

Impact

Operations

Cyber attacks adversely affect an organization's day-to-day operations. Since the effects often are financially quantifiable, analysts can use dollar amounts to communicate the impact attacks have on how an organization functions.

Direct Costs

Cyber attacks have a financial impact on organizations. Prioritizing threats according to their cost in terms of remediation and mitigation can resonate with technical and non-technical stakeholders.

Incident Response

Consider the costs to perform an investigation, remediation, and forensics; including required software/licenses for incident response tools.

Downtime

Business costs of a network-reliant service being unavailable, including missed transactions or loss of potential revenue also play a role

Mitigation and/or Prevention

Factor in costs of additional hardware/software required to mitigate a specific threat.

Business Operations

In addition to the known costs of responding to an attack, organizations also should consider the cascading effects an attack can cause and their associated costs.

Supply Chain

Costs associated with the inability to meet demand, delay to operations, and having to supplement/replace suppliers can significantly impact an organization.

Logistics

An organization must function whether it is enduring an attack or not, so make sure to consider the cost of continuing operations during and after an attack, such as re-routing communications, securing intellectual property, adding equipment/personnel to avoid another similar attack, and upgrading systems/networks/processes.

Future Earnings

Loss of intellectual property may reveal R&D investments or R&D strategies, delay product releases, affect future acquisitions, and cause a loss of competitive advantage.

Strategic Interests

Some impacts are harder to quantify, but they are no less important. Strategic interests capture the intangible aspects of the organization that can be affected by a cyber threat.

Organizational Interests

Plans, people, and products offer tremendous insight into why an organization is targeted and where a threat can do the most damage if certain information is compromised.

Strategic Planning

Consider the impact of losing strategic vision data, such as annual reports, 1/3/5 year strategic outlooks, operational policies, mergers, and acquisitions.

Stakeholders

Assess how threats impact shareholders, board of directors, and employees.

Organizational Culture

Factor in the impact of legal/regulatory requirements from governments, law enforcement, regional entities (European Union), and external business arrangements. Also consider changes to the organization's culture, including work-from-home policies, complex password requirements, and restricted network access.

External Interests

Organizations do not operate in a bubble, and neither should threat prioritization. Consider the ramifications cyber attacks can have on organizational partnerships, reputation, culture, geopolitics, and market space.

Market/Industry

How are competitors affected by the cyber threat? Is the industry equally affected by the threat? Consider national and foreign competition in threat prioritization.

Geopolitical

Does the threat affect political relationships, or the ability to operate in foreign countries? Will the impact of the threat affect the stock market? Is the local/regional economy impacted? All of these factors play a role that decision makers will want information on.

Partnerships

Consider the impact to third parties, including information-sharing partners (government/industry/service provider) and other business relations (companies/governments/regions). Assess the validity of shared data if strategic partners are affected.

Brand Reputation

Brand Reputation: Understand the impact to the brand and its implications on public opinion.