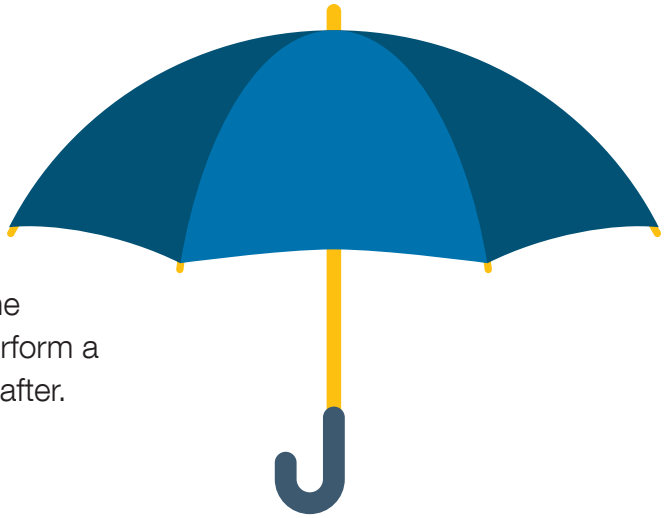
#ForensicPerspectives

Maximize your cyber insurance coverage



Will your company's insurance adequately mitigate the economic impact of a cyber incident? The time to perform a coverage assessment is now – and periodically thereafter.

Cyber policies

Cyber policies typically cover a range of expenses incurred in a data breach, including:

- Notification costs
- Credit monitoring
- Fines
- Penalties
- Costs to defend regulatory claims
- Business interruption

Non-cyber policies

You don't necessarily need a policy with the word "cyber" in it. If your company has one of the policies below, you may already have some level of coverage in the event of a cyber incident.

Kidnap and ransom insurance
Some policies cover situations where computers and systems have been "constructively kidnapped" by ransomware.

Fidelity (or "crime") insurance
May cover situations of employee-caused theft or sabotage.

Professional liability/errors and omissions policies
Some policies can cover losses resulting from when an employee makes a mistake resulting in cyber-related damage (e.g., spread of malware).

General liability
Some policies may indemnify and provide a defense against a wide variety of claims, including claims alleging violation of privacy rights and some policies may afford coverage for theft of consumer data, misuse of customer information, copyright infringement, and other types of unfair competition.

Directors and officers (D&O) policy
Covers board members if named as defendants in a cyber-related derivatives action.

Property insurance
Policies written on an "all-risk" basis may cover physical damage caused by malware.

Kristofer Swanson, CPA/CFF, CFE, CAMS | Vice President & Practice Leader, Forensic Services
+1-312-619-3313 | kswanson@crai.com