A more comprehensive way of looking at cyber-risks in supply chains is required, when considering the increasing complexity of the supply networks and the exposure to unexpected disruptions, caused by cyber-attacks. This article describes some of the reasons why current risk assessment methods are insufficient. The article provides an analogy for understanding the dynamic effects in a company. It describes in general terms what it means to understand cyber-risks from the control perspective, and it describes a new way to understand supply chain resilience. The focus is changed from the reliability of the supply chain components to the control and a deeper understanding of the supply chain system.