




XL Insurance



## Cyber & Technology: Proactive Complimentary Services

Insureds can choose **one** of the following services from one of the below vendors during their first policy year with AXA XL. To take advantage of any of the below services, please contact your local Cyber & Technology Underwriter or Elissa Doroff at 212.915.6542 or [elissa.doroff@axaxl.com](mailto:elissa.doroff@axaxl.com).

Insureds also have access to our cyber portal: CyberRiskConnect.com. Access relevant cyber content to help your organization successfully manage data breaches, network attacks and other cyber events. Learn more at: <http://CyberRiskConnect.com>.

Vendor	Pre-Breach Services
	<ul style="list-style-type: none"><li>• <b>90-day complimentary installation of Palo Alto Networks “Traps” Advanced Endpoint Protection and Security Services (SecurePoint™) by Clarium Managed Services -Traps™</b> replaces traditional anti-virus with an enterprise level multi-method prevention approach that secures endpoints against known and unknown malware, exploits, and zero-day threats before they can compromise a system. This is a cutting-edge Prevention agent, rather than a conventional Detection and Remediation solution.</li></ul> <p><b>SecurePoint™</b></p> <ul style="list-style-type: none"><li>• <b>Up to a full day of complimentary remote engineering and installation support for AXA XL Insureds.</b></li><li>• Cloud based rapid deployment of protection to endpoints, regardless of where located.</li><li>• Global end-point monitoring service by Clarium 24/7/365</li><li>• Live threat hunting</li><li>• Continuous on-line analysis through Clarium utilizing Palo Alto Networks WildFire™ threat cloud</li><li>• Persistent off network analysis</li><li>• Automatic updates – no need for periodic patches</li><li>• Complete anti-virus replacement</li><li>• Lightweight agent that supports the most comprehensive list of operating systems including legacy, ICS, and SCADA.</li></ul> <p><b>SecureVault™ includes all the above plus:</b></p> <ul style="list-style-type: none"><li>• Assessor+ Cyber Risk Posture and Compliance Readiness Assessment (at inception)</li><li>• Compliance reporting (On-going throughout the life of the service)</li></ul> <p><b>After 90 days, The Insured can decide whether to continue the trial with no obligation or additional steps to discontinue service.</b></p>

	<ul style="list-style-type: none"><li>• <b>Social Engineering and Phishing Campaign:</b> Kivu performs a social engineering test, including email spoofing and phishing campaign. We send bogus emails with attachments and embedded hyper-links to ascertain the rates at which employees open these emails and click on links and attachments. In addition, we perform pretext phone based testing of users. We will attempt to gain confidential information such as usernames and passwords from a defined set of users in the organization.</li></ul>
	<p><b>Scope of Service (2 Hours):</b></p> <ul style="list-style-type: none"><li>• <b>Cybersecurity Compliance:</b> Many businesses are required to operate within information security frameworks pursuant to various statutes and regulations. Lewis Brisbois has written a handbook regarding these laws and will provide general guidance about best practices for compliance.</li><li>• <b>Incident Response Planning:</b> Every business should have an incident response plan to protect its digital assets and prepare to respond to data security incidents. Lewis Brisbois will provide high level guidance on the content and process of developing an incident response plan mapped to the NIST Special Publication 800-61, Rev. 2 and will describe the anatomy of a data breach.</li><li>• <b>Third Party Contract Review:</b> Many businesses engaged third party vendors, including managed service providers, to provide various services that may impact consumer data. Lewis Brisbois will review a sample third party vendor contract and provide general guidance about numerous provisions pertaining to data privacy and information security in order to limit liability.</li><li>• <b>Product and Service Review:</b> With increasing regulation and third party liability associated with products and services utilized by many companies, it is essential to consider the impact thereof on the privacy and security of consumer data. Lewis Brisbois will provide general guidance to mitigate risk associated with data privacy and cybersecurity as it pertains to new products and services.</li><li>• <b>Emerging Legal Issues:</b> Lewis Brisbois attorneys understand complex technology and regularly manage issues pertaining to emerging technologies and services. Lewis Brisbois will provide general guidance to mitigate risk associated with the provision or use of new technologies and services and to assist clients in navigating difficult legal challenges associated therewith.</li></ul>

	<p><b>Breach Plan Connect™: A Portal Dedicated to Data Breach Planning</b></p> <p>Powered by NetDiligence®, this portal helps your organization develop an Incident Response Plan (IRP) so you can execute incident response efficiently and effectively when a breach event occurs. Breach Plan Connect features an online “Customize Your Plan” tool that guides your organization step-by-step in developing a customized Incident Response Plan. Our tool makes sure that your plan contains all the elements of a sound plan — one that will stand up to regulator scrutiny. You’ll start by building out your internal and external (third-party) Incident Response Teams. Once that’s done, the tool guides you through establishing your organization’s foundational protocols, such as response priorities, severity classifications and internal communications guidelines. Finally, the tool helps you create action-oriented procedures for responding to a live event, including the steps to take and the proper sequence in which to take them.</p> <p>Key Features:</p> <ul style="list-style-type: none"> <li>• Mobile-friendly Platform – Access your plan at any time, from anywhere, on any device.</li> <li>• Hosted Service – Access your plan even when your organization’s systems are compromised or inoperable.</li> <li>• Scheduled Reminders – Receive emails reminding you to review and test your plan.</li> <li>• Free Cyber Risk Assessment Survey – Evaluate and benchmark your privacy and security practices.</li> </ul>
	<p><b>Biometric Privacy Law Consultation:</b> The collection, use, storage, possession, or disclosure of biometric information, as well as obtaining biometric information through other means (e.g., timekeeping, facilities and systems access, profiling, background checks) may create legal obligations to provide notice, get consent, develop policies and procedures, and apply heightened data security. Your coverage includes up to two hours of consultation with lawyers specializing in biometric privacy law to help identify applicable legal obligations, ask the right questions of your biometric technology provider, and develop a compliance strategy.</p>



- **CISO Workshop (2 hours):** We will facilitate a two-hour workshop with your information security leadership to understand your organization's environment, critical business processes, and risk landscape. Leveraging our deep experience in varied industries, our experts will provide strategic advice on your cyber security plans, helping you prioritize your ongoing initiatives to achieve your objectives. Alternatively, this session can be leveraged as a question and answer session with one of our seasoned cybersecurity professionals.
- **Data Privacy Workshop (2 hours):** Leveraging our global footprint and our team's locally-sourced knowledge of international data privacy regulations, we will facilitate a two-hour workshop with you to understand your compliance requirements and recommend appropriate best practices based on our experience helping others comply with data privacy regulations such as the GDPR and CCPA.
- **Phishing Testing:** We will work with you to design and execute one phishing campaign to help you gauge your organization's general cybersecurity awareness. Leveraging our proprietary online S-RM Phish Portal, we will provide you access to the campaign results and access to online cybersecurity awareness training for employees that fail the phishing test.
- **Incident Response Workshop / Plan Review:** Leveraging our deep expertise in crisis management, our experts will perform a review of your existing cyber incident response plan, providing you with actionable recommendations for improvement. If an incident response plan is not yet defined, our experts will facilitate a two-hour workshop with your stakeholders to understand your requirements and assist you with developing an effective incident response plan framework.



- **Cyber Security Incident Response:** Sylint's team of professionals provides highly effective incident response services to address a broad range of cyber events. Our veteran team of engineers, forensic analysts, and investigators work quickly to assess an often-fluid situation and craft a tailored response strategy.  
Scope of Service (2 Hours):
  - Initial Triage Call
  - Development of Strategic Response Actions
  - Pathway to Containment
- **Cyber Security Risk Assessment:** Using various frameworks, Sylint can help Clients identify gaps in security coverage to address specific industry/regulatory/best-practice requirements. We help organizations identify various vulnerabilities that may be subject to exploitation and recommend prioritized actions.  
Scope of Service (2 Hours):
  - Initial Exploratory Review
  - Discussion on Applicable Standards/Regulations
  - Identification of High Value Assets
  - Future Considerations
- **PCI Compliance Consultation:** Sylint guides businesses through complex Data Security Standards and mandatory requirements to protect CHD. This collaborative review provides businesses with a better understanding of the PCI assessment process and methods to achieve greater cyber security and PCI compliance.  
Scope of Service (2 Hours):
  - Review of PCI Requirements
  - Exploration of PCI In-Scope Environment
  - Recommendations on Optimal Resource Allocation