

Protecting Your Business With Cyber Insurance

Provided by ToughComp

Cyber threats remain a pressing concern for organizations across sectors. Just one cyberattack can cause significant operational disruption, regulatory scrutiny and financial losses, including costs for incident response, investigation and recovery.



Data breaches cost organizations an average of **\$4.99 million globally**.
(2026 IBM Cost of a Data Breach Report)



Malicious attacks using AI cost an average of \$6.04 million, approximately **\$1 million more** than breaches without AI involvement.
(2026 IBM Cost of a Data Breach Report)

Although strong cyber practices, including a cyber-aware workforce, good cyber hygiene and a strong reporting culture, can reduce the likelihood and severity of an attack, they can't eliminate the risk entirely. Cyber insurance can financially protect organizations from a range of first- and third-party costs.

Key Areas to Review



Understand coverage types. Confirm whether the policy includes first-party coverage, which pays for direct losses such as recovery costs, and third-party coverage for claims made by others affected by the breach.



Review ransomware coverage. Confirm the policy's position on ransomware payments, negotiation support and recovery costs, since coverage varies widely between policies.



Check business interruption coverage. Confirm whether the policy covers lost income and additional expenses if a cyber incident disrupts business operations.



Review social engineering coverage. Confirm whether the policy includes a social engineering endorsement, since standard crime and cyber policies sometimes limit or exclude losses from business email compromise (BEC), invoice fraud and similar scams.

Smart Protection, Stronger Resilience

Robust cyber hygiene reduces risk. Cyber insurance can protect against the cost when incidents occur. Contact us to explore tailored cyber insurance solutions.