

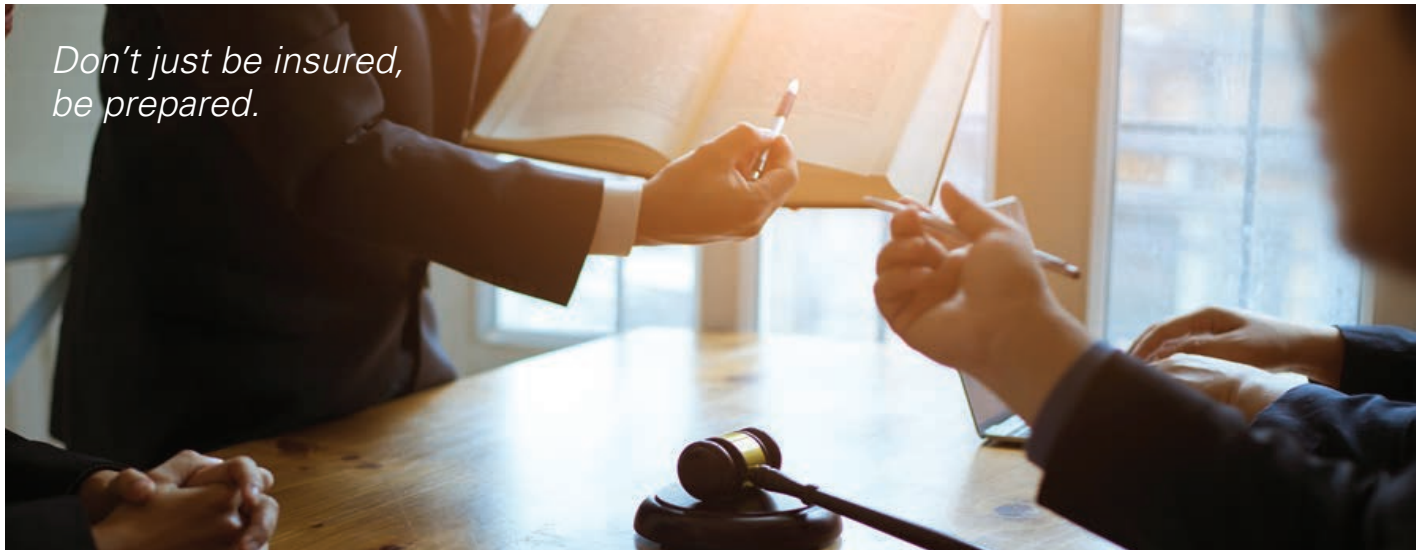


Do You Have Enough Cyber Coverage For Your Firm?

There are instances where your limit may not be adequate for your firm. How do we know? Consider this...

CLAIM SCENARIO

An attorney at a law firm found a compromised work station where a hacker appeared to have captured a copy of the firm's client files, including health records and social security numbers. The hacker claimed to have access to the firm's entire client record database and threatened to release it publicly if the firm did not pay a \$300,000 ransom. The law firm reported the incident under their Cyber Liability Insurance. The estimated loss of this scenario is over \$400,000.



*Don't just be insured,
be prepared.*

You don't have to be a fortune 500 company to experience such high costs. We've seen individual professionals incur devastating costs out of pocket for similar situations. Be prepared. Higher limits of our cyber liability insurance solutions are available in addition to the coverage provided with your Professional Liability or Legal Malpractice insurance policy.

Advantages of purchasing higher limits through us:

- Cyber Liability (e-JD®) available for up to \$10 million per claim and in the aggregate.
- Qualifying insureds receive preferred rates on higher limits of cyber insurance.
- \$0 deductible for certain insuring agreements.
- Additional Defense Cost and Separate Breach Event Costs limits available.
- Full Prior Acts coverage available.
- Seamless claims handling when transitioning from embedded coverage to higher limits coverage.



oblic
Ohio Bar Liability Insurance Co.



Cyber & Professional Lines Group

Cyber Statistics



Ransomware demands have risen in 2019

2019

\$25K to \$1M



Cybercrime claims have seen an increase of 152% in 2019 over 2018

2019

152%

2018



Ransomware is the top cause for cyber loss in 2019



Cyber exposures are constantly evolving and so is our coverage to ensure your practice is protected.

Enhancements now include:

- Broad coverage for data that is stored with a third party including, BPO service providers, outsourced IT providers and independent contractors.
- Broad coverage for System Failure that includes data recovery and business interruption.
- Coverage for extortion expenses incurred and extortion monies paid as a direct result of a credible Cyber Extortion threat.
- Coverage for Post Breach Remediation Costs incurred to mitigate the potential of a future security or privacy breach.

We'll make sure you have the right coverage, expertise and excellent claims handling.

For more information, please contact your agent or Professional Liability carrier.



OHIO STATE BAR
ASSOCIATION
Insurance Agency



TOKI MARINE
HCC

Cyber & Professional Lines Group

tmhcc.com/pro



Ohio Bar Liability Insurance Co.

Description of Coverage:

Bricking Loss – Losses incurred to replace computer hardware or electronic equipment that becomes nonfunctional or useless (but not physically damaged) due to unauthorized or malicious reprogramming of software or firmware.

Bodily Injury Liability

Liability for damages resulting from the failure to prevent or avoid bodily injury caused by a security breach or privacy breach.

Property Damage Liability

Liability for damages resulting from the failure to prevent or avoid property damage caused by a security breach or privacy breach.

Property Damage Loss

Physical damage to property caused by or resulting from a hacking attack.

Multimedia Liability

Liability resulting from the dissemination of online or offline media material, including claims alleging copyright/trademark infringement, libel, slander, plagiarism or personal injury.

Security and Privacy Liability

Liability resulting from a security breach or privacy breach, including failure to safeguard electronic or non-electronic confidential information.

Privacy Regulatory Defense and Penalties

Regulatory fines and penalties and/or regulatory compensatory awards incurred in privacy regulatory proceedings/investigations brought by federal, state, local, or foreign governmental agencies.

PCI DSS Liability

Liability for assessments, fines, or penalties imposed by banks or credit card companies due to non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) or payment card company rules

TCPA Defense

Defense of claims alleging violation of the Telephone Consumer Protection Act, the Telemarketing and Consumer Fraud and Abuse Prevention Act, the CAN-Spam Act, or any similar federal, state, local or foreign law regulating the use of telephonic or electronic communications for solicitation purposes.

Breach Event Costs

Reasonable and necessary mitigation costs and expenses incurred as a result of a privacy breach, security breach or adverse media report.

Post Breach Remediation Costs

Post-breach remediation costs incurred to mitigate the potential of a future security breach or privacy breach.

BrandGuard[®]

Loss of net profit incurred as a direct result of an adverse media report or notification to affected individuals following a security breach or privacy breach.



System Failure

(1) Reasonable and necessary amounts incurred to recover and/or replace electronic data that is compromised, damaged, lost, erased, corrupted or stolen and (2) Business income loss and interruption expenses incurred due to an unplanned outage, interruption, failure, suspension or degradation of service of an insured computer system, including any such incident caused by a hacking attack.

Dependent System Failure

(1) Reasonable and necessary amounts incurred to recover and/or replace electronic data that is compromised, damaged, lost, erased, corrupted or stolen and (2) Business income loss and extra expenses incurred due to an unplanned outage, interruption, failure, suspension or degradation of service of a service provider computer system that is caused by specified cyber perils, including a denial of service attack, malicious code, and acts of cyber terrorism.

Cyber Extortion

Extortion expenses incurred and extortion monies paid as a direct result of a credible cyber extortion threat.

Cyber Crime

(1) Financial Fraud; (2) Telecom Fraud including Utilities Fraud; and (3) Phishing Fraud.

Reward Expenses

Reasonable amounts paid to an informant for information not otherwise available, which leads to the arrest and conviction of a person or group responsible for a privacy breach, security breach, system failure, cyber extortion threat, financial fraud, telecommunications fraud or phishing attack.

Court Attendance Costs

Reasonable costs incurred to attend court, arbitration, mediation or other legal proceedings or hearings as a witness in a claim.