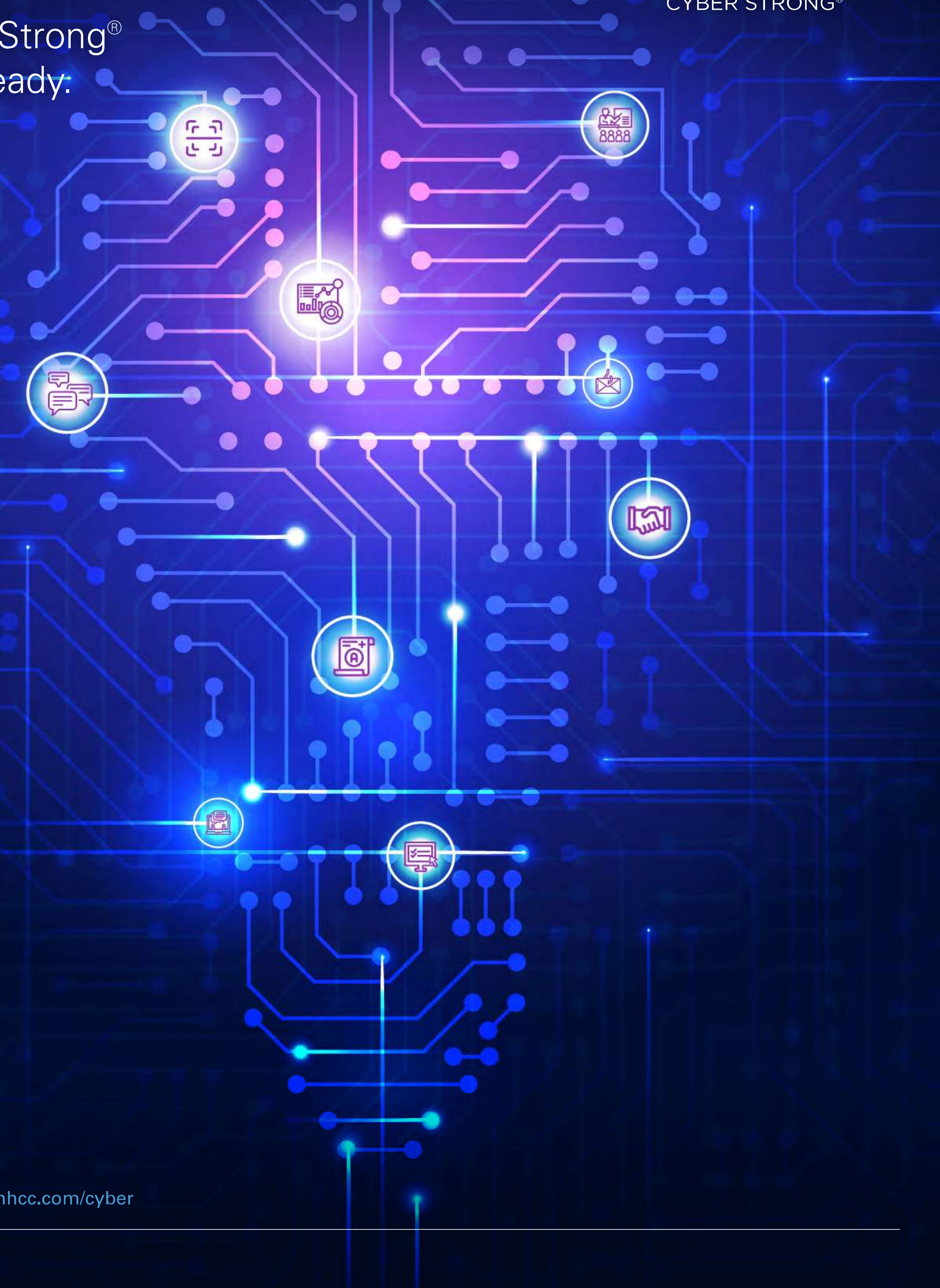
NORTHERN OHIO E&S AGENCY

TOKIO MARINE
HCC

CYBER STRONG®

NetGuard® Plus
Cyber Liability

Cyber Strong®
and Ready.



tmhcc.com/cyber

Ransomware and other cyber threats are on the rise.

>500% increase in average ransom payments

since 2018[1]

The largest ransomware losses can exceed $100 million

in 2021[1]

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 authentification offering. DUO

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

[1] *"Cyber Claims Study 2021 Report." NetDiligence, May 23, 2022. https://netdiligence.com/cyber-claims-study-2021-report/.*

NetGuard® Plus
Cyber Liability

cyberNET®

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

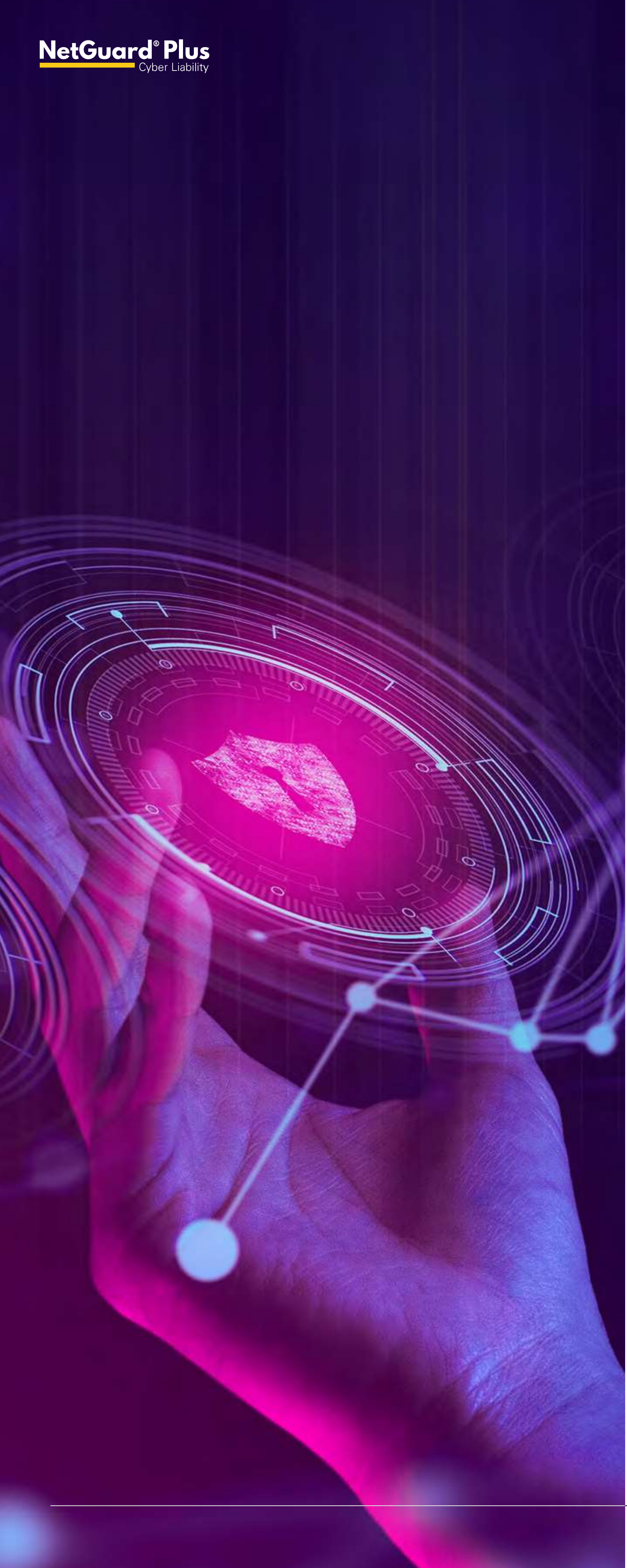
Log onto **cybernet.tmhcc.com** with access to:

- 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 though CyberNET®.

SUMMARY OF FINDINGS
RANSOMWARE INITIAL ACCESS EXPOSURE
POSSIBLE MALWARE INFECTION DETECTED



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.

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.

CROWDSTRIKE

TOKIO MARINE
HCC

Businesses have become targets of ransomware attacks which are sophisticated and have been known to penetrate vulnerabilities at the user level. We do not want our insureds to fall victim to this new trend.

We worked with **CrowdStrike**, a leader in cloud-delivered endpoint and workload protection to offer their **Falcon Prevent™** to address the complex threat landscape, unifying next-generation antivirus (NGAV), endpoint detection and response (EDR), cyber threat intelligence, managed threat hunting capabilities and security hygiene.

Often times these sophisticated attacks are able to bypass detection by the victim's legacy anti-virus protection. With CrowdStrike's leading endpoint protection solutions, our policyholders will have technology that works to stop breaches. We negotiated great rates on all their products. Policyholders that implement a next generation antivirus software will also receive a discount on their policy.

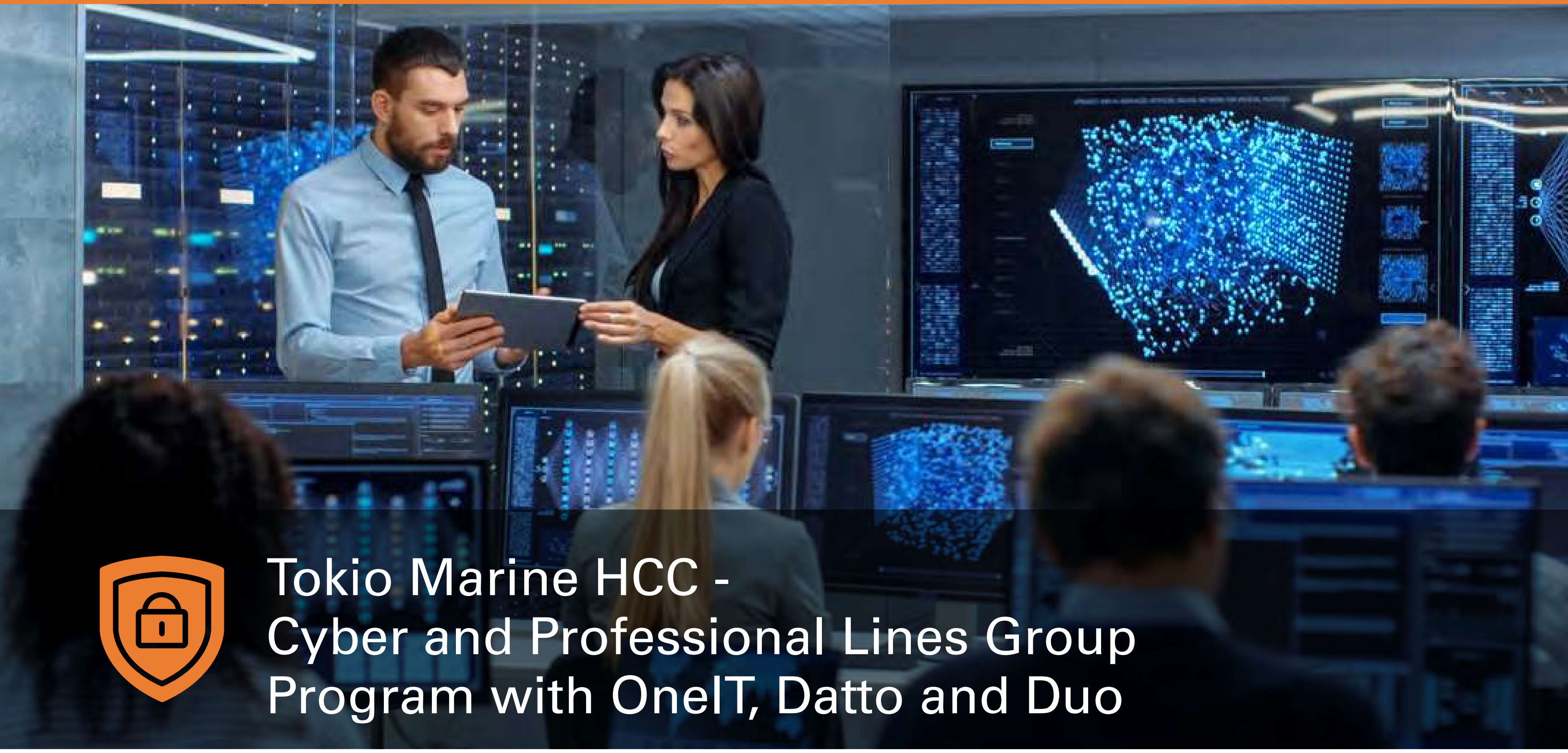
To access preferred rates click the link:
go.crowdstrike.com/tmhccandcrowdstrike

MODULE & DESCRIPTION	FALCON PRO	FALCON ENTERPRISE	FALCON PREMIUM	FALCON COMPLETE
FALCON PREVENT Next-Generation Antivirus	✓	✓	✓	**Fully Managed endpoint protection** delivered as a service by a Crowdstrike team of experts.
FALCON X Threat Intelligence	⊕	⊕	⊕	
FALCON DEVICE CONTROL USB Device Control	⊕	⊕	⊕	
FALCON FIREWALL MANAGEMENT Host Firewall Control	⊕	⊕	⊕	
FALCON INSIGHT Endpoint Detection & Response		✓	✓	
FALCON OVERWATCH Threat Hunting		⊕	⊕	
FALCON DISCOVER IT Hygiene			✓	
CROWDSTRIKE SERVICES Incident response & Proactive Services	OPTIONAL	OPTIONAL	OPTIONAL	

Flexible Bundles: ✓ *Included Component* ⊕ *Elective Component*

OneIT

datto | DUO

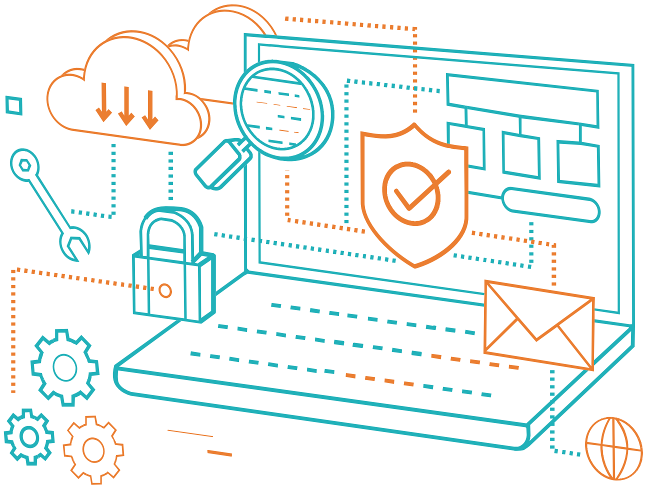


Tokio Marine HCC - Cyber and Professional Lines Group Program with OneIT, Datto and Duo

A complete cyber-security strategy must not only focus on defending against ransomware attacks but also on rapid and effective remediation when a breach occurs.

Tokio Marine HCC - Cyber and Professional Lines Group worked with **IT Managed Service Provider (MSP), OneIT**, to highlight the need for two equally critical elements in a policyholder's ransomware readiness strategy: multi-factor authentication and offsite data storage and recovery.

At Tokio Marine HCC, we are focused on helping your policyholders find strategies that will reduce ransomware damages and business disruption.



We're serious about our commitment to protecting businesses from ransomware.

We negotiated preferred rates with OneIT to offer our policyholders multi-factor authentication using **Cisco's Duo Security** and disaster-recovery and business continuity technology using **Datto**, the leading global provider of cloud-based software and technology solutions. Policyholders that implement multi-factor authentication and a cloud backup technology service will also receive a discount on their policy.

Click the link to access preferred rates:
youroneit.com/tmhcc

TOKIO MARINE
HCC

NORTHERN OHIO E&S AGENCY INC

TOKIO MARINE
HCC

Cyber **Smarter.**

Cyber Pre-Breach & Post-Breach Response Services

tmhcc.com/cyber

We Know Cyber

We recognize that a one-size solution does not fit all. **Tokio Marine HCC's** experienced underwriters welcome the opportunity to develop creative solutions to tailor coverage for your client's needs.

We insure thousands of companies from Fortune 500 to small to midsize businesses. Our in-house claims experts have handled thousands of cyber incidents each year across a range of financial services, retail, hospitality, educational, healthcare and governmental organizations.

It's not just enough to have a policy in place, you want the security to know you can count on us before and after a breach happens. We worked with preferred vendors to provide next generation anti-virus software, back-up cloud provider, and multi-factor authentication to protect from unwanted infiltration of the network. With our cyber security website, CyberNET®, your insureds have access to cyber expert consultants available online or via phone to advise how to mitigate data and privacy breaches, prepare an incident response plan and respond to a suspected breach.

At CyberNET.tmhcc.com, our policyholders get access to:

- Cyber Security Trainings
- Phishing Simulations
- Cyber Risk Report with Domain & Dark Web Security Scans

Additional benefits received as a policyholder:

- Preferred rates and partnerships with security control
- Access to cyber security consultants
- 24/7 expert claims handling

System Control:
Pre-Breach Readiness

Tokio Marine HCC insurance policyholders can access a curated list of service providers that offer a variety of risk mitigation services to help businesses reduce their risk of a cyber breach and benefit with reduced premium rates if certain controls are implemented before your policy binds. Services range from antivirus software to penetration testing to PCI compliance review.

This is a comprehensive list of service providers in good standing with **Tokio Marine HCC - Cyber and Professional Lines Group.** Services are to be secured directly with each entity and are not covered as part of your insurance policy.

CROWDSTRIKE Kroll ankura epiQ SYSTEMS

Some rates have been negotiated and are determined per project and vary according to the size and scope of services.

SERVICE	VENDOR	WEBSITE	PHONE	EMAIL
NEXT GENERATION ANTI-VIRUS SOFTWARE				
	CrowdStrike	Crowdstrike.com	917.797.7510	adam.cottini@crowdstrike.com
TWO-FACTOR AUTHENTICATION (2FA)				
	Duo Security	youroneit.com	703.570.4103	mike.zaroudny@youroneit.com
CLOUD BACKUP PROVIDER				
	Datto powered by OneIT	youroneit.com	703.570.4103	mike.zaroudny@youroneit.com
TABLETOP READINESS ASSESSMENT				
	ePlace Solutions	eplacesolutions.com	800.387.4468	efalke@eplaceinc.com
	Kroll	Kroll.com	615.924.7932	hillary.parkins@kroll.com
	Arete Advisors	Areteir.com	561.231.2758	jpasker@areteir.com
	Wilson Elser	Wilsonelser.com	601.499.8083	robert.walker@wilsonelser.com
	Tracepoint	Tracepoint.com	844.TRACE04	info@tracepoint.com
NETWORK SECURITY/PENETRATION TESTING				
	Kroll	Kroll.com	615.924.7932	hillary.parkins@kroll.com
	Ankura	Akura.com	215.832.4485	incident@ankura.com
	Arete Advisors	Areteir.com	561.231.2758	jpasker@areteir.com
SECURITY AWARENESS/PHISHING SIMULATION				
	ePlace Solutions	eplacesolutions.com	800.387.4468	efalke@eplaceinc.com
	Kroll	Kroll.com	615.924.7932	hillary.parkins@kroll.com
	Proofpoint	Proofpoint.com	877.634.7660	
PCI COMPLIANCE REVIEW				
	ePlace Solutions	eplacesolutions.com	800.387.4468	efalke@eplaceinc.com
	Kroll	Kroll.com	615.924.7932	hillary.parkins@kroll.com

Breach Control:
Post-Breach Readiness

When it comes to providing exceptional service for your policyholders and rapid, expert breach response, **Tokio Marine HCC's** in-house Incident Response Team and experienced cyber claims team gives careful consideration to the needs of each insured. Our goal is to get your insured back up and running and reach a successful resolution. How do we do it?

> "Our Cyber Incident Response Team expedites recovery and minimizes downtime for our policyholders. We're available 24/7 to navigate them through active cyber events."
>
> Richard Savage
> Director | Cyber Incident Response

Incident Response and Claims Process

1 Report

Incidents or claims are reported to:

888.627.8995

CyberClaims@tmhcc.com

2 Respond

Policyholders are put in contact with an in-house Incident Response Specialist or claims team member who makes recommendations and guides our policyholders through every step of the process.

3 Investigate

Our in-house Incident Response Specialist recommends tools and mitigation steps while ensuring appropriate investigations are conducted.

4 Recover

Our in-house Incident Response Team advises the insured about the best recovery path and recommends recovery experts to assist with technical expertise and support.

5 Notify

In the event of a data breach, our in-house Incident Response Team and claim expert recommends a breach coach/privacy counsel, credit monitoring and notification vendors.

6 Defend

If the policyholder is the subject of litigation, our claim experts will engage outside counsel and advise on the best defense and/or settlement strategy.

We work and collaborate with a trusted team of providers. We know every cyber claim is unique, so our incident response and claims team provide a range of options to best fit your policyholders' business and security needs.

> "We deliver superior claims service and assistance. Our Cyber Claims professionals are highly knowledgeable and pride themselves in responsiveness, efficiency, effectiveness, and going above and beyond for our insureds during challenging circumstances."
>
> Tamara Ashjian
> Director, Claims | Cyber & Tech

Our cyber claims team can be reached at:
888.627.8995
CyberClaims@tmhcc.com

TOKIO MARINE
HCC
NORTHERN OHIO E&S AGENCY
tmhcc.com/cyber