Manole Capital Management Cybersecurity Note

November 2020

The Case for Cybersecurity

When was the last time you used a computer or phone to handle some kind of sensitive information? Whether or not you care to admit it, it is likely fairly recent. Think of all the times you have bought something online, checked bank statements, used a brokerage account, half-mindedly accepted the use of data tracking software like "cookies", or perhaps you have committed the all too common sin of agreeing to a list of terms of conditions from which you did not read a single word. Our point is, you have probably left pieces of private information scattered across the web, and they might add up to be more than you think. All these relatively mundane parts of our lives require large swaths of our personal information to function properly and increase efficiency, including names, addresses, credit card numbers, social security information, the list goes on. The rise of eCommerce has significantly increased our online fingerprints. Generally, we expect personal information stored on the internet to be secure, so that it remains out of the hands of malicious online actors; however, this is not always the case.

According to Statista, 165 million sensitive records were exposed in 2019 in the US from cybersecurity breaches. These breaches can be catastrophic for many individuals, having their identities, payment, and other personal information stolen. Gone are the days of large-scale battles fought with bullets and grenades, replaced by government-funded strategic sabotage of critical pieces of public and private technological infrastructure. The United States, Israel, Russia, China, North & South Korea, Iran and many other nations are placing increasing emphasis on their digital warfare efforts. Digital attacks are far more effective than conventional warfare, with little risk of tangible loss. Attacks of this nature target sensitive government documents, personal information of high-profile citizens, private company data, and even key infrastructure like power grids.

Terms / Definitions:

Cybersecurity is undoubtedly a complex topic. Many of our brightest minds in computer science, engineering, and mathematics are working to solve a myriad of security problems to ensure data remains secure. Unfortunately, there is no single or straightforward method of fully accomplishing this. Attack methods vary widely, depending on the goal of the attacker. However, most hackers tend to rely on a few common methods, which we will now try to discuss, without getting too technical. The below examples are not an comprehensive list, but we hope it begins to illustrate why cybersecurity providers cannot deliver a simple, one-size-fits-all approach.

Threats:

A. ***Malware***: This term describes a multitude of malicious software, which usually occurs when a user clicks on a malicious link or email attachment. Afterward, malicious software gets unknowingly installed on a user's device without their authorization. This includes ***spyware*** (stealing data from a computing instrument by installing malicious software on a user's device without their knowledge).

B. ***Phishing***: This occurs when an attacker sends an email, pretending to be a trusted source or colleague, to get a victim to share sensitive data (such as credit card data and passwords). By mimicking a trusted, reputable entity, phishing attacks attempt to trick a user into clicking on a malicious attachment or link. Once this occurs, fraudsters can then hijack an account or computer. It is very hard to fight something you do not understand, so the first defensive step is to be aware of what a phishing attempt looks like. Examples are emails asking for the confirmation of personal information, suspicious looking details, poorly written emails or an unusual sense of urgency.

C. ***Man in the Middle Attack (MitM):*** This occurs when an hacker inserts themselves into a transaction or transfer of data between two parties. This allows them to steal and alter data without the victims knowledge. This attack most commonly occurs on unsecured public Wi-Fi networks, where information can be stolen as it is passed through the network.

D. ***Denial-of-Service (DoS) Attack***: This occurs when servers and networks are overwhelmed with large amounts of traffic. This attack prevents a system from fulfilling actual requests and can be thought of as a "traffic jam". When this occurs, it is known as a DDoS or distributed denial-of-service.

E. ***Structured Query Language or SQL Injection:*** A SQL injection attack uses malicious code, passes it to a server, and forces it to reveal sensitive information it normally would not. Sometimes launching this type of attack can be as simple as submitting code into an unprotected website search box.

F. ***Ransomware:*** the name for malicious software, which gains access and then locks down access to vital data, like files, systems, servers, etc. This type of attack commonly targets a business or municipality and then demands a certain fee (often in bitcoin or cryptocurrencies) for unlocking the system.

Data breaches have gained widespread attention, as businesses have become increasingly reliant on workforce mobility, digital data, and the cloud. With sensitive business data stored on local machines, databases, and/or cloud servers, breaching data is as simple as gaining access to a businesses restricted network. Cybersecurity systems are able to use a variety of defenses in order to mitigate and/or even prevent these attacks. Some of these include:

Protection / Solutions:

A. ***Antivirus***: Usually a single program responsible for protecting from, scanning for, and removing multiple kinds of malware as described above. Great for protecting a single device, such as a home computer or laptop, from a wide variety of common threats.

B. ***Firewalls***: These filter data "going to and coming from" a network, like a protected wall. A barrier is created between the internal and external network, based on a certain set of security rules.

C. ***Endpoint Security:*** There are multiple types of devices that can access a network. These "endpoints" can include company computers, laptops, or employee smartphones. All of these devices pose a security threat to the business network, as a network is only as strong as its weakest link. With endpoint access, a hacker could navigate a network and end up accessing sensitive information. Endpoint security safeguards a network by recognizing if these devices and users are permissioned to enter. This kind of protection is usually used for large, complicated enterprises or those with a wide range of entry points. Antivirus and firewall protection are considered crucial elements of endpoint security.

D. ***Network Security:*** This kind of security often comes after endpoint security. This is often defined in generic terms, but network security protects your network from a variety of security threats typically by locking network entry, only allowing authorized users access, and giving users access to only certain pieces of the network.

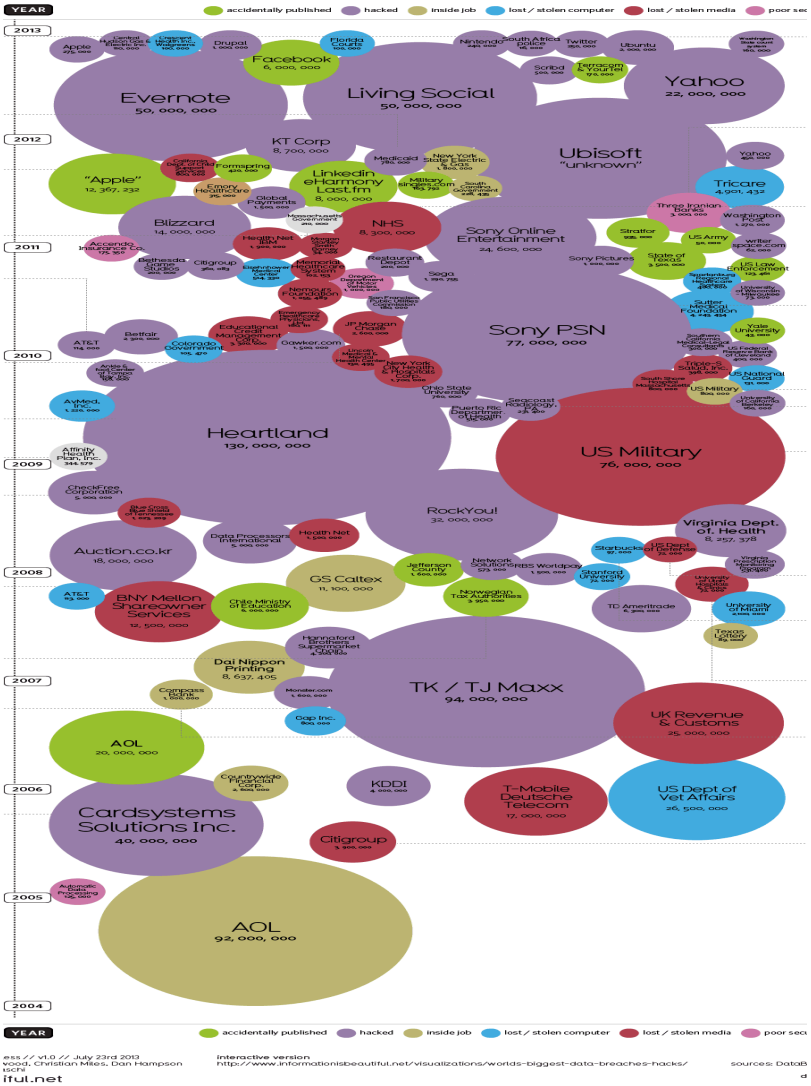
Hopefully, these terms and definitions help to set the stage for your understanding of cybersecurity. We wanted to begin our analysis with a general overview of the types of threats, as well as the different protective measures or cybersecurity defenses. As we continue, we will attempt to shine a light on how cybersecurity companies use these defenses to offer services to clients.

Breaches & Cyberattacks:

The history of data breaches and cyberattacks is unfortunately quite large. As the next chart shows, there have literally been thousands of sizeable cyberattacks and data breaches.

According to TechTarget, a data breach is "an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used" by an unauthorized individual or entity. This could entail sensitive trade secrets, intellectual property or health and payment card information. How long have these breaches been occurring? Let's review some of the largest data breaches of all-time.

Why are breaches getting more dangerous and larger in scope? This is because the world's volume of data has been growing exponentially year after year. This gives cyber criminals a greater opportunity to expose massive volumes of data in a single breach. While individuals are responsible for 70% of data creation, 80% of that data is stored by enterprises. According to CSC.com, data production in 2020 will be 44x greater than it was in 2009. Also, over 1/3rd of all data is now passing through the cloud.



Over the last decade, the largest data breaches have been eBay's 2014 breach of 145 million accounts, JP Morgan's 2014 breach of 76 million households and Heartland Payments Systems 2008 breach of 134 million accounts. More recently, the number of accounts affected have skyrocketed. Over the last 5 to 6 years, the largest data breaches were Yahoo in 2013 which impacted 3 billion accounts, FriendFinder Networks in 2016 which affected 412 million accounts and Marriott-Starwood in 2015 impacting 383 million accounts.

The Yahoo attack comprised users names, email addresses, phone numbers, dates of birth, encrypted passwords, and some security questions. The FriendFinder Network attack stole even more sensitive information, as FriendFinder is not your typical dating website. FriendFinder is an adult entertainment company, so its breach of usernames, passwords, emails and other personal information was a particularly sensitive subject. After Marriott purchased Starwood in 2014, it became the world's largest hotel chain. Unfortunately, hackers were already in Starwood's systems and they were able to get access to passport data, phone numbers, emails and credit card details. All the above are examples where cybercriminals sought personal information for financial gain; however, today hackers are not just individuals or cartels seeking riches. Cybercrime has now become the forte of certain nation states.

In 2014, Sony Pictures was attacked by the "Guardians of Peace" following the release of its controversial movie *The Interview.* It was widely thought that this attack was the perpetrated by the North Korean government, since the movie's plot was to assassinate North Korean leader Kim Jong Un. The cyberattack stole huge amounts of information from Sony's network and ultimately released thousands of confidential and embarrassing emails.

Then, in 2015, it was widely believed that the Iranian government hacked into the Sands Casino, following some very controversial statements by its founder, Sheldon Adelson. On February 10th of 2015, the world's largest gaming company was thrown into chaos, as its email went down, its computers were rendered useless and its phones were disabled. The cyberattack essentially shutdown all of Sands Casino's technology systems. These examples should demonstrate how important cybersecurity is for all individuals, commercial entities and even nations.

Just a month ago, a cyberattack brought down the New Zealand Exchange. The NZX is the locally listed operator of the exchange, where roughly $25 billion is annually traded. The problems were caused by a DDoS or distributed denial of service, where the NZX network was flooded with so much information and traffic that it crashed. Since the traffic was well-distributed across NZX's global network, it is impossible to determine the source of the attack. As this shows, hackers and cybercriminals can take down a national stock exchange. What would happen if this occurred on the NYSE, Nasdaq, German or London exchanges? The stock market is always looking for great, growth stories. Unfortunately, the threat of cybercrime is one area showing enormous secular growth.

Why Fintech?

Manole Capital defines FINTECH as ***"anything utilizing technology to improve an established process."*** We intentionally take a very broad definition of FINTECH and own many companies that others would never classify as FINTECH. Within the technology space, we do not own Facebook, Amazon, Apple, Google, Microsoft or Nexflix. Within the financial industry, we do not own any traditional banks or insurance companies. For us, FINTECH is a unique and emerging hybrid. We own companies that have certain traits and characteristics we believe will lead to outperformance. Also, we own companies that are mis-classified by GICS as industrial companies, despite the fact that they do not manufacture anything.

When it comes to cybersecurity, we believe some companies are using technology to provide security services to both consumers and businesses. We have found that the two biggest industries potentially at risk are healthcare and finance. Laws and regulations have been written in each industry, to provide guidelines for companies to follow, with HIPAA addressing healthcare and PCI Data Security Standards for payments. These regulations provide a framework for the safeguards, storage, and use practices for handling sensitive information, but not all industries have set rules and regulations.. Even with this regulations in place, it cannot definitively stop data breaches from occurring.

While healthcare providers are particularly vulnerable from a from a data breach, with sizeable penalties under HIPPA laws for inadequately protecting personal health information, the financial sector has been the target of the most, high-profile attacks. In 2008, Heartland Payments suffered a data breach compromising 130 million records from over 250,000 businesses. Heartland is a payment processor, that authorizes, clears and settles credit and debit card transactions. This New Jersey-based processor was breached through malware that was planted on its network for months, without the company's knowledge. This malware recorded card data, as it arrived from its retailers. This data breach is regarded as the largest credit card scam in history.

In 2019, Capital One had a massive hack that compromised information on 106 million card customers. This hack exposed addresses, dates of birth and self-reported incomes that had applied for a card from 2005 to early 2019. Even some social security numbers, bank account numbers and credit scores were impacted. This hack was considered the largest-ever data breach of a big bank and regulators were going to impose penalties onto Capital One for their "failure to promptly install protective software" and fend off these type of attacks. The Office of the Comptroller of the Currency said that Capital One failed "to establish effective risk assessment processes" and it did not "correct the deficiencies in a timely manner." The OCC and the Federal Reserve then insisted that Capital One make risk-management changes and increase their cybersecurity defenses. What was

the penalty for this lapse of judgement? Apparently, the regulator felt it was worth $80 million, which is probably an amount Capital One easily had in insurance.

It isn't difficult to understand why these financial companies are a primary target for hackers. Financial institutions and banks have tons of personal information and they are the gatekeeper of people's assets. Just like infamous bank robber Willie Sutton said, "I rob banks because that's where the money is." While all companies are at risk, the greatest threat appears to be for large healthcare and financial companies.

Looking at our FINTECH definition, we believe the advancements in technology have forced certain companies to increase the protection of sensitive and valuable data. In our opinion, we feel that cybersecurity companies are using technology to improve a process, ideally adding a layer of security and protection. From our perspective, we have no problem classifying these technology, software and security companies under our FINTECH umbrella.

Getting Better or Worse?:

All these potential threats are becoming increasingly more common, especially when one considers the recent shift of working remotely, due to the global pandemic. Our personal and commercial cybersecurity needs continue to grow, but we tend to set less resources aside to fight this threat. Quite simply, the attacks are no longer just simple cases of stealing a credit card for personal gain, now these criminals and nation states are becoming more sophisticated, dangerous and costly.

With the shift toward working from home, the cybersecurity vulnerabilities have only escalated. Before the pandemic, certain firms claimed to have thousands of threats per day. Now that workers are at home, the attacks are surging. Unfortunately, firms have indicated that the attacks and threats have increased by orders-of-magnitudes. In a May 2020 Senate Judiciary Committee meeting, one FBI official said the number of complaints of internet crime have more than doubled. At the same hearing, one Secret Service official said he expects over $30 billion in stimulus funds will end up being stolen through various scams.

IBM conducted a survey in early June and the statistics were not promising. It found that 53% of its used a personal laptop for business related work, which often lack a firewall or software safeguard. 29% of remote workers said they allowed their kids to use their computer for gaming, online shopping, etc. 45% said their employer has not provided security training during this work from home environment. 37% of work-from-home employees reuse the same passwords for business applications, as they do for personal information. Even more alarming, 53% of the survey stated that their employer has no new security policies in managing personally identifiable information.

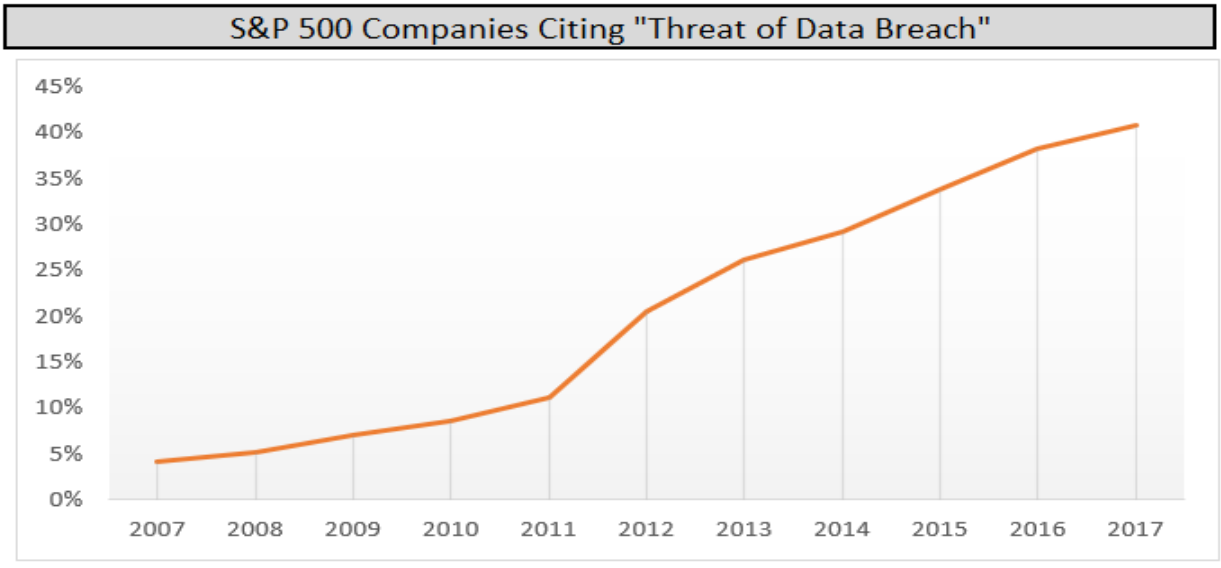
With Zoom video calls now an important component of our business lives, hackers have responded. Some are sending video-conference invitations, which really actually embed malware and steal network credentials. Others simply target employees with simple scam emails. While most attempts are ignored or thwarted, all it takes is one entry point for a cybercriminal to succeed. We believe that work-from-home employees are the first line of defense for most companies. It is just like the old adage that "a chain is only as strong as its weakest link."

Corporate Risk:

It is becoming more and more evident, that public companies are at serious risk if they do not have a formal cybersecurity plan. When Uber was had 57 million accounts hacked in 2016, it sat on this information for a year. Since it was a private company (planning on going public), it even paid a $100,000 ransom to the hackers to hide the breach. Public companies do not have the same luxury of sweeping troubling information "under the rug".

Back in 2014 and 2015, both Home Depot and Target reported the news of their hacks, within days of identifying the breach. Following Home Depot's September 2014 breach, it identified $198 million of related costs, but it had $100 million of insurance to help offset the expense. It has been 6 years since Home Depot's breach and it has done little to impact their brand and customers willingness to shop at their stores. Large corporations can manage these disruptions, but small businesses do not have the same luxury. In a data breach, the average cost per record lost in a data breach is $148 and the average total costs of a breach is $3.9 million. Even a small business with only 1,000 lost records, could see costs in the tens of thousands of dollars. In these challenging times, this could be "the straw that broke the camel's back."

Addressing the situation and taking proactive measures to ensure hacks do not happen, seems like the best possible solution to pursue. From our perspective, we believe that public companies have a duty to protect customer information and have an increasing amount of pressure to ensure they adequately address the risk of cybersecurity. As seen in the below chart, a Sentieo and Barron's analysis found that large US companies are still not taking this threat seriously. The analysis looked at annual 10-k filings and found that only half of S&P 500 companies are citing the threat of a data breach in their risk section. While the metrics are only through 2017, we have to believe that the curve continues "up and to the right". The unfortunate trend is increasing, with more companies beginning to address the threat. However, the concern level from is far from overwhelming. We believe it is time that executives accept the fact that companies will be breached and start thinking "outside the box" when it comes to data security. To be in denial of this, is just not accepting reality.



The Cost of Overconfidence:

For businesses, investing in cybersecurity is a simple cost-benefit analysis. In our opinion, having strong cybersecurity is as essential as electricity. At a minimum, it should be viewed similar to business insurance. All management teams and boards should view cybersecurity as a small price to pay, as compared to the potential long-term damage to one's brand or the costs associated with a security breach.

According to a study conducted by the *Online Trust Alliance*, global cyber-attacks continue to significantly rise (in frequency and dollar damage). IBM estimates that the average financial impact of a breach is $3.8 million, although this figure grows exponentially as larger enterprises are affected. We would argue that this financial cost understates the true impact from a security breach, as many merchants are then subjected to costly and high profile class-action lawsuits.

Not only is the business hurt, but their brand and reputation can become permanently tarnished. A recent BAE Systems survey found that a considerable majority of executives cited "reputational damage" and "subsequent legal liability" as their two highest concerns. This security breach lesson has been experienced by executives at Equifax, First American Financial, Facebook, Apple and numerous other companies. Despite these high profile lapses, many companies still overestimate the efficacy of their current cybersecurity platforms. Want proof of this overconfidence? Statistics Canada reported that more than one in five Canadian companies were victims of a cyberattack in 2017, even though 84% of Canadian executives thought their organization was a "top performer" in cybersecurity.

One of the bigger problems we see, is the vast amount of information businesses are storing. In our opinion, companies should be focusing on minimizing or even eliminating their unnecessary data collection practices. In the name of security, many companies are over-collecting or over-storing sensitive client information. By keeping this sensitive information, a company places themselves (and their customers) at considerably more risk, versus if they had simply deleted the data or never collected it at all. For example, there was no justification for Target to have stored the four-digit PIN numbers of their customers' debit cards. In fact, payment standards mandated that they do not do this. This obviously was a terrible and probably unintentional decision made by Target.

Management Priorities:

We believe the short-term nature of Wall Street has negatively impacted certain management teams. Some companies are being led by individuals with a short-term revenue and earnings focus. These teams are running their business from quarter-to-quarter, with the goal of simply exceeding sell-side analyst forecasts. Instead of focusing on the long-term success of their company, these managers are taking a short-sighted risk.

This disconnect is largely driven by an internal lack of knowledge. Cyber criminals are dynamic and constantly adapting; management teams must also be adept and resourceful. If executives do not place enough emphasis on security, a breach will surely occur. Once a breach has occurred, it is way too late to spend and invest in security protocols. A study by the *Harvard Business Review* found that the traditional role of the Chief Information Security Officer is outdated. Their research showed that having one individual charged with handling all factors of cybersecurity is inappropriate and that all executives should bear some of responsibility (flowing all the way up to the Board of Directors). With the advent and growth of outsourcing, there are a growing number of third-party vendors providing cybersecurity solutions.

Certain companies are placing more emphasis on their cybersecurity skills. During the pandemic, companies have faced an onslaught of attempted hacks, from scam emails and phishing attacks. Most corporate security chiefs report up to the CTO (chief technology officer), but this is changing. Some have created a new role called the chief information security officer or CISO. More executives and senior managers feel the need to stay aware of the risks, so certain firms have their cybersecurity teams report directly to the management committee. Companies are obviously focused on the global pandemic, but many forward-thinking teams are equally as dedicated to ensuring that lax security doesn't impact the businesses long-term plans. The world's largest companies are being attacked and modern enterprises require a comprehensive, full-circle approach to data protection and security. In this modern threat landscape, a reactive approach will not work.

Computers:

Computers and technology continue to improve, but the threat to our personal data is also increasing. Some of the largest threats come from quantum computers. While still in their infancy, these computers have theoretical capabilities and properties that are astounding. These machines harness quantum physics, to radically speed up complex calculations. Traditional computers store and process information using either zeros or ones, but quantum computers use quantum bits or qubits (stores information as both zeros and ones simultaneously, known as superposition). While regular or even super computers cannot break a security token 1,000 digits long, quantum computers use reverse multiplication and could be many millions of times faster.

JPMorgan Chase has been developing a process to better identify high-priority data, items it believes need to be protected for several years. They are looking into protecting this sensitive and potentially "at risk" data with the development of powerful quantum computers. Over the last six years, Visa has asked its security experts and software engineers to analyze post-quantum cryptography. It has published details about the public-key cryptography and experts believe it would take a computer with 250 million qubits to break today's security. Rajat Taneja is President of Technology at Visa and he said, "the data we have is sensitive, and it is vast in quantity, so protecting that data is job number one for us." Early-stage quantum computers have only a fraction of that power, but computers continue to get better and better. According to Techrepublic, the fastest to date is 64 qbits. Cryptographers are known for being paranoid, but some of their fears just might be justified.

Making this matter worse, is the fact that millions of cybersecurity jobs are currently unfilled. In early December, the Wall Street Journal published an article on the mismatch between entry-level job skills and what employers are looking for in cybersecurity employees. According to a report from the International Information System Security Certification Consortium, known as ISC2, there are 3.1 million professionals needed to bridge the cybersecurity talent gap. Unfortunately for thousands of companies, cybercrime technology is advancing at a rapid pace and cybersecurity talent simply does not exist to match the demand.

Software-as-a-Service:

It seems like software companies have been on a decade long tear, with some being best performing names in the stock market. In recent years, Software-as-a-Service or SaaS has become a dominant theme. It also appears that many IT executives have decentralized and shortened their sales process. With the software sales process getting nimbler, many SaaS companies have benefitted.

SaaS companies often start with freemium models, attempting to get engineers and developers hooked on their product. The software product is extremely scalable, as once it is built, it can be leveraged across thousands of business clients. If designed properly, SaaS models offer a company enormous TAM or total addressable market opportunities. Once a SaaS business reaches scale, the profitability is impressive. Gross and operating margins can become very high, as each new customer can generate +90% incremental margins. These SaaS models generate wonderful sustainable and recurring revenue, which ultimately leads to sizeable and predictable free cash flow. If these SaaS business models target the right theme or vertical, some can become excellent investments.

In terms of growth, the forward expectation for SaaS models remains robust. In 2019, across the entire industry, annual SaaS revenue growth was 16.1%. We are surprised that SaaS is estimated to equate to only ¼ of global enterprise software market. Looking over the next 10 years, research from ARK Invest forecasts a very healthy 21% compound annual growth.

We do not place much emphasis on the overall market growth, but believe it is wise to focus on specific verticals or niche's that might perform better than the average. The barriers to entry are not terribly high in software, so it is important to become a critical component of a business's infrastructure. An area we have tried to focus in on is vertical SaaS, as opposed to horizontal SaaS. For us, vertical SaaS firms are very focused on a specific industry (i.e. medical, security, etc), while horizontal SaaS tends to be function based (i.e. HR, payroll, etc)

As we have discussed, the barriers to entry are not terribly high in certain parts of the software business. From our perspective, we prefer niche players, that can specialize in an unique aspect of an industry. In addition, the costs to build a scalable software product can be high, so funding is critical in the early years. During COVID-19, many SaaS companies have struggled because their sales cycle is long and driven by costly sales teams. As one would expect, those software firms that rely on large and sporadic deals have suffered. Also, those that target small businesses clients are currently facing major challenges to get new customers in the door, given this difficult environment.

The metrics we will discuss below are just a start for one's analysis. In addition to these figures, one has to understand ROI (return on investment), replacement costs and switching risks. If a client can easily switch from your software to a cheaper competitors, you are in trouble. SaaS models can make it very easy for a customer to change software providers, if there isn't significant integration into a business's technology stack. Understanding stickiness and how important your software is to a client can be critical to long-term success.

Economics 101 / SaaS Business Models:

As we analyze the SaaS market, we always start with top line growth. Companies must be able to generate solid and consistent revenue growth. Many analysts will stop with revenue growth, since so many companies fail to produce free cash flow and earnings. This is often the case with relatively young SaaS businesses, as they are entirely focused on growing revenue. For us, we need to take a few steps down on the income and cash flow statements to truly get an understanding of what makes these companies tick.

After revenue, we spend a considerable amount of time focusing on margins. Once again, new start-up's are investing so heavily in sales, marketing and costs associated with R&D, that both gross and operating margins are often negative. Some SaaS sell-side analysts like to focus on the ***"Rule of 40".*** This is a simple rule that some analysts look to as a gauge, where a software business must generate a combined revenue and gross profit margin over 40%. We do not believe this is terribly important metric to monitor, because fundamental analysis must be more detailed and focused. A company can have significant revenue growth, with no focus on profitability, and we simply would not be impressed. Other companies will re-invest back into their business, in the form of hiring salespeople or R&D, and that could absolutely be the best long-term decision. For us, the mosaic is much more complex and nuanced than the basic "Rule of 40" gauge.

Before we get to earnings and free cash flow, companies must be able to leverage their business. We are not discussing leverage, in terms of debt on the balance sheet. For us, leveraging a business is turning solid revenue growth into earnings by steadily improving one's margins. This is often an evolution over time. As revenue continues to grow, it is critical for our companies to steadily move both gross and operating margins higher. This is our version of a SaaS company delivering improving economies of scale. Sometimes the process can be lumpy with software companies, but we believe it is important for a business to focus on profitability and improve margins over time. Once a company can show Wall Street that it has the capability to produce steady earnings, growth of the valuation multiple will follow. We believe that valuation multiples are dependent and driven by the underlying strength of one's business model.

So, we just discussed revenue becoming gross and operating margin, which then becomes earnings and free cash flow. If you can find a software firm delivering on these important items, you are onto something. However, there is much more one needs to focus on and analyze. Another area we like to analyze is churn and retention for software companies. If one starts by offering "free" software, the goal is to sell that customer more and more services over time. Some clients might leave, some might stay with the free product, but others will decide to increase their usage of additional services. Another metric we like to track is "net dollar retention", which gives insight into the percentage of current customer revenue retained (looking backwards 12-months), after factoring in upgrades, downgrades and churn. If this calculation is over 100%, a company could essentially grow its revenue without adding any new customers. Many companies will define this metric differently, but it absolutely must incorporate churn. With software subscription models, we have found tracking churn to be an essential item to monitor. A high retention rate often is the sign of a healthy SaaS model.

Another important metric we track for subscription models is CAC (customer acquisitions costs) and calculating how long it takes to payback that cost. Obviously, one wants as short a payback period as possible. The concept is to bring onboard new customers, as cheaply as possible and pay for that marketing costs quickly. In subscription models, especially those with low churn, this can be the "holy grail". A CAC payback period shows how many months it takes to recoup a software company's sales and marketing costs, based upon the current revenue run rate. Once again, the lower the CAC payback period indicates a company could have a strong product, with sustainable future growth. Its calculation can vary from business to business, but we like to start with prior quarter sales and marketing costs and divide that by net new ARR (annualized run rate revenue) times gross margin. Once that is calculated, we multiple by 12, to turn the metric into a number of months to payback.

For example, if Company A had the following results:

- $100 million in S&M costs last quarter
- $75 million in annualized run rate revenue and 60% gross margins
- The CAC payback would be ($100m / 60% x $75 million) x 12 or 26.7 months

This is just an example, where Company A can recoup its S&M costs, compared to new gross profit generated in only 26 to 27 months. Industry metrics on CAC payback show the median average is 29 months, the top quartile is 20 months and the top decile is only 13 months.

There are additional items we tend to look at like balance sheet strength, competitive moat, easy-to-understand businesses, management teams that have been in place for years, interesting niches, etc.

Now that we have identified the cybersecurity sector as an attractive, secular growth industry, we then wanted to look into a few of the publicly-traded companies specializing in this niche. As always, we will examine a variety of qualitative and quantitative factors. Over the next few pages, we will review CrowdStrike (CRWD).

CrowdStrike:

Crowdstrike was founded in 2011 and is based in Sunnyvale California. It was started with a strict purpose in mind, to "reinvent security for the cloud era." Their motto is "We Stop…So You Can Go."

A decade ago, cyber criminals had the advantage over the existing "cookie cutter" security products on the market. Seeing this opportunity, Crowdstrike created a security platform which integrated modern technologies, such as artificial intelligence (AI), cloud computing, and graph databases. Crowdstrike created the Falcon platform, its modernized and multifaceted defense system. Crowdstrike was the first cloud-native SaaS (Software-as-a-Service) security platform.

Description:

Crowdstrike is helping companies (both large and small) stop breaches and improve their performance. In addition to high profile businesses, Crowdstrike also provides protection for many governmental organizations. As of the 2nd quarter of FY'21, Crowdstrike had over 7,000 subscription customers. Crowdstrike has 49 of the Fortune 100, 40 of the top global 100 companies and 11 of the top 20 banks. Making things as easy for the client as possible, nearly all of its products are available for purchase directly from CrowdStrike's website.

With a share price of $129 per share and 219 million shares outstanding, the market capitalization of Crowdstrike is over $28 billion. It has $1.1 billion of cash and no debt on its balance sheet, so the enterprise value of Crowdstrike is $27 billion. In 2020, the stock performance has been impressive, up roughly 200% this year.

The Technology:

We will get into some of the finer details, but we wanted to start the analysis from a 30,000 foot perspective. Many security products are expensive, complex and frankly ineffective. Certain on-premises solutions are costly and inflexible. In today's work-from-home environment, companies need to better manage their workloads.

These problems and many more are what drives Crowdstrike's solution, covering workstations, servers, datacenters, cloud, module, etc which can all be managed on one centralized platform.

To begin, we think it is important to articulate why "cloud native" technology is better. A native app is a software application built in a specific programming language, for the specific device platform. For example, Native iOS apps are written in Swift or Objective-C while native Android apps are written in Java. A cloud native app is specifically built to operate and work in a cloud environment. In terms of data access, the cloud can provide constant protection. Secondly, in terms of data analysis, the cloud allows for platforms to continuously learn. Finally, the cloud platform collects data once, but gets to reuse its information many, many times. These are just a few of the advantages of a cloud native platform.

Crowdstrike starts by breaking its business into 6 different cloud-native platform elements:

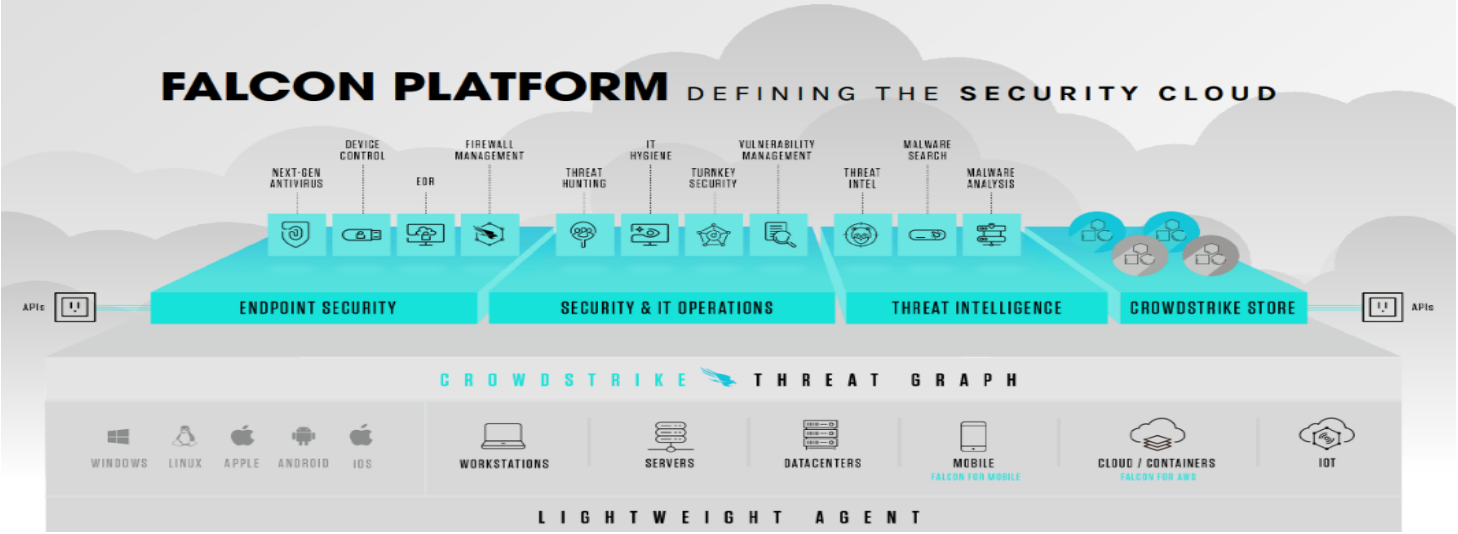
1. next generation antivirus,
2. endpoint detection and response,
3. threat intelligence,
4. threat hunting,
5. IT hygiene and
6. incident response and proactive services.

At its core, Crowdstrike's flagship platform, called ***Falcon***, operates as an endpoint protection service, composed of two key technologies.

1. ***Lightweight Detection Agent:*** This is installed on all endpoint devices, such as computers, laptops, and employee smartphones (any device which has access to a central network). This scalable technology provides effective local detection and prevention capabilities on all devices, while also transmitting data into a larger, cloud-based platform.

2. ***Threat Graph Database:*** This is the second piece of the Falcon system. It collects all data streamed from detection agents on each endpoint and amasses it together in the cloud. Each week, over 3 trillion events are captured. This data is then analyzed using AI and behavioral pattern-matching techniques to detect irregularities and threats. The AI technology gets smarter, as it consumes more data. This constant data analysis allows the defense structure to continuously improve and grow stronger. By analyzing and gathering more and more data, the system can cut-off and detect abnormalities.

We are not technologists and we didn't stay at a Holiday Inn last night. We strive to take a complicated subject matter and dumb it down so our parents can ever understand the subject matter. If we have already confused you and used too much technology-speak, we thought a picture could assist with your understanding.



Protection:

In that Falcon graph, you can see each phone, computer, server endpoint along the bottom. Falcon continuously monitors and protects each device by a single agent. This agent offloads computationally intensive tasks to Crowdstrike's cloud-native Threat Graph, so protection does not interfere with one's daily tasks. This essentially makes the service easily scalable and highly adaptable.

The Threat Graph is able to effectively process three trillion endpoint-related events per week, in real time. In addition, it indexes these events for future use to continuously improve its security. If Threat Graph discovers something "out of the ordinary" in one customer environment, its centralized nature allows all customers to benefit automatically in real time. This type of autonomous monitoring, helps Crowdstrike spot potential attacks across the entire customer base. The company believes that this service, called the Security Cloud, holds the potential to reshape the entire cybersecurity industry.

For Crowdstrike, big data is power. Its two-step approach of separating endpoint agents from complex analysis of large datasets allows the platform to remain lightweight and nimble across a variety of endpoint devices, while still retaining the computational power necessary to detect a wide variety of threats. If a technologist were to create category-defining cloud platforms, they would likely start with Salesforce, for their CRM capabilities. In terms of HR in the cloud, one might pick Workday. When it comes to security in the cloud, we believe Crowdstrike is the clear leader.

Cross Sell:

Once a servicing agreement has been reached, Crowdstrike utilizes a "land-and-expand" sales strategy in order to boost recurring product sales. Once a customer installs the Falcon platform, they are able to register any number of additional cloud-based modules, dependent on the level and type of protection required. Customers have the ability to purchase and deploy additional platforms onto the same agent already present on the endpoint.

Cross-selling is an important aspect of Crowdstrike's business model. One a company begins to understand the power of its Falcon platform, customers begin to use more of its modules. For example, in FY'18, the percentage of subscription customers using 4 or more modules was only 17%. Only 3 years later, this is now 57%. As customers utilize more modules, CrowdStrike earns significantly more revenue and profits. This is benefit of attractive unit economics and scale. By this time next year, CrowdStrike believes that 39% of its subscription customers will be using 5 or more of its cloud modules.

We believe Crowdstrike sells a value proposition based around the ease of adoption, rapid time-to-value, and superior efficacy rates in preventing and stopping threats with its products. The platform is primarily sold through a direct sales team, segmented based on the number of endpoints a customer needs to protect. This strategy mostly relies on existing customer relationships in order to further build its client network, as well as utilizing an existing alliance of technology partners who are able to build applications with data and analytics from the Falcon platform. With an industry-leading 4.9 out of 5 star rating, CrowdStrike reputation speaks for itself, making it an easy sell to potential new clients.

Revenue:

Wall Street seems to be infatuated with revenue growth, and we can certainly understand some aspect of this. The overall market is infatuated with FAANGM (Facebook, Amazon, Apple, Netflix, Google, Microsoft), represented by these firms now exceeding 25% of the S&P 500's valuation. We like to differentiate between companies with just impressive revenue growth, versus those with good sales growth and strong (at least for us) free cash flow. In our opinion, there are too many companies that have great revenue growth, but they cannot or choose not to generate free cash flow. For us, we mandate that our holdings generate and focus on free cash flow.

Goldman research recently reported that Crowdstrike has "doubled its market penetration with an already robust market share" Many sell-side analysts estimate that Crowdstrike is growing at 2x the rate of its fast-growing software peers. The TAM (total addressable market) opportunity for Crowdstrike is large and it continues to expand. The estimated TAM in 2020 is $26.9 billion, and it should experience nearly double-digit growth to $31.9 billion by 2022 (according to numerous sell-side analysts).

CrowdStrike has built an industry-leading brand due to the proven success of its Falcon platform. This allows it to rely on many of its high-profile customers to reach more clients (downstream) and ultimately drive additional revenue. Once a new customer has purchased the core platform, its strategy is to expand the sale to additional existing services. This cross-selling technique allows for potential revenue growth from current customers.

So, we begin our analysis with sales, but intend to dive much deeper into their model. Crowdstrike's superior security platform and sales network have resulted in strong annual top line revenue growth, seeing close to 100% YOY increases in the past 4 years. During the most recent quarter (FY'21, 2nd quarter), Crowdstrike generated nearly $800 million in annual recurring revenue, growing at an annual run rate of 87%. Focusing on annual recurring revenue for a moment, the last 6 quarters of growth have been nothing short of amazing. Starting with the 1st quarter of FY'20, the YoY growth rates have been 114%, 104%, 97%, 92%, 88% and 87%.

93% of this attractive revenue base is subscription revenue, also growing at an impressive year-over-year rate of 89%. This revenue base is not terribly concentrated, as Crowdstrike has 7,230 subscription customers. It is also impressive to look at the last 6 quarters of YoY subscription customers growth. Starting with the 1st quarter of FY'20, the YoY customer count growth has been 105%, 111%, 112%, 116%, 105% and 91%. Doubling their customer counts annual is quite remarkable, especially since these clients generate predictable and sustainable recurring revenue.

For the next few years, we envision Crowdstrike being able to continue to grow at a healthy pace. In fiscal (year-end in January) 2020, Crowdstrike grew revenues 93% year-over-year and generated $481 million of total revenue. We like that 91% of its revenue is from predictable and recurring, subscription-based sources. The sell-side is modeling in $822 million of revenue this fiscal year and $1.1115 billion of revenue next fiscal year. This equates to growth rate of 71% this year and 36% next fiscal year. Clearly, Crowdstrike is still posting impressive top-line growth.

Turning Sales Into Profits:

Crowdstrike's management has laid out a "long-term target model", which calls for various objectives as a percentage of revenue. For example, Crowdstrike's management team is looking for subscription gross margin to be in the 75% to 80% level. It also discusses a target operating margin of 20%, which is wonderful to hear. However, we want to go further down the income statement and focus in on some of the larger expenses.

Specifically, we want to discuss how CrowdStrike might look to take that extraordinary revenue growth and turn it into free cash flow.

We begin with gross profit and CrowdStrike's solid gross margins. Back in FY'17, gross margins were 36%. Over the last three fiscal years, it has improved to 54%, then 65% and then 71% in FY'20. Over the last three fiscal years, Crowdstrike has essentially doubled its gross profit margin. While this type of growth cannot continue forever, we anticipate gross margins will be in the mid-70's next year and into the 80% by FY'22. This is nice to see, but much more to understanding the Crowdstrike model and opportunity.

In terms of generating leverage, CrowdStrike needs to properly manage its operating expenses. The biggest component is S&M (sales and marketing), representing 55% of FY'20 total revenue. On an absolute dollar spend, S&M grew 54% last year. Crowdstrike's management team believes that its S&M spending goal is dramatically lower, as a percentage of total revenue. Over time, management believes that S&M, as a percentage of total sales, can ultimately flatten out in the low-to-mid 30% range. We think this could occur in the next 3 to 4 years.

In addition, R&D (research and development) was 27% of total revenue and it rose by over 50% last fiscal year. Crowdstrike's management team believes that its R&D spending, as a percentage of total revenue, should also be lower. Over time, management believes that R&D, as a percentage of total sales, can ultimately flatten out in the mid-teens to 20% range. This too should occur in the next few years.

The third bucket of expenses is G&A (general and administrative), which was 19% of the top line. Over the next few years, Crowdstrike should be able to leverage their infrastructure and get this into the high-single-digit range. Management believes this can be in the 7% to 9% range, over the next couple of years.

On an absolute dollar level, we fully expect all of these operating expenses to grow from these levels. That growth will fuel Crowdstrike's top line. However, we model significant leverage in these overall costs, as a percentage of total revenue. The company states that these continued, large investments in growth are necessary, in order to capture the growing market opportunity, especially as the need for intelligent cybersecurity solutions continues to expand. It strongly believes that these large fixed costs will ultimately place their platform in a far superior position to its competition, both in customer base, and in product efficacy. We totally agree and this investment has allowed Crowdstrike to post customer subscriptions, annualized recurring revenue, and net retention growth rates of near or over 100% for the past 3 years.

We would anticipate that each of these three buckets continues to shrink, as a percentage of revenue, allowing the company to deliver solid operating margins in the 20% range. We believe that the ultimate operating margins of CrowdStrike could be meaningfully higher than this 20%, except the company remains committed to heavily investing for future growth. This is important to fueling CrowdStrike's impressive revenue growth and we believe that management will prudently weigh the costs of driving this growth.

Now, we will attempt to take revenue less expenses and arrive at free cash flow. For starters, we are pained to say, but there needs to be stock compensation factored into the equation. We are strong believers that stock compensation should be included as a real expense. If they were not worth anything, we would be happy to accept these "worthless" grants from employees. That being said, technology companies are built by key employees that make contributions to a firm, above and beyond what a company can afford to pay them directly in a salary.

Looking at CrowdStrike's Non-GAAP or proforma results, we need to start with a GAAP or accounting loss from operations. From FY'17 to FY'20, this GAAP operating loss grew from $90.6 million, to $131.4 million, to $136.9 million, to $140.1 million. Stock compensation gets added back and it has grown from $2 million in FY'17 to $79.9 million last fiscal year. Surprisingly, there isn't much in terms of amortization of acquired intangible assets to add back, only $0.5 million. In addition, there is a modest lawsuit settlement to consider, which was $1.3 million. If one agrees to adding back stock compensation and 1x legal issues, the non-GAAP loss from operations last fiscal year was $62.6 million. On 148.1 million shares, that equates to a non-GAAP loss per share of $0.42.

To arrive at a reasonable calculation of free cash flow, we take GAAP operating activities and reduce it by purchases of P&E, as well as capitalized software. Using this formula, free cash flow turned positive in the 3rd quarter of FY'20. Starting with that quarter, this adjusted free cash flow calculation has grown from $7 million to $50.7 million in the 4th quarter of FY'20 to $87 million in the 1st quarter of FY'21 to $32.4 million last quarter. Considering there is some seasonality to this business, we will look at the last 6 month average of $60 million and assume a run rate of $240 million. On 148.1 million shares, that would equate to adjusted free cash flow of $1.61 per share. We think this adjusted free cash flow could grow in the 20% to 30% range for the next several years. For example, we envision FY'22 adjusted free cash flow should easily exceed $300 million. On a market capitalization of $32 billion, CrowdStrike trades at roughly a 1% free cash flow yield. Is that a screaming value? No it isn't, but one has to place a premium valuation for a company with this impressive opportunity and top line growth.

Crowdstrike has no long-term debt or redeemable preferred stock, securities outstanding, and holds enough cash to cover its current liabilities twice over. As we just discussed, Crowdstrike has recently turned the page on generating operating cash flow. We believe this demonstrates that the Crowdstrike's current heavy focus on product investments are beginning to bear fruit. The free cash flow will dramatically increase, once the management team believes it can fully leverage the existing model. As of today, the expectations for EBITDA this fiscal year and next year are modest. The Street sits at roughly $50 million of EBITDA this fiscal year and $100 million next. While doubling EBITDA is great, it really is just scratching the surface of profitability. Crowdstrike is at an interesting inflection point. Its revenue growth is extraordinary, but it has not yet become wildly profitable. It generates free cash flow, but the margins have yet to become fully leveraged.

We fully anticipate free cash flow growth exceeding revenue growth for the next several years. Applying a current or forward valuation to this modest level of free cash flow is still difficult, but at least it is not a revenue multiple. We just believe companies using revenue multiples are often firms that simply don't generate any free cash flow, something which history has taught us to be concerned with. At this point in time, CrowdStrike has positioned itself in the top spot of cybersecurity software companies. To remain the industry leader, it needs to re-invest large amounts towards R&D and marketing. This essentially allows it to widen its moat and build higher and higher barriers to entry. In the near future, we believe Crowdstrike will be able to open up the free cash flow spigot, as its margins continue to improve.

Metrics:

As we just talked about, Crowdstrike's revenue growth is impressive and its margins are beginning to climb. It generates free cash flow, but reported earnings are still underwhelming. In order to frame a valuation, we must look forward, to a time where Crowdstrike is more mature and its business becomes leverageable.

At this point, we tend to look towards some of the key metrics we described earlier. We do not focus on that "Rule of 40", but Crowdstrike would be well above that level (revenue growth of 93% and gross profit of 71% in FY'20). From our perspective, this is too rudimentary of a metric. The cross-selling philosophy (discussed earlier) has proven to be a highly successful sales strategy for Crowdstrike. This philosophy allows it to boast a dollar-based net retention rate of customer subscriptions of 124% (as of 1/31/20). Crowdstrike's S&M costs appear to be working, as its CAC payback is excellent. With S&M costs of $76 million (FY'20 4q), gross profit of 77% and net new ARR of $686 million (FY'21 1q), the CAC payback period is only 13.7 months. This means that it takes just over a year for Crowdstrike to recoup its S&M costs from new gross profits. This would put Crowdstrike into the top decile of other software firms, of under 13 months.

Cybersecurity Conclusion:

We hope that this article has helped you better understand the risks that each individual and company faces. There is no "silver bullet" of protection against hackers and cybercriminals. In today's technologically-savvy world, companies need to fully understand that protecting information is paramount.

There needs to be a critical shift in thinking, from the board level on down. Individuals and firms need to be more stringent and have extensive data protection policies. Otherwise, their entire business is at risk. We

believe that it is necessary to have a comprehensive plan and think in terms of not if a breach might occur, but when a breach will occur.

Crowdstrike Conclusion:

We believe that Crowdstrike is ultimately poised for success. With its proven track record of producing effective and modular products, high-profile customer base, and a growing total available market, Crowdstrike looks to be a great long-term investment.

Although its traditional valuation calculation would not be considered a bargain, one needs to understand the potential and future outlook for this business. Crowdstrike dominates a secular growth industry – cybersecurity. It offers its product (i.e. software) to both small and large entities and it should be very scalable. Once management makes the decision to turn the profitability on, we believe the valuation will become much more attractive.

At this point in time, it is still building the foundation for its long-term success. The current price is not attractive (for value investors), but the company does trade similar to its software peers. We believe that Crowdstrike deserves a premium, because its end-market and vertical niche (cybersecurity) is so attractive. Global companies need to focus on security and many still have yet to place enough emphasis on this significant business risk. Over the next few years, we believe many more companies will start to appreciate Crowdstrike's ease-of-use and dominant market positioning. From our perspective, we believe Crowdstrike can deliver long-term value for their clients, as well as us – its shareholders.

Disclaimer

DISCLAIMER:

Firm: Manole Capital Management LLC is a registered investment adviser. The firm is defined to include all accounts managed by Manole Capital Management LLC. **In general:** This disclaimer applies to this document and the verbal or written comments of any person representing it. The information presented is available for client or potential client use only. This summary, which has been furnished on a confidential basis to the recipient, does not constitute an offer of any securities or investment advisory services, which may be made only by means of a private placement memorandum or similar materials which contain a description of material terms and risks. This summary is intended exclusively for the use of the person it has been delivered to by Warren Fisher and it is not to be reproduced or redistributed to any other person without the prior consent of Warren Fisher. **Past Performance:** Past performance generally is not, and should not be construed as, an indication of future results. The information provided should not be relied upon as the basis for making any investment decisions or for selecting The Firm. Past portfolio characteristics are not necessarily indicative of future portfolio characteristics and can be changed. Past strategy allocations are not necessarily indicative of future allocations. Strategy allocations are based on the capital used for the strategy mentioned. This document may contain forward-looking statements and projections that are based on current beliefs and assumptions and on information currently available. **Risk of Loss:** An investment involves a high degree of risk, including the possibility of a total loss thereof. Any investment or strategy managed by The Firm is speculative in nature and there can be no assurance that the investment objective(s) will be achieved. Investors must be prepared to bear the risk of a total loss of their investment. **Distribution:** Manole Capital expressly prohibits any reproduction, in hard copy, electronic or any other form, or any re-distribution of this presentation to any third party without the prior written consent of Manole. This presentation is not intended for distribution to, or use by, any person or entity in any jurisdiction or country where such distribution or use is contrary to local law or regulation. **Additional information:** Prospective investors are urged to carefully read the applicable memorandums in its entirety. All information is believed to be reasonable, but involve risks, uncertainties and assumptions and prospective investors may not put undue reliance on any of these statements. Information provided herein is presented as of December 2015 (unless otherwise noted) and is derived from sources Warren Fisher considers reliable, but it cannot guarantee its complete accuracy. Any information may be changed or updated without notice to the recipient. **Tax, legal or accounting advice:** This presentation is not intended to provide, and should not be relied upon for, accounting, legal or tax advice or investment recommendations. Any statements of the US federal tax consequences contained in this presentation were not intended to be used and cannot be used to avoid penalties under the US Internal Revenue Code or to promote, market or recommend to another party any tax related matters addressed herein.