Cyber Services for Loss Mitigation

Signature Assessments Overview

CHUBB®

Welcome to Chubb's Cyber Services for Loss Mitigation! We offer these services because we believe that being ready to respond will help reduce the exposure to a loss when a cyber event occurs. As a Chubb cyber policyholder, you have access to a suite of **Loss Mitigation Services** to help mitigate potential cyber exposures *before* an event happens as well as several **Signature Assessments** which can help your organization quickly gauge and understand key areas of cyber risk. Loss Mitigation services are provided directly to your organization by a panel of Chubb pre-approved vendors at a pre-negotiated flat rate. For a complete list of services, please visit: www.chubb.com/us/cyberservices.

Response Readiness Assessment	
Delivered by Fidelis	Evaluate your organization's response plan or get started creating one. Fidelis Cybersecurity will provide a personalized consultation to walk your organization through a streamlined process and assess your incident response plan based on industry standards. In cases where a response plan does not already exist, Fidelis will help your organization through a process to jump start the development of one. Fidelis will first request that your organization execute a mutual non-disclosure agreement to establish a confidential relationship with your organization. Fidelis will then provide its multipart assessment for your organization to complete. The assessment will include requests for any existing incident response plan documentation that Fidelis can include in the overall review. Fidelis will then conduct a review of the materials, focusing on the internal and external response capabilities of your organization. The final report will include findings and suggested action items for your organization to remediate. The scope includes missing documents, technical and software recommendations and regulatory benchmarks. More information on Fidelis can be found at www.fideliscybersecurity.com.

Security Performance Benchmarking	
Delivered by BitSight	Monitor the security of your organization and third party vendors through external data gathered from the public Internet. Cyber policyholders receive a personalized login to the BitSight portal for 12 months, allowing you to continuous monitoring of their organization and up to three vendors of their choice. BitSight's online platform continuously analyzes, rates and monitors the security posture of organizations, all from the outside. Ratings are generated on a daily basis, giving continuous visibility into the performance of your security program. With the ability to determine the security details used to generate your organization's rating, pertinent security issues can be mitigated and tracked over time. More information on BitSight can be found at www.bitsighttech.com.
Network Vulnerability Testing	
Delivered by NetDiligence	Assess vulnerabilities on your external network - a common method threat actors use to gain access to organizations' networks. NetDiligence will conduct an automated vulnerability scan of up to eight external network addresses that represent some of your organization's external systems, such as firewalls, web applications and mail servers. Once the scan is completed, an Interpretive Summary Report is generated to bring together the key points and risk factors that should be prioritized for remediation. In addition to the summary report, the "raw" results are also provided to help your IT Staff validate and remediate the findings. Additional internal scanning options are available but require the assistance of on-site IT/networking personnel who can perform installation and placement of a "virtual scanner software" on the internal network. More information on NetDiligence can be found at www.netdiligence.com.
Phishing Simulation	
Delivered by PhishMe	Test a sample of your employees to see how well they respond to a simulated phishing attack. Electronic mail continues to be used by threat actors as a primary delivery mechanism to entice employees to click on malicious links or attachments. For the unaware employee, taking action on these malicious emails can lead to malware infection, theft of usernames/passwords or cyber extortion via ransomware. For this effort, PhishMe will work with your organization to run two phishing simulations over the course of four months: (1) a *Click Only* scenario where an email urges the recipient to click on an embedded link; and (2) a *Data Entry* scenario where an email containing a link to a customized landing page entices the user to enter their valid credentials (e.g., user ID, passwords), allowing the attacker to gain access to an organization's network environment. Individuals who fall victim to the simulation are directed to complete online training material on phishing and its effects on company security. At the conclusion of each simulation, PhishMe will provide your organization with a report containing extensive analytics, including an executive summary, simulation findings and a response analysis that details the overall susceptibility rate, reporting rate, and the repeat offense rate. No user-sensitive data is stored during simulations. More information on PhishMe can be found at www.phishme.com.

Chubb. Insured.℠