Practical Tips for In-House Counsel From Recent Cybersecurity Decisions

"The possibility of a cybersecurity incident—and ensuing litigation—is a fact of life for almost every business. Even companies that do not process or handle consumer information collect personal information about their employees that can be targeted by hackers or phishing scams or even inadvertently disclosed, exposing the company to potential liability," warns Seth Harrington, Michelle Visser and David Cohen in Orrick's ***blog***.

"While eliminating cybersecurity litigation risk entirely likely is not feasible, recent cases do highlight some steps that companies seeking to reduce potential exposure to cybersecurity litigation can take:
(1) Recognize that pre-incident statements about the company's cybersecurity measures can be used to sustain deception-related claims.
(2) Assess the "reasonableness" of your cybersecurity, despite the difficulty of doing so.
(3) Pay attention to how you structure cybersecurity initiatives to protect related documents and communications based on the attorney-client privilege and work product protection.
(4) Recognize that your statements about a cybersecurity incident may be relied on by courts to sustain plaintiffs' claims.
(5) Consider arbitration clauses, but do so cautiously.
(6) Consider opportunities to contractually allocate or disclaim liability."

Read the article.