

A hand in a dark blue sleeve points towards a central blue hexagon labeled 'RISK MANAGEMENT'. The background is a light blue grid of hexagons, some of which contain text. The overall image has a blurred background of people in a professional setting.

RISK MANAGEMENT

Avoid

Identify

Accept

Strategy

Reduce

Action
plan

Transfer

Control

Third Parties

Mitigate

Third Party Risk Management

Not always viable



Supply Chain Attacks

These occur when cyber criminals infiltrate a target through an outside partner or provider with access to the target's systems, network and data.



Solar Wind Attack

Over 250 organizations and more than 18,000 customers were affected after the attackers were able to inject malware into the company software "Orion"



Supply Chain Attacks

Expected to increase over the next few years



Supply Chain Attacks

A successful attack against the target
= A successful attack against many



TPCRM

Third-party cyber risk management (TPCRM) is an organized approach of analyzing, controlling, monitoring and mitigating cyber risks associated with third-party vendors, suppliers and service providers.



TPCRM Risks

- Inherent Risk - The risks involved just by dealing with the third party absent of any security controls.
- Residual Risk* - The risks that remain after all security controls have been accounted for.



Next Lesson

The 6 steps involved in TPCRM.

