organizations should consider them in their cyber readiness. But she notes that, while these functions "line up very closely with the FTC's expectations," how companies apply them can vary. Ms. Hutnik also notes, "The best of plans and life sometimes collide." A company may have a security plan that served it well for the past several years but "the fact is that things keep evolving." Companies need to be mindful of that and ask themselves whether their current data security plan still works, their training program is effective, their firewalls are sufficient, and remote access is secure enough. "Unless you are actually looking and have controls in place to see if your program is working, it is going to be really tricky to figure out if you have a gap that needs to be addressed," says Hutnik.