



## OVERVIEW

### DoS vs DDoS

Most commonly associated with websites, denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks can temporarily slow or stop business operations for an unprepared organization. These can be simplistic volumetric attacks that flood the capacity of a website or more complex attacks that use bots and reflection-amplification techniques to achieve similar ends. Even more sophisticated attacks involve crafting payloads which exhaust or crash specific services that don't require massive volume to exploit. However, volume usually helps the efficacy of these attacks, so they may also be "distributed."

If a business relies on their website to make money, this threat is obvious. However, protocols other than HTTP/S may be vulnerable - telecoms or even smaller companies that run their own publicly accessible DNS servers may be vulnerable to attacks, and since DNS underpins most of the modern internet, the effects can be severe. The 2016 attack on DNS provider Dyn, which knocked 14,000 websites offline, is a prime example of this type of incident.

## BEST PRACTICE

### System Interruption

Resilience's Cyber Meteorology Framework models cyber risk trends and helps companies stay up-to-date with current best practices and mitigation guidance. The DDoS-related systems interruption model recommends that organizations do the following to prevent and mitigate these attacks:

1. Serve applications and website from Content Delivery Networks (CDN) where possible
2. Build applications on Infrastructure-as-a-Service (IaaS) or hosting platforms that offer managed DDoS protection
3. Deploy web application firewalls and other solutions that can protect both on-premises and cloud-based applications

# INSURANCE

## Business Interruption

Coverage for DDOS attacks can provide both first-party and third-party protection. This means that if you're hit with a DDOS attack or if a third party claims you could have done more to prevent a DDOS attack, you are covered. Speak to your broker to learn more.

## Example Claim

National luxury goods retailer suffers a DDOS attack that brings down its e-retail website for three days during the holiday season, making online shopping impossible.

