CYBER | Pre-Breach Risk Management Solutions

Ascot policyholders have access to a wide range of proactive services and tools to reduce their risk surface, which will enable them to respond better to a cyber-related event. The services and tools identified below include endpoint protection, pre-incident ransomware alerts, simulated phishing campaigns, tabletop exercises, incident response planning, regulatory compliance roadmaps, and access to a comprehensive cyber risk management hub.

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 subscription to a variety of solutions, offered at a discounted rate.
Modern Endpoint Protection Solutions	CrowdStrike is the leader in cloud-delivered endpoint security and provides 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 an annual subscription to one of a variety of solutions, offered at a discounted rate.
Pre-Incident Monitoring and Alerts	DarkWebIQ is a public-private partnership with exclusive visibility into ransomware gang targeting. DarkWebIQ 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 at 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, as well as receive discounted annual subscription rates to a variety of solutions."
Risk Management Hub	Ascot has partnered with NetDiligence to provide its Insureds with access to eRiskHub, a complimentary risk management online hub. NetDiligence offers solutions and tools to assist Insureds of any size with minimizing their cyber exposure.

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. Insureds may access these services for a discounted flat fee, including:

- **Tabletop Exercise**: Facilitation of a Breach Response Workshop exercise (3–4-hour session with Insured's Incident Response Team). (In-person or 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.