How can the principle of parsimony be applied to the design of cybersecurity systems, and what are the potential benefits and drawbacks of keeping security solutions as simple as possible?

Applying the principle of parsimony to the design of cybersecurity systems can have benefits for both the people managing the system and the system itself. Blocking unused ports, limiting system functionality, applying least privilege permissions, and having a centralized point to monitor and manage a network are all examples of keeping a system simple and efficient. By having a plethora of different programs and security solutions running on hosts, it can become hard to effectively discover vulnerabilities, which can lead to delayed patches. Utilizing the principle of least privilege ensures that users can access only the resources they need to complete their assigned tasks, leading to a reduced risk of human error. Simplicity in a cybersecurity system is generally a good policy to follow, but without proper management and adaptation to emerging technologies, the system will remain vulnerable.