Key Investment Takeaways from RSA

- Majority of companies are early-stage and still trading at revenue multiples
- Most of the larger cyberservices companies have traded in the last 2 years and are unlikely to be up for sale again in the near future
- Service providers at RSA included:
  - MSSPs (Managed Security Service Providers): Similar business model to MSPs but greater exposure to liability from cyberattacks
  - Penetration testers: These providers scan and "hack" into companies' security infrastructure to identify vulnerabilities using both manual hacking and automated scanning tools
  - Cybersecurity consultants: Consulting model of offering engagements to identify and diagnose vulnerabilities, typically with a proprietary software platform
  - Digital forensics and incident response (DFIR): Following an incident, DFIR firms collect and analyze data for legal compliance and remediation purposes. They are typically referred to customers by insurance companies

Potential Companies of Interest

- FLASHPOINT
  - Provides threat intelligence for a company beyond their internal infrastructure
  - Offers initial consulting engagements to analyze public information from chat services, social media, black markets, stolen credit card databases, as well as internal company information to identify vulnerabilities. Customers then gain access to their proprietary platform, which continuously scans these sources, generating recurring revenue post-engagement
  - Closed a majority growth investment from Audax in July 2021 and acquired Risk Based Security in Jan 2022
  - Connected w/ the CEO, Josh Lefkowitz, at RSA, who offered to make a connection to Audax
- A-LIGN
  - Provider of compliance and auditing services for various federal, state, and industry certification requirements (e.g., HITRUST, FedRAMP). Offers consulting services to help clients prepare for these certifications as well as assessments post-certification to ensure that the client remains in compliance
  - $70mm in revenue; closed a growth investment from Warburg in Aug 2021 w/ Stephanie Geveda on the board
- NETSPI™
  - Penetration testing provider that offers 1-4 week engagements as well as continuous "reoccurring" testing services. During these engagements, penetration testers use 3rd party software to scan companies for vulnerabilities while attempting to manually hack into application / network infrastructure. Once scan results are available, penetration testers analyze and validate results to identify the highest priority vulnerabilities for remediation
  - $90mm in revenue and growing 50% YoY

Summary of Discussion w/ HW (Anthony and Priyanka)

- Cybersecurity
  - Opensystems
    - MSSP with offices in the EU, US, and APAC that offers managed detection and response and endpoint detection services, with a particular focus on Microsoft ecosystem. Not yet ready for sale but expected to come to market in next 18 months
    - $100mm in revenue; likely to trade at a revenue multiple and is profitable
  - A-LIGN (see prior)
- Accessibility Testing
  - Accessibility (JMI)
    - $50mm in revenue and $10mm in EBITDA
  - Deque Systems
    - Consultants scan and review code and analyze user interface to assess its accessibility for, e.g., IDEA. After an engagement, customers subscribe to a proprietary plug-in that continuously scans and reviews the code for accessibility
    - Customers include 8 / 10 largest banks, Microsoft, Duolingo, The Economist, etc.
- Gov Tech
  - GCOM Software
    - MSP for state-level agencies, primarily in NY, MD, and VA but present in 31 / 50 states. Focused on community engagement and digital transformation. 10-20 year long government relationships
    - Growing 15% YoY '20-'22 w/ $35mm in EBITDA and 20-30% EBITDA margins. Owned by Sagewood (5th year)
  - MGT Consulting
    - MSP for public agencies, education sector, and hospitals with both consulting and managed services
    - $75mm in revenue; Trivest is a minority investor
- Pricing optimization models
  - Companies consult on SKU optimization by reviewing their internal data and building pricing models to optimize pricing. These companies typically receive 15-20% of "saved discounts" or "higher revenue"
- Gorilla Logic is $100mm in revenue and mid-teens in EBITDA but will be a while before it comes to market

Market Trends

- More vulnerabilities are becoming identified and remediated but labor and resources shortage prevent companies from addressing all. Even low priority vulnerabilities are problematic if they fail to be addressed over time as hackers can create "chain attacks" and take advantage of these vulnerabilities
    - Increasing focus on ensuring security of suppliers, particularly after the Target breach (which was hacked through a 3rd party vendor), resulting in the trickling down of cybersecurity services to smaller companies
- Labor shortage leading to i) increased focus on retention, ii) increasing recruitment commission and incentives, and iii) increasing automation of products but surprisingly little conversation about certifications, temp staffing, or outsourcing
    - Cybersecurity analysts are expected to be generalists and wear multiple hats
    - Difficult to train entry-level talent, however, given the specialist nature of the job and lack of internal resources for training
- Cybersecurity analysts are inundated by data and significant time is spent validating and analyzing data from software scans
- CISO's biggest allies within an organization is Legal and Compliance while their biggest competition is the Engineering department given limited time and engineering resources available