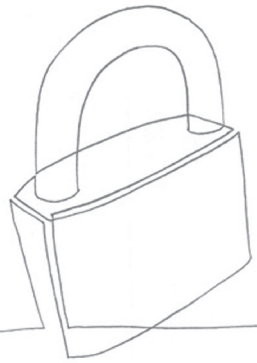
Post Breach Services

Beazley recognizes the need for post breach consultation and remediation services after your systems have been breached.

Any business will sooner or later be confronted with the challenge of a cyber breach. Proper prevention is important to protect your organization from future threats. In addition to the pre-breach and risk management services provided to our insureds, Beazley offers Beazley InfoSec policyholders post breach consultation and remediation services by endorsement.

For incidents in which the insured's computer systems are compromised, Beazley's post breach remedial services endorsement includes up to 100 hours per Policy Period of targeted post breach computer security consultation and remedial services from Lodestone Security or an alternative vendor selected by Beazley in the event one is needed. These services will address computer network and system issues and vulnerabilities identified by approved forensic service providers in response to a breach.

This offering is available in addition to existing policy limits. Coverage does not include the cost to purchase or upgrade hardware or software.



Lodestone is a wholly owned subsidiary of Beazley plc that was created to provide cyber security consulting services tailored to the small and mid-sized business (SMB) market, because you shouldn't have to be a Fortune 500 company to afford rigorous cyber security.

If an insured triggers forensic services in connection with Breach Response Services under their policy, and the incident involves the actual unauthorized access or use of their organization's computer systems, they should contact BBR Services, bbr.claims@beazley.com. An insured must request these services within 60 days following the determination of the data or security breach. Their BBR Services manager will coordinate an introductory call with Lodestone Security.

Services available*

- **External vulnerability posture improvement**
  Combining automated scanning with manual assessment techniques to evaluate the security of internet exposed network devices and servers – a common point of entry for attackers including VPN and Remote access systems.

  Activities include: host discovery, host enumeration, scanning for network and basic web application vulnerabilities, and manual verification of results.

- **Insider threat posture improvement**
  Working from inside your network, conducting an internal vulnerability assessment and recommend improvements to the security of network devices and servers including network architecture, firewall, host configuration, application servers, and databases.

- **Vulnerability management program improvement**
  Assessing a client's existing vulnerability management program and making recommendations for establishing appropriate people, process, and technology resources.

*Services are optional

Post Breach Services
continued

CBSL556_US_05/18

- **Security awareness program improvement (social engineering/phishing)**
  Many breaches are the result of weak passwords or social engineering vulnerabilities such as, conveying sensitive information by telephone, complying with phishing email instructions, or using USB devices infected with malware. Helping create security awareness and training to educate end-users on the threats from common activities they perform.
- **Wireless security posture improvement**
  Reviewing wireless networks for exposure and vulnerability and make recommendations to enhance the wireless security posture. For example, determining how far the wireless signal propagates, whether rogue access points exist, if secure encryption is in use and if appropriate authentication mechanisms are in place.
- **Application security posture improvement**
  Reviewing of the security of the client's target applications, assessing the infrastructure, configuration, input handling, application logic, and security controls in place. This review is performed against applications built in-house by the client, as well as current or potential 3rd party vendor services and applications. Looking for vulnerabilities that could give an attacker access to the data the application protects, or the system it is hosted on. Lodestones' collective experience covers a wide variety of environments, including Web apps & services, Android & iOS apps, Binary applications, through Embedded and Internet of Things (IoT).
- **Application security program improvement**
  Evaluating the maturity of the existing application SDLC and works with your organization to determine the target state using an industry standard security program maturity model. This includes security practices within Governance, Construction, Verification, and Deployment of your Application Development program. Developing an executive roadmap, CISO roadmap, and Project roadmap.
- **Incident response program improvement**
  Reviewing current organization, documentation, methodology, and technical capabilities to determine strengths, weaknesses, and steps required to improve the organization's ability to respond to computer security incidents. Designing, developing or refining governance, skills, process and technology an organization uses to respond to computer security incidents with the goal of improving your organization's incident response practices.
- **Policy, procedure and standards improvement**
  Evaluating and making recommendations to improve the effectiveness of existing policies and/or develop enhanced security policies with established security guidelines. Applying best practices consistent with standards; such as, Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), Gramm Leach Bliley (GLB), National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO) 27001/27002.

beazley

Learn more:
www.beazley.com/infosec