



Jan 05, 2021

Categories:

[Blogs](#)

[Podcast](#)

[Technology Blog](#)

Authors:

[Joseph J. Dehner](#)

Data Privacy Detective Podcast – Episode 60: Cyber Insurance, What it Does and Doesn't Cover

As businesses move into 2021, what insurance can they have to limit cyber risk? What does cyber insurance cover and not cover? How is it priced and secured?

Data Privacy Detective guest Sean McGee is a Vice President of [USI Insurance Services](#), an independent company serving global clientele and accessing global insurance markets. Also, an Ohio and Kentucky attorney, at USI Sean advises customers on a broad array of business risks, including those arising from personal data collection and use.

Cyber insurance emerged in 1997. Insurance Journal reported 2019 premiums of over \$2.2 billion, spread among a competitive range of providers, with growth anticipated in number of policies, variety of risks covered, and premiums. As one example, the average payment for ransomware attacks jumped to almost \$85,000 by year-end 2019, almost double the prior year's average, triggering an adjustment of price for covering this type of risk.

Cyber insurance pricing is competitive. It depends on a company's responses to questionnaires that can be 20 pages in length and interviews with CIO's and others. Underwriters assess the strength and scope of an applicant's cyber protection program before quoting a premium.

A solid cyber policy will generally cover direct costs resulting from a data breach or incident. These include attorney fees and other costs of defense, resolution of private and public claims, expenses to recover purloined data, business interruption (subject to defined caps and other details), and similar out-of-pocket losses suffered from a cyber-attack. Policies generally cover global losses, including direct losses suffered in the European Union under GDPR.

Coverage typically does not extend to more indirect losses, such as damage to reputation, costs to improve a system after an attack, or

potential future lost profits as distinguished from business interruption loss. The more indirect or difficult to measure a loss is, the less likely it will be insured. Deductibles, caps and other limits, and unusual types of risks should be carefully reviewed before finalizing an insurance purchase.

Top tips for businesses considering cyber insurance:

- Have a top-to-bottom training program to help every individual avoid phishing and other incidents that lead to data breaches, ransomware attacks and other losses.
- Have a data response plan in place before it's needed, ready to activate immediately when required.
- Think holistically. Preventing data attacks is not just a hardware problem. Review regularly measures to upgrade data protection, protect personal and proprietary data, and limit losses from data risks.

If you have ideas for more interviews or stories, please email info@thedataprivacydetective.com.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.