

Sean Shreve

23FEB2026

CYSE 200T

Professor Duvall

Discussion Board: Protecting Availability

In this discussion board, you are the CISO for a publicly traded company. What protections would you implement to ensure availability of your systems (and why)?

If availability is compromised, that means the downtime impacts revenue, customer trust, shareholder confidence, and would be overall detrimental to business operations. There are several options to prevent attacks on availability, but I would utilize the two following preventative policies.

First, I would provide back-ups to the back-ups. Also known as redundancy, I would implement this in nearly every aspect of the supply chain as well as customer access points. Distribution centers, cloud based environments, clustered servers, and power supplies. No single point of failure would exist for the company.

Second, direct denial of service (DDoS) attacks would have to be prevented. Mitigation of such attacks would increase uptime of company operations, in particular website functionality. Proactive monitoring through operation centers would help to increase incident response before outages would become to severe.

To support these two priorities, proper patching and upkeep will be a must to ensure exploitation is kept at a minimum. Keep the holes patched, the backdoors locked, and maintain a diligent watch should ensure availability of the company's systems.