Meyer IT Systems

Connecting the World

5 THINGS TO DO TO MEET THE FTC SAFEGUARD GUIDELINES AND REQUIREMENTS

John Meyer

www.meyeritsystems.com

5 THINGS TO DO TO MEET THE FTC SAFEGUARD GUIDELINES AND REQUIREMENTS

1) DESIGNATE A QUALIFIED INDIVIDUAL

FTC Safeguards Rule requires a "Qualified Individual" to be overseeing the implementation of the information security program. This can be either an employee or can be outsourced to a service provider. They will also be responsible for enforcing the information security program. The Qualified Individual isn't required to hold any special certifications, only experience in managing security operations. This person should have a solid understanding of IT Networks, Security and the process of storing, transferring, securing, and destroying data.

2) IDENTIFY ALL ASSETS WITH ACCESS TO CUSTOMER DATA

A network map or diagram of where the customer data is and what assets have access to it is crucial. This is important because it will show who has access to everything, whether it is employees or a third-party. This can be done through the digital footprint mapping. This will need to include any third-party vendors that have stipulations with a customer data retention period even when partnership has ended. You will need to make the proper adjustments as needed to meet the FTC Safeguard Guidelines.

3) TRACK FLOW OF CUSTOMER DATA

You need to track the flow of customer data to show how customer data is being collected, stored, transmitted and destroyed. This will give you the lifecycle of customer data and where it is during all stages of the lifecycle. Any information that contains nonpublic personal information is considered customer information. Even though the FTC is concerned with highly-sensitive financial information, like Social Security Numbers, Credit Card information and more, all general contact information could be mapped as it can be used for other social engineering that leads to security incidents.

4) PERFORM A RISK (VULNERABILITY) ASSESSMENT

A Risk Assessment needs to be performed to evaluate the posture of the company's security. This assessment will show where your network is the strongest and the weakest. This can be compared to the diagram of customer data flow to show how much risk the customer data is at. This will give you a good idea of where to start focusing on implementing security measures to meet Safeguard requirements. The risk assessment should be used alongside employee questionnaires, phishing tests, employee training, penetration testing and application assessments. These risk assessments need to be done every 6 months.

5) IMPLEMENT SAFEGUARDS TO ENSURE INTEGRITY

Once the Risk Assessment is done and the security risks have been discovered, the Qualified Individual should deploy solutions for each of the risks, verify that the solution has been implemented properly, and actively monitor the network for any possible vulnerabilities or attacks. The safeguards can include things like: Zero-Trust Architecture, Multi-Factor Authentication, Encryption of Customer Data, Segmentation of Networks, Monitor Attack Surfaces, a Written Incident Response Plan, Annual Penetration Testing, Annual Employee Training, Periodic Phishing Tests, Periodic Employee Questionnaires, Semi-Annual Security Reporting and Anticipate then Evaluate Changes to Your Information System Network.