

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, simulated phishing campaigns, tabletop exercises, incident response planning, regulatory compliance roadmaps, and access to a comprehensive cyber risk management hub.



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.



Phishing Campaign

Bait & Phish is a security awareness company that provides access to phishing readiness programs through simulated phishing attacks and training. From the initial kick-off call to reporting, Bait & Phish allows Insureds to simulate phishing attacks and provides detailed reporting in real-time. Insureds are eligible to receive email phishing and security awareness training at a discounted rate.



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.

- **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.



Data Regulation Advisory Services

Clyde & Co* offers our Insureds a complimentary thirty-minute consultation to discuss their regulatory compliance needs. Insureds are welcome to invite their general counsel, marketing and finance departments, human resources and IT groups to discuss their organization's data collection, management, retention and sharing policies, as well as the corresponding regulatory requirements. With guidance from Clyde & Co attorneys, our Insureds should gain a better understanding of the current regulatory landscape, which they can use to reinforce their own compliance program.

Key Features:

- **Gratis thirty-minute conference call** with key stakeholders
- **Discussion of data collection, management, retention and sharing policies**
- **Survey of applicable regulations**
- **Additional legal services available at cost to the Insureds, including:** draft narrative of data collection practices; comprehensive regulatory compliance guidance; and data collection training



Ascot has partnered with NetDiligence to provide its Insureds with access to eRiskHub, a complementary risk management online hub. NetDiligence offers solutions and tools to assist Insureds of any size with minimizing their cyber exposure.

*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.*