# Investment Themes in Cybersecurity

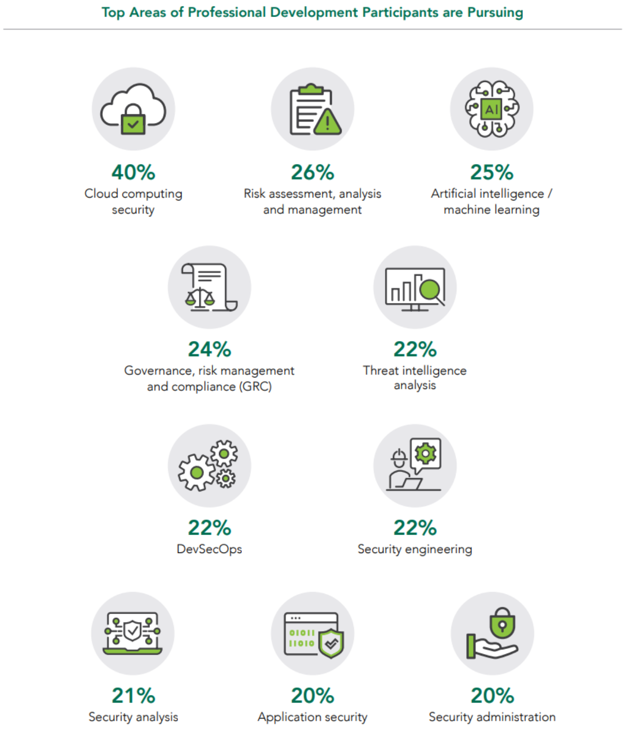
## Overview of Cybersecurity Professional Training Market

In 2021, there were 1.1 million cybersecurity professionals in the US, up 30% from 2019 estimates of 800k. Despite this increase in the cybersecurity workforce, there remains an estimated shortage of 464k cybersecurity professionals, representing a shortfall of c. 30% relative to need. This shortfall has only been exasperated by the shift to remote working. These labor shortages result in misconfigured systems and rushed deployments, creating additional cyber risk for companies.

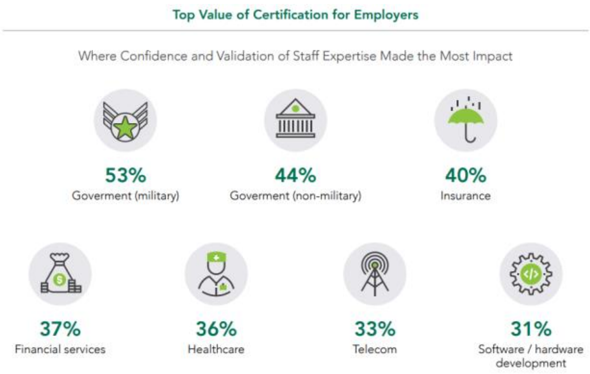
Training bodies have played a disproportionate role in producing cybersecurity professionals relative to universities, which have been the traditional pipeline for IT talent. Given that universities take 1-2 years to design curriculum, they have not been able to produce and administer programs quickly enough to address the labor shortage. Furthermore, cybersecurity requires professionals to constantly adapt to changing technologies and skills and university programs can quickly become obsolete, whereas certifying bodies can roll out new programs within months.

Additionally, many companies lack the internal talent to properly vet and hire candidates for cyber roles, and thus rely on third-party certifications / credentials as an indicator of sufficient qualifications and skills of potential cyber employees. Aside from the large technology companies, most companies are only beginning to build out internal cyber capabilities and need only a few professionals on hand, even if they are working with a managed service provider to outsource the majority of their security needs.

While there is a multitude of cybersecurity certifications, there remains no single standard for cybersecurity professionals. The chart below shows the topics of most interest to cybersecurity professionals.


Top Areas of Professional Development Participants are Pursuing

Unlike other highly regulated industries, cybersecurity professionals in the US are not required to be certified to perform their job. Certifications are most valued by employers in regulated industries such as the government, insurance, and financial services sector, as outlined in the below diagram, per a survey conducted by ISC^2.



Cybersecurity Professional Training Market Segmentation

The cybersecurity professional training market is segmented into the following use cases:

- Training and certifications for tactical cyber skills
    - These programs provide a baseline knowledge of different cybersecurity topics, from cloud security to ethical hacking, as well as fundamental cybersecurity skills. Typically, participants must complete a training course virtually or in-person over the span of a few days. Then, the participants complete a multiple-choice exam or an hours-long exercise to earn a certificate demonstrating their mastery of the material
    - Most companies offer training programs virtually or in-person that cost several thousands of dollars. Customers may have to pay an additional fee to complete the certification. Not all certifications require completing the training from the company or partner organizations, so a cybersecurity professional may complete the exam without completing the training. Professionals are expected to pay a fee to renew their certification every 3-4 years.
- "Cyber ranges", i.e., simulation platforms of cyberattacks
    - Given the evolving nature of cybersecurity, these platforms offer professionals an opportunity to simulate cyberattacks in a variety of environments (e.g., AWS cloud, etc.). This allows professionals to translate theory into practice so that they are more prepared for a live attack
    - These platforms partner with universities and training partners (e.g., SANS Institute), which incorporate the platforms into their training programs for professionals. Training partners are charged typically for number of days access to the platform per user, and then pass along the cost to the customer
- Regulatory compliance training and certifications
    - These programs certify that a cybersecurity professional is knowledgeable of existing regulatory frameworks (e.g., ISO 27001 is a standard for managing information security). These certifications target auditors, quality assurance professionals, and advisors on cyber risk. These certifications appear to be primarily provided by non-profit organizations (e.g., ISACA)

Typically, participants are cybersecurity professionals who already have a few years of experience and are looking to develop specialized expertise in a topic (e.g., penetration testing). There are a few programs that offer courses targeting professionals without any background in IT or cybersecurity, but these are in the minority. A cybersecurity professional will typically ask their employer to pay for these programs to develop additional expertise in a topic. The professional may be motivated to deepen his / her expertise to earn a promotion within the company, as well as ensure that his / her skills remain relevant. Continual training is needed for all cybersecurity professionals across all levels of expertise, even CISOs.

A few organizations also act as trade associations or thought leaders in the space. For example, the SANS Institute is considered one of the most prestigious training organizations with connections to the leading security organizations in the space. To illustrate with an example, during the investigation of the San Bernardino shooter, the FBI partnered with SANS-certified employees at Azimuth Security to hack into the iPhone. Organizations like the SANS Institute regularly publish white papers, webcasts, and attend well-known conferences in the industry like RSA.

## Investment Thesis and Considerations (Preliminary)

### *Investment Thesis*

- Positive market tailwinds with the demand for cybersecurity specialists is growing faster than the supply
- Growing market as deeper and more specialized cyber expertise is needed to serve organizations, especially as technology evolves and threats then evolve in tandem
- Opportunity to scale geographically, enter new sales channels (e.g., expand university partnerships), and offer specializations for verticals
- Opportunity to potentially invest in a "gold standard" certification, which could evolve to cover new areas as the fundamental risks / needs of increasingly digitized organizations also evolve
- Potential for a recurring revenue-based business model if ongoing fees are tied to ongoing certification

### *Investment Considerations*

- Risk of becoming obsolete if programs do not stay current on the newest threats and technologies
- Limited set of scaled for-profit training and certifying bodies
- Increasing competition from various EdTech platforms (e.g., Coursera, edX)

There are no public cybersecurity training companies and limited information on precedent transactions.

## Summary of Cybersecurity Professional Certification Companies

| Company | Description | Example Programs | Business Model | Transaction History | Differentiators |
|---|---|---|---|---|---|
| **Cybersecurity Professional Certifications** (Blue indicates potential targets) | | | | | |
| **Cyber Ranges** | | | | | |
| CYBERBIT<br>PROTECTING A NEW DIMENSION | - Cyber training platform that provides on-demand simulated attacks in different environments, as well as classes and assessments<br>- Provides a dashboard to track employee progress in performance | - Offers the platform across the most popular commercial tools (e.g., Amazon, IBM, McAfee) | - Enterprise: Sells a set number of training days on the platform<br>- University / training partnerships: Training partners (e.g., university, SANS Institute) purchase # of training days to operate Cyberbit platform for their own courses | - Founded and spun out of Elbit Systems (Israel-based defense company)<br>- 6/18: Raised $30mm from Claridge Israel<br>- 5/20: Raised $70mm from Charlesbank ($22mm primary / $48mm secondary)<br>- Elbit Systems remains a shareholder | - Most established cyber range w/ partnerships w/ universities (e.g., Purdue) and cybersecurity training providers (e.g., SANS Institute)<br>- Provides hands-on experience to employees |
| IMMERSIVELABS | - SaaS platform to simulate cyber attacks across a broad range of technical and business roles, from penetration testers to C-suite | - Offers a platform of 500k+ cyber exercises | - Enterprise product but TBD business model | - 11/19: Raised $40mm in Series B funding from Summit Partners and Goldman Sachs<br>- 6/21: Raised $75mm in Series C funding from Insight Partners, Menlo Ventures, Citi Ventures, and Goldman Sachs | - Offers simulations for non-technical roles as well |
| **Regulatory Compliance Programs** | | | | | |
| ISACA | - Membership organization for IT professionals on governance and audits<br>- Offers 8 certificates, provides training books and virtual classes, and hosts an annual conference | - Offers certificates for IT audits, risk and IT control, information security manager, governance of enterprise IT, NIST practitioner, data privacy solutions engineer, IT associate, and emerging technology | - Training: Provides online courses for <$500<br>- Certificates: Requires completing 1-4 exams, which cost <$150 to complete and are renewed every 3 years<br>- Membership fees: $10 annual fees | Non-profit (?) | - CISA certification for IT auditors is one of the most well known in the field |

| Company | Description | Example Programs | Business Model | Transaction History | Differentiators |
|---|---|---|---|---|---|
| **Cybersecurity Professional Certifications** (Blue indicates potential targets) | | | | | |
| **Trainings and Certifications for Tactical Cyber Knowledge** | | | | | |
| SANS | - Research institute that trains and certifies >12k professionals in the US per year w/ both in-person and on-demand training | - 100+ courses covering cloud security, ethical hacking, incident response, breach prevention, and audit and controls<br>- Broad range of levels from beginners to advanced<br>- Also offers a bachelors and masters program | - In-person options cost $6-$10k for 5-7 days of training<br>- On demand bundles are an additional $800-$1k<br>- GIAC certifications are an additional $850 and require completing an exam<br>- Certificates must be renewed every 4 years | Privately owned w/ no outside investor | - Considered the gold standard within the industry due to quality of instructors<br>- Provides advanced courses that are most expensive in the industry<br>- Has a separate for-profit GIAC certification body |
| EC-Council | - Provides training across different cyber disciplines w/ a focus on ethical hacking<br>- Offers self-study virtual options and in-person training<br>- Primary customer is the Pentagon<br>- Has certified >237k professionals globally | - 40 courses covering ethical hacking, block chain, cloud security, penetration testing, network security, application security, etc. | - In-person and virtual courses cost $2k-$5k with bundles offered for add-ons (e.g., unlimited video subscription, extension of course)<br>- Certificates must be renewed every 3 years<br>- Also charges an annual $80 membership fee | - 9/21: EQT invested $150mm at $400mm EV, advised by Nomura<br>- Plans on IPO or selling entire business in 1-3 years<br>- Disparate ownership by largest trainers w/ HK holding company | - Known for ethical hacking program<br>- Provides intermediate-level courses |
| CompTIA | - Non-profit trade association of >100k members for IT, cybersecurity, data and analytics, and project management professionals | - 4 core series in IT fundamentals, infrastructure (e.g., cloud), and cybersecurity<br>- Also offers "trust marks" to certify businesses for their security capabilities and credentials | - Offers primarily e-learning options for <$1k that are available for 1 year w/ exam vouchers for <$400 to become certified<br>- Certifications must be renewed every 3 years | Non-profit | - CompTIA+ training or approved partners are required for certification<br>- Provides primarily lower cost, beginner-level courses |
| (ISC)2® | - Largest cybersecurity professional org. of >168k members that offers trainings, certifications, and events | - Offers programs for cloud security, healthcare security, security administration, and leadership & operations | - In-person certification exams are conducted by Pearson Vue<br>- Does not offer training itself and relies on authorized partners | Non-profit | - Provides primarily beginner-level certifications<br>- Relies on partners to provide the training |
| INFOSEC | - Offers security awareness training programs, live boot camps, cyber ranges<br>- Has trained >100k professionals | - Live boot camps include trainings for 10 different security roles<br>- Security awareness programs are directed towards employee awareness of cyber threats | - B2C training platform costs $599 / year, which provides access to library of training and practice exams<br>- B2B training platform costs $799 / year and provides access to additional labs, custom learning plans, etc. | - 1/22: Acquired by Cengage for $190mm | - Includes programs for both cybersecurity professionals as well as security awareness programs for broader company employees |
| OFFENSIVE security | - Offers advanced training and certifications primarily in penetration testing, with hands-on labs to practice skills | - Offers 6 courses across penetration testing, web application, exploit development, and security operations<br>- Certificates require completing a 24 – 48 hour simulated exam | - Courses cost $1.5-$2.5k with an option to add the virtual lab<br>- Exam retakes cost $250<br>- Does not have renewal fees | - 9/18: Received growth equity of $25mm from Spectrum Equity | - One of the most difficult courses available in the industry<br>- Does not have renewal fees |
| CyberVista | - Diagnoses IT teams and offers tailored corporate trainings based on their needs<br>- Certified training partner for certifications (e.g., CompTIA, ISACA, (ISC)2) | - Offers training for different IT roles (e.g., cloud security, incident responses)<br>- Offers training for certificate exams (e.g., EC-Council, CompTIA) | - Primarily enterprise sales, e.g., worked with the US Army to increase pass rates for CompTIA+ certification | - Subsidiary of Graham Holdings Co. and sister company to Kaplan<br>- Potential carve-out opportunity? | - Does not offer any certifications<br>- Offers solely enterprise solutions |
| CYBRARY | - Catalog of cybersecurity courses w/ 1000+ courses available – similar to a "Coursera for cybersecurity" | - Offers courses in cloud security, GRC, IT / network ops, management and leadership, offensive security, scripting, and secure coding<br>- Also offers virtual labs and practice tests for certifications | - Subscription basis, priced at $39 - $50 / month for access<br>- Also offers enterprise solutions | - 9/17: Received $3.5mm in series A funding from Arthur Ventures<br>- 11/19: Received $15mm in series B funding from BuildGroup, Arthur Ventures, and Gula Tech Adventures | - Coursera-model of being a marketplace for cybersecurity training |

## Overview of the Cybersecurity Governance, Risk, and Compliance (GRC) Market

Over the past few years, there has been greater attention to the quantification, assessment, and disclosure of cyber risk as (i) regulatory bodies propose additional disclosure requirements, (ii) corporate Boards of Directors look for ways to assess and quantify the potential monetary damages of a cyber breach, (iii) cyber insurance becomes more widely adopted, and the insurance companies seek additional data to help them more accurately underwrite cyber risk, and (iv) companies look to monitor the cyber risk of third-party vendors. For these reasons, there is an increasing need for businesses that can help companies assess cyber risk in a transparent and understandable manner.

The Cyber GRC market can be segmented into the following services. (Note that this is a preliminary taxonomy that needs additional refinement.)

- Cyber risk assessment and auditing advisory services
  - Advisors ranging from large system integrators (e.g., Accenture, IBM, PwC) to boutique firms (e.g., A-LIGN) complete internal audits of a company's technological systems to identify areas of greatest technical and business risk. Advisors also audit the company to ensure that it is in compliance with the regulation relevant to its industry, size, and geography. This includes having the Board and IT department complete a questionnaire about governance practices, assessing protocols for an incident, reviewing IT infrastructure, and providing a remediation plan for any vulnerabilities. Advisors may then be hired for ongoing work to implement the remediation plan if the customer lacks certain internal capabilities
  - These advisors do not make any related guarantees but help customers stay in compliance with the relevant regulation
- Cyber risk quantification ("CRQ") platforms
  - This is a newer market that has only emerged in the last five years. CRQ platforms have proprietary algorithms that scrape Internet data for historical data breaches and potential vulnerabilities, then based on these results, provide a score that assesses the company's cyber risk (similar to a FICO credit score). Scores are continuously updated as the platform performs additional scans over time, whereas audits are typically conducted at a given point in time
  - Additionally, platforms may be hired to conduct internal assessments, which is integrated into their database for other customers. CRQ companies can help quantify the cyber risk associated with different technology platforms, helping CISOs decide the ROI of a given technology investment
  - Companies subscribe to platforms on a recurring basis, generating recurring revenue streams. Platforms range in the extent to which they offer add-on advisory services
  - A few companies have been acquired already by strategics:
    - Dec '19: Risk Recon was acquired by Mastercard to integrate into its suite of cyber solutions for financial institutions
    - July '21: RiskIQ was acquired by Microsoft to strengthen the security of its cloud solutions
- GRC management platforms
  - These tools feed risk and compliance data gathered from across a company's systems into the company's broader GRC management platform, which helps to automatically generate reports on the status and risk level of its cyber footprint

Investment Thesis and Considerations (Preliminary)

*Investment Thesis*

- Regulatory compliance requirements are becoming increasing strict over time, resulting in increased demand for services that can streamline the compliance and auditing process as well as provide business insights on cyber risk
- Opportunity to acquire a CRQ or GRC management platform and merge with an auditing advisor to provide a holistic solution that provides detailed point-in-time assessments, tracks cyber risk over time, and provides a workforce able to help with appropriate remediation
- Strategic exit options include large tech companies, system integrators, and financial services companies

*Investment Considerations*

- Market is nascent and it remains unclear who will be the leaders or if there is a market need for multiple Cyber GRC providers
- Few scaled providers, with most having received only VC funding to-date
- Platforms are software-based, which may be difficult for WNA to diligence
- Evolving regulatory and threat environment requires companies to quickly adapt their technology and services

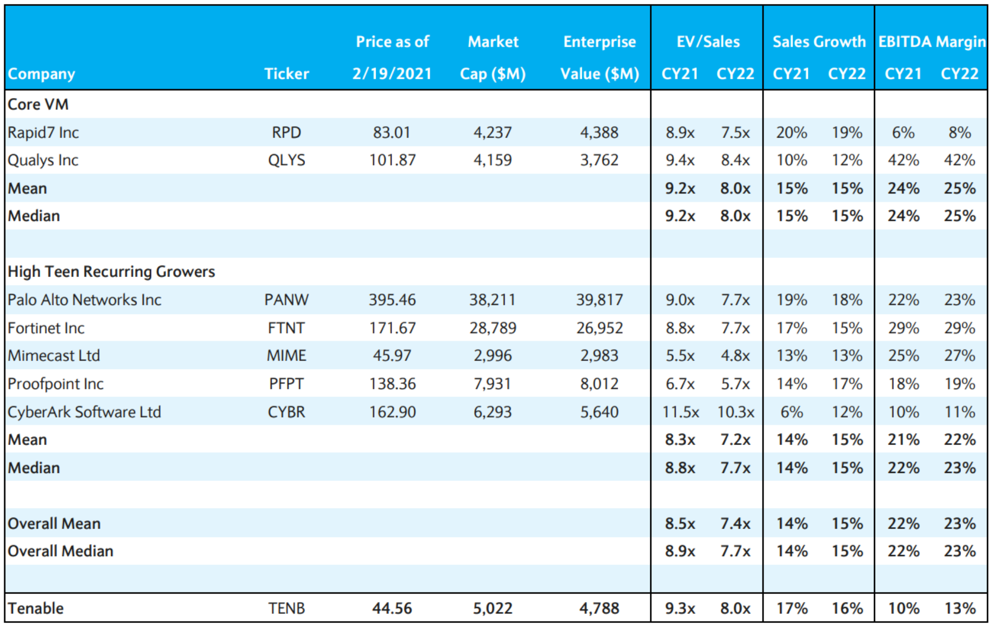
There are only a few public cybersecurity GRC companies and limited information on precedent transactions. These companies have been trading at similar multiples as other cybersecurity software providers that have been growing 15%+ YoY in revenue. Note the low EBITDA margins for these businesses, which also result in an inflated EV / EBITDA multiple given that they are primarily trading on an EV / revenue multiple.

Public comparables as of Feb '22:

- Tenanble (TENB): $5.9bn in EV trading at 101.5x EV / '22E EBITDA and 8.5x EV / '22E Sales
- Rapid7 (RPD): $6.3bn in EV trading at 182x EV / '22E EBITDA and 9.4x EV / '22E Sales
- Qualys (QLYS): $$4.7bn in EV trading at 25.5x EV / '22E EBITDA and 9.5x EV / '22E Sales

FIGURE 21

**Our valuation sheet for Tenable consists of two groups: (1) core vulnerability management companies; (2) security names growing mid-teens with profitability**



| | | Price as of | Market | Enterprise | EV/Sales | | Sales Growth | | EBITDA Margin | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Company** | **Ticker** | **2/19/2021** | **Cap ($M)** | **Value ($M)** | **CY21** | **CY22** | **CY21** | **CY22** | **CY21** | **CY22** |
| Core VM | | | | | | | | | | |
| Rapid7 Inc | RPD | 83.01 | 4,237 | 4,388 | 8.9x | 7.5x | 20% | 19% | 6% | 8% |
| Qualys Inc | QLYS | 101.87 | 4,159 | 3,762 | 9.4x | 8.4x | 10% | 12% | 42% | 42% |
| **Mean** | | | | | **9.2x** | **8.0x** | **15%** | **15%** | **24%** | **25%** |
| **Median** | | | | | **9.2x** | **8.0x** | **15%** | **15%** | **24%** | **25%** |
| | | | | | | | | | | |
| High Teen Recurring Growers | | | | | | | | | | |
| Palo Alto Networks Inc | PANW | 395.46 | 38,211 | 39,817 | 9.0x | 7.7x | 19% | 18% | 22% | 23% |
| Fortinet Inc | FTNT | 171.67 | 28,789 | 26,952 | 8.8x | 7.7x | 17% | 15% | 29% | 29% |
| Mimecast Ltd | MIME | 45.97 | 2,996 | 2,983 | 5.5x | 4.8x | 13% | 13% | 25% | 27% |
| Proofpoint Inc | PFPT | 138.36 | 7,931 | 8,012 | 6.7x | 5.7x | 14% | 17% | 18% | 19% |
| CyberArk Software Ltd | CYBR | 162.90 | 6,293 | 5,640 | 11.5x | 10.3x | 6% | 12% | 10% | 11% |
| **Mean** | | | | | **8.3x** | **7.2x** | **14%** | **15%** | **21%** | **22%** |
| **Median** | | | | | **8.8x** | **7.7x** | **14%** | **15%** | **22%** | **23%** |
| | | | | | | | | | | |
| **Overall Mean** | | | | | **8.5x** | **7.4x** | **14%** | **15%** | **22%** | **23%** |
| **Overall Median** | | | | | **8.9x** | **7.7x** | **14%** | **15%** | **22%** | **23%** |
| | | | | | | | | | | |
| **Tenable** | **TENB** | **44.56** | **5,022** | **4,788** | **9.3x** | **8.0x** | **17%** | **16%** | **10%** | **13%** |

Source: Bloomberg, Barclays Research, Consensus Estimates

Summary of Cybersecurity GRC Companies

| Company | Description | Transaction History |
|---|---|---|
| **Cybersecurity GRC Market** (Blue indicates potential targets) | | |
| **Cyber Risk Assessment and Auditing Advisory Services** (TBD) | | |
| **Cybersecurity Risk Quantification** | | |
| BITSIGHT<br>The Standard in SECURITY RATINGS | - First cybersecurity ratings platform that pulls external data of peer organizations, 3rd party vendors, and internal cyber security data to quantify the cyber risk of a company real-time<br>- Quantifies cyber risk in terms of potential financial damage, allowing the board and business leaders to contextualize cyber risk<br>- Generates >$100mm in revenue | - 6/13: Raised $24mm in Series A funding from Globespan Capital Partners, Menlo Ventures, Flybridge Capital Partners, and Commonwealth Capital Ventures<br>- 6/15: Raised $23mm in Series B funding led by Comcast Ventures<br>- 8/16: Raised $40mm in Series C funding led by GGV Capital<br>- 7/18: Raised $60mm in Series D funding from Warburg Pincus<br>- 9/21: Raised $250mm from Moody's to complete an acquisition of VisibleRisk |
| Security Scorecard | - Platform that produces real-time scores of cyber risk for customers but is less focused on "financial quantification" vs. BitSight<br>- Last Series E funding round valued it at $1bn | - 3/15: Raised $12.5mm in Series A funding led by Sequoia<br>- 6/16: Raised $20mm in Series B funding led by Google Ventures<br>- 10/17: Raised $27.5mm in Series C funding led by Nokia Growth Partners<br>- 3/19: Raised $50mm in Series D funding led by Riverwood Capital<br>- 3/21: Raised $180mm in Series E funding from investors including Silver Lake Waterman, T. Rowe Price Associates, Kayne Anderson Rudnick, and Fitch Ventures, as well as pats investors |
| **GRC Management Platform** | | |
| metricstream<br>thrive on risk | - GRC platform that collects risk and compliance data across the company and third-party vendors to produce real-time reporting, risk analytics, and regulatory notifications | - 11/17: Completed a $65mm financing round from Clearlake Capital, EDBI, and existing VC investors |

## Other Investment Themes in Cybersecurity

There are other potential investment themes related to cybersecurity, which may warrant additional research:

- Cybersecurity Awareness Training
  - Cybersecurity awareness training is conducted for employees of a company to i) train employees on how to recognize suspicious cyber activity and ii) assess company knowledge on cyberattacks
  - Training platforms include simulated phishing attempts, engaging videos and quizzes for corporate training, and dashboards with assessments of company progress and how prepared the company is for a cyber attack
  - KnowBe4 is the largest provider in the space and is currently valued at $4bn EV, trading at 67.9x EV / '22E EBITDA
- Incident Response Services
- Penetration Testing & Breach Simulation Services

## Next Steps

- Have discussions with the contacts below regarding WNA's overall interest in cybersecurity and ask about potential targets
- Set up a meeting w/ Ben T. for a "teach and learn" on cybersecurity and IT services
  - According to Alphasights, it costs 5 credits (c. $5k [?]) to retain Ben T. and obtain his contact information, in addition to an agreed-upon fee and travel costs

Relevant Contacts

- Bankers
  - Harris Williams: Anthony B. and Priyanka N. – ask for relevant cybersecurity contacts
  - Nomura: Jwalant Nanavati and Diego Mahecha (advisors to EC-Council)

    - Baird: Craig R., and also Scott B. – ask for relevant cybersecurity contacts
- Consultants
    - Bain: David Deming – PEG partner for TMT deals
    - EY: Klaas Jacobs
    - Former CEOs: Ben Trowbridge
        - Former CEO of Alsbridge, leading 3rd party IT Outsourcing / Telecoms / Benchmarking consultant
        - Former Global Cybersecurity as a Service Leader of EY
        - Board member of Arctic Security, Abacode Cybersecurity & Compliance, Working Solutions, and Southwest Power Pool