

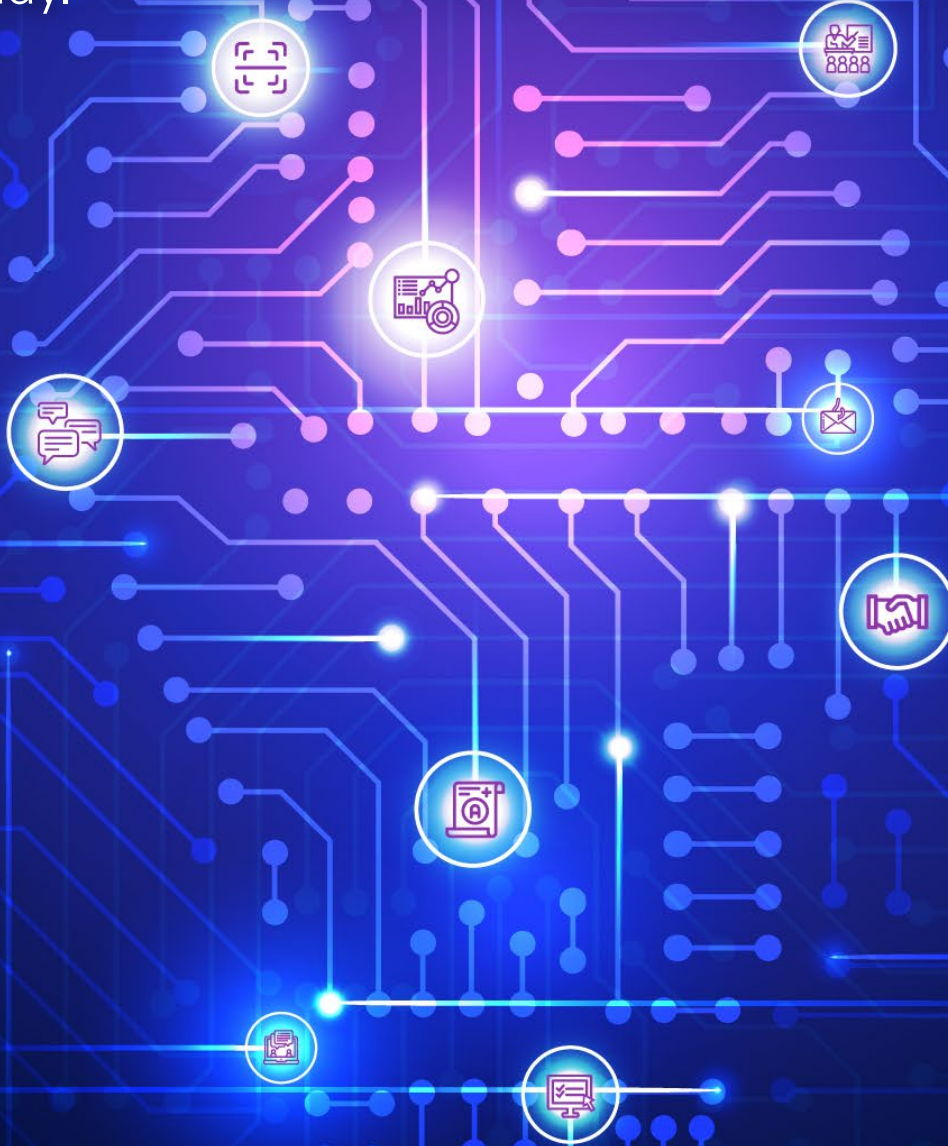
# NetGuard<sup>®</sup> Plus

Cyber Liability

Cyber Strong<sup>®</sup>  
and Ready.



CYBER STRONG<sup>®</sup>



## Ransomware and other cyber threats are on the rise.

---



>500% increase in  
average ransom payments  
since 2018<sup>1</sup>



The largest ransomware losses  
can exceed \$100 million  
in 2021<sup>1</sup>

We do more than insure you – we partner with you to help you make the best decisions for your business. The current cyber landscape can be difficult to navigate, and recent events highlight the need for solutions beyond insurance. We provide proactive controls to reduce your exposure to a cyber event. With over a decade of deep underwriting expertise, solid foundation, proven track record and excellent industry ratings, you benefit from broad coverage and exclusive access to tools and services to manage, monitor and take control of your network.

With us, you are more than insured, you are prepared.

---

We've negotiated steep discounts for our policyholders with cyber threat prevention vendors to protect you from a cyber-attack.

Learn more about CrowdStrike's Falcon Prevent NGAV and EDR.

 CROWDSTRIKE

Learn more about Datto's BCDR & SaaS Protect, the leading global provider of cloud-based software.

 datto

Learn more about Cisco's Duo multifactor authentication offering.



We offer proactive risk scanning and notification to assess and monitor potential threats.

# cyberNET<sup>®</sup>

We also provide proactive services, so you can stop a cyber-attack before it happens.

Log onto [cybernet.tmhcc.com](https://cybernet.tmhcc.com) with access to:



Cyber Security Training



Phishing Simulations



Cyber Risk Report with Domain  
& Dark Web Security Scans



Access to Cyber Security Experts



Cyber News Alerts & Blog



Continuous Exposure Monitoring

## Cyber Risk Report

Your quote includes a cyber risk report with insights on your network vulnerabilities. As a policyholder, you can continue to access a comprehensive risk report through CyberNET<sup>®</sup>.



## Be Cyber Strong®

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.

CPLG leverages data and artificial intelligence (AI) during the underwriting process to accurately accommodate the exposure, claims, and loss history of each unique risk.

### NetGuard® Plus Third Party coverage includes:

- Multimedia Liability
- Security and Privacy Liability
- Privacy Regulatory Defense and Penalties
- PCI DSS Liability
- Bodily Injury Liability
- Property Damage Liability
- TCPA Defense

### NetGuard® Plus First Party coverage includes:

- Breach Event Costs
- Post Breach Remediation Costs
- BrandGuard®
- System Failure
- Dependent System Failure
- Cyber Extortion
- Cyber Crime
- Bricking Loss
- Property Damage Loss
- Reward Expenses
- Court Attendance Costs

Our team tracks current attack patterns, detects many types of exposures and aims to provide support to affected customers before threat actors exploit those opportunities to gain access to their networks.



For over a decade, we have been working and collaborating with a trusted team of providers. We know every cyber claim is unique, so our claims team provides a range of options to best fit your business and security needs.

We know criminals strike anytime and anywhere – that’s why our in-house claims team is there for you 24/7 in the event of a cyber incident.

Our cyber claims team can be reached at:

Call us at: 888.627.8995

Email us at: [CyberClaims@tmhcc.com](mailto:CyberClaims@tmhcc.com)

---

### **Cyber Underwriting Team**

#### **Contact Us**

**Jacob Ingerslev**, Senior Vice President  
Cyber & Tech E&O  
[jingerslev@tmhcc.com](mailto:jingerslev@tmhcc.com) | 312.609.7168

**Tina Levine**, Vice President,  
Underwriting Product Management  
Cyber & Tech E&O  
[tlevine@tmhcc.com](mailto:tlevine@tmhcc.com) | 818.479.4301

**Barret McGinnis**, Director, Underwriting, West Coast,  
Cyber & Tech E&O  
[bmcginnis@tmhcc.com](mailto:bmcginnis@tmhcc.com) | 818.933.4228

**Kelsey French**, Director, Underwriting, Midwest  
Cyber & Tech E&O  
[kfrench@tmhcc.com](mailto:kfrench@tmhcc.com) | 312.414.9187

**Eugene Eychis**, Director, Underwriting, Northeast  
Cyber & Tech E&O  
[eeychis@tmhcc.com](mailto:eeychis@tmhcc.com) | 212.326.9377

**Neha Gupta**, Director, Underwriting, Southeast,  
Cyber & Tech E&O  
[ngupta1@tmhcc.com](mailto:ngupta1@tmhcc.com) | 770.863.4228

Visit us: [tmhcc.com/cyber](https://tmhcc.com/cyber)

---

 Visit us on LinkedIn

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.



# NetGuard® Plus- Cyber Liability 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.

## **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.