# Research report: Endpoint Security – Software Supply Chain Attacks

VB Business Panel

80% percent of respondents believe that over the next three years, software supply chain attacks could pose one of their biggest cyber threats. However, only 35% consider supply chain attacks an area of focus.

66% of respondents reported that their organisation has experienced a software supply chain attack.

Of which 90% incurred financial cost as a result. The average cost of an attack was over $1.1 million.

The vast majority (87%) of those that suffered a software supply chain attack had either a full strategy in place, or some level of response pre-planned at the time of their attack.

The industries that experienced the most supply chain attacks were biotechnology, pharmaceuticals, hospitality, entertainment and media, and IT services, although attacks occurred across a wide range of sectors.

Software suppliers aren't being vetted enough: although close to 90% of those surveyed see vetting as critical, only one-third of respondents vet all of their suppliers. 58% of senior IT decision-makers indicated they plan to evaluate their suppliers more rigorously.

Only 37% of respondents in the US, UK and Singapore said their organisation has vetted all suppliers, new or existing in the past 12 months and only a quarter believe with certainty their organisation will increase its supply chain resilience in the future.

## Who did we interview?

1,300 senior IT decision-makers and IT security professionals in the United States, Canada, United Kingdom, Mexico, Australia, Germany, Japan and Singapore, across a wide range of industries.

**90 %** believe they are at risk for a software supply chain attack.

Research published in July 2018