

# Common cyber insurance objections

## Objection

## Response

*We don't need cyber insurance. We invest in IT security...*

**You're still likely exposed.** Not only are cyber threats continually evolving to bypass the latest security measures, but even large corporates who spend vast amounts on cybersecurity still routinely get hit.

**People are still the weakest link in an organization's IT security chain.** Approximately three quarters of the cyber claims we deal with involve some kind of easily-preventable human error.

Theft of funds, ransomware, extortion and non-malicious data breaches **usually start with a human error** or oversight such as leaving a laptop on a train or clicking on a phishing link, which then allows cybercriminals to access your systems from the inside.

Cyber insurance is a cost-effective way to not only get access to risk management tools like phishing-focused employee training programs, but also to **cover the financial loss if someone makes a mistake.**

*We outsource all of our IT, so we don't have an exposure...*

Unfortunately, **using a third party for IT doesn't eliminate your exposure.**

If you outsource your data storage to a third party and that third party is breached, you will still likely be **responsible for notifying affected individuals** and dealing with subsequent regulatory actions.

What's more, many businesses rely on third parties for business-critical operations, and should those providers experience a system failure, **it could have a catastrophic effect on your ability to trade**, resulting in a business interruption loss.

Most third-party technology service providers have **standard terms of service that limit their liability** in the event that a breach or system outage causes financial harm to one of their clients.

*We don't collect any sensitive data, so we don't need cyber insurance...*

Two of the most common sources of cyber claims **aren't related to privacy at all — funds transfer fraud** is often carried out by criminals using fraudulent emails to divert the transfer of funds from a legitimate account to their own, while **ransomware** can cripple any organization by freezing or damaging business-critical computer systems.

Neither of these types of incidents would be considered a data breach, but **both can lead to severe financial damage** and are insurable under a cyber policy.

**Any business that uses technology to operate will have a range of other cyber exposures which a cyber policy can address.**

## Objection

*Cyber attacks only affect big business. We're too small to be a target...*

## Response

Although cyber attacks affecting large organizations are most often in the news, **over half of all cyber attacks are aimed at small businesses.**

This trend is continuing to rise. In 2018, **attacks on small and medium-sized businesses rose by a staggering 424%.**

Cybercriminals see smaller organizations as **low-hanging fruit** because they often lack the resources necessary to invest in IT security or provide cyber security training. Cyber insurance is a great solution for smaller organizations because not only does it cover the growing number of cyber attacks on these businesses, but it gives you **instant access to a number of technical and legal experts** needed following a cyber event, but who you might not have in-house.

*Cyber is already covered by other lines of insurance...*

Cyber cover in traditional lines of insurance often **falls very short of the cover found in a standalone cyber policy.** While there may be elements of cyber cover existing within traditional insurance policies, it tends to be only partial cover at best.

Property policies were designed to cover your bricks and mortar, not your digital assets; crime policies rarely cover social engineering scams — a huge source of financial losses for businesses of all sizes - without onerous terms and conditions; and professional liability policies generally don't cover the first party costs associated with responding to a cyber event.

A standalone cyber policy is designed to **cover the gaps left by traditional insurance** policies, and importantly, comes with **access to expert cyber claims handlers** who are trained to get your business back on track with minimum disruption and financial impact.

*Cyber insurance is too expensive...*

**Cybercrime rates are quickly overtaking traditional crime rates,** making cyber risk one of the most pressing business issues of today.

For the **sizable losses** you could be face with — often in the hundreds of thousands — from stolen funds, lost revenue or considerable clean up costs, it is worth the extra insurance spend.

**Cyber insurance gives you instant access to a wide range of technical specialists** who are experts at helping businesses quickly recover from cyber events. Policies also come with a range of **free cybersecurity tools** that you might spend hundreds or thousands on implementing yourself.

Visit [victorinsurance.com](https://victorinsurance.com) or connect with your business development contact to learn more.

This document is for illustrative purposes only and is not a contract. It is intended to provide a general overview of the program described. Please remember only the insurance policy can give actual terms, coverage, amounts, conditions and exclusions. Program availability and coverage are subject to individual underwriting criteria.

© 2023 Victor Insurance Managers LLC | 80088

Victor Insurance Services LLC in MN | DBA in CA and NY: Victor Insurance Services | CA Ins. Lic. # 0156109