



## NetGuard® Plus Cyber Liability

Our state-of-the-art NetGuard® Plus cyber liability insurance solution combines broad first-party and third-party coverage with access to expert cyber security services and claims professionals. Our cyber liability insurance solution is an effective combination of great coverage, state-of-the-art risk mitigation services, and unparalleled support from our inhouse claims experts.

### Highlights of our advanced NetGuard® Plus cyber liability policy include:

- Bodily Injury Liability (3rd Party)
- Property Damage Liability (3rd Party)
- Bricking Loss Coverage (1st party)
- Property Damage Loss Coverage (1st party)
- Cyber Risk Scan
- Free Pre-breach Expert Consultation
- \$0 Retention for initial legal advice regarding a security/privacy incident
- Additional Defense Costs Limit Built into the Policy
- Telephone Consumer Protection Act (TCPA) Defense Coverage
- Dependent System Failure Coverage Built into the Policy
- Reward Expenses for informants providing information about a cyber incident
- Separate Breach Event Costs Limit Enhancement Built into the Policy
- Post-breach Remediation Costs
- System Failure coverage with broad coverage for data recovery and business interruption



Every NetGuard® Plus quote includes a free cyber risk summary. Each bound NetGuard® Plus policy includes a full cyber vulnerability report.



Cyber & Professional Lines Group

[tmhcc.com/pro](https://tmhcc.com/pro)

## 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 a hacking attack, up to 125% of replacement value.

### 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 your 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-only coverage for 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.

## NetGuard® Plus Cyber Liability



### System Failure

Reasonable and necessary amounts incurred to recover and/or replace electronic data that is compromised, damaged, lost, erased, corrupted or stolen, and 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

Reasonable and necessary amounts incurred to recover and/or electronic data that is compromised, damaged, lost, erased, corrupted or stolen, and 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.

## Services and Risk Management Solutions

As a Tokio Marine HCC TechGuard® policyholder, your policy includes TMHCC CyberNET®, giving you access to:



### Cyber Awareness Trainings

Take more control internally by deploying proper cyber trainings with ease, especially with a Training Coordinator. They will send training instructions, track course assignments, and deliver a completion report for compliance and regulatory purposes.



### Phishing Simulation

Detect not only external threats, but internal ones as well. We run a phishing simulation to test your employees ability to identify suspicious emails. Studies have shown that phishing simulations and related education improve employee's awareness retention rates by 100%.



### Cyber Vulnerability, Domain & Web Security Scan

Identifies potential security vulnerabilities in your internet-facing systems. We assess out-of-date software, open RDP ports, if there are other similar registered domains developed for phishing attacks, malware from over hundreds of databases and provide this to you on a monthly basis.



### Cyber Security Experts

Discuss legal privacy matters, best practices, training, and best practice guides for your business. This includes unlimited consultation that doesn't require any membership fee or retainer.



### Knowledge Center Portal

A comprehensive database full of sample data security policies, procedures, and agreements, incident response planning materials, risk assessment tools, vendor management resources, step-by-step compliance guidance, and more.



### News Alerts

Delivered straight to your inbox so you stay up-to-date on changes in regulation, latest cyber incidents, and alerts.



### Claims Team

Our in-house specialists know that cyber criminals strike at anytime and anywhere. For your cyber coverages, you have access to our cyber team 24/7.



### Tabletop Testing\*

Tests your company's ability to respond to a cyber security incident. The tabletop exercise is designed to simulate a cyber incident so you know what happens and what must be addressed to ensure you don't have one. \*Available for qualifying insureds



### Dark Web Security Scans

We scour the dark web so we can alert you if your employee's login credentials are being sold by hackers.

## Expert Cyber Claims Handling

Our cyber claims team provides rapid response support for your clients. We handle over 1,000 cyber claims each year, and with more than 20 in-house cyber claims team members, TMHCC provides expert service and support when it's needed most. Working in close coordination with nationally-recognized privacy & security experts, the TMHCC claims team is at your side every step of the way. Our cyber claims team provides assistance with:

- Retaining a "Breach Coach" and legal counsel services, IT security and forensic experts, and public relations/ advertising support
- Breach notification
- Establishing a call center and breach notification website
- Providing credit monitoring and identity theft restoration services to affected individuals

## Industry Leading Expertise

### Cyber Breach Response Network

Our team of incident response experts are leaders in the field and are here to help you. We have the experience and know-how to respond quickly and get your business back on track. The following is a partial list of experts with whom we are proud to collaborate:

- Wilson Elser Moskowitz Edelman & Dicker LLP
- Lewis Brisbois Bisgaard & Smith
- Epiq
- Mullen Coughlin LLC
- McDonald Hopkins LLC
- Arete
- Ankura Consulting Group, LLC
- Tracepoint
- Jackson Lewis P.C.
- Crypsis



## TMHCC Cyber & Professional Lines

### Contact Us

**Ari Giller**, Vice President, Underwriting Midwest  
Cyber & Tech E&O  
agiller@tmhcc.com | 312.690.7111

**Tina Levine**, Director, Underwriting Southeast  
Cyber & Tech E&O  
tlevine@tmhcc.com | 818.479.4301

**DJ Carlisle**, Underwriting Manager, Northeast  
Cyber & Tech E&O  
dcarlisle@tmhcc.com | 646.889.2341

**Matthew Thoburn**, Director, Underwriting West Coast  
Cyber & Tech E&O  
mthoburn@tmhcc.com | 818.382.6102

Tokio Marine HCC is the marketing name used to describe the affiliated companies under the common ownership of HCC Insurance Holdings, Inc., a Delaware-incorporated insurance holding company. Headquartered in Houston, Texas, Tokio Marine HCC is a leading specialty insurance group with offices in the United States, the United Kingdom and Continental Europe.

[tmhcc.com/pro](https://tmhcc.com/pro)