Assessing Your Cybersecurity Preparedness: It May Be Time to Update Your Bank's Information Security Plan and Response Program

With increased oversight, regulatory scrutiny and risk related to cybersecurity, now is the time for those in the banking industry to be proactive in managing cybersecurity risk. Waiting until a breach occurs to formulate or review your game plan may be "too little, too late". An assessment of your current cybersecurity preparedness may be the best place to start.

Assessment

The Federal Financial Institutions Examination Council (FFIEC) recently released a Cybersecurity Assessment Tool to help institutions identify their risks and assess their cybersecurity preparedness. Financial institutions may use the Assessment Tool to perform a self-assessment and inform their risk management strategies. The Assessment Tool contains two basic parts: Inherent Risk Profile and Cybersecurity Maturity. The Inherent Risk Profile assesses existing cybersecurity risks. The assessment includes review of five categories: (1) technologies and connections, (2) delivery channels, (3) online/mobile products and technology services, (4) organizational characteristics, and (5) external threats. It looks at the type, volume, and complexity of each category. The Cybersecurity Maturity evaluation determines the maturity level in five different domains: (1) Cyber Risk Management and Oversight, (2) Threat Intelligence and Collaboration, (3) Cybersecurity Controls, (4) External Dependency Management, and (5) Cyber Incident Management and Resilience. It seeks to determine the extent to which an institution has controls in place for a particular risk and how mature those controls are.

Because the Assessment Tool incorporates cybersecurity-related principles from regulatory guidance, the results of the assessment can help you identify areas in your bank's current security plan and response program that may need to be enhanced.

An overall review of your security plan and response program in conjunction with the assessment is also a great opportunity to confirm that your security plan and response program are consistent with the requirements set forth in the applicable Interagency Guidance.

Security Plan

The Interagency Guidance Establishing Information Security Standards adopted by the federal banking regulators to implement the federal Gramm-Leach-Bliley Act's (GLBA) safeguards requirements require institutions to develop an information security plan that contains administrative, technical and physical safeguards to ensure the security, confidentiality, and integrity of customer information, protect against any anticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Response Program

The Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice adopted by the federal banking regulators (which expand on the Interagency Guidance Establishing Information Security Standards' recommendation that institutions implement a risk-based response program) requires institutions to develop a response program which should contain procedures for assessing the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused; notifying its primary federal regulator when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information; consistent with the Agency's Suspicious Activity Report ("SAR") regulations, notifying appropriate law enforcement authorities; taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information (e.g., by monitoring, freezing, or closing affected accounts and preserving records and other evidence); and notifying customers when warranted.

Cybersecurity risk cannot be completely eliminated, but it can be effectively managed. By proactively assessing your cybersecurity preparedness and updating your security plan and response program in an informed manner, you can provide confidence to regulators that you are responsibly managing an increasingly important risk.

W. Brad Neighbors is a partner in Balch & Bingham's Birmingham office and represents banks and other institutions in transactional and regulatory compliance matters, and regularly advises clients on privacy and data security issues.