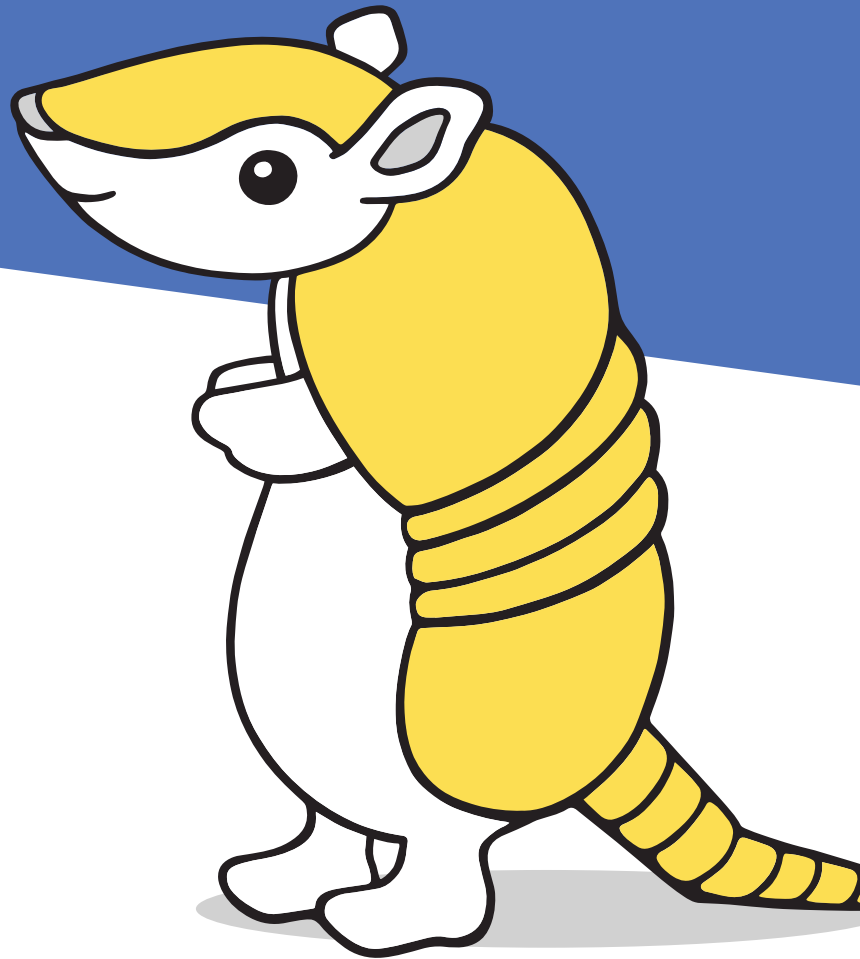


# 8 Myths SMEs Should Stop Believing About the Cyber Insurance Market



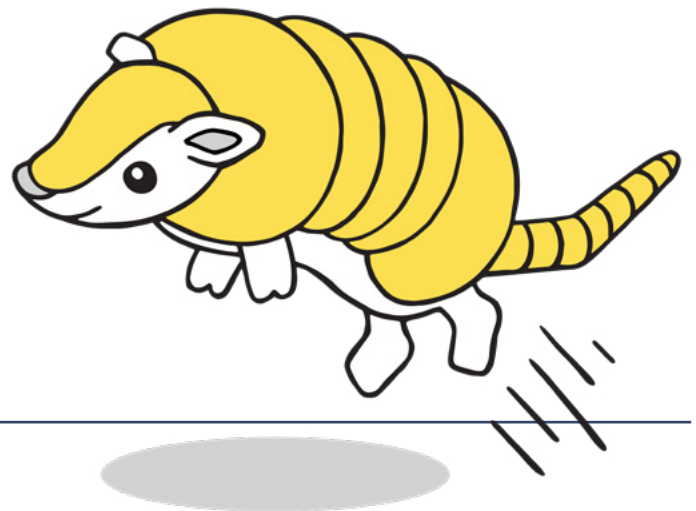
Cyber insurance makes a lot of sense for small to [medium-sized businesses \(SMEs\)](#). It protects companies from residual risk in the event of a cyberattack; and in many ways, it can even help them build better defenses in the first place.

Cyber risk is a real threat to all companies, regardless of size. According to a 2018 [Deloitte study](#), 45% of companies reported one or more cybersecurity events. One year later, that percentage had grown to 61%. That same study cites more than 60% of small to medium enterprises were victims of cyberattacks, yet the SME market has been relatively slow to adopt cybersecurity insurance coverage.

A lot has changed over the past three years. In response to increasing dangers and an increased number of claims, cyber insurance premiums have skyrocketed as well. Yet, while larger numbers of businesses have become more aware of the dangers cyber threats pose, cyber insurance continues to be low on the priority list. SME cyber insurance adoption is rising, but not as quickly as it should be.

One of the main reasons for this lag is that, despite the recent growth, the world of cyber insurance continues to be largely misunderstood. This is especially true when it comes to SMEs, which tend to believe falsehoods related to cyber insurance. Perpetuated by confusion and misconceptions, these myths continue to prevent SMEs from investing in cyber insurance, even though it fits this market well.

In this eBook, we will take a look at the most common cyber insurance myths SMEs believe and show you what the truth is.





## MYTH 1 CYBER INSURANCE IS TOO EXPENSIVE

**Myth: A lot of SMEs believe that cyber insurance is too expensive.**

**Busted: Cyber insurance costs and premiums are going up, but that increase is directly proportional to the risks associated with cyber threats. Think of property damage insurance, for example. Rising costs reflect the increase in incidents and the likelihood that one will happen to your business. The same is true with cyber insurance.**

These increases, however, are mostly related to larger companies. One of the main reasons cyber insurance tends to cost less for SMEs is because they have a smaller digital footprint. Most small businesses don't have as many devices, offices, or as much data with which to contend. This means that, in the event of an attack, the insurer will likely not have to pay as much for recovery costs.

Some of the key factors taken into account when calculating the cost of cyber insurance include:

- The size of the business (in terms of revenue and employees).
- The type of industry.
- The company's history with data breaches.
- How much data the business is processing.
- The kind of cyber security infrastructure already in place.

Given how the pandemic has made major shifts in company workforces and overall infrastructure, cyber insurance companies are reacting to the fact that these shifts were made quickly with little security in mind. Many companies haven't bolstered the security around a remote workforce, and threat actors know it's a major opportunity for them.



## MYTH 2

# COMPANIES ARE ALREADY COVERED BY BUSINESS OWNERS' POLICIES, GENERAL LIABILITY INSURANCE, AND PROPERTY INSURANCE

**Myth: If you have a business owner's policy, general liability insurance, and/or property insurance, you're already covered in the event of a cyberattack.**

**Busted: This myth is based on a half-truth. The aforementioned types of insurance may cover a minimal aspect of cyber risk and cybersecurity incidents. Some of the cybersecurity-related elements that might be covered by general liability insurance include:**

- Reputational damage: if your company's image is damaged following a cyber incident (e.g., due to a data leak), you might be able to receive compensation through general liability insurance.
- Bodily injury: if somebody is physically injured as a result of a cyberattack on your company and it's deemed to be your company's fault, you might be able to receive compensation. Many people believe cyberattacks only have digital repercussions, but they can sometimes inflict physical damage too. For instance, in 2021, [cyber attackers breached into a Florida](#) water plant and changed the amount of lye that goes into the water (and did so to very dangerous levels).

This means that general liability insurance doesn't usually cover:

- Data theft.
- Damage to business systems.
- Repair costs, investigative costs, loss of business income, data recovery expenses, and other [financial losses](#) resulting from a cyberattack.

Many business insurance policies weren't designed or written to cover losses associated with cyber risk and cyberattacks, so some of these policies may sublimit how much insurance is available or outright exclude them. These gaps (and many others) need to be covered by specialized cybersecurity insurance.



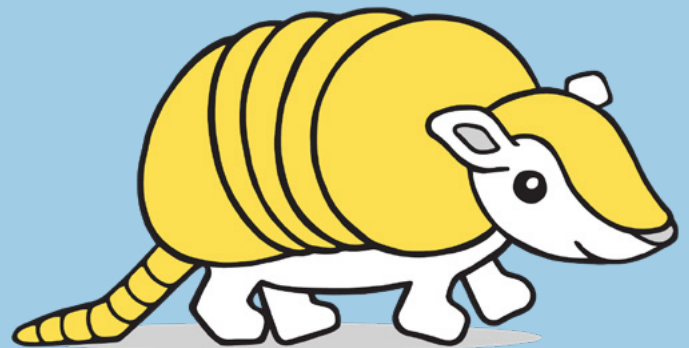
## MYTH 3

# CYBER INSURANCE CAN'T BE BOUGHT AS A STANDALONE POLICY

**Myth: You can't buy cyber insurance as a standalone policy. Either you must buy a general liability insurance policy first, or your cyber insurance has to be linked with other types of packages (such as general business insurance).**

**Busted: This is another widely spread myth that was debunked by most cyber insurance providers in recent years. A SME can buy a standalone cybersecurity insurance policy from one provider and a general business liability insurance from a different provider.**

Cyber insurance is a very specific type of insurance, so it does not have to be connected to the more traditional insurance packages. Buying it from a specialized company can provide an advantage because you will benefit from their team's cybersecurity expertise. They will undoubtedly have a better understanding of how businesses should fortify themselves in order to be less susceptible to cyberattacks. Cyber insurance carriers are also more likely to have robust and affirmative coverage grants as well as a panel of IR vendors that can immediately address any incidents or compromises. Insurers that don't traditionally offer cyber risk insurance aren't likely to have such specialized services and benefits.





## MYTH 4

# SMES DON'T HAVE THE BUDGET FOR CYBER INSURANCE

**Myth: A lot of SMEs avoid purchasing cyber insurance, believing they don't have the budget for it.**

**Busted: It's easy to think cyber insurance is just another line item you can deprioritize. And it's even easier to fall back on the "SMEs have a tight budget" excuse.**

However, cyber insurance should not be seen as just another cost. It should be seen as an investment.

It's hard to believe a small business can be the target of a cyberattack, but it happens more often than you think. [Research by Verizon](#) shows that at least 20% of all cybercriminal acts target SMEs and there is [data](#) from other parts of the world (such as Singapore, for example), where that number gets as high as 40%.

Data breaches are extremely costly with the highest average cost recorded this year, at [\\$4.24 million](#). Acting later, rather than sooner, can make matters even pricier. Purchasing cyber insurance should not be optional, it should be a top priority.

Having a cyber insurance policy removes the risk from a company and protects the balance sheet while adding to that company's overall financial health. This is largely why [investors value companies](#) that are cyber secure and cyber insured. They understand that "we have no budget" is a pseudo reason not to be cyber insured.





## MYTH 5

# CYBER INSURANCE IS A LUXURY

**Myth: Part of why a lot of SMEs think they “don’t have the budget” for cyber insurance is related to the fact that they consider it a luxury. Much like fledgling entrepreneurs thinking they don’t need a Mercedes Maybach in their suburban garage, SMEs think cyber insurance is not necessary until the company is already grown and can afford it.**

**Busted: You may not need a Maybach in your garage, but you do need cyber insurance. And you need it now, rather than later. Why? Given the fact that almost half of all small businesses admit to having been victims of cyberattacks in the last twelve months, it’s not hyperbole to suggest being adequately insured could well predict whether your company survives, much less grows. In other words, the quicker you get cyber insured, the sooner you’re protected from that ugly potential.**

Moreover, getting cyber insurance earlier can bring benefits as you grow your business. For instance, your cyber insurer might be able to provide you with better price points in the future and you might also end up negotiating better terms.

Cyber insurance is not like an expensive car that’s “nice to have when you get the money.” It’s more like your house insurance. You may not have a mansion with a waterfront view (yet), but you still want to be certain you’re insured in the event of a catastrophe that could destroy your home.



## MYTH 6

# SMALLER COMPANIES DON'T NEED CYBER INSURANCE

**Myth: Small companies don't need cyber insurance. Why would cybercriminals make the effort to attack them when there are so many other, much larger companies they can go after?**

**Busted: The cybersecurity danger SMEs face is very real, as the data shows. Cybercrime has grown to be less discriminating in this respect, and the rate of SMEs becoming victims of cyberattacks has grown exponentially over the last few years.**

As more large enterprises become increasingly secure, many cybercriminals prefer to use automated attacks and aim for low-hanging fruit. Small businesses make the perfect target, particularly when they are not fully protected.

As a SME, [you need cyber insurance](#) as much as a small plant needs to be protected from storms in order to grow.







## MYTH 7

# STAND-ALONE POLICIES AREN'T AS GOOD AS COMPREHENSIVE POLICIES

**Myth: If you want to get great cyber insurance, you should aim for a comprehensive policy as opposed to one that stands alone.**

**Busted: Comprehensive policies might make you feel like “more dots are connected,” meaning you are better insured from every point of view.**

That’s neither true nor untrue, as it is determined on a case-by-case basis. How much coverage you get depends on the policy itself, not on whether the policy is comprehensive or stands alone. Also, because some cyber insurers are solely focused on providing cyber insurance, you might actually get better overall terms than you would with a comprehensive policy. Don’t dismiss stand-alone cyber insurance thinking it’s not good. It can be exactly what you need and depends on the terms you negotiate, not on whether your cyber insurance policy is part of an overall insurance policy. Stand-alone policies have a full suite of insuring agreements that many “comprehensive” policies do not—potentially making them a more attractive option.





## MYTH 8

# IT'S BETTER TO FOCUS ON CYBERSECURITY

**Myth: Don't bother with cyber insurance, focus on cybersecurity as it's a lot more important than insurance. Plus, it will help you avoid having to make a claim on your insurance policy in the first place.**

**Busted: Investing in strengthening your security posture and investing in cyber insurance are not mutually exclusive. If anything, deciding to get cyber insured will help you build stronger cyber resilience.**

Getting cyber insured might also help you build a better, healthier cybersecurity culture. Since security is built into the culture and processes, this will consequently help keep your company more secure from a cyber threat perspective. A healthy cybersecurity-focused company culture can include:

- Open communication about cybersecurity risks and threats.
- Making sure everyone in the company is aware of his or her role in keeping the company's data safe.
- Making sure that all employees are properly trained to maintain cyber hygiene and stay away from phishing attempts.
- Encouraging employees to report any suspicious activity they might come across.

Cyber insurance and cyber resilience do not exclude each other; they complement each other. Together they help your business stay safe when facing cyber risks.

# CONCLUSION

Cyber insurance is still misunderstood because it is new to the market. Hopefully, busting the myths in this eBook helped you gain a better understanding of what cyber insurance policies are and what they are not.

As mentioned above, cyber insurance and cybersecurity are complementary. They work together to assure your approach to cybersecurity is well-rounded and realistic, all while protecting the financial health of your company. Which is precisely why a modern MSSP can help build up cyber resilience, making it easier and faster for you to procure cyber insurance that fits your current business needs and budget. If we had to narrow it all down to one nugget of information, it's this: cyber insurance is not a luxury, it's not something just "nice to have," cyber insurance is affordable security that protects both your data and your dollars.

# HOW SOLCYBER CAN HELP

Speak to us about our [SolCyber Insurance+ Program](#), and how we help businesses not only build up their cyber resilience fast but get access to expedited cyber insurance approvals and discounted premiums.

