A perfect partner for a less-than-perfect world.®

CYBER

Pre-Breach Risk Management Solutions

Ascot policyholders have access to a wide range of proactive services and tools designed to reduce risk surface and enable a stronger response to cyber events.

knowbe4 Phishing and Human Risk Management	**KnowBe4** is a global security awareness company. The KnowBe4 HRM+ platform includes modules for awareness and compliance training, cloud email security, real-time security coaching, crowdsourced anti-phishing, AI Defense Agents, and more. KnowBe4 transforms your largest attack surface—your workforce—into your biggest asset, actively protecting your organization against cybersecurity threats. Insureds are eligible to receive a discounted subscription to KnowBe4 solutions.
CROWDSTRIKE Modern Endpoint Protection Solutions	**CrowdStrike** is an industry leader in cloud-delivered endpoint security, providing insureds with the most advanced protection available to defend against all types of attacks, from commodity malware to more sophisticated attacks, such as ransomware. CrowdStrike's Falcon platform offers a variety of protection solutions, including next-generation antivirus and endpoint detection and response. For the most robust protection, the Falcon Complete solution offers a turnkey, fully managed detection and response (MDR) service that delivers expert investigation and surgical response 24/7/365. Insureds are eligible to receive a discounted annual subscription to one of a variety of solutions.
DARKWEB IQ Pre-Incident Monitoring and Alerts	**DarkWebIQ** is a public-private partnership with exclusive visibility into ransomware gang targeting. Solutions include Ransomware Detection-and-Response (RDR) to infiltrate criminal supply chains and intervene in attacks targeting you, and Supply Chain Security+, an early warning system for incidents affecting critical third parties. Ascot cyber policyholders are eligible to activate free Code Red Alerts, which act as an early warning alert system in the event of an imminent attack risk, and to receive discounted annual subscription rates to a variety of solutions.
NetDiligence® Risk Management Hub	**NetDiligence** provides Ascot insureds with access to eRiskHub, a complimentary, online risk management hub. NetDiligence offers solutions and tools to assist insureds of any size with minimizing cyber exposure.

Continued on next page.

Ascot's pre-breach solutions are provided to Insureds to use as tools to better understand and evaluate their cyber risk exposures and to possibly identify and remediate potential vulnerability areas. These services do not replace or modify any provisions of your policy. Please read all provisions of your policy, including all attachments, for information on the coverage provided. Certain services are being provided to you by the above third-party vendors and in using these services you must agree to any terms of use & privacy policies required. Ascot makes no warranty, guarantee, or representation as to the accuracy or sufficiency of any such services. The use of the services and the implementation of any product or practices suggested by any third party is at your sole discretion. Before you engage with any pre-breach service provider, you should conduct your own due diligence to ensure the company and its services meet your organizational needs. Ascot disclaims all warranties, express or implied, and in no event will Ascot assume any liability for the performance of the third-party vendors. *All information, content and material referred to herein is for general informational purposes only and not for the purpose of providing legal advice. Insureds should contact their attorney or other legal professional for advice with respect to any particular legal issue.

A perfect partner for a less-than-perfect world.®

CYBER

Pre-Breach Risk Management Solutions

McDonald Hopkins
A business advisory and advocacy law firm®

Tabletop Exercises and Proactive Legal Services

McDonald Hopkins* provides an array of proactive data privacy and cybersecurity services. Ascot Cyber insureds have access to a complimentary one-hour remote/video tabletop exercise, a complimentary 30-minute AI consultation, and several additional services available for a discounted flat fee.

Complimentary Services:

- **Tabletop Exercise**: Facilitation of a one-hour remote/video Breach Response Workshop exercise with Insured's Incident Response Team. In-person or video options available.
- **AI Consultation**: Complimentary 30-minute scoping call to discuss the Insured's needs and identify relevant services. These may include guidance on AI-related privacy and employment compliance, vendor contracts, acceptable use and governance policies, litigation defense, and evolving AI laws. Following the call, McDonald Hopkins will provide an estimated budget for relevant services.

Fee-Based Services:

- **Tabletop Exercise:** Facilitation of a Breach Response Workshop exercise (3-4-hour session with insured's Incident Response Team). In-person or remote/video options available.
- **Incident Response Planning**: Review, revision, or creation of an incident response plan and playbook or the establishment of an incident response team, including the identification of individual roles and responsibilities.
- **Employee Training**: Development of employee training modules to address Insured's data privacy and security policies, including best practices, the role of employees in protecting sensitive data, phishing scams, social engineering, ransomware threats, laptop security, mobile device security, passwords and encryption, data disposal and destruction, data breaches, risk reduction, and reporting of suspected privacy and security incidents.
- **Data Privacy Review and Compliance Evaluation**: Evaluation of Insured's current data security policies and practices.
- **Policy and Procedures**: Review, revision, or creation of written information security program, privacy policy, social media policy, computer and electronic device usage policy, BYOD policy, document destruction and retention policy, telecommunication/remote access policy, physical and logical access security policy, acceptable use policy, password management policy, vendor management policy, information classification and handling policy, and HIPAA policies.
- **Agreements**: Review, revision, or creation of employment (confidentiality) agreements, non-disclosure agreements, third-party vendor agreements, business associate agreements, visitor agreements, end-user agreements, payment card merchant agreements, and cloud vendor agreements.