



One of the greatest risks that law firms face is the loss or misuse of sensitive client data. Due to viruses, malware, hacking and even inadvertent misuse or misplacement of a mobile device or laptop, your clients' valuable information is also a significant liability.

With cyber risks continuing to grow, Lawyers' Mutual Insurance Company has partnered with Tokio Marine HCC - Cyber & Professional Lines Group to provide all qualified members with a comprehensive cyber risk solution custom-built for legal professionals and designed to complement your existing legal liability coverage.

Our Cyber Insurance solution starts with risk management and mitigation tools to help you prepare and prevent, and follows through with comprehensive coverage in the event that your practice is the victim of a cyber incident.

## RISK MANAGEMENT & MITIGATION TOOLS



### Online Training and Support

Our cyber risk management website has tools and resources to help you safeguard information, increase awareness of cyber risk and respond in the event of a breach.

This online resource is available 24/7 and includes:

- Tips on effective data security practices
- Compliance materials by state
- Employee training courses
- Samples and Templates to help you implement policies and breach response procedures

To access online training & support, click on "Cyber Coverage" at [www.lawyersmutual.com](http://www.lawyersmutual.com)



### Data Breach and Emergency Contact:

To report a suspected data breach please contact Tokio Marine HCC – Cyber & Professional Lines Group, by phone or e-mail, and advise that you are a Lawyers' Mutual Insurance Company member.

During Business Hours: 888.627.8995  
Monday - Friday 8:00 AM - 5:00 PM Pacific

E-mail: [CPL.claims@TMHCC.com](mailto:CPL.claims@TMHCC.com)

After Hours Hotline: 888.627.8995

## CYBER INSURANCE COVERAGE INCLUDES:

- ▶ **Privacy Breach Response Costs, Notification Expenses, and Breach Support Credit Monitoring Expenses** – Coverage for reasonable and necessary mitigation costs and expenses incurred as a result of an adverse media report, security breach or privacy breach, including legal expenses, public relations expenses, advertising and IT forensic expenses, postage, and the costs to provide call centers, credit monitoring, and identity theft assistance for up to 12 months.
- **Proactive Privacy Breach Response Costs** – Coverage for reasonable and necessary public relations expenses incurred in response to a security breach or privacy breach, but prior to the publication of an adverse media report, in an effort to avert or mitigate the potential impact of such adverse media report. Proactive privacy breach response costs are a sublimit of the Privacy Breach Response Costs, Notification Expenses and Breach Support Credit Monitoring Expenses coverage limit.
- **Voluntary Notification Expenses** – Coverage for reasonable expenses incurred by the Insured in notifying any individual or organization of a privacy breach, where there is no specific requirement by law to do so. Voluntary notification expenses are a sublimit of the Privacy Breach Response Costs, Notification Expenses and Breach Support Credit Monitoring Expenses coverage limit.
- ▶ **Network Asset Protection** – Coverage for reasonable and necessary amounts incurred by the Insured to recover and/or replace data that is compromised, damaged, lost, erased or corrupted due to: (1) accidental damage or destruction of electronic media or computer hardware, (2) administrative or operational mistakes in the handling of electronic data, or (3) computer crime/attacks, including malicious code and denial of service attacks.
- ▶ **Cyber Extortion** – Coverage for reasonable and necessary extortion expenses incurred and extortion monies paid as a direct result of a credible cyber extortion threat made against the Insured.

