**reasons for network security**

it relates to an organizations business continuity

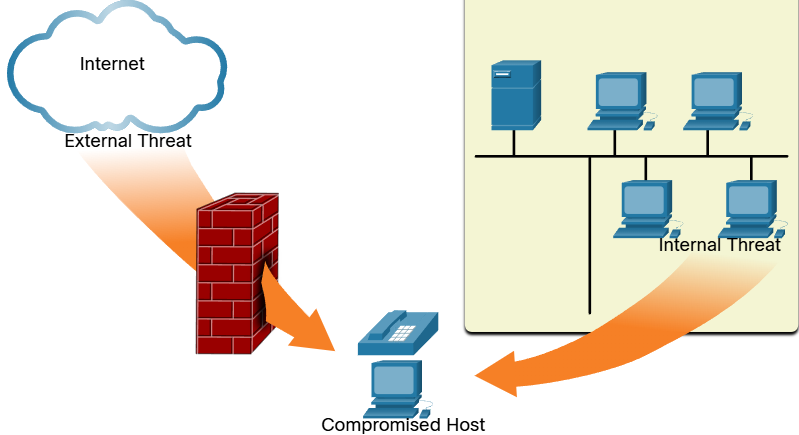
maintaining a secure network ensures the safety of network usrs and protects commercial interests.

Many tools are available to help network administrators adapt, develop, and implement threat mitigation techniques. For instance, the Cisco Talos Intelligence Group website, shown in the figure, provides comprehensive security and threat intelligence to defend customers and protect their assets.

**vectors of network attacks**

attack vector

is a path by which a threat actor can gain access to a server, host, or network

they originate from inside or outside the network  


Internal threats have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices. Employees may also have knowledge of the corporate network, its resources, and its confidential data.

**data loss**

* Data is likely to be an organization’s most valuable asset
* Data loss, or data exfiltration, is when data is intentionally or unintentionally lost,   
  stolen, or leaked to the outside world. The data loss can result in: Brand damage and loss of reputation
* - Loss of competitive advantage
* - Loss of customers
* - Loss of revenue
* - Litigation/legal action that results in fines and civil penalties
* - Significant cost and effort to notify affected parties and recover from the   
   breach

**Common data loss vectors**

social networking (social engineering, phishing…)

unencrypted devices

cloud storage devices (sensitive data can be lost if compromised)

removable media

hard copy (data should be shredded when no longer required)

improper access control (stolen, weak passwords)