Key Cyber Coverages Where the Details Matter Most

By Shannon Beric

In today's rapidly evolving digital landscape, cyber insurance has become a critical safeguard for businesses facing an ever-growing range of cyber threats. However, not all policies provide the same level of protection, and subtle differences in policy wording can significantly impact whether a claim is covered. Understanding key cyber coverages and the specific terms and conditions within a policy is essential to avoiding unexpected gaps that could leave an organization vulnerable.

It's important to explore the critical nuances of cyber insurance policies and how policy language can determine the extent of coverage when it matters most.

The following are examples of coverages that can vary in definition and may or may not be included in a cyber policy, depending on the specific terms and conditions.

- **Wrongful Collection:** This refers to liability arising from the improper collection, unauthorized sharing, storage, or handling of personal data, potentially violating privacy laws such as GDPR, CCPA, or other data protection regulations. Coverage for wrongful collection is not always included in cyber policies by default and is often available as an add-on or under specific conditions. Coverage typically applies to accidental violations, not willful misconduct. Additionally, exclusions may apply, particularly for intentional violations or data collection practices deemed deceptive or illegal from the outset. Some policies also do not cover regulatory fines resulting from privacy law breaches, making it essential to review policy terms carefully.
- **Social Engineering Fraud – Including Goods**: Social Engineering Fraud (SEF) refers to the manipulation or deception of individuals within an organization to gain unauthorized access to confidential information, financial resources, or goods. This often involves tactics like impersonation, pretexting, or phishing, where fraudsters manipulate employees into taking actions that benefit the criminal, such as transferring funds or releasing sensitive data. In the context of goods, SEF may involve schemes where fraudsters convince an organization to ship products to an address under their control, often using false invoicing or other deceptive practices. Policies with SEF coverage may provide protection for financial losses or goods lost due to such fraudulent schemes, though it's essential to review specific terms and conditions to confirm coverage for goods.
- **Invoice Manipulation:** This coverage protects against financial losses resulting from the fraudulent alteration, redirection, or falsification of invoices, such as when fraudsters modify payment instructions, alter invoice details, or create fake invoices to divert payments. Depending on the nature of the fraud, these losses could be covered under either a Cyber Policy or a Crime Policy. If the fraud involves an internal actor, such as an employee, a Crime Policy is typically more appropriate. However, if the fraud is committed by an external hacker through methods like BEC, phishing, or invoice email compromise, a Cyber Policy with the appropriate endorsement would provide coverage. In cases involving both internal and external fraud risks, it may be necessary to consider both policies with the relevant endorsements for full protection.

Understanding the nuances of cyber insurance is crucial for businesses to ensure adequate protection against evolving risks. Key coverages like wrongful collection, social engineering fraud, and invoice manipulation may or may not be included in a Cyber Policy, and the specific details of each coverage are important. To avoid coverage gaps, businesses must carefully review their policies and endorsements to ensure they have the right protections in place for their specific needs.

Disclaimer: Views expressed here are for general informational purposes only and do not constitute legal advice. Coverage specifics vary by policy, carrier, and jurisdiction, and any descriptions herein are subject to the actual terms, conditions, limitations, and exclusions of the applicable insurance policy. No representation is made that any particular coverage or policy form will be applicable to or sufficient for your needs. Readers should consult with their legal counsel, compliance advisors, and licensed insurance professionals for guidance regarding their unique circumstances.

About the Author

Shannon Beric – Principal, Senior Vice President, Broker

Shannon has over 25 years of expertise in Professional Liability and over 15 years in Cyber Liability. She has provided continuing education on these topics to retail agents since 2007. She was a featured author of a *Rough Notes* article in 2020, and she moderated a session at the Annual PLUS Conference in Chicago in 2024.

direct: 206.816.6710 | email: sberic@brcins.com