Financial Industry Regulation Authority (FINRA)

FINRA is dedicated to investor protection and market integrity through effective and efficient regulation of broker-dealers. FINRA is not part of the government. They are an independent, not-for-profit organization authorized by Congress to protect America's investors by making sure the broker-dealer industry operates fairly and honestly.

2015 FINRA Report on Cybersecurity Practice

Key points in the report:

- Sound governance framework with strong leadership
- Risk assessments is the foundation for understanding cybersecurity risks
- Implementing technical controls is essential to the firms cybersecurity program
- Well trained staff is important to defense against cyberattacks

Report link:
http://bit.ly/2nc4oNz

FairWarning Maps to FINRA Cybersecurity Principles and Effective Practices

- Cybersecurity Risk Assessment – firm should conduct regular risk assessments to identify cybersecurity risks associated with firm assets and vendors and prioritize their remediation.
    - Identify and maintain an inventory of assets authorized to access the firm's network and as a subset, critical assets that should be accorded prioritized protection (page 12)
- Technical Controls – firms should implement technical controls to protect firm software and hardware that stores and processes data (page 16)
    - User Monitoring – firms should establish controls to detect misuse of sensitive entitlements. Firm should seek to define business rules that differentiate between normal and abnormal use of sensitive entitlements and to create monitoring controls to rapidly detect and investigate abnormal behavior (page 19)
    - Terminating access – policies and procedures should be in place associated with entitlement maintenance and access reviews to ensure that role assignments and entitlements identified are no longer needed are terminated in a timely manner (page 20)
    - Cloud and other third-party services – if a firm uses cloud services, it is important that all of these IAM concepts be applied there as well. (page 20)
- Incident Response Planning – firms should establish policies and procedures for escalating and responding to cybersecurity incidents (page 23)
    - Containment and mitigation strategies for multiple incident types
    - Investigation and damage assessment process
    - Preparation of communication/notification plans for outreach to relevant stakeholders (FINRA Rule 4530(b))