

JULY 14, 2022



Busting the Myths About Cyber Insurance

Janie Ma | Management Liability Insurance Specialist

As published in the July 2022 issue of Alaska Business Magazine

Over the last two years, as many of us have been forced to suddenly work from home, the dependence on technology to remain connected has reached an all-time high to keep businesses running. As a result, we have seen a dramatic rise in myriad cyberattacks into organizations' networks. As these attacks increase, so does the need for strong cyber insurance products to protect our businesses, but many have still not considered cyber insurance.

One reason is that many owners don't understand exactly what cyber insurance can provide. Below, we discuss four common cyber liability insurance myths and the truth about what this coverage can do for your business.

1. Cyber liability policies just provide financial protection. Most policies also provide resources that can help prevent attacks, as well as manage the fallout from a cyberattack:

- + Breach coach: this is usually an attorney to help walk you through the response process.
- + IT forensic team: this team will investigate the breach and determine how it occurred, and what data was accessed.
- + Legal team: once the IT forensic team has identified the compromised information, this team of attorneys will help identify your notification responsibilities in any applicable jurisdictions. They will also defend your organization against third-party lawsuits.
- + Crisis management team: this is usually a PR firm that can help with necessary public relations.
- + Pre-breach services: discounted IT security services, sample response plans, whitepapers, limit calculators, and IT security news feeds.

ABOUT PARKER, SMITH & FEEK

Parker, Smith & Feek is a private brokerage firm driven by client service. We offer a range of services, including commercial insurance, risk management, surety, employee benefits, and personal insurance. PS&F is ranked nationally as one of the 40 largest privately held risk management and insurance brokers. We are committed to serving the community and proud to be one of the top corporate philanthropists in the region.

LEARN MORE

[About Parker, Smith & Feek](#)

[Our Industries](#)

[Our Services](#)

CONTACT US

[Email](#)

Tel: 800.457.0220

FOLLOW US

continued >

2. My organization is too small to be a prime target for cybercriminals. However, a recent study found that 43% of cyberattacks are against small businesses and only 14% of those are prepared to defend themselves. According to Forbes, an employer with less than 100 employees will experience 350% more social engineering attacks than a larger enterprise. Additionally, cyberattacks occur every 11 seconds and as a result, in 2021, losses from cybercrime damages were anticipated to have reached \$6 trillion. There is no size threshold that will make a business immune.

3. A technology E&O policy will provide the same protection as cyber liability. Technology E&O coverage is intended to cover technology providers and will respond to a failure in the provider's products or services that results in consequential damages to customers. Cyber liability policies, however, provide first- and third-party coverage for an organization that has been affected by a breach on your network or system. Many technology E&O policies add cyber liability coverage, but these are not the same.

4. Cyber liability policies only cover liability claims. However, cyber liability is more than a third-party policy and provides many first-party coverages as well:

- + Investigating the breach source
- + Notifying customers that their personal information was exposed
- + Crisis management and business interruption loss
- + Restoring lost data or destroyed assets
- + Damage to physical hardware
- + Regulatory and PCI compliance fines
- + Social engineering and computer fraud crimes
- + Extortion demands

Bear in mind that some of the above causes of first-party loss, such as the unlawful collection of personal data or the failure to follow a company's privacy policies, may not even include a network breach.

Despite the amount of time and effort spent on cyber controls, all businesses are still vulnerable to attacks. Cyber insurance provides both financial and operational resources that can help you respond to an attack, with limited disruption to get your systems back up and running.

For additional information or questions, please contact [Parker, Smith & Feek's Commercial Department](#).

References and Resources

1. <https://www.embroker.com/blog/cyber-attack-statistics/>
2. [https://financesonline.com/cybersecurity-statistics/#:~:text=Cybercrime%20Statistics,-One%20of%20the&text=Global%20cybercrime%20damage%20in%202021,\(Cybercrime%20Magazine%2C%202020\)](https://financesonline.com/cybersecurity-statistics/#:~:text=Cybercrime%20Statistics,-One%20of%20the&text=Global%20cybercrime%20damage%20in%202021,(Cybercrime%20Magazine%2C%202020))
3. <https://www.thehartford.com/professional-liability-insurance/errors-omissions-insurance/technology>
4. <https://www.forbes.com/sites/edwardsegal/2022/03/30/cyber-criminals/?sh=460742b052ae>
5. <https://www.washingtonpost.com/politics/2021/02/22/cybersecurity-202-cybercrime-skyrocketed-workplaces-went-virtual-2020/>