Digital Forensics and Incident Response Overview

Over the last few years, there has been a significant increase in cyberattacks, particularly in ransomware, with threats estimated to increase by 81% since the beginning of the pandemic. As a result, there has been increased demand for Digital Forensics and Incident Response (DFIR) services, especially given most firms' lack of knowledge or experience dealing with cyberattacks. For example, Arete Incident Response, a DFIR firm, reported a 150% growth in revenue in Q1'21.

DFIR firms offer highly specialized services and have an in-depth knowledge of digital forensics, ability to detect malicious or illegal actors, and compliance requirements, as well as experience handling evidence and supporting court cases. Advisors often have previous law enforcement experience with government agencies like the CIA or FBI, providing them with a unique background on how to respond to threat actors.

DFIR services can be segmented into the following:

- Digital Forensics
    - Examination and analysis of applications, data, networks and endpoint systems, both on-premises and in the cloud, for use in investigations
    - Digital forensics experts understand how to collect and restore data in such a way that it can be used as evidence in court. They have certifications from organizations like the SANS Institute, which provide them with a distinct perspective from other cybersecurity professionals
- Incident assessment
    - Determination of whether an organization has been breached by an external threat or by an insider, and assessment of the scope, timeline, root cause and impact of breaches
- Incident response
    - Restoring company operations and finding decryptors for data recovery as quickly as possible; installing end-point detection software across devices and eradicating malware
    - In the event of ransomware incidents, notification of relevant authorities, such as the FBI and CISA, in line with legal and compliance requirements in the relevant jurisdiction
    - May also entail ransomware negotiation with threat actors
- Post-incident remediation
    - Recommendations on how to avoid and mitigate future cyberattacks – may include cross-selling of managed services, although this remains a small portion of revenue (<10%) for most DFIR firms

Typically, clients use DFIR firms on a reactive basis following a cyberattack that shuts down company operations or extorts funds. Given that most companies lack the technical or compliance expertise to respond to a cyberattack, a DFIR firm is almost always brought in. Most often, clients reach out to their cyber insurance provider, who has a pre-approved list of DFIR vendors. Then, the insurer sends the request to their approved DFIR vendors and whoever responds first typically receives the work. DFIR vendors are expected to respond within a few hours. Given that clients are more focused on restoring company operations as quickly as possible, they typically use the vendor that insurers recommend.

Cyberinsurers select preferred vendors every 2-4 years to be on their panel through a process similar to an RFP. Cyberinsurers announce that they are opening their panel to new vendors, and DFIR firms respond with resumes of their consultants, summary of technological capabilities, testimonials and references, and a proposed fee schedule. Insurers select vendors based on the strength of these responses, as well as personal relationships with the DFIR firms.

DFIR firms may also be hired on retainer, although this is less common. In this case, the client has an annual set number of hours or spend budgeted for DFIR services. In the case of an incident, these DFIR firms will prioritize clients on retainer and respond immediately 80-90% of the time.

Competitive Landscape

There is a wide range of companies that offer DFIR services, with some offering it as part of a suite of cybersecurity services to others offering DFIR as a stand-alone service.

- Managed Detection Response (MDR) providers: These firms are primarily known for their proprietary cybersecurity software solutions, such as endpoint detection software. MDR firms, however, have been adding services like DFIR to create cross-selling opportunities with existing customers. Example MDR providers include Crowdstrike, Mandiant, and Palo Alto Networks. Given the high price tag and service levels of these companies, MDR providers typically only serve customers generating $600mm+ in revenue on retainer and are not working with channels like insurance companies. MDR providers have often developed DFIR capabilities through acquisitions (e.g., Palo Alto Networks' acquisition of Crypsis Group)
- DFIR specialists: These companies mostly offer DFIR services and are typically more focused on the digital forensics and compliance aspects of DFIR. They may also have proprietary internal databases or professionals with experience working on high-profile cyber attacks (e.g., Solarwind attack, Target breach). DFIR specialists rely on the insurance channel for sales, so they primarily differentiate themselves by i) how responsive they are to insurance requests, ii) fee schedule, and iii) exclusive relationships with insurers.
- Managed Security Service Providers (MSSPs): Due to the complexity of managing cyber risk, companies may outsource their entire cybersecurity operations to an MSSP. An MSSP manages the day-to-day operations, ranging from monitoring for threats to managing governance rights. An MSSP may offer DFIR services, but customers may also wish to bring in a 3rd party DFIR provider if they feel that the MSSP failed to secure and protect their networks. MSSPs may also lack the technical expertise to handle more advanced incidents or compliance background

Many DFIR specialists have added managed services to their capabilities, using their DFIR services to generate leads for managed services. Although managed services remain a small portion of revenue for DFIR providers, incident response serves as a natural lead into managed services since i) end-point detection has already been installed on the company's devices for analysis and ii) the incident can be used as a motivation to switch managed services. Managed services provide recurring revenue and can reduce the dependence on insurance companies for sales. Given that MSSPs are valued at 10-15x due to the recurring nature of their business whereas DFIR firms are trading at <10x, adding managed services can be value accretive.

However, as mentioned above, companies may not necessarily wish to use the same DFIR firm as their MSSP, especially if they suspect that the breach occurred due to shortcomings of the MSSP.

Smaller firms, however, have struggled to integrated managed services. Culturally, there is a difference between the two sets of services where DFIR services are focused on on-off incidents while managed services are focused on recurring, day-to-day operations. As one expert described it, "DFIR professionals are firemen – they don't know how to sell add-on products and services like better smoke alarms because it feels unseemly." Additionally, the leadership of DFIR firms are known for their strong technical and forensics background, but are not necessarily astute business leaders.

Investment Thesis and Considerations

Investment Thesis

- Positive market tailwinds given the increase in cyberattacks and lack of internal expertise on how to respond
- Critical and niche service that requires unique expertise given the compliance requirements
- Opportunity to create a scaled middle-market DFIR provider that is professionalized (e.g., improving and expanding the Sales & Marketing team – most have minimal spend here)
- Opportunity to add managed services and generate recurring revenue as well as higher valuation multiple

Investment Considerations

- Competitive market with a difficult GTM strategy given the heavy reliance on insurers for sales, many of whom are leaving the cyberinsurance market due to the difficulty in underwriting risk
- Little recurring revenue or sticky customer relationships, although managed services present an opportunity to change the business model (but presents its own cyber risks)
- Advisory model is dependent on talent recruitment and retention, which may pose key man risk

Potential Targets

Company	Description	Transaction History
Cybersecurity DFIR Market		
SYGNIA	- Co-founded by elite security specialists from Israel, Sygnia offers security assessments of digital assets, penetration testing, and incident response services – not a stand-alone DFIR company - Opened a London office to expand Europe business in Nov. 2021	- 2015: Team8 seeded $4.3mm into Sygnia, which operated in stealth mode until 2017 - 10/18: Acquired by Temasek for $250mm EV
KIVU	- Viewed as the go-to DFIR firm for ransomware attacks; has completed 3.5k+ engagements and vendor status w/ c. 60 cyber insurance carriers - Also offers managed services and post-incident recovery and transformation services - However, anecdotally has experienced large turnover due to poor working culture created by leadership	- 2/19: Acquired by Bow River Capital for an undisclosed amount - Investment criteria states that Bow River Capital make control investments in companies of $3-$15mm in EBITDA
Arete	- Founded in '16, global DFIR firm that has completed 5k+ engagements w/ services in APAC - Known for offshoring a significant portion of its work to establish lower fees for insurers - Q1'21: Revenue grew 150% vs. prior year and doubled their employee count	- No information available online
COVEWARE	- DFIR firm that has a proprietary technology platform that collects data on ransomware and incident response - Does not offer managed services at the time - CEO was former CEO of SecurityScorecard, a GRC cybersecurity platform and former head of NASDAQ Private Market division	- No information available online

Revature Refresh

Revature focuses on recruiting, training, and deploying entry-level IT talent, which is described below.

Recruitment and training: Revature takes candidates with no prior job experience in IT, typically college graduates, and enrolls them in Revature's in-house IT bootcamp. Revature's bootcamp is rigorous and takes 1-3 months to complete. Before COVID, classes were conducted in-person every day from 8 am to 5 pm, with students expected to spend time completing homework after class and during the weekend. During the bootcamp, candidates are employed by Revature and paid a salary equivalent to minimum wage for 40-hour work weeks, regardless of how many hours candidates dedicate to the bootcamp. Since COVID, classes have taken place virtually.

Additionally, candidates sign a contract with Revature agreeing to be placed in whatever technology specialization Revature selects for the candidate based on their staffing needs. For example, Revature may assess its pipeline and determine that it needs 80% of its students to be trained in core IT skills, 10% in cybersecurity, and the remaining in niche specializations like cloud applications.

Employee Placement: Once the candidates complete Revature's bootcamp, Revature partners with companies, typically Fortune 500 firms, to place talent. Revature will work with clients' hiring managers to determine the skillset and background (e.g., diversity hires) of hires that they are looking for and provide, e.g., 10 candidates to consider. Candidates undergo the clients' interview process and if they are not selected, Revature tries to place them at another client.

Revature's clients benefit from having a set of candidates that have already been vetted by Revature and undergone their training process. On the flipside, Revature employees benefit from having the opportunity work for a prestigious company that they may not have ordinarily been considered for. However, Revature employees have no input on what companies or geographies they are staffed to and may be dissatisfied with the placement, which is one of the primary challenges for Revature.

Post-Employment: Once a Revature employee is hired at a partner organization, the employee is considered contingent labor for Revature's clients. The employee is contracted with Revature for 2 years but is staffed with the client for 1-2 years. The client pays Revature an established hourly rate for the employee, Revature takes a share of this revenue, and the remaining is passed to the employee. Revature is responsible for the employee's benefits and acts as a liaison between parties if the employee or client are unhappy. The employee cannot cancel the 2-year contract without paying a substantial fee, estimated at $46k.

After these two years, the employee is no longer with Revature and can convert into a full-time employee with the client, if the client wishes to hire them. Revature advertises an 89% retention rate of employees at its clients after year 4 on its website.

Why it has struggled historically

Revature has received numerous poor online reviews criticizing the stringency of their contract terms and relatively low salaries. When one googles "Revature reviews," one of the first search results is titled, "Is the company Revature a scam or questionable?" Although these reviews may reflect the most disgruntled Revature employees, they most commonly point to the following pain points:

- Low pay
  - Revature employees are paid c. $45k in the first year and c. $55k in the second year, unless if in a high cost of living situation, although this may increase if inflation persists. Given that clients typically compensate Revature the same hourly rates as other FTEs and Revature takes a share of this salary, Revature employees receive a lower salary relative to other IT professionals. However, Revature believes that employees are receiving an opportunity to work at a job that they otherwise would not have received without Revature's platform
- No input on location or role placement
  - Typically, the partnering company work with Revature employees during the entire two year contract. However, if they no longer need the Revature employee before the contract ends, Revature may restaff the employee at another location. In these situations, the employee has no input on location or role placement. Worst-case scenario, an employee may have to move to different locations with little to no compensation for e.g., moving expenses, breaking a lease, paying for a longer-term Airbnb, etc.
- High penalties for breaking contract

- In order to ensure that candidates do not use Revature's training platform and then quit soon after, Revature has high penalties for breaking its two-year contracts. Anecdotally, former employees have estimated the penalty at c. $46k. Although the penalties ensure that candidates are not abusing the Revature platform, the combination of the restrictive nature of placement and high financial penalty present employees with little recourse if they are dissatisfied with the job

Despite these complaints, Revature provides a clear value proposition to the candidates in providing them with training and experience that they otherwise may not have been able to gain on their own. However, IT talent is highly valued in the current market and candidates may find less burdensome opportunities to develop their career in IT.

Of note, Revature struggled initially during COVID when employers implemented hiring freezes and layoffs, but demand quickly rebounded as organizations focused on increased digitalization and IT transformation.

Key Takeaways

Revature has an interesting model because of its ability to convert professionals with no technical background into entry-level IT talent. However, the business model appears to be financially viable primarily due to the stringent contract terms placed on employees. In numerous online reviews posted on Reddit, Indeed, and Quora, Revature employees said to only use the platform as "the absolute last resort." This raises a question of whether Wendel should be tied to such a business model, as well as a business question of whether Revature's model is sustainable if its poor reputation persists.

Other Updates

- SANS Institute: According to Ben T., SANS Institute is likely $300-$500mm in revenue, which is likely too big for WNA unless if WNA became a minority stakeholder. He believes that the most likely reason why the SANS Institute hasn't worked with investors is because the business has good cash flow and does not need outside capital. Ben T. knows the former Head of Marketing at the SANS Institute
- OffSec: According to JW's contact at Spectrum Equity, revenue is $50mm "and profitable" – likely too small for WNA
- Banker meetings: We currently have meetings on the calendar to meet with Macquarie and Canaccord to discuss TMT