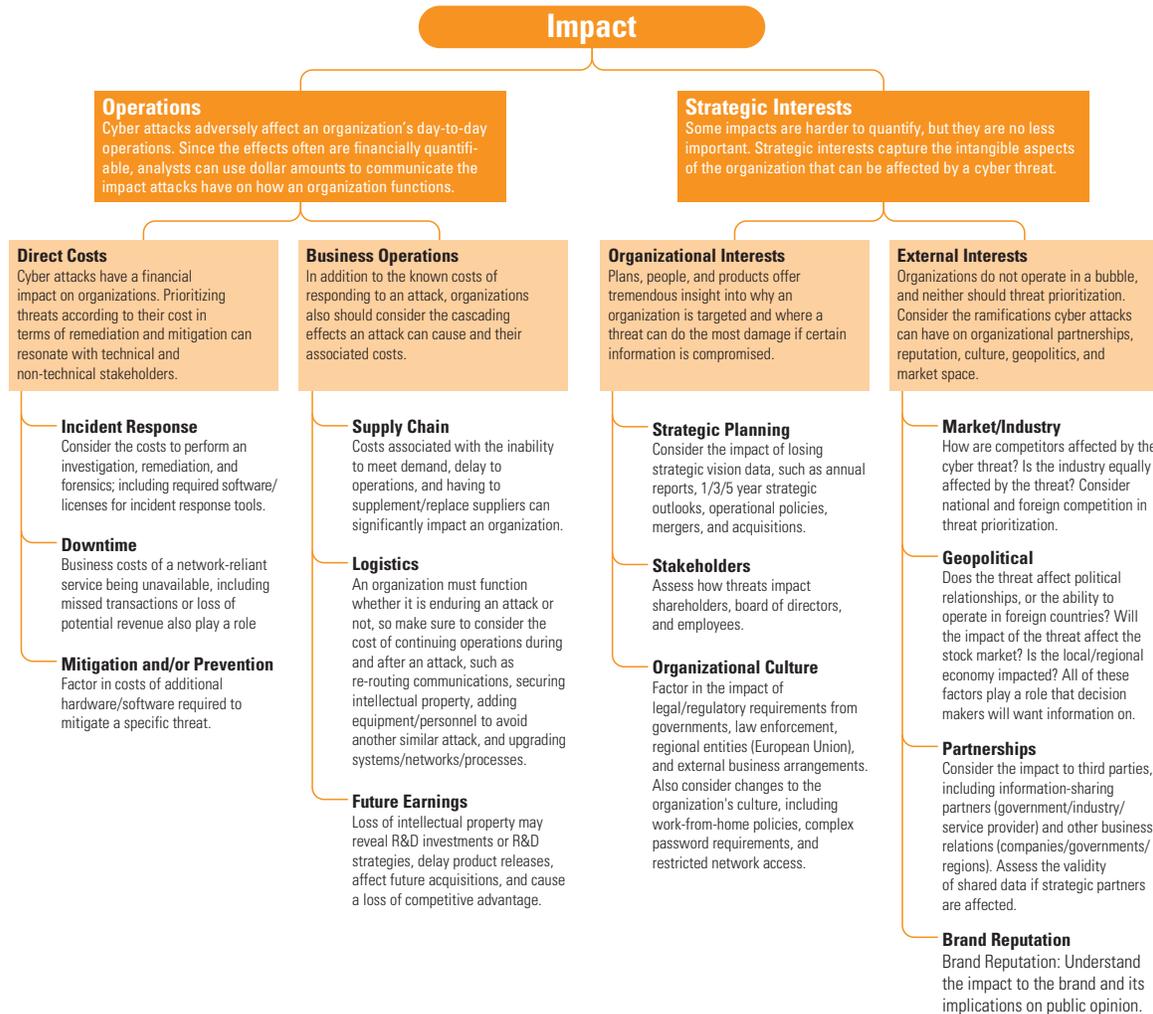


Impact

Analyzing the effects cyber attacks have on an organization's operations and strategic interests provides quantifiable, business-related information to justify its impact on the organization. A CITP participant quantified the impact of cyber threats to their leadership by assessing how much money the organization would pay to reroute its product distribution channels after a hacker compromised the network and disclosed specific travel routes to competitors intent on disrupting this distribution.



Indicators of Success

- Internally, analysts establish frequent communication with the business units responsible for operations to discuss threats, alter threat prioritization, and predict new threats. These business units can include R&D, physical security, risk management, IT, human resources, insider threat, and business intelligence.
- Analysts identify and remediate the cascading effects a cyber attack could have by targeting one part of the organization's operational network and systems.
- Analysts recognize how a cyber attack could impact the organization's ability to operate and communicate to stakeholders and institute appropriate contingencies to eliminate this impact when an attack occurs in the future.
- Knowledge of the impact cyber attacks can have on an organization's operations enables analysts to determine the financial costs to recover and repair damage done by the threats that the analysts' prioritization efforts deem most likely to harm the organization.
- Analysts ensure that threat prioritization isn't based off personal biases or those of decision makers, stakeholders, service providers, or the media.
- Analysts correlate logs of IPs accessing the parts of their organization's website containing data on strategic planning and intellectual property with known bad IPs to predict where threats will be concentrated now and in the future.
- Analysts understand the financial cost associated with a geopolitical event in a country threatening their organization's Internet presence in that market.
- Analysts recognize that if peers in their industry and the organization's economic interests are being attacked, the likelihood of being targeted increases and they take preventative measures to ensure that doesn't happen.