Supply chains have become more vulnerable in recent years, and high-profile cyber-attacks that have crippled the supply chains of well-known companies reveal that the point of entry for hackers is often through the weakest link in the chain. Exacerbated by growing complexity and the need to be visible, these supply chains share vital streams of information every minute of the day, thereby becoming an easy and highly lucrative target for talented criminals, causing financial losses as well as damaging brand reputation and value. Companies must therefore invest in supply chain capabilities to withstand cyber-attacks (i.e., cyber-resilience) in order to guard against potential threats. They must also embrace the reality that this often-unseen dimension of risk is the “new normal”. Although interest on this topic has grown in the business world, less has been reported by the academic community. One reason for this could be due to the convergence of two different disciplines, information technology and supply chains, where supply chain cyber-risk and cyber-resilience appear to have a natural fit. The topic of cyber-resilience in supply chains is still in early stages of development, and this is one of the first journals to focus a special issue on it. Currently, the closest academic literature is within the realms of supply chain risk and resilience, where numerous models and frameworks exist. In this article, this literature is explored to identify whether these models can incorporate the dimension of cyber-risk and cyber-resilience. In doing so, we create a research agenda for supply chain cyber-resilience and provide recommendations for both academia and practice.