IAA's IA Compliance 2022
Building Confidence in Your Cybersecurity Program
Pete Baldwin, Faegre Drinker Biddle & Reath LLP

1. Understanding the Current Threat Environment

- **FBI Internet Crime Complaint Center (IC3)**
  - The mission of IC3 is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated criminal activity and to develop alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness. (https://www.ic3.gov/)
- **DHS Cybersecurity and Infrastructure Security Agency (CISA)**
  - CISA is an operational component of the Department of Homeland Security. CISA's role is to improve cybersecurity across all levels of government, coordinate cybersecurity programs with U.S. states, and improve the government's cybersecurity protections against private and nation-state hackers. In support of this mission, CISA's National Cybersecurity and Communications Integration Center (NCCIC) acts a hub for information and expertise, sharing alerts with the cybersecurity community. (https://www.cisa.gov/cybersecurity)
- **Financial Services Information Sharing and Analysis Center (FS-ISAC)**
  - FS-ISAC is a global cyber intelligence sharing community solely focused on financial services. The organization leverages its intelligence platform, resiliency resources, and a trusted peer-to-peer network of experts to anticipate, mitigate, and respond to cyber threats. (https://www.fsisac.com/)
- **FBI InfraGard**
  - InfraGard is a partnership between the FBI and members of the private sector for the protection of U.S. Critical Infrastructure. InfraGard connects owners and operators within critical infrastructure to the FBI, to provide education, information sharing, networking, and workshops on emerging technologies and threats. Membership includes: business executives, entrepreneurs, lawyers, security personnel, military and government officials, IT professionals, academia and state and local law enforcement – all dedicated to contributing industry-specific insight and advancing national security. (https://www.infragard.org/)
- **U.S. Secret Service (USSS) Electronic Crimes Task Force (ECTF)**
  - USSS is responsible for detecting, investigating, and arresting any person who violates certain laws related to financial systems. Cyber Fraud Task Forces (CFTFs), the focal point of USSS's cyber investigative efforts, are a

partnership between USSS, other law enforcement agencies, prosecutors, private industry, and academia. CFTFs combat cybercrime through prevention, detection, mitigation, and investigation. The Global Investigative Operations Center (GIOC) conducts analysis of non-traditional data sources and works with CFTFs on combating transnational organized criminal organizations. USSS's intrusion responders are at the frontlines of large scale network intrusions and malware attacks, as well as the trafficking of stolen financial data and other cybercrimes. (https://www.secretservice.gov/investigation/cyber)

- **SEC Cybersecurity**
  - The SEC uses its civil law authority to bring cyber-related enforcement actions that protect investors, hold bad actors accountable, and deter future wrongdoing. The Division of Enforcement's Cyber Unit was established in September 2017 and has substantial cyber-related expertise. The Cyber Unit focuses on violations involving digital assets, initial coin offerings and cryptocurrencies; cybersecurity controls at regulated entities; issuer disclosures of cybersecurity incidents and risks; trading on the basis of hacked nonpublic information; and cyber-related manipulations, such as brokerage account takeovers and market manipulations using electronic and social media platforms. (https://www.sec.gov/spotlight/cybersecurity)
- **New York Department of Financial Services Cybersecurity Resource Center**
  - NYDFS maintains a webpage with cybersecurity guidance and other resources (https://www.dfs.ny.gov/industry_guidance/cybersecurity)

2. **Regulatory Overview**

- **Gramm-Leach-Bliley Act, 15 U.S.C. § 6801(a)-(b) (GLBA)**
  - Title V, Subtitle A of the GLBA governs the treatment of consumers' nonpublic personal information by financial institutions, including investment advisors
  - GLBA requires financial institutions to "respect the privacy of its customers and to protect the security and confidentiality of these customers' nonpublic personal information" by requiring federal agencies to mandate "appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards."
- **SEC Regulation S-P, 17 C.F.R. § 248.30 (the Safeguards Rule)**
  - Regulation S-P requires registered broker-dealers, investment companies, and investment advisers to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information." See Release 34-42974, Privacy of Consumer Financial Information (Regulation S-P), Section III, Subpart E - Safeguard Procedures, (June 22, 2000)

- **SEC Regulation S-ID, 17 C.F.R. § 248.201 (the Identity Theft Red Flags Rule)**
    - The Red Flags Rule requires certain regulated entities to adopt a written identity theft program that includes policies and procedures designed to identify relevant types of identity theft red flags, detect the occurrence of those red flags, respond appropriately to the detected red flags, and periodically update the identity theft program. Entities that are required to adopt identity theft programs also must provide for the administration of the program, including staff training and oversight of service providers. An identity theft program should be appropriate to the size and complexity of the entity and the nature and scope of its activities
- **State Data Breach Notification Laws**
    - All 50 states have enacted data breach notification laws that require entities to notify individuals and state enforcement agencies of a data breach in certain circumstances
- **State Data Security Laws**
    - More than half of all U.S. states have enacted laws requiring reasonable security measures with respect to consumers' sensitive personal information
    - These laws generally require businesses that own, maintain, or license the personal information of individuals to maintain "reasonable security procedures and practices" appropriate to the nature of the information and to protect the information from unauthorized access, destruction, use, modification or disclosure
    - Example: New York's SHIELD Act
- **New York Department of Financial Services (NYDFS) Cybersecurity Regulation, 23 N.Y.C.R.R. Part 500**
    - Effective March 1, 2017, NYDFS promulgated a regulation establishing cybersecurity requirements for financial services companies
    - The Cybersecurity Regulation imposes strict cybersecurity rules on covered organizations, such as banks, mortgage companies, and insurance firms. The regulation requires financial companies to install a detailed cybersecurity plan, enact a comprehensive cybersecurity policy, and initiate and maintain an ongoing reporting system for cybersecurity events
    - The Cybersecurity Regulation applies to all entities operating under NYDFS licensure, registration, charter, or those that are otherwise NYDFS regulated, as well as to unregulated third-party service providers working with regulated entities
- **Other State Insurance Laws**
    - A growing number of states have adopted laws, modeled after the National Association of Insurance Commissioners (NAIC) Insurance Data Security

Model Law, that establish prescriptive data security standards for insurers in order to mitigate the potential damage from a cyberattack or data breach

- State insurance laws generally require entities to develop, implement and maintain an information security program based on its risk assessment

- **California Consumer Privacy Act (CCPA)**
  - Primarily a privacy-focused law with partial exemption for GLBA-covered consumer information
  - Provides a private right of action, which is available to "[a]ny consumer whose nonencrypted and nonredacted personal information … is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information …."

- ***Proposed*** **New SEC Cybersecurity Risk Management Rules for Investment Advisors**
  - On Feb. 9, 2022 the SEC voted to propose cybersecurity rules applicable to investment advisors and to registered investment companies
  - If adopted, the proposed rules – Rule 206(4)-9 under the Investment Advisors Act of 1940, as amended, and Rule 38a-2 under the Investment Company Act of 1940, as amended – would require investment advisors and funds to implement written policies and procedures to address cybersecurity risks, and create new reporting, disclosure, and record keeping obligations
  - https://www.sec.gov/rules/proposed/2022/33-11028.pdf

- **Enforcement Trends**
  - As cyberattacks have increased, state and federal regulators have correspondingly stepped up efforts to investigate and bring enforcement actions – which often include large fines – against companies that are perceived to have been negligent in their cybersecurity efforts
  - Two of the most active agencies have been the SEC and NYDFS
  - In 2021, the SEC announced multiple high-profile enforcement actions against businesses that were found to have inadequate cybersecurity programs, policies, or responses
  - Within the past year, NYDFS has announced several enforcement actions stemming from violations of the Cybersecurity Regulations
  - Both the SEC and NYDFS have also issued guidance to regulated entities on cybersecurity
  - The recent enforcement actions are a sign of agencies' increasing willingness to scrutinize and penalize lax cybersecurity practices

3. Relevant Cybersecurity Frameworks

- **International Standards Organization (ISO) 27001**
  - The international standard for managing information security
  - Certification to the ISO 27001 standard is recognized worldwide as an indication that your information security management system is aligned with industry best practices
  - https://www.iso.org/isoiec-27001-information-security.html
- **National Institute of Standards and Technology (NIST) Cybersecurity Framework**
  - U.S. standard designed to organize and improve a company's overall cybersecurity posture
  - Includes a set of guidelines and best practices which can be used in almost any type of network design, and considered one of the best U.S. cybersecurity framework standards
  - https://www.nist.gov/cyberframework
- **NIST Ransomware Profile (NISTIR 8374)**
  - Can be used as a guide to managing the risk of ransomware events and can help gauge an organization's level of readiness to mitigate ransomware threats and to react to the potential impact of events
  - https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8374-draft.pdf
- **Zero Trust Architecture**
  - NIST cybersecurity framework published in August 2020 with the goal of hampering the spread and success of ransomware
  - Eliminate implicit trust within a network and continually validate every state of your digital interaction
  - https://www.nist.gov/publications/zero-trust-architecture
- **Center for Internet Security (CIS) Top 20 Controls**
  - A set of high-priority defensive actions that provide a starting point for companies seeking to strengthen their cybersecurity defenses
  - The CIS controls order six "basic," ten "foundational," and four "organizational" controls
  - https://www.cisecurity.org/about-us