A Study on Cybersecurity Start-ups:

A Financial Approach to Analyze Industry Trends, Entrepreneurship Ecosystems and Start-up Exits

By

Chi Zhang

B.A., University of Waterloo, 2011

SUBMITTED TO THE MIT SLOAN SCHOOL OF MANAGEMENT IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN MANAGEMENT STUDIES
AT THE MASSACHUSETTS INSTITUTE OF TECHNOLOGY

JUNE 2016

Signature of Author: Signature redacted

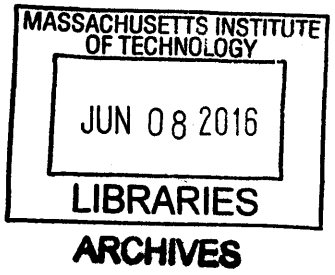
MIT Sloan School of Management
May 6, 2016

Certified By: Signature redacted

Stuart E. Madnick
John Norris Maguire Professor of Information Technologies, MIT Sloan School of Management
And Professor of Engineering Systems, MIT School of Engineering
Thesis Supervisor

Accepted By: Signature redacted

Rodrigo S. Verdi
Assistant Professor of Accounting
Program Director, M.S. in Management Studies Program
MIT Sloan School of Management



[Page intentionally left blank]

A Study on Cybersecurity Startups:

A Financial Approach to Analyze Industry Trends, Entrepreneurship Ecosystems and Start-up Exits

By

Chi Zhang

Submitted to the MIT Sloan School of Management on May 6, 2016
in partial fulfillment of the requirements for the degree of Master of Science in Management Studies

ABSTRACT

Now a multi-billion dollar industry, cybersecurity is becoming one of the most attractive industries for investors today. Despite emerging government involvement for cybersecurity governance and even cybersecurity warfare, private sector still dominates cybersecurity today and will remain the backbone of the industry due to its ubiquitous nature and rapid technological evolution. Consequently, success factors behind cybersecurity entrepreneurship in this industry is a necessary topic to study.

Entrepreneurship has attracted scholars' attention for decades, and especially in the context of cybersecurity, an industry built solely by entrepreneurs thus far, what in particular drives them to success? My studies focus on three aspects of cybersecurity entrepreneurship, and explore how they contribute to entrepreneurial success in cybersecurity. First I begin by examining key characteristics within the cybersecurity industry, and spell out the emerging trends in investments. I then study the ecosystems behind cybersecurity entrepreneurship, studying the effectiveness of government policies and the impact of culture. Finally, I explore cybersecurity start-ups and compare how they are different from the broader Software and Services industry from a financial perspective. The results from this study helps to map out the key distinctions of cybersecurity entrepreneurship and attempts to identify key interests in this area for future study.

Thesis Supervisor: Professor Stuart Madnick
Title: John Norris Maguire Professor of Information Technologies, MIT Sloan School of Management and Professor of Engineering Systems, School of Engineering

[Page intentionally left blank]

Acknowledgement

I would like to express my sincere gratitude to Professor Stuart Madnick for his guidance and continued support. I cannot complete this thesis without his wisdom. His suggestion for me to conduct a study that combines cybersecurity, a hot industry, with entrepreneurship, a hot topic was both an exciting academic process and a unique learning experience.

I would also like to dedicate my gratitude to the (IC) 3 research group: Michael Siegel, Chris Zannetos, Dr. Raphael Yahalom, Michael Coden, Dr. Mohammed Jalali, and Dr. Keman Wang for sharing their expert knowledge and connecting me to crucial resources.

In addition, I would like to thank my interviewees in addition to the abovementioned (IC)3 members: Steven Whittaker (BT), Rob Partridge (BT), Greg Dracon (.406 Ventures), Rick Grinnell (Fairhaven Capital) and Benjamin Howe (AGC Partners) for sharing their industry experience and expertise.

Lastly, I would like to thank my family, friends, and MSMS classmates for their continued love and support. Their encouragement serves as my motivation for continued self-improvements.

[Page intentionally left blank]

A Study on Cybersecurity Start-ups:

Table of Contents

Table of Figures

Table of Tables

Chapter 1. Introduction and Motivation

1.1 Introduction

Since von Neumann's work on self-replication lead to the first computer virus, the Creeper virus[1], viruses and worms began to threaten the security of every member on the flourishing internet. With the evolution of technology, many of the most crucial functions and assets are accessed on the internet today, including personal identification records, bank accounts, and intellectual properties. However, along with the benefits and the convenience the internet brings, it is estimated some 3 billion people use the internet today[2] under continuous threat from anonymous individual hackers to organized government cyber warfare. Today, cyber-attacks not only focus on decapitating your systems, they also focus on stealing information and virtual assets as seen in the TJX[3] case, as well as targeted strike to cause damage physically, as seen in the Stuxnet[4] case. A study conducted by MIT researchers examined highlighted the threat of traditional IT control systems and strategies, and further analyzed their underlying vulnerabilities related to such cases in 2014, and recommended a top down systems thinking approach such as STAMP[5].

Unlike national security, cybersecurity is a brand new area historically explored by primarily corporation until the establishment of United States Cyber Command in 2009. Even then, the cybersecurity is special, since offenders may attack any entity on the internet, regardless of their nature, size, capacity or economic value. While most companies refuse to disclose, U.S. companies saw 160 successful cyber-attacks on a weekly basis[6]. In an early 2015 interview with Inga Beale, the CEO of Lloyds, a British insurance company, estimated that the insurance industry took $2.5B in premiums on policies to protect companies from losses resulting from hacks, and she estimates cyber-attacks cost as much as $400B a year[7]. It begs the question, who should we entrust to combat this problem?

Part of the answer is, despite internet's military origin, almost all cybersecurity providers today are from the private sector. After decades of development, cybersecurity remains a hot industry today and attracts a lot of investments. It is estimated that in 2015, cybersecurity becomes a $75B[8] industry, and investments in the industry has grown from $1.1B to $3.8B from 2011 to 2015[9]. In addition to the well-known giants in cybersecurity such as Kaspersky Lab and McAfee,

---

[1] (Thomas Chen, 2004)
[2] (International Telecommunications Union, 2016)
[3] (CERT, Carnegie Mellon University, n.d.)
[4] (Zetter, 2014)
[5] (Nourian & Madnick, 2014)
[6] (Walters, 2015)
[7] (Gandel, 2015)
[8] (Press, 2015)
[9] (CBInsights, 2016)

a few notable cybersecurity companies has gone public in the last few years, including FireEye, Imperva, and Barracuda Networks.

1.2 Motivations

Cybersecurity industry is indeed a unique industry. A unique factor of cybersecurity companies that are frequently discussed is that they often start from solving a problem. Eugene Kaspersky started in anti-virus in 1997[10], before going on to establish a multinational cybersecurity corporation. However, not many other cybersecurity companies are as lucky as Kaspersky Labs. The impression of cybersecurity start-ups are that they often choose to exit through mergers and acquisitions (M&A). Consider for instance, there are 297 cybersecurity M&A[11] deals in year 2015, but only a mere 3 cybersecurity firms that went on for an initial public offering (IPO)[12] in the same year. One often notice that cybersecurity starts, compared to other tech start-ups, generally sell "earlier", meaning the cybersecurity start-ups either have a comparatively shorter life span or exit at a relatively lower valuation. But is this perception what's really happening?

Another impression of cybersecurity firms is that it is more difficult to sell their products, since their solutions may not be easily understandable. Naturally, cybersecurity companies often employ more sales engineers than other tech firms. But is this impression true?

In addition, when talking about cybersecurity practices and talents, one often think that cybersecurity is a subcategory of the broader IT community. Especially when recruiting, although requiring very unique skill sets, in the eyes of a job seeker, most cybersecurity firms do not differ from general IT firms. There is currently no defined pathway to become a cybersecurity specialist, they often start from a general IT student, and adapt to undetermined career paths solving different security problems. Fortunately, some schools are recognizing this huge demand, and are offering cybersecurity certificates, for instance University of Maryland University College, and Harvard Extension School. For long-term sustainable growth, any industry will benefit from a mature model to develop supply of talents. What does this mean for cybersecurity?

Recently, some notice a "funding drought" in cybersecurity entrepreneurship. For instance, a Reuters article claims that "the U.S. cyber security industry, once one of the hottest targets for venture capitalists, is now grappling with a funding slump that has forced some startups to sell themselves or cut spending"[13]. The notion is that cybersecurity startups are "over-hyped", thus it is important to understand not only the key trends of the cybersecurity industry, but also the

[10] (Bradley, 2013)
[11] (AGC Partners, 2016)
[12] (AGC Partners, 2016)
[13] (Finkle, 2016)

dynamics of cybersecurity start-ups, and what implications we can draw to verify this hypothesis of a "funding drought" and what start-ups could do to cope with it.

The end goal of this thesis is to explore cybersecurity entrepreneurship in a systematic fashion, by analyzing the industry specific factors, and potentially come up with a long-term, sustainable way to facilitate cybersecurity entrepreneurship.

1.3 Methodology

This thesis will explore the main difference between start-ups in cybersecurity industry and other industries. There are three main focuses of the thesis:

1. Cybersecurity Industry: mainly focuses on how and why the cybersecurity industry is different from other industries.
2. Entrepreneurship Ecosystems: explores how the ecosystems affect cybersecurity entrepreneurship, namely government policies, and culture.
3. Cybersecurity Entrepreneurship: discusses from a finance point of view, how the cybersecurity start-ups are unique when compared against other tech start-ups.

Beginning with exploring the unique characteristics of the cybersecurity industry, this thesis focuses on secondary research to identify the different categories of cybersecurity start-ups and upcoming recent trends. The next section will discuss the cybersecurity ecosystem, focusing on three distinct countries: the U.S., Israel, and China to study how entrepreneurship ecosystem impacts cybersecurity. Finally, this thesis introduces characteristics of cybersecurity start-ups, specifically, how they are different from the broader information technology industry.

1.3.1 Literature Review

To systematically study how cybersecurity start-ups are different from traditional IT start-ups, it is important to consider the existing tools and frameworks. Professor Edward Roberts at MIT Sloan was one of the pioneers in exploring entrepreneurial success factors. He categorized entrepreneurial success factors for technology firms into pre-founding, at founding, and post-founding. The framework Prof. Roberts developed and documented in the paper "The Success of High-Technology Firms: Early Technological and Marketing Influences"[14] are listed as below:

Pre-Founding:

- Family Background
- Education
- Age and Work Experience: technical, sales, management
- Personality and Motivations

[14] (Roberts, 1992)

At Founding:

- Technological Base
  - Degrees of Technology Transfer from source organization
  - Product Orientation
- Financial Base

Post Founding:

- Marketing Orientation
  - Market Interactions
  - Marketing organization and practices
- Managerial Orientation
  - Managerial skills
  - Problem Focus
  - Acquisitions
- Financing

After examining these factors with regards to how the companies perform, Prof. Roberts concludes that technology transfer is a great indication of success, partially because a lot of high-tech entrepreneurship started out from a lab, and the access to capital intensive facilities without actual investments helped them reduce financial risk of starting a firm. In addition, most successful companies tend to move away from the government dominant markets, while sales experience was important for the founder and the firms' performance. Furthermore, he noticed companies that are aware of their competition outperform the ones who are not.

Are cybersecurity companies the same? When applying entrepreneurial success factors to examine specific cases, Prof. Roberts used primarily sales growth to measure successfulness. While Prof. Roberts provided a great guiding framework for contributing personal factors to entrepreneurial success, this thesis will dedicate the largely unexplored industry specific factors for cybersecurity entrepreneurship from a more financial approach. While many of the personal factors are difficult to analyze because of data collection, by evaluating market performances of cybersecurity start-ups from a financial angle, this thesis aims to complement prior studies from an industry specific perspective.

We often hear about the prominence of Israeli start-ups in this area, is it indeed true? If it is true that Israelis produce more cybersecurity start-ups, what can we conclude from their success to help cybersecurity entrepreneurs in other countries to succeed?

1.3.2 Interviewee Background

To gain further understanding regarding both the industry and the entrepreneurship process, several interviews were conducted with the distinction of cybersecurity industry in mind. In addition to numbers and statistics, it was important to learn from the key players with first-hand experience in the cybersecurity industry to understand how it became a unique industry. The mere fact that entrepreneurs started companies to address cybersecurity problems was fascinating, why did they choose cybersecurity over something else? To better understand the industry practices and experiences, interviewees were selected from different backgrounds: entrepreneurs, academics, institutional users and investors.

Dr. Raphael Yahalom (Interview Date: Feb. 16th, 2016)

Dr. Yahalom is a research affiliate in management science at MIT Sloan. His research focuses on "emerging solutions that will reshape the cybersecurity industry and on new evidence-based predictive methods analyzing and prioritizing cyber-security risks, and for measuring cyber-security progress and business-value. [15]"

Dr. Yahalom possesses a decorated portfolio of professional experiences. He was an entrepreneur, the co-founder of Onaro, He is also the developer of "*The Yahalom Protocol*" and was invited to research at multiple institutions including AT&T Bell labs, Cambridge University Newton Institute, and Cornell University. Dr. Yahalom received his PhD in Computer Science from Cambridge University BSc in Electrical Engineering/Computer Engineering from the Technion[16].

Chris Zannetos (Interview Date: February 17th, 2016)

Mr. Christopher Zannetos is a research affiliate of management science in MIT Sloan School of Management, a member of the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (IC)3. His work focuses on security and risk management for both the critical physical and electronic infrastructure. He was the co-founder & CEO of Courion Corporation, a multi-national identity & access management software company. Mr. Zannetos received both Bachelor and Master degrees from MIT.

Steve Whittaker (Interview Date: March 8th, 2016)

Mr. Steven Whittaker is the head of strategic U.S. University Research Partnership at British Telecom. His remarkable career as the MIT visiting scientist representing BT has started thirty-one years ago, and he has been monitoring the technological development since then.

Rob Partridge (Interview Date: March 8th, 2016)

---

[15] (Yahalom, n.d.)
[16] (Yahalom, n.d.)

Mr. Robert Partridge serves as the head of the British Telecom Security Academy, a learning and development function he has created from scratch. He is responsible for raising cybersecurity awareness for everyone in British Telecom (BT) and is dedicated to change unsafe behaviors within BT. In addition to learning and development, Mr. Partridge also is responsible for creating a pipeline of talent to sustain safety and security in the future. Prior to the creation of BT Security Academy, Mr. Partridge has been with BT for many years in the learning and development function.

Greg Dracon (Interview Date: March 9th, 2016)

Mr. Dracon has been an entrepreneur and an investor, with long term expertise in the cybersecurity industry. He is currently a partner at .406 ventures, focusing his investments on cybersecurity and other IT related start-ups.

Rick Grinnell (Interview Date: Apr. 15th, 2016)

Mr. Grinnell is the managing partner at Fairhaven Capital Partners. He possesses rich experience in venture capital investments, particularly in the cybersecurity industry. He is involved in the founding of Resilient Systems, a company that has been recently acquired by IBM.

Chapter 2. Characteristics of Cybersecurity Industry

2.1 Different Categories of Cybersecurity Start-ups

Cybersecurity industry is traditionally viewed as a part of the broader IT industry. After decades of evolution, one can argue that cybersecurity industry is not only a part of the broader IT industry, but also an extension to the IT industry. When a large operating system provider like Microsoft provides services to billions of PC users worldwide, cyber threats are inevitable. Similarly, when large cloud computing companies such as Amazon provide cloud computing capabilities, data is vulnerable. Because of the ubiquitous nature of cybersecurity, it also includes services that provide data analytics or algorithms for physical security and threat detection. Mahendra Ramsinghani, the founder of cybersecurity seed round investment firm Secure Octane describes cybersecurity industry as "a lot of startups/solutions are niche offerings. There is no "one-size-fits-all" security platform — it's a mind-numbingly fragmented market". He is quite correct in his claim. To understand exactly how fragmented cybersecurity industry really is, it is important to categorize the industry, and we can do so by dividing the industry by their security types, solution types, and service types. In terms of industry categorization, according to MarketsandMarkets[17] Analysis, we can divide categorize the industry in Table 2-1:

[17] (MarketsandMarkets, 2016)

Table 2-1: Cybersecurity Industry Categorization

By Security Types	By Solution	By Service
• Network security	• Identity and Access Management (IAM)	• Consulting
• Endpoint security	• Risk and compliance management	• Design and integration
• Application security	• Encryption	• Risk and threat assessment
• Content security	• Data loss prevention	• Managed security services
• Wireless security	• Unified threat management	• Training and education
• Cloud security	• Firewall	
	• Antivirus and antimalware	
	• IDS/IPS	
	• SIEM	
	• Disaster recovery	
	• DDOS mitigation	
	• Whitelisting	
	• Others	

Categorizing the industry by security types, solution, and service helps us to understand of cybersecurity industry in a more structured way. However, they can create extra layers of complexity when a firm combines multiple sub-categories in their product/service offering. For instance, a firm addressing data loss prevention has multiple ways to provide services, they may choose to do design and integration, or they can also choose to provide consulting services. In addition, in a sub-category of cybersecurity, there can be divided further into finer categories – Identity and Access Management (IAM) for example, MarketsandMarkets Analysis[18] divides it into six components: provisioning, directory technologies, single sign on (SSO), password management, advanced authentication, and audit, compliance and governance. Among these six components, four categories of players are further categorized:

1. Solution developers: CA Technologies, Microsoft, Oracle, IBM
2. Resellers/channel partners: CTI, Hub city media, Aurion pro sena, IC Synergy
3. IAM-as-a-service providers: Amazon web services, Okta, Courion
4. Professional service providers: Accenture, TCS, CGI, HP

[18] (MarketsandMarkets, 2016)

In addition to fragmentation, complications arise when considering verticals, geographic regions, and basis of deployment. Furthermore, many of the largest players are not exclusively in the IAM business. Consider Microsoft for instance, in addition to providing IAM services, they also provide other cybersecurity products and services including but not limited to: anti-virus and anti-malware services, configuration & log management, and endpoint management. This is also true for other segments within the cybersecurity industry.

The fragmented nature of cybersecurity industry and the prominence of large and complex cybersecurity providers effectively tell the story that today's cybersecurity provider needs to be sophisticated enough in terms of both technical capabilities and financial resources to cope with increasingly complicated threats. When considering the rate of technological advancement of cyber threats, not even larger institutions can solve all the emerging problems. They thus purchase smaller start-ups to acquire their capabilities, which provides great incentive and exit opportunities for cybersecurity entrepreneurs. And later when we examine exit characteristics, we will further discuss the growing need for service providers to acquire smaller companies.

The Ponemon Institute has conducted a survey that included over 1,000 cybersecurity professionals in North America, Europe and EMEA regions, and according to the "percentage change in importance of enabling technologies" results listed in Figure 2-1 below, there are distinct trends in the perception of these cybersecurity professionals with regards to promising areas in cybersecurity. The number in the graph indicates the percentage change in importance rating for 25 technologies. Respondents rate data encryption at the utmost importance, with encryption for data at rest showing a 24% increase in importance ratings, while encryption for data in motion sees an increase of 19%. Data analytics, SIEM, and forensics are not far from the top, seeing roughly 20% increase in the respondents' importance rating. These ratings reflect the industry's perception to the critical enabling technologies, and thus to some extend reflect real demands in the current security world.

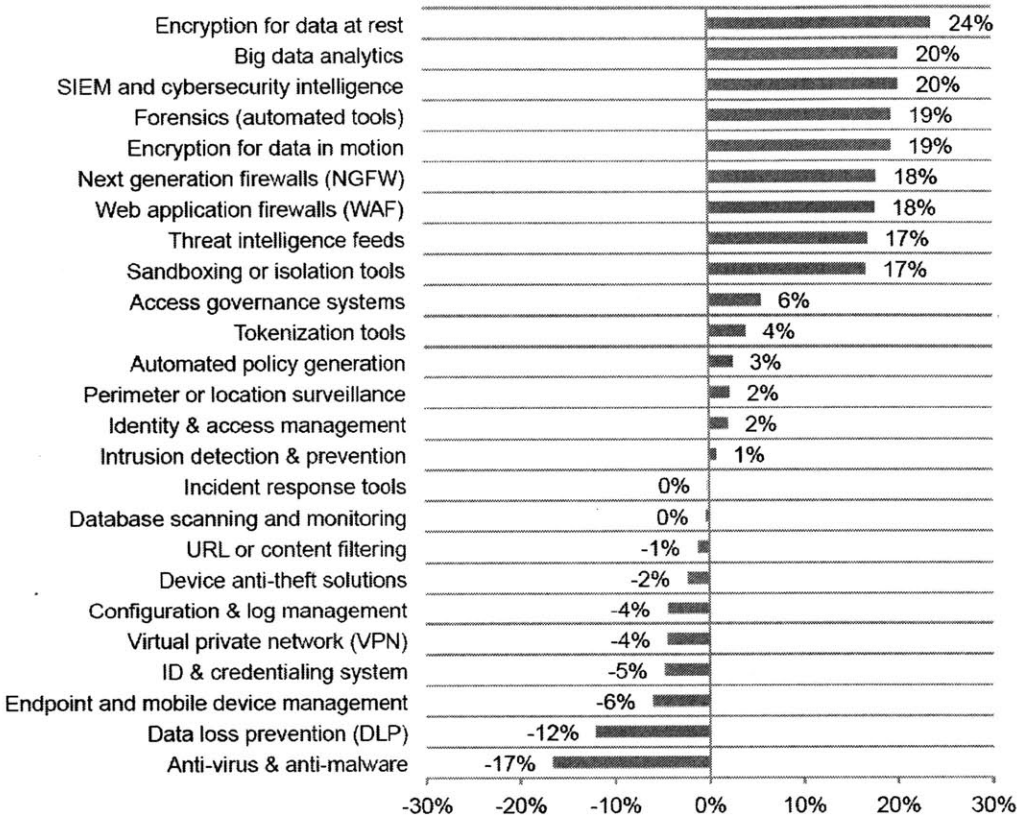


Figure 2-1: Percentage change in importance of enabling security technologies[19]

An Interesting pattern we also observe is that Anti-virus & anti-malware has dropped significantly in importance rating. Combining this information with the gainers, specifically encryption, big data analytics, intelligence, and forensics, we can clearly observe a shift from reactive approaches, like anti-malware to proactive approaches, like secure engineering. In an interview, Dr. Yahalom stresses that the cybersecurity industry is backward looking in nature, solving yesterday's problem with today's technology. But the threats are forward looking, therefore there is a mismatch of intentions and resources. As a result, he believes that when assessing the potential of a cybersecurity firm, it is less important to look at what their current solution is, but more important to assess the founding team members.

2.2 Stock Market Performances

When looking at the differences in cybersecurity firms and general IT firms, it is important to consider what the investor thinks of their value. Specifically, by looking at the relative valuation of cybersecurity companies, we can understand how the market perceives the value of cybersecurity firms. The financial market is a complicated world, whereby firms differ

[19] (Ponemon Institute LLC, 2015)

dramatically in not only valuation price but also valuation method. For instance, to value public companies, the price-earnings ratio (P/E) is a great tool. P/E measures how much investors are willing to pay for each dollar of a firm's earnings, and a high P/E indicates a firm is associated with high value. This perceived high value often indicates investor's expectation for the firm's future growth. As a result, a comparison of P/E ratio between cybersecurity firms and other tech firms tells us how investors value cybersecurity firms versus the rest of the IT firms. Meanwhile, when valuing non-public firms, especially those early stage firms, P/E ratio is not a good valuation metric, since it is entirely possible that a firm with great growth potential in the future does not make a positive profit at the current stage (i.e. Amazon). Consequently, when evaluating the non-public companies, we look at a comparable multiple called enterprise value over revenue (EV/R).

The world's first cybersecurity exchange traded fund (ETF), HACK, provides a great benchmark that serves as the foundation of our comparison. As at Feb. 26, 2016, HACK companies average 25.9x[20] PE, significantly higher than Nasdaq 100's 20.68[21]. This phenomenon indicates that cybersecurity public companies are expected to grow faster than the rest of IT firms, and are generally more "expensive", as investors pay more for a dollar of the firm's income compared to the rest of the IT firms.

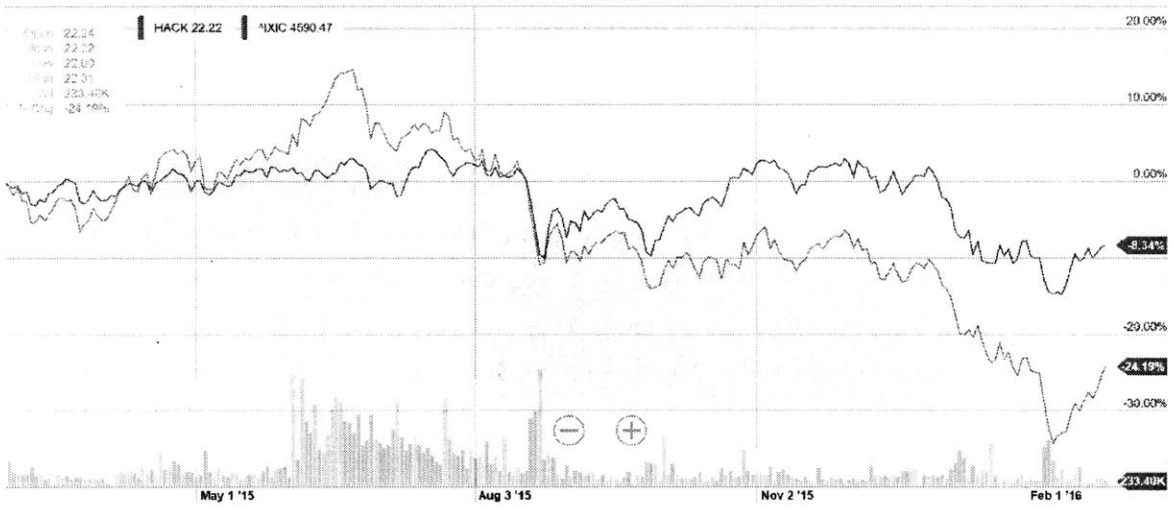


Figure 2-2 Returns Comparison[22]

Now that we conclude cybersecurity companies are valued higher than other IT companies in general, does it also mean they generate superior returns than their peers? To compare, Figure 2-2 quoted from Yahoo Finance provides comparison between the HACK ETF's performance and the NASDAQ composite. The line in red in this time-series chart indicates the performance of NASDAQ composite (IXIC), while the line in blue marks HACK's performance. We can see

[20] (CNN Money, 2016)
[21] (WSJ, 2016)
[22] (Yahoo, 2016)

clearly that between Q2 and Q3 2015, HACK outperformed NASDAQ composite, and ever since Q3 205, HACK has been noticeably underperforming. This trend suggests that cybersecurity stocks are much more volatile than other tech stocks, thus more risky for secondary-market investors. Meanwhile, the performance of HACK also indicates that cybersecurity stocks are in general cyclical, meaning their performance is better during boom periods and worse during recessions.

Assuming the conclusion that cybersecurity companies are more volatile is valid, a possible explanation for the valuation observation is that these firms are difficult to value. Cybersecurity product and services pricing largely depend on an event not occurring, bearing resembling similarities to the insurance industry. However, the backward looking nature for actuarial scientists is not exactly applicable to cybersecurity products and services, as it is both difficult to value the cyber capabilities provided by cybersecurity products and services, and the likelihood of them being breached within a given time period.

There may be many reasons that contribute to this phenomenon. Before we get into the discussion of whether cybersecurity firms are undervalued now (or overvalued previously), one needs to note that while HACK is a dedicated cybersecurity ETF, there has been question in their stock selection since it is actively managed. For instance, 4.47% of HACK's[23] total assets are invested in Cisco Systems INC as of February 27th, 2016, and Cisco is generally considered an IT infrastructure company rather than a cybersecurity company. In addition, the trading prices of these firms are largely affected by market sentiments and investors' perceived value of a cybersecurity firm, hence may defer from their actual value. An explanation may be that these public cybersecurity firms are simply overvalued in the past few years because of market conditions. It is difficult to separate the influence of market cycles on secondary market valuations, and the fact that most cybersecurity firms have not been public for too long adds extra difficulty to draw any reasonable conclusion based on their secondary market performance. Consequently, we can only conclude that under current market conditions, the HACK index is more volatile than NASDAQ 100 index, but the exact reason behind their volatility requires further studies.

2.3 Recent Trends

Unlike those in the more mature industries, start-ups in cybersecurity must adapt to more rapidly changing trends to keep themselves on par with the threats. Interviewee Rick Grinnell specifically noted that cybersecurity firms should generally see a higher "technology turnover", since old defense technology gets outdated very fast. Through primary and secondary research, the following trends are identified in the context of 2016 cybersecurity industry.

[23] (Pure Funds, 2016)

2.3.1 The Rising Threats of Nation State Attackers

Ponemon Institute's study identified that cybersecurity leaders perceive that there will be significant increase in the threat of cyber-attack from nation state attackers[24]. Their study in the form of surveys covering 1,006 cybersecurity leaders in different organizations across the U.S., U.K./Europe, and MENA identifies the nation state attackers to have the largest increase of perceived "security risk rating", followed by "cyber warfare or cyber terrorism", "breaches involving high-value information", and "stealth and sophistication of cyber attackers".

Although this part of the study merely collects and analyze the information from the cybersecurity professionals and leaders with respect to their perceived threats. The Obama administration has "in recent years accused China's companies of benefiting from billions of dollars' worth of intellectual property stolen from the networks of U.S. firms."[25] This issue becomes increasingly interesting when the President of China, Xi Jinping, reportedly promised during a visit that China will not "conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[26]

One implication of this potential threat is that, while there are many security capabilities out there, there are even more vulnerabilities. Rarely any company can match the resources and the power behind a nation state attacker, since the complexity of cyber warfare capabilities behind a nation state attacker is far ahead of the commercial world. The Ukrainian grid attack is a great example, a carefully coordinated attack using a variety of simple techniques to conduct "a first-of-its-kind confirmed cyber-warfare attack affecting civilians"[27]. The attack is reported by CNN in the following manner:

"(The attack) involved a team of sophisticated hackers who attacked six different power companies at the same time, according to the U.S. officials. Destructive malware wrecked computers and wiped out sensitive control systems for parts of the Ukraine power grid, making it more difficult for technicians to restore power."[28]

The attack left 103 cities and towns[29] powerless during the middle of a cold December, causing in tremendous civilian damages, yet the offenders remain "unidentified" and unscathed.

In addition to the unrivaled technical capabilities, nation state attackers also have other weapons to penetrate a cyber defense: through physical means such as espionage or through

---

[24] (Ponemon Institute LLC, 2015)
[25] (Risen, 2015)
[26] (White House Office of the Press Secretary, 2015)
[27] (Perez, 2016)
[28] (Perez, 2016)
[29] (Perez, 2016)

regulatory actions. And they are generally equally hard to identify. Even today, the attackers behind the Stuxnet attack still remain unidentified according to official accounts. Even if one were to identify the nation state attackers, there are very few things a civil organization can do against them. Furthermore, if the nation state attacker steal trade secrets to benefit their own companies to compete, the outcome is devastatingly dis-incentivizing for entrepreneurship and innovation.

Fortunately, many nations are starting to recognize cybersecurity as a part of national security. In 2015, President Obama recognizes in the National Security Strategy "the importance of cybersecurity across the elements of national power"[30]. Consequently, cyber-deterrence emerges as a popular topic for political scientist and the effectiveness of cyber-deterrence, among other solutions to address nation state attackers, will be interesting to follow.

2.3.2 Emerging Risks from Internet of Things

The recent rise of smart devices and Internet of Things (IoT) is another top concern for cybersecurity professionals. When we connect new devices to the internet, we effectively open new doors for attackers to penetrate. On the internet, when connecting multiple devices, we suddenly increase our exposure to the same threat exponentially.

In a 2015 study, Hewlett Packard identified numerous ways that IoT can present major cyber-threats[31]:

- Privacy concerns
- Insufficient authentication and authorization
- Insecure web interface
- Lack of transport encryption
- Insecure software and firmware

Interviewee Chris Zannetos added that security is often a point solution that becomes a part of other products, while the cybersecurity firms are narrowly focused. For the offenders however, there are many attack vectors, this increases the complexity of security systems and creates a mismatch of expertise and resources. Furthermore, Chris mentions that cybersecurity is potentially more complex yet least understood than any other IT Industry, because of its problem solving nature and threats' ubiquity. This may consequently lead to more difficult proof of concept, and thus higher need for sales engineers.

These concerns, along with the ubiquitous nature of cyber threats, affect every company in pursing the IoT concepts. Privacy concerns for instance, are reflected in the Ashley Madison

[30] (Newmeyer, 2015)
[31] (Hewlett Packard, 2015)

attack, the aftermath sent Ashley Madison into a half billion dollar law suit[32] with even bigger potential damages to its reputation. To address some of the concerns, WhatsApp for example, recently announced their plan to end-to-end encryption[33] so that a stolen chat log cannot be read aside from the intended user. IoT companies will inevitably recognize the importance of cybersecurity, and the real question now is how they will deal with it.

2.3.3 Increasing Uses of Cyber Capabilities in Physical Security

One of the hottest topics in the IT industry back in 2014 was big data. From consumer patterns to industry growth trends, from financial securities to targeted ads, it appeared as if big data can answer every question ever asked. Whether big data can really answer every question is still in doubt, but big data has certainly helped the security world by providing threat identification and detection capabilities.

A rising start-up in Israel, Windward, is providing such capabilities to the maritime world. They are a company that focuses in maritime data intelligence, and provides their customers with visibility, patterns and threat detection[34]. Starting out in data analytics in 2010, Windward grew rapidly and attracted many well-known investors, including the chief executive of Reuters Tom Glocer, Horizon Ventures, and General David Petraeus. Their ability to attract investors shows how the impact of bringing cyber capabilities into physical security is recognized not only by the clients, but also investors.

There are many companies like Windward, providing physical security with cyber capabilities. Some of them are not new, for example the companies offering CCTV cameras. However, it is important to keep in mind that these companies are also potential targets of cyber-attack. In case of breach, these companies expose the civilians to even greater potential damages, since they are generally equipped with superior cyber capabilities. How they cope with cyber threats themselves will be an on-going concern.

2.3.4 Over-crowded Cybersecurity Financing Market

As shown in Figure 2-2, cybersecurity financing volume exploded in 2014, and M&A volume exploded in 2015.

[32] (BBC, 2015)
[33] (WhatsApp, 2016)
[34] (Windward, 2016)

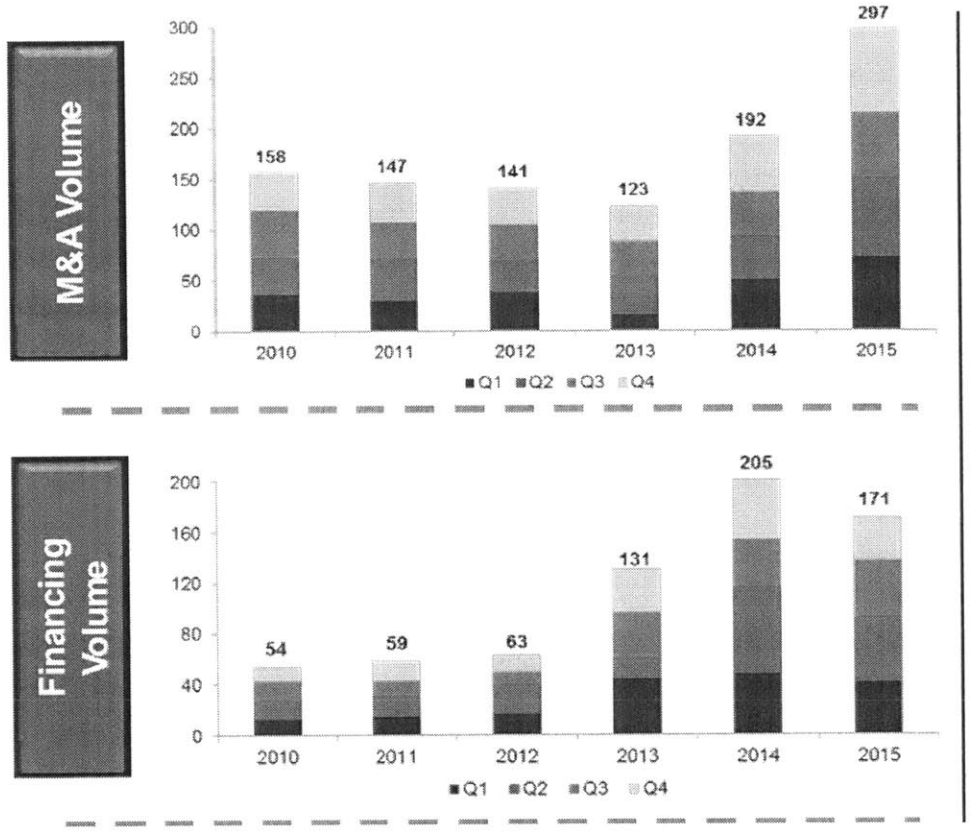


Figure 2-3: Cybersecurity Investment Trends[35]

Interviewee Greg Dracon, a partner at .406 Ventures discloses that when he raised his last fund several years ago, investors were questioning his investment plan to allocate roughly a third of the portfolio in cybersecurity. When he raised another fund recently, investors no longer question the validity of portfolio allocation in cybersecurity. From fringe to mainstream, the explosion of cybersecurity investments is a clear indication that a wave of great cybersecurity start-ups is incoming. Whether they are truly innovative and/or will add a diverse range of weapons into the security arsenal still remains in doubt. Interviewee Dr. Raphael Yahalom echoed the views from the previous Reuters article in the notion of "over-crowdedness" of cybersecurity entrepreneurship. Dr. Yahalom believes that the entire cybersecurity industry is "backward looking" in nature, and is focused on "solving yesterday's problem". At the same time, he also believes that while many of the cybersecurity firms are trying to solve problems, they are often too specific in their approach, thus not scalable. From Figure 2-3, we can notice that the financing volume for cybersecurity start-ups peaked in 2014, and the M&A volume rose dramatically in the subsequent year. If our interviewees are correct in their opinion that cybersecurity entrepreneurship ecosystem is overcrowded, it is entirely possible that we observe a sharp decline in the cybersecurity M&A volume for year 2016. Consequently, business model and exit options

[35] (AGC Partners, 2016)

become a larger concern for both entrepreneurs and investors. Especially for entrepreneurs, they need to stay wise with their capital consumption, or the "burn rate", and make sure they plan ahead for every funding event that lead to a potential exit. When considering exits, they must also be focused and stay realistic.

Chapter 3. Entrepreneurship Ecosystems

3.1 Impact of Political Factors on Cybersecurity Entrepreneurship

In terms of political structure, the U.S., Israel, and China are among the most differentiated instances in the world. In addition to the obvious divide between the civil law and common law systems, the U.S. has followed a "small government" and "free market economy" ideology, and has carried the ideology to internet governance, while governments in the other two countries are much more controlling. In addition to political structures and policies, the influence of military and other government agencies/initiatives are also discussed in this section.

3.1.1 Cybersecurity Ecosystem in the U.S.

While many may view the U.S. cybersecurity ecosystem as a "self-regulated" free market system, the U.S. government has been involved in many fronts of the cybersecurity initiatives, and is one of the first nations to establish a dedicated cyber command. In terms of cybersecurity strategy, the U.S. government has established the following five priorities[36]:

1. Protecting the country's critical infrastructure — our most important information systems — from cyber threats.
2. Improving our ability to identify and report cyber incidents so that we can respond in a timely manner.
3. Engaging with international partners to promote internet freedom and build support for an open, interoperable, secure, and reliable cyberspace.
4. Securing federal networks by setting clear security targets and holding agencies accountable for meeting those targets.
5. Shaping a cyber-savvy workforce and moving beyond passwords in partnership with the private sector.

Since 2011, President Obama has signed four executive orders regarding cybersecurity[37]:

- Presidential Policy Directive 28 (PPD-28) "Signals Intelligence Activities," 2014
- Executive Order (E.o.) 13636 "Improving Critical Infrastructure Cybersecurity," 2013
- Presidential Policy Directive 21 (PPD-21) "Critical Infrastructure Security and Resilience," 2013

[36] (The White House, 2016)
[37] (The White House, 2016)

- Presidential Policy Directive 8 (PPD-8) "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," 2011

These orders were then executed with great urgency. For example, after the establishment of critical infrastructure cybersecurity order, the North American Electric Reliability Corporation (NERC) released a series of Critical Infrastructure Protection (CIP) standards. The NERC CIP v5 that was passed on September 22nd, 2013 remained the most recent version. The NERC CIP v5 represented processes for mitigating cyber risks in "bulk power systems"[38], and the majority of the standards would come into effect after 2016.

The policies and standards are well established, but their effectiveness still needs to be tested. To test the effectiveness of these policies and standards in a "self-regulated" free market with respect to financially observable patterns, an initial hypothesis would be "regulations and standards impact cybersecurity investments". The definition of "investments" is further defined as the mergers & acquisition (M&A) volume, in terms of M&A occurrences. If the hypothesis is worth testing, then there must be an observable pattern of increases in M&A volume after the NERC CIP v5 announcement date, compared to before its release. From the data provided by AGC Partners' Security Market Update 2016, the first test results are included in Figure 3-1:

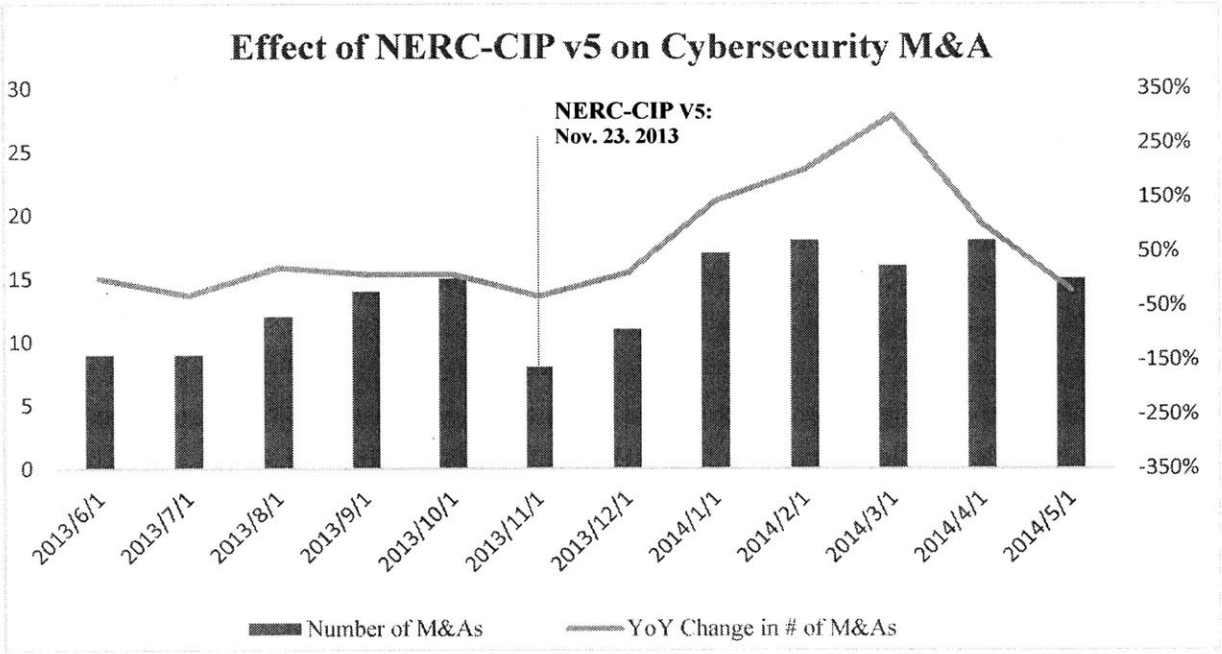


Figure 3-1: Effect of NERC CIP v5 on Cybersecurity M&A

We can observe that while the volume of cybersecurity M&A has not seen a significant increase starting November, 2013, the year over year (YoY) change of M&A volume has

[38] (NERC, 2014)

experienced an obvious increase that lasted four months, peaked in March, 2014. There may exist several reasons behind the observed effect of NERC-CIP v5. Intuitively, following a required standard that will be implemented in three years, large companies that will be affected by these standards will naturally demand such capabilities. These large companies consequently engage in M&A activities to acquire technical capabilities. Interviewee Chris Zannetos interprets such a change from the other side, he believes that such M&A transactions are more common to the capability/service providers, such as FireEye, Cisco, and Microsoft. They are acquiring in anticipation to the market demand, and have decided to utilize external mergers instead of internal development for the necessary capabilities. Regardless of whether it is the result of an end user originated acquisition or a service provider originated acquisition, it is reasonable to assume that these acquisition are done to acquire technology, and thus in this case, external acquisitions are preferred to internal R&D. This phenomenon is further echoed by Interviewee Steven Whittaker. Mr. Whittaker mentions from a large organization's perspective, that when an organization purchases security solutions, it generally prefers a large vender with a consolidated solution, a one-stop-shop. This happens both for convenience reasons and for security reasons, since usually larger organizations appear as more trustworthy partners to clients. Consequently, large organizations need to continue to integrate more technical capabilities to stay competitive in the rapidly changing industry.

If the above hypothesis held, then we would be able to conclude that despite "free market" style of governance, cybersecurity policies are still powerful and effective, and they indeed shape market behavior. As a result, the U.S. government will need to not only pay attention to the national security aspects of policy and standard setting, but also take into consideration the reaction of the industry and capital markets, especially considering the impact of a hypothetical case of breach in a NERC-CIP v5 compliant critical infrastructure system in the future. It certainly adds another layer of responsibility and complication into future cybersecurity policies.

However, statistics shown in *Figure 2-3* is far from the true picture. The biggest limitation of the analysis is that while it takes a look at the announcement of NERC-CIP v5, it does not control for other variables, such as competing policies and standards. Similarly, it does not take into account other socio-economic factors during the same period of time, for instance the possibility of capital flow into IT companies around a period of high NASDAQ valuations. Another problem with the analysis is that because of the limited data collection, it only accounts for the year over year change from 2012 – 2013 to 2013 – 2014. The small range of data collection ine entrepreneurial failure in the finan

3.1.2 Cybersecurity System in Israel

Israel is another nation that is very successful in cybersecurity industry. In addition to the famous entrepreneurship ecosystem, Israel also attracted numerous large companies to establish cyber R&D centers in Israel. Examples include Microsoft, Amdocs, and Intel. Opposite to the U.S., Israel adopts a much more government led approach to the cybersecurity industry. Although they do not have a published version of cybersecurity policy like the U.S., research analyst suggests that their national cybersecurity is organized around the following four pillars[39]:

1. *Support for a national cyber defense vision at the highest levels of national leadership*
2. *Continuous upgrade of IDF's cyber defensive and offensive capabilities, as in the unit 8200*
3. *Israel's cutting-edge R&D programs for boosting both civilian and dual-use cyber capabilities*
4. *The development of a unique, comprehensive national cyber ecosystem*

Israeli government does not only lead the policies and standards, but are also directly involved in many aspects of the ecosystem. The Israeli government leads both public and private initiatives. According to Michael McNerney, former Cyber Policy Advisor to the US Secretary of Defense:

"*Israel is smart to focus on a collective and participatory approach to online security because the inter-connectedness of online systems and proliferation of mobile devices make every individual a potential point for cyber-breach.*"[40]

When the Israeli government supports major IT vendors to establish research facilities[41] in Israel, the government also led VC initiative, the "Yozma", invested $100 million to create 10 VC funds in the 1990s and promised to wave double taxation for foreign funds[42]. It is no wonder why Israel has become the number two cybersecurity exporter, behind the U.S. In 2013 alone, Israel accounted for $3 billion in cybersecurity export, translated into 5% of the total worldwide market[43].

The cybersecurity entrepreneurship ecosystem in Israel is arguably more developed than general tech. We often view Israel as a start-up nation because of three major factors: intellectual capital, entrepreneurial culture, and government/military support. In an interview with Dr. Raphael Yahalom, co-founder of Onaro and a former member of the Unit 8-200 in Israel, he believes that

[39] (Raska, 2015)
[40] (So, 2014)
[41] (Suciu, 2015)
[42] (Senor, 2009)
[43] (So, 2014)

Israel's "heavy tech focus, mandatory military service and security minded thinking" are among the top reasons why Israeli start-ups succeed in tech entrepreneurships and particularly cybersecurity. Speaking from experience, Dr. Yahalom also addresses why Israeli culture contributes to entrepreneurial success: they honor problem solving, assume responsibilities and reward risk taking, thus is very entrepreneurial in nature.

The Israeli military, IDF, is another major force behind the success of Israeli cybersecurity industry. Mandatory military service and security oriented military training provides large benefits to the cybersecurity industry by training technical talents in bulk. Some research institutes are backed by the IDF, in particular the intelligence unit, the 8200, and some technologies they develop can be commercialized and used by civilians[44]. In fact, the unit 8200 is pivotal in the broader Israeli entrepreneurship ecosystem. In interviewee Dr. Raphael Yahalom's words, investors "won't even look at you" if a firm does not have a founding member that served in the unit 8200. Many cybersecurity start-ups with founders who have been through the unit 8200 went on to become famous companies, including[45]: Argus Cyber Security, Adallom, Palo Alto Networks, NSO, CyberArk, Imperva, Check Points Software Technologies, and Hyperwise Security.

However, one of the commonalities among the abovementioned companies is that they are now all based in the U.S. or at least listed in the U.S. stock exchanges. In fact, not limited to cybersecurity firms, Israeli start-ups in general tend to move to the U.S. after they have reached certain milestones. Many believe the outflow of Israeli startups and technology is due to the lack of market access. Indeed, Israel is a country with only 8 million people, 0.1% of world's population. Comparatively the U.S. is the single largest (or second largest in PPP terms) in the world, and with undoubtedly the largest tech community. It is then the natural decision for Israeli start-ups to scale by moving to the U.S. with closer proximity to their clients.

3.1.3 Cybersecurity Ecosystem in China

China holds a very different approach to cybersecurity and the entrepreneurship ecosystem. China's approach to cybersecurity is to centralize almost all functions and integrate cybersecurity with internet governance, which includes filtering of "negative" contents, such as porn, political contents and separatist/activist contents. The state administration has always held cyber space in tight control, and before the current versions of back-end censorship, the state council started with other attempts initially. The Chinese Ministry of Industry and Information Technology (MIIT) required all computer users to install a centrally funded censorship software, the "Green Dam" in

[44] (Suciu, 2015)
[45] (Tendler, 2015)

2009[46]. The Green Dam project turned out to be a failure because of its internally flawed design, and confusing interface. Ironically, it increased security concerns because of its poor engineering and backdoors, while having a detrimental effect on the basic PC experience for its users[47]. Later, Chinese government adopted a different approach to censorship, requiring all companies to comply with self-censorship rules in addition to the famous "Great Fire Wall". It is not common to see "harmonized" words on the Chinese public forums, for instance, the name of President Xi, Jinping's daughter, Mingze (明泽) has been censored according to "state legislations". When search the word on Baidu, China's dominant search engine, the results are not displayed and Baidu would notify the user the keyword "is not compliant with related laws and policies", despite the fact that there is no published law against searching for the combination of these two specific characters.

In addition, the cybersecurity market has never really been open to foreign parties. But some areas of for specialized security products or services are primarily occupied by foreign companies, due to the lack of available technology in their local counterparts. For instance, the VoIP phones used in the financial institutions and the secure point to point connections are provided by foreign companies, because of the "resilience", and "anti-DDOS attack capabilities", according an unnamed interviewee in a major state-owned bank.

In terms of entrepreneurship, Chinese internet companies started almost a decade after Israel, and adopted a fundamentally different approach. They focused on serving only the vast local market, and saw immediate early successes. In the 1990s, the early days of Chinese internet, a few local cybersecurity start-ups seized the opportunity and dominated the local anti-virus market. One of them, namely Kingsoft, became not only the leader of Chinese consumer cybersecurity, but also the "West Point" in Chinese entrepreneurship ecosystem. Many successful Chinese entrepreneurs today were alumni of Kingsoft, notables include: LEI Jun (surname capitalized), angel investor and founder of Xiaomi, and FENG Xin, founder of KM Player. However, a criticism to their successes is the belief that they are partially aided by China's generally unwelcoming and increasingly hostile policies towards foreign internet companies, even those with minority foreign ownership. Google has been driven out of the Chinese market since 2011, and Twitter and Facebook remains banned in China[48]. On January 1st, 2016, a law took effect that requires all telecommunications and internet companies operating in China to provide law enforcement with technical assistance, including decryption of sensitive data[49]. At the same time, the generally unfavorable sentiment towards foreign companies restrict the industries that foreign owned

[46] (OpenNet Initiative, 2009)
[47] (OpenNet Initiative, 2009)
[48] (Einhorn, 2016)
[49] (Einhorn, 2016)

companies can operate, which costed Yahoo their rightful ownership of AliPay (now Ant Financial) in 2011, estimated value of $60 billion in 2016[50].

Today, China's determination to transition and move up the industry value chain and bolster its economic system with a healthy entrepreneurship and innovation ecosystem provide an unprecedented opportunity for its local entrepreneurs. But the business landscape in Chinese cybersecurity industry is much different from the rest of the world. The clients of security startups in China are primarily large corporations, since the smaller companies are generally not aware of security risks, or choose to ignore due to lack of compliance requirements. The larger corporations in China are mostly state-owned, making sales very difficult for smaller companies, as they generally favor larger, more established and more well-known providers. In addition, many think of the Chinese government as a coherent whole, it is worth mentioning that the political system in China is in fact much less integrated. While the State Council holds the ultimate power in China, the central government (the ministries), local government (provincial/municipal) and state-owned enterprises all have their different incentives. The top down policies attempt to incentivize lower level agencies to install security hardware, software and processes in their daily practices, but the lower level agencies hardly understand anything about cybersecurity, and the awareness of data security is very low. Chinese companies have been very diligent in collecting personal information, but the data they collect are rarely protected. Internal data in some large state-owned enterprises, such as company phone book for instance, has been constantly sold to unknown third parties, which may include insurance agents, realtors, and sometimes even scam criminals. Furthermore, the Chinese government employees are rarely educated in the latest technology. Many government PCs are still operating Microsoft Windows XP, an operating system that has been discontinued for security support.

Under these unique characteristics, Chinese cybersecurity start-ups evolved to serve in very different manners. Anti-malware giant, Qihoo 360 for instance, announced that they would continue to provide security fixes on their Windows XP version of 360 Safe Guard, and provide their products free of charge. But aside from these stand-alone cases of successes, there has been no evidence of a larger cybersecurity entrepreneurship ecosystem in China, compared to the U.S. and Israel. And it is largely unsure at this stage whether such an ecosystem will ever exist, judging from China's state-led approach to cybersecurity.

[50] (Rao, 2016)

3.2 Impact of Socio-Economic Factors on Cybersecurity Entrepreneurship

A major factor that is gaining constant traction when studying entrepreneurship is the impact of culture. For instance, it is a widely observed fact that the Israelis and Americans are more tolerant to failure than the Europeans and the Asians. Having higher tolerance to risk consequently reduces the perceived risk associated with starting a business, thus encouraging entrepreneurship. In addition, cross cultural teams have access to a wide pool of talents to their disposal. But what should cross cultural start-up teams be aware of? Are there certain types of culture that works better with others?

In a 2013 presentation[51], Neal Hartman, an MIT researcher stated that in many Asian, Latin American and African cultures there is a very high perception among young people that entrepreneurship is an exciting way to start careers. But in European cultures, entrepreneurship is often associated with the risk of failure and entrepreneurship is not as popular among young people. Russia and UAE are listed as the countries with the lowest entrepreneurship intention rate according to his studies, while Israel are among the highest and the most successful.

Since the early 1990s, Israel has emerged as a reputable "start-up nation", breeding waves after waves of start-ups. Israeli start-ups are especially prominent in the cybersecurity industry, with numerous start-ups being acquired and two recent IPOs: Varonis and CyberArk. The Israeli culture is definitely one of the factors behind their cybersecurity success. Dan Senor expressed in his book, Start-up Nation, that the immigration and their cultural diversity in Israel is a contributing factor to entrepreneurial success:

"What the Soviet émigrés brought with them is symptomatic of what Israeli venture capitalist Erel Margalit believes can be found in a number of dynamic economies. "Ask yourself, why is it happening here?" he said of the Israeli tech boom. We were sitting in a trendy Jerusalem restaurant he owns, next to a complex he built that houses his venture fund and a stable of start-ups. "Why is it happening on the East Coast or the West Coast of the United States? A lot of it has to do with immigrant societies. In France, if you are from a very established family, and you work in an established pharmaceutical company, for example, and you have a big office and perks and a secretary and all that, would you get up and leave and risk everything to create something new? You wouldn't. You're too comfortable. But if you're an immigrant in a new place, and you're poor," Margalit continued, "or you were once rich and your family was stripped of its wealth—then you have drive. You don't see what you've got to lose; you see what you could win. That's the attitude we have here—across the entire population."[52]

---

[51] (Hartman, 2013)
[52] (Senor, 2009)

Dan Senor brought up a very interesting behavior of the immigrants in Israel, the combination of their reward seeking instincts and their relative low opportunity cost of entrepreneurship. His opinion is further complemented by interviewee Dr. Yahalom, who expressed that "Israeli culture honors problem solving, assuming responsibilities and risk taking, therefore in nature very entrepreneurial. The fact that security is highly related to problem solving means that the Israeli success in cybersecurity entrepreneurship is not a coincidence".

In terms of cybersecurity entrepreneurship ecosystems, we observe that the Silicon Valley and Boston are among the top start-up clusters in this industry. Many Silicon Valley based cybersecurity start-ups have grown into great successes, recent examples include: FireEye, Palo Alto Networks, and Imperva. The Boston area is also a center for cybersecurity, producing great companies in cybersecurity such as Sophos, Rapid7, and Barracuda Networks. Interviewee Rick Grinnell compares these two cybersecurity start-up ecosystem in a very interesting way, he views Silicon Valley/Bay Area ecosystem as "the Yankees", and Boston as the "Red Sox" – one flourishing with prestige and capital while the other bathing in glorious past and bright future.

One common factor behind the success cases in both regions, is the prominence of higher education institutes. Many of the world's best universities are located near these two regions, examples including: MIT, Harvard, Stanford, Caltech, and University of California. An obvious benefit from these research institutions is the availability of technology transfers. Professor Ed Roberts' research indicated that the technology transfer from research institutions is an important success factor:

"Firms who transferred greater amount of technology are more likely to succeed. "Of 119 firms spun-off from four MIT laboratories and one MIT engineering department, those that transferred the greater amounts of technology were consistently the most successful (p = .02). This was also true of the entrepreneurs who departed from the electronic systems company."[53]

Professor Ed Roberts intuitively interpreted the benefits of technology transfers, and concluded that technology transfers are less costly and quicker to implement compared to in-house development. He further examined those who fail to transfer technology, and concluded that:

"Firms that fail to transfer technology show the most evident and negative outcomes. Eleven out of 103 companies in one sample transferred no technology from their source organizations. Only one of those 11 firms scores above the bottom two-thirds of the companies in performance."[54]

We can see that the spinoffs with technology transfers significantly outperformed the ones without technology transfers in this study. Akamai is one of such examples in the cybersecurity

[53] (Roberts, 1992)
[54] (Roberts, 1992)

industry, starting from MIT research, entering the MIT $50K competition in 1998 and developed into a world-class company. However, this study was conducted by Professor Ed Roberts in 1992, over two decades ago. The rapid progression of technology since then have contributed to significant non-technology transfer start-ups, consumer internet companies in particular, for instance Facebook and Amazon, have enjoyed great successes without technology transfer. As a result, despite prior studies and observable trends, it is difficult to draw a definitive conclusion to whether technology transfer directly impacts the success of cybersecurity start-up and the magnitude of the impact without further studies.

The benefits of universities are not limited to technology transfers, they also provide high quality talents in the form of faculty, researchers, and students. Cybersecurity is a complex industry in terms technology, design, and engineering. According to interviewee Chris Zannetos, "cybersecurity is potentially more complex yet least understood than any other IT Industry, because of its problem solving nature and threats' ubiquity. This consequently leads to more difficult proof of concept, and thus higher need for sales engineers". In this context, top talents are essential for the success of a technologically complex industry.

However, there is a shortage of cybersecurity talents on a global scale today. According to Cisco, "cybersecurity skills are in high demand, yet in short supply"[55]. The talent gap in the U.S. alone can be observed through some numbers. Fortune columnist Gerrard Cowan reported that:

"*In 2014, companies posted 49,493 jobs that require Certified Information Systems Security Professional (CISSP) certification, a major cybersecurity qualification. However, only 65,362 people are CISSP certified in total, and most of them already have jobs, according to an October report from U.S. defense giant Raytheon and the National Cyber Security Alliance (NCSA)*"[56]

Interviewee Steve Whittaker from British Telecom have also separately highlighted this phenomenon. He believes that three years ago, cybersecurity start-ups and corporate functions required very high level of technical skills, but today, more and more firms/corporations have adopted a systematic and automated approach to security. This results in cybersecurity being a less skill intensive job in the lower tiers, but requires immensely deeper theoretical knowledge and more comprehensive skillsets among the management or the founding team to succeed. Although the universities are producing in abundance the technical computer science talents, we seem to fall short in terms of educating students on the more theoretical and fundamental parts of Science, Technology, Engineering and Math (STEM) subjects. When coming to solve problems and fix what isn't working like a security professional, programming expertise alone is not enough, which results in a shortage of security professionals. Furthermore, there is currently no defined path for a cybersecurity professional. Most security professionals come from a computer science background,

[55] (Cisco Security Advisory Services, 2015)
[56] (Cowan, 2015)

not a specialized cybersecurity background, and it is rare that a college student will be educated or informed with cybersecurity during the recruiting process. Some other talent gaps are also worth noticing:

"The Raytheon/NCSA report also identified a talent "gap within the gap": far fewer women than men are entering cybersecurity. The survey found that, globally, 33% of young men said they were more likely to consider a career in the field than they would have been a year before. That figure was 24% for women. The report suggested that much of this has to do with communication: 66% of women said that no teacher or counselor had ever discussed careers in cybersecurity with them, compared with 57% of men.[57]"

Interviewee Rob Partridge adds that it is important for the prospective security professionals to have a clear understanding what a career as a security specialist will look like. Like any other profession, cybersecurity needs its own pipeline of talents and clear paths of career progression, which is not present in the industry today.

Israel by contrast, has an abundance of intellectual capital in cybersecurity. In addition to the famous IDF and unit 8200, the fact that they are bordered with a lot of traditional enemies and the survival mindset has contributed to their focus in security. Unfortunately, because of the small domestic market, many Israel companies relocate to the U.S. in the scaling phase. When comparing to China, a country with arguably less security focused talents in the private sector, the enormous market size made entrepreneurship possible and even very successful in a few cases, for instance the abovementioned Qihoo 360 and Kingsoft.

Comparatively, in terms of the socio-economic factors affecting cybersecurity entrepreneurship ecosystems, the U.S. has the best combination of culture, technologies, research institute, talents, and market proximity, while Israel falls short in terms of market proximity and arguably research institutes. While it is almost impossible for Israel to physically improve in market proximity, with the internet connecting and integrating the world, whether market proximity is or still is a contributing factor to entrepreneurial success, and whether we are seeing a reversal of trend will an interesting topic to study.

[57] (Cowan, 2015)

Chapter 4. Cybersecurity Entrepreneurship

The hottest word in IT entrepreneurship throughout 2015 was "unicorn". The tech entrepreneurship ecosystem is awfully obsessed with the $1 billion threshold, which ascends a startup to the "unicorn" status. However, even in the "golden age" of cybersecurity entrepreneurship, when VC investments steadily grew by approximately 40 percent a year in the last five years, investor Mahendra Ramsinghani still considers cybersecurity start-ups "cockroaches", more than "unicorns". His comments are as follows:

"*Many security startups are not unicorns; rather, they are cockroaches — they rarely die, and in tough times, they can switch into a frugal/consulting mode. Like cockroaches, they can survive long nuclear winters. Security companies can be capital-efficient, and typically consume ~$40 million to reach break-even. This gives them a survival edge*"[58]

While the analogy of "unicorns" and "cockroaches" is interesting, cybersecurity start-ups indeed possess more distinctive features and deeper reasons behind the perception that "they rarely die".

4.1 Cybersecurity Exit Characteristics

Firms cannot operate without sufficient funding, and as an early stage tech start-up, it is difficult to access loan capital due to the lack of collaterals and consistent cash flows. These firms thus tend to use equity as their primary source of funding, and receive funding by offering equity to early stage investors such as angel investors and/or venture capitals. In addition to financial capital, investors also bring experience and network to help their portfolio companies. They provide them with support in day to day activities, recruiting, and strategic decisions. For an early stage equity investor, among their top concern is the factor called an exit, an anticipated event that will allow them to sell their portion of a firm's equity for an expected rate of capital gain, usually 3-5x, but sometimes 100x, even 1000x.

Usually there are two ways for investors, or even the entrepreneurs themselves to exit, either through an initial public offering (IPO), or through mergers & acquisitions (M&A). An IPO exit allows the firm to offer its equity on the public markets, such as New York Stock Exchange (NYSE), thus providing liquidity to all shareholders (after the "lock-up" period). On the other hand, an M&A refers to an event where the firm sells a portion or all of its equity to an acquirer for a specific price. In the U.S., investors and entrepreneurs prefer an M&A exit in general, since it is "cleaner and tidier". Interviewee, ex-entrepreneur Chris Zannetos estimates that 90% of the entrepreneurs would prefer exiting through M&A. If our initial hypothesis – cybersecurity firms are more likely to exit through M&A is correct, it effectively tells us that cybersecurity

[58] (Ramsinghani, 2016)

entrepreneurs are in a good situation. Among these reasons, a much debated topic is the fact that cybersecurity firms typically are organized around problem solving, thus backward looking in nature. After they solve an existing problem, usually larger companies would acquire cybersecurity start-ups for convenience but also for "security" reasons – corporations usually prefer to trust their own subsidiary than a complete third party provider, especially when it comes to security.

	2012			2013			2014			2015		
	IPO	M&A[59]	Ratio	IPO	M&A	Ratio	IPO	M&A	Ratio	IPO	M&A	Ratio
Software and Services	20[60]	1700	**1.18%**	29	1515	**1.91%**	35	1818	**1.93%**	17	1798	**0.95%**
Cybersecurity[61]	7	141	**4.96%**	2	123	**1.63%**	4	192	**2.08%**	3	297	**1.01%**

Table 4-1: Comparison of Exits between Cybersecurity and Software and Services

To explore and compare whether cybersecurity firms are really more likely to exit through M&A deals, a good method is to compare the percentage of cybersecurity firms that proceed to an IPO against those who sell through M&A in the specific given period of time and region. Table 4 -1 shows us that comparatively, cybersecurity industry actually has higher percentage of IPOs compared to M&As for all of the years excluding 2013.

Considering the significantly smaller sample size of cybersecurity IPOs, we can at least conclude that the notion that cybersecurity firms tend to exit through M&A rather than an IPO is rather a misconception. First, we previously stated that entrepreneurs prefer an M&A exit, and that cybersecurity firms are often built around such an exit therefore focused on problem solving in a narrow scope. But from the data we obtain indicating that cybersecurity firms do not have a observably higher exits in the form of an M&A, we can conclude that whether a start-up is in the cybersecurity industry or not plays little in determining whether the entrepreneur will reach his/her target by exiting through M&A. Secondly, while cybersecurity start-ups can be very focused around specific problem solving, they need to be prepared to grow into larger organizations and absorbing other capabilities to provide bundle solutions. Lastly, the data shown in Table 4 -1 does not take into consideration the size of deals, or valuation. The results can be improved by examining the total or average valuation from these exits, in addition to their volume in numbers.

[59] (Capital IQ, 2016)
[60] (Capital IQ, 2016)
[61] (AGC Partners, 2016)

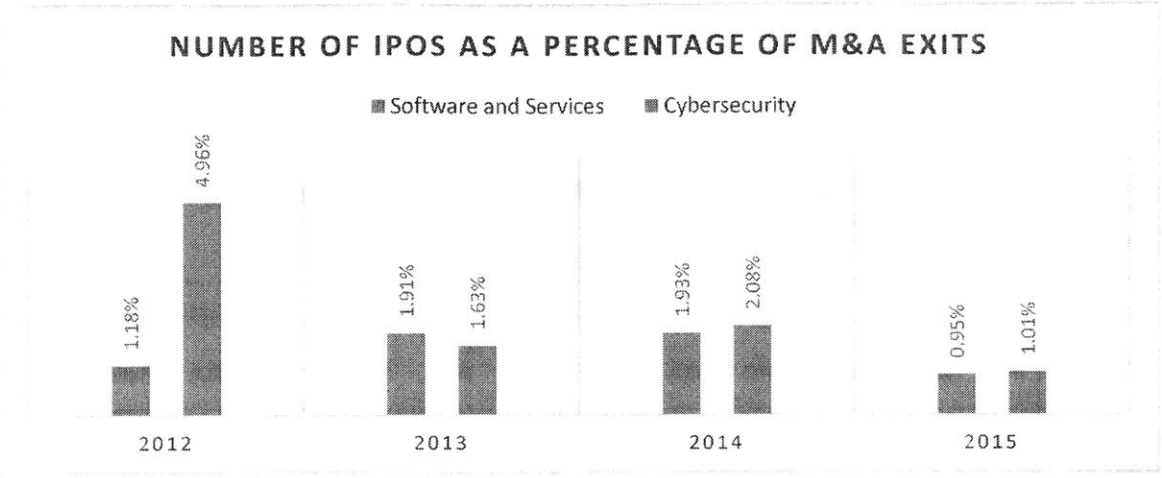


Figure 4-1: Percentage of IPO Exits Compared to M&A

Consequently, we can draw a conclusion that cybersecurity firms do not behave differently than normal IT start-ups in terms of their choice of exits based on evidences in the last four years. Figure 4-1 provides a visualized comparison that there is really no preference for cybersecurity firms to exit through M&A instead of IPO. The decision to pursue an IPO rather than simply sell through M&A is affected by many more complications that are not related to a company's operations, i.e. market conditions. Furthermore, because of the abovementioned benefits associated with an IPO, it is a natural first choice exit for any company. Therefore, it is entirely possible that many firms who went public did not have an alternative option, i.e. a competitive bid from a potential acquirer. Exiting through IPO or M&A does not impact investors as much, since they can sell their shares on the public market following a successful IPO attempt. But for entrepreneurs, an IPO effectively means that they cannot completely exit their company, since selling substantial amount of their shares act like a negative signal to the public market, which would cause the prices to slump. In this regard, seeing roughly the same behavioral characteristics for cybersecurity start-ups compared to the general tech start-ups tell us that cybersecurity entrepreneurs not only need to worry about building their technology and market, but should also be prepared to build a long lasting company.

Another important factor to consider when analyzing exit characteristics is the time to exit. In a world filled with capital backed hyper-growth unicorns (for instance, Uber), a company can grow to $500 million in market capitalization in just 1.6 years[62]. In contrast, although many smaller (under $200 million market cap.) cybersecurity firms exit in 2-3 years, larger ones (over $500 million) often take a decade to exit[63]. Investor Mahendra Ramsinghani considers cybersecurity firms highly efficient in "capital consumption", meaning they utilize their funds

[62] (Ramsinghani, 2016)
[63] (Ramsinghani, 2016)

effectively, but "time-to-exit" is much longer[64]. In Figure 4-2, Mr. Ramsinghani lists some of the cybersecurity exits with respect to time to exit and respective valuation. We can observe clearly that the data provided separates cybersecurity exits in three categories, $50 million or under, $50 million - $200 million, and $200 million and up. While we only see their valuation and time to exit with no comparison, the cybersecurity companies that reach the "unicorn" status of $1 billion valuation, namely Trusteer, Airwatch and Sourcefire, all took roughly a decade to exit. Comparing to companies like Uber and Snapchat, they indeed took a long time.

Company	Acquirer	Total Capital Invested	Acquisition Value	Time To Exit	Multiple of LTM Revenue
Authy	Twilio	$3.8 M	$25 M	~ 2 years	30 x
Skyfence	Imperva	$3 M	$60 M	~ 2 years	50 x
Cassida	Spunk	$11.5 M	$190 M	~ 2 years	NA
Cyvera	Palo Alto N.	$13.1 M	$200 M	~ 3 years	200 x
Aorato	Microsoft	$11 M	$200 M	~ 2 years	200 x
Solera N.	Blue Coat S.	$51.7 M	$240 M	~ 8 years	24 x
OpenDNS	Cisco	$51 M	$635 M	~ 10 years	9 x
Mandiant	FireEye	$70 M	$989 M	~ 10 years	9.7 x
Trusteer	IBM	$10.1 M	$1 B	~ 7 years	25.7 x
Airwatch	VMWare	$225 M	$1.54 B	~ 11 years	15.4 x
Sourcefire	Cisco	$56 M	$2.7 B	~ 12 years	11 x

Figure 4-2: Cybersecurity Exit Range[65]

This opinion is the exactly contrary to some other industry experts. Interviewees Dr. Raphael Yahalom and Rick Grinnell argue that cybersecurity firms take shorter to exit, because cybersecurity is a rapidly evolving industry, therefore the lifespan for start-up technologies should be shorter than in other industries. However it is possible that many start-ups pivot from their original technology or utilize their capabilities to deliver different services, which combined with their cost effective nature, contribute to a longer time to exit.

On the other side of the table, while existing buyers like the operating system giants, such as Microsoft, Google, and Intel, continue to pour money into security companies, many observe that the carriers such as AT&T and SingTel have also set their eyes on security firms[66].

Cybersecurity entrepreneurs should worry less about how to exit, since they generally have better capital efficiency and can thus sustain themselves over a longer time horizon. On the flip side, they are often not scalable, in which case exit is not a realistic option at all. For those that scale well, M&A exits are convenient when we observe large buyers like Microsoft and AT&T

[64] (Ramsinghani, 2016)
[65] (Ramsinghani, 2016)
[66] (Ramsinghani, 2016)

lurking around the block. The important lesson for investors is that cybersecurity start-ups are typically late bloomers, they usually do not grow at the exponential pace like some other tech start-ups, but they "rarely die". Consequently, they are usually great investments in earlier stages of a VC fund, since the return characteristics require the fund to stay with them for longer in general, but comparatively less attractive for VC funds that are in their later stages. The same logic also applies to entrepreneurs, when selecting VCs, cybersecurity entrepreneurs would benefit more by choosing one that has recently raised funding compared to other tech firms.

4.2 Cybersecurity Start-up Valuations

As previously mentioned, the number of companies that proceed to an initial public offering is only a small portion, even in cybersecurity industry. The majority of companies exit through M&A. Since many of the non-public firms are in their earlier stage, it is entirely possible that they are experience negative income and is still going through the "money burning" phase. Consequently, the P/E Ratio alone is no longer sufficient to evaluate the potential of a non-public firm. Traditionally, a non-public firm can be valued at the enterprise value over revenue multiple (EV/REV), but with the emergence of firms that do not worry about profitability upfront (such as Uber), valuation becomes much more complicated. To evaluate a company with rapidly growing number of users and great future earning potential, multiples based on current earnings may not be too relevant, since they may not have any current revenue at all. As a result, the most ideal comparison for these companies is their firm value.

Few practical complications arise when comparing early round firm values, since there are usually many terms attached when early investors such as angel investors and venture capitals offer term sheets that implicitly affect the value of the firm. For instance, a simple word change from "convertible" preferred shares to "participating" preferred shares can shift the entrepreneur's payoff dramatically, and when it is combined with redemption features, the firm value is effectively reduced from the explicit valuation. As a result, the more practical comparison is the value, or size of the deals.

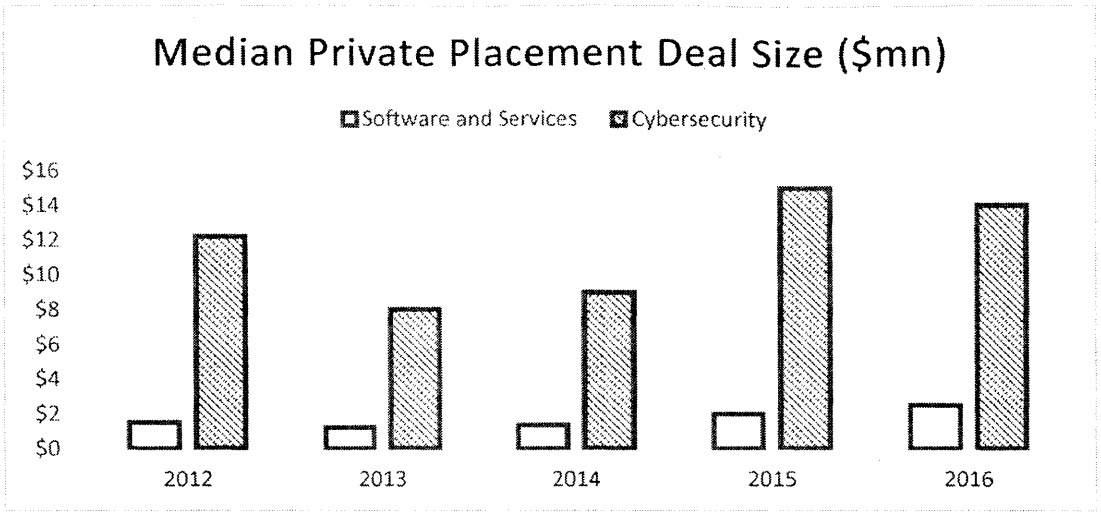


Figure 4-3: Median Private Placement Deal Size

Figure 4-3 provides a comparison between the median private placement deal sizes in cybersecurity industry and the broader software and services industry. One can observe a big gap between the deal sizes. In a simple world where this comparison accurately and exhaustively reflects what happens in the markets, we would be able to conclude that cybersecurity firms are much better at attracting investors, and they are probably also more likely to succeed, since larger funding usually indicates later rounds. However, this data comparison is limited in several ways. The first limitation is that deal size does not directly relate to the ideal measure – firm value. A firm valuing $ 1 billion can take a 1% investment at $ 10 million, while a $100 million firm can take a 10% investment at the exact same deal size. The second limitation is that deal size comparison between different companies in different stages are essentially not reasonable comparisons. A seed round start-up usually only require and receive $ 1 million or less, while a C or D round start-up typically receives no less than $ 10 million in capital injection each round.

Despite these limitations, from the deal size comparison, it is possible to conclude that larger deal size generally signal larger companies, hence later stage companies. Therefore, it is also possible to observe that cybersecurity companies are more likely to survive and progress to later rounds, which means they are less likely to fail in early rounds. This finding is consistent with Mahendra Ramsinghani's aforementioned claim that "Many security startups are not unicorns; rather, they are cockroaches — they rarely die".

An important factor behind this phenomenon that is worthy of further investigation is the capital intensity of the underlying cybersecurity startups. For instance, it is not uncommon for tech start-ups, from developers of wearable devices to those of virtual reality headsets, to be involved in capital intensive manufacturing processes. By contrast, cybersecurity start-ups rarely make large investments beyond the necessary hardware and computing capabilities, and they almost never deliver their products in the form of physical devices or gadgets. In addition, cybersecurity

start-ups usually dodge capital intensive software, graphics, and content development by focusing on one vector and solving one type of problems, unlike software development firms in the gaming and consumer facing applications industry.

4.3 Business Models

Rapid development in tech industry facilitated many interesting business models recently. In addition to the traditional product sales and subscription model, we can observe an emerging "freemium" model of providing low to zero cost core product and making money on value added services. This "freemium" model is often adopted by consumer IT firms and gaming companies. Some firms take it even further, providing services for low fees or even free, acquire a large user base, and "monetize" through exits. Recent examples of Instagram and Waze are proofs of such successes without mature profitability. These examples are especially meaningful for those cybersecurity startups that solve a specific problem but have trouble providing a large enough "platform" to attract market awareness. By focusing on providing products and services to the market, monetization by selling solves a problem that many cybersecurity startups face – educating the market.

While selling to a larger company may seem appealing, Instagram and Waze are not easy examples to follow. Their secret sauce for success is growth, measured in user acquisition and market share. Instagram is a familiar name to nearly everyone who lives in the Western Hemisphere, and Facebook's $1 billion acquisition of Instagram in 2012 was not a big surprise, since Instagram had 27 million users. Waze on the other hand, was not as famous, but equally as expensive. The reason why Google paid $1 billion for Waze a year later in 2013, was that it had almost 50 million users[67], almost twice the size of Instagram. Their growth was the defining factor of success, compared to solid monetization. In Instagram's case, it was founded in 2010, and grew to $1 billion in merely two years.

It is no surprise that growth has been viewed as the Holy Grail to tech startups, this "sacred ingredient" to success has also been witnessed countless times in cybersecurity start-ups. However, according to AGC Partners, growth alone "is no longer a golden ticket", and investors now are looking at growth coupled with profitability[68]. With the concern of profitability, monetization thus becomes the new challenge for start-ups. This does not mean that growth is of lesser importance. Consider the recent example of Twitter, while they announced that they met the revenue target set by Wall Street analysts for the last three quarters of 2015, their stock price still plunged because the monthly average users (MAU) remained at 320 million, showing no growth from Q3 2015[69].

---

[67] (Empson, 2013)
[68] (AGC Partners, 2016)
[69] (Los Angeles Times, 2016)

The above-mentioned British Telecom is an interesting case, and a special one. Their experience is representative of other large multinational corporations that have comparable scale of operations. For smaller users however, a proof of concept will be much more difficult. To quantify the effectiveness of security services, China's Qihoo 360 (Qihoo 360 Technology Co., Ltd) has pioneered a successful model for the security companies that serve the consumer market. Qihoo 360 is a leading Chinese internet company, and the number one provider of Internet and mobile security products in China as measured by its user base[70]. Qihoo 360's IPO in 2011 was a notable one, their shares sent the markets wild and recorded a 134% gain in its first day of trading on NYSE[71]. In December 2015, Qihoo 360 announced that it has entered into a "definitive merger agreement" to be delisted and privatized[72]. The all-cash transaction is valued at $77 per share, $9.3 billion in total. Their sheer size and performance has left an undoubted legacy of success in the Chinese cybersecurity industry.

Qihoo 360 offers many products dividing into three layers: the core security layer, the access layer, and the service layer[73]. In the core security layer, they offer their most famous and widely used product, the *360 Safe Guard*, complemented by 360 *Anti-Virus* and 360 *Mobile Safe*.

In the access layer, Qihoo 360 offers browsers for both PC and mobile phones. In the service layer, they offer *360 search*, *360 shopping*, and *360 gaming center*. The most distinctive feature of Qihoo 360 is perhaps their model to offer a wide range of products and services to its consumers for free. Unlike other security software providers, it costs nothing to use Qihoo 360's core security layer products and the majority of other products, with a few exceptions in gaming products. Despite offering products to consumers for free, Qihoo 360 is a very profitable company. They have reported revenue of $1.39 billion in fiscal year (FY) 2014[74], up 107% from $671.1 million in FY 2013. At the same time, net income for FY 2014 was $222.8 million, up 123.5% from FY 2013.

While offering heavily subsidized products to capture market share is no longer a mysterious business model for most of the internet firms in the U.S., Qihoo 360's success in monetizing free security products is still a remarkable achievement. The most intuitive monetization tool for a security firm operating in this model is online advertisements. And indeed, in FY 2014, Qihoo 360 have managed to record $756.4 million in online advertising revenue[75], accounting for over a half of their total revenue. This astonishing figure is achieved by attracting half a billion users for its products and platforms – in FY 2014, Qihoo 360 have reported 509 million monthly active users of Qihoo 360's PC-based products, and 744 million smartphone users

[70] (Qihoo 360 Technology Co., Ltd, 2015)
[71] (The Wall Street Journal, 2011)
[72] (Qihoo 360 Technology Co., Ltd, 2015)
[73] (Qihoo 360, 2014)
[74] (Qihoo 360 Technology Co.,Ltd., 2015)
[75] (Qihoo 360 Technology Co.,Ltd., 2015)

of their primary mobile security product. Comparing to a well-known Internet unicorn that is running a similar revenue model – Twitter, Qihoo 360 has done a great job in acquiring users and generating profits. Twitter reported $1.4 billion revenue from 288 million monthly active users in 2014, but suffered a $577 million net loss[76].

A large contributing factor in Qihoo 360's growth in FY 2014 advertising revenue is their search advertisements[77]. While internet giants such as Microsoft are struggling with search monetization, Qihoo 360 has quietly captured the number 2 spot in China's search engine market. In addition, to fully monetize on their vast user base, Qihoo 360's portfolio of complementary, synergistic products fueled much of the revenue growth in FY2014. In fact, the year over year (YoY) revenue growth for online advertising was 81%, but their Internet value-added services, which included mobile gaming and app store business lines, saw a YoY growth of 142%. And this all started with a free anti-virus product!

To further decode Qihoo 360's success in monetization, it is crucial to understand how they captured such a vast user base, for instance half a billion users on their PC products and 740 million users on mobile phone platforms. Qihoo 360's earliest product, the *360 Safe Guard,* offered not only easy to use (while its effectiveness is debatable) anti-virus product, it also featured a "start-up clock", that displayed information such as how many seconds it took your PC to boot, and what percentile do you rank among your peers (in China). After drawing users' attention to boot speed, Qihoo 360 follows up by offering built-in product features to help clean up registry files, delete cookies and defragment the hard drive(s). The 360 Safe Guard occasionally utilizes a popup to display information such as how many hours it protected its user for, how many files it scanned and how many threats it neutralized. It was these value-added product features and subtle means of market education that helped Qihoo 360 to pull ahead of their competitors. And despite some controversy in test results and conflicts with Tencent, Qihoo 360 continues to deliver robust results today. From an IPO price of $14.50[78] in March 2011 to a privatization price of $77 in December 2015, Qihoo 360 delivered 430% return to investors in less than 6 years.

The case of Qihoo 360 is significant in that it pioneered a free to use model for cybersecurity products, and monetized through online advertisements and other electronic information related services instead of the traditional sales of packaged software products or the subscription model. To achieve its rapid early growth and product offering however, any company would require strong access to capital markets. It was thus not surprising to identify big names such as Sequoia Capital, Highland Capital, and CDH in Qihoo 360's IPO documents. Although

---

[76] (Twitter)
[77] (Qihoo 360 Technology Co.,Ltd., 2015)
[78] (Nasdaq)

the case of Qihoo 360 indicates the success of an atypical cybersecurity firm, one that focuses on consumer and platform rather than businesses and content, this case indeed opens up some interesting discussions related to the power of free product models, proof of concept, and quantifying results for future cybersecurity entrepreneurs.

Fortunately today, we see many cybersecurity names in the $1 billion club, including Okta, Tanium, Illumio, and Zscaler[79]. Illumio in particular, despite the belief that cybersecurity companies take longer time-to-exit, reached the $1 billion club in just a year, showing great scalability and strong growth. With many worried about the cybersecurity firms' unstable secondary market performances, maybe the next generation cybersecurity start-ups will inevitably adopt the capital ramped hyper-growth model, thus becoming more like the other tech start-ups.

While all start-ups want to be in the high profitability, high growth zone, only a few can achieve that status. Cybersecurity start-ups may face the profitability-growth dilemma more than other tech start-ups, since cybersecurity products and services are usually hard to measure in effectiveness. It is thus difficult to bring in revenue without incurring promotion costs such as sales engineers and/or product trials in their early stages. On the other hand, while cybersecurity firms can easily monetize through providing consulting when things are not doing well, the consulting model struggles to provide rapid growth, and consulting is often not where the cybersecurity start-ups wanted to be. Many interviewees mentioned that products/services cybersecurity firms provide are usually trying to prevent something bad from happening, and therefore hard to measure the value of that service. Consider for instance when a company faces the decision between spending $1 million or $2 million on cybersecurity annually. How should they evaluate which approach to take? It is difficult to measure the effect of such investments to arrive at a definitive conclusion such as the $2 million investment provided us twice the security as the $1 million investment.

Indeed, in a market where the output cannot be easily quantified and comprehended, it is important to examine the decision making process involving security, and this process provides us a good understanding of the clients' priority when seeking security products/services. An important finding is that in some organizations, the decision to invest in certain security projects is often not evaluated in monetary terms. In an interview with Rob Partridge from British Telecom, he mentioned that British Telecom evaluates security related projects in a "balanced score-card" approach. Since British Telecom keeps a very long horizon in mind when making these decisions, they are not as concerned about the immediate profit & losses. Security investment decisions are made according to their technical specifications and the strategic alignment of each project. In these companies, security would be an enabling technology or feature of their monetization

[79] (AGC Partners, 2016)

products and services, consequently they do not need to seek monetization from the target security companies, synergies and technology are their main focus when engaging in M&A activities.

Recently, two types of companies are especially interested in buying cybersecurity companies for synergy: the "OS layer" and "the carriers"[80]. The OS layer refers to operating systems and core platform providers, such as Microsoft, Intel, and Google. In fact, considering the number of cybersecurity acquisitions, companies such as IBM, Intel, and Microsoft are among the top buyers from 2008 to 2016[81]. The carriers (such as British Telecom) are perceived as emerging buyers as they seek opportunities to upsell and gain trust with the proliferation of data centers and cloud providers[82].

[80] (Ramsinghani, 2016)
[81] (AGC Partners, 2016)
[82] (Ramsinghani, 2016)

Chapter 5. Conclusions

5.1 Important Findings for Cybersecurity Entrepreneurship

Cybersecurity is a unique industry, in the sense that it is both an application and an enabling technology. Through the last two decades, cybersecurity has clearly evolved from a reactive problem solving function to a complex, layered industry covering from prevention to detection and reaction. While we continue to develop and acquire new technological capabilities, the increasingly integrated cyber/physical systems are constantly exposed to exponentially increasing vulnerabilities. To combat these problems, the industry has shifted their focus from reactive approaches to proactive approaches, from problem solving to security engineering. Among the enabling technologies, encryption, big data analytics, and intelligence related technologies are among the most anticipated segments of cybersecurity. Secondary market performances indicate that while cybersecurity companies are in general valued higher than their peers, they are also observably more volatile.

Meanwhile, cybersecurity professionals must be prepared to deal with nation state (or other complex organization) attackers, cyberwarfare, or cyber terrorism. Those developing capabilities or applications in the Internet of Things field need to stay on high-alert to mitigate risks from the new access points. These risks are not only threatening the data or intellectual properties, but also threatening the safety of cyber systems or even physical infrastructures. Rising digital and cyber technologies are now capable of providing physical security for many industries, for instance, big data analytics, intelligence and forensics. However, they must also be aware of their own cybersecurity to deliver their service with a resilient system that stays active on a continuous basis and protects the data they collect. In addition, the recent surge of capital into cybersecurity start-ups may be leading towards a bubble in cybersecurity investments. Therefore it is increasingly important for entrepreneurs to consider their business model, plan ahead for each funding event, and build their companies towards a realistic exit.

When evaluating the entrepreneurship ecosystems, culture, prominence of universities, and availability of intellectual capital are influential to a cybersecurity ecosystem. The U.S. possesses the best combination of socio-economic factors that influence cybersecurity entrepreneurship, or the larger entrepreneurship ecosystem as a whole, and it is interesting to observe how another innovation powerhouse – Israel adapts to the market proximity challenge. Politically, it is evident that government initiatives can greatly impact cybersecurity, both directly and indirectly. While the U.S. adopts a more "free market" approach, the Israeli have their governments directly and deeply involved in every aspect of cybersecurity, from technology generation to entrepreneurship. China on the other hand, has their cybersecurity developments almost entirely dependent on

government initiatives and the large conglomerates. Whether a cybersecurity entrepreneurship ecosystem fits in China's national interest remains a doubt.

The favored exit for cybersecurity start-ups is the same compared to the broader IT industry, but in most cases, firms do not have a choice between M&A and IPO. Market conditions are often the sole determinants of exit options, while most entrepreneurs think of M&A as an easier and a preferred exit option, many proceed to IPO. Scalability and profitability has becoming an increasingly important topic, one that cybersecurity start-ups may not been answering well in the past but inevitable in the future. Application of technology and focusing on providing synergistic or complementary products and services will be more important for cybersecurity start-ups when thinking about exits in the near future. In today's market, we see many large buyers lurking around the corner for those start-ups with scale, but for those with only growth and no profitability, the golden age may be over. They may need to consider selling to an upstream or downstream industry player, or even a competitor to realize potential synergies. And the manner in which they provide and prove their value is also important. In addition to the integrated capabilities and B2B model, cybersecurity firms are also well positioned to compete with the mass market consumer facing model to claim large market shares and monetize through access to information.

5.2 Limitations and Further Research

In addition to the limitations and topics for further research mentioned previously, the biggest limitation of this thesis is the lack of failure cases. Availability of data regarding entrepreneurship failures has been a major obstacle, and controlling for different variables to examine entrepreneurial failure in the financial context will also be a difficult experiment to structure.

Furthermore, many of the abovementioned conclusions are limited in terms of validity due to lack of empirical tests. While entrepreneurship and innovation is a hot topic, much of the study in industry specific entrepreneurship lack data and need to rely on qualitative interviews.

Finally, the design has been broad to include a wide variety of speakers from different stakeholder groups within the entrepreneurship ecosystem, researchers, entrepreneurs, large corporations, and investors. But obtaining a sizeable sample is difficult for each of the category. If more interviews or even potentially mass survey is a possibility, data collection would enable much more meaningful tests.

[Page intentionally left blank]

Bibliography

AGC Partners. (2016). *Security Market Update.* AGC Partners.

BBC. (2015, 08 23). *Ashley Madison faces huge class-action lawsuit.* Retrieved from BBC: http://www.bbc.com/news/business-34032760

Bradley, T. (2013, 09 13). *In Their Own Words: Kaspersky Lab Cofounder And CEO Eugene Kaspersky.* Retrieved from Forbes: http://www.forbes.com/sites/tonybradley/2013/09/23/in-their-own-words-kaspersky-lab-cofounder-and-ceo-eugene-kaspersky/#1f23d3b52d49

Capital IQ. (2016, 03 05). *Software and Services IPO US 2012/01/01-2016/03/05.* Retrieved from Capital IQ Database.

Capital IQ. (2016, 03 05). *Software and Services M&A 2012/01/01-2016/03/05.* Retrieved from Capital IQ Data Base.

CBInsights. (2016, 01 27). *Mega-Rounds To Cybersecurity Help Push Funding To New High In 2015.* Retrieved 02 13, 2016, from CB Insights: https://www.cbinsights.com/blog/cybersecurity-funding-2015/

CERT, Carnegie Mellon University. (n.d.). *TJX & Heartland.* Retrieved 02 13, 2016, from CERT: http://www.cert.org/digital-intelligence/case-studies/tjx-heartland.cfm?

Cisco Security Advisory Services. (2015). *Mitigating the Cybersecurity: Top Insights and Actions from Cisco Security Advisory Services.*

CNN Money. (2016, 02 26). *PureFunds ISE Cyber Security™ ETF.* Retrieved from CNN Money: http://money.cnn.com/quote/etf/etf.html?symb=HACK

Cowan, G. (2015, 12 07). *High-paying Cybersecurity Jobs Go Begging Across the World.* Retrieved from Fortune: http://fortune.com/2015/12/07/high-paying-cybersecurity-jobs-go-begging-across-the-world/

Einhorn, B. (2016, 01 21). *A Cybersecurity Law in China Squeezes Foreign Tech Companies.* Retrieved from Bloomberg Businessweek: http://www.bloomberg.com/news/articles/2016-01-21/a-cybersecurity-law-in-china-squeezes-foreign-tech-companies

Empson, R. (2013, 06 11). *WTF Is Waze And Why Did Google Just Pay A Billion+ For It?* Retrieved from Techcrunch: http://techcrunch.com/2013/06/11/behind-the-maps-whats-in-a-waze-and-why-did-google-just-pay-a-billion-for-it/

Finkle, H. S. (2016, 02 23). *Cyber security startups face funding drought.* Retrieved from Reuters: http://www.reuters.com/article/us-cyber-venturecapital-analysis-idUSKCN0VW2IZ

Gandel, S. (2015, 01 23). *Lloyd's CEO: Cyber attacks cost companies $400 billion every year.* Retrieved from Fortune: http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/

Hartman, N. (2013). *1000 and 1 Entrepreneur Cultures.* Retrieved from Knowledge Stream: http://digitaloctober.ru/en/events/knowledge_stream_1000_i_1_kultura_predprinimatelstva

Hewlett Packard. (2015). *Internet of things.*

International Telecommunications Union. (2016). *ICT Facts and Figures 2015.* Retrieved from ITU Home Page: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Los Angeles Times. (2016, 02 21). *Twitter shares nosedive after sluggish fourth quarter.* Retrieved from Rapid City Journal: http://rapidcityjournal.com/business/twitter-shares-nosedive-after-sluggish-fourth-quarter/article_004ede20-8957-527a-92d5-3880c76b5e5c.html

MarketsandMarkets. (2016). *Global Cyber Security Industry 2016 Market Research Report.* MarketsandMarkets Analysis.

Nasdaq. (n.d.). *QIHOO 360 TECHNOLOGY CO LTD (QIHU) IPO.* Retrieved 03 16, 2016, from Nasdaq: http://www.nasdaq.com/markets/ipos/company/qihoo-360-technology-co-ltd-850169-66570

NERC. (2014). *CIP V5 Transition Program.* Retrieved from NERC: http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx

Newmeyer, K. (2015, 02 06). *Cybersecurity in the President's National Security Strategy.* Retrieved from National Cybersecurity Institute: http://www.nationalcybersecurityinstitute.org/international/cybersecurity-in-the-presidents-national-security-strategy/

Nourian, A., & Madnick, S. (2014). A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems: Applied to Stuxnet. *IEEE Systems Journal.*

OpenNet Initiative. (2009). *China's Green Dam: The Implications of Government Control Encroaching on the Home PC.* Retrieved from OpenNet Initiative: https://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc

Perez, E. (2016, 02 11). *U.S. official blames Russia for power grid attack in Ukraine.* Retrieved from CNN Politics: http://www.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/

Ponemon Institute LLC. (2015). *2015 Global Megatrends in Cybersecurity.* Ponemon Institute LLC.

Press, G. (2015, 11 1). *This Week In Tech History: The Birth Of The Cybersecurity And Computer Industries*. Retrieved from Forbes: http://www.forbes.com/sites/gilpress/2015/11/01/this-week-in-tech-history-the-birth-of-the-cybersecurity-and-computer-industries/#185d19286e4f

Pure Funds. (2016, 02 27). *Pure Cyber Security*. Retrieved from Pure Funds: http://www.pureetfs.com/etfs/hack.html

Qihoo 360. (2014). *Products and Services*. Retrieved from Investor Relations of Qihoo 360 Technology Co.,Ltd.: http://corp.360.cn/ps/overview.html

Qihoo 360 Technology Co., Ltd. (2015, 12 18). *Qihoo 360 Enters into Definitive Agreement for Going Private Transaction*. Retrieved from http://ir.360.cn/phoenix.zhtml?c=243376&p=irol-newsArticle&ID=2123936

Qihoo 360 Technology Co.,Ltd. (2015, 03 09). *Q42014*. Retrieved from Quarterly Reports: http://ir.360.cn/phoenix.zhtml?c=243376&p=irol-reportsOther

Ramsinghani, M. (2016, 01 06). *Cockroaches Versus Unicorns: The Golden Age Of Cybersecurity Startups*. Retrieved from Techcrunch: http://techcrunch.com/2016/01/06/cockroaches-vs-unicorns-the-golden-age-of-cybersecurity-startups/

Rao, L. (2016, 03 07). *Alibaba's Finance Arm Ant Financial Valued at $60 Billion*. Retrieved from Fortune: http://fortune.com/2016/03/07/ant-financial-alipay-60-billion/

Raska, M. (2015). *Confronting Cybersecurity Challenges: Israel's Evolving Cyber Defence Strategy*. Singapore: Nanyang Technology University.

Risen, T. (2015, 11 30). *Obama Pressures China's Xi Jinping on Cybersecurity*. Retrieved from US News: http://www.usnews.com/news/articles/2015/11/30/obama-pressures-chinas-xi-jinping-on-cybersecurity

Roberts, E. (1992). The Success of High-Technology Firms: Early Technological and Marketing Influences. *TIMS/ORSA Interfaces Vol. 22, No. 4 1992*, 3-12.

Senor, D. (2009). Start-up Nation: The Story of Israel's Economic Miracle. In D. Senor, *Start-up Nation: The Story of Israel's Economic Miracle*. New York: Hachette Book Group.

So, D. (2014, 12 10). *Cyber Security Nation: Why Israel Leads The World In Protecting The Web*. Retrieved from No Camels: http://nocamels.com/2014/12/cyber-security-nation-israel/

Suciu, P. (2015, 09 01). *Why Israel dominates in cyber security*. Retrieved from Fortune: http://fortune.com/2015/09/01/why-israel-dominates-in-cyber-security/

Tendler, I. (2015, 03 20). *From The Israeli Army Unit 8200 To Silicon Valley*. Retrieved from Tech Crunch: http://techcrunch.com/2015/03/20/from-the-8200-to-silicon-valley/

The Wall Street Journal. (2011, 03 11). *Qihoo Tops Chinese IPOs in U.S. This Year*. Retrieved from The Wall Street Journal: http://www.wsj.com/articles/SB10001424052748703712504576232084175020582

The White House. (2016). *Foreign Policy*. Retrieved from The White House: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity

Thomas Chen, J.-M. R. (2004). Statistical Methods in Computer Security. In J.-M. R. Thomas Chen, *Statistical Methods in Computer Security*. doi:ISBN 0-8247-5939-7

Twitter. (n.d.). *Annual Report 2014*. Retrieved 03 16, 2016, from Twitter Investor Relations: https://investor.twitterinc.com/annuals-proxies.cfm

Walters, R. (2015, 11 18). *Cyber Attacks on U.S. Companies Since November 2014*. Retrieved from Heritage.org: http://www.heritage.org/research/reports/2015/11/cyber-attacks-on-us-companies-since-november-2014

WhatsApp. (2016, 04 05). *end-to-end encryption*. Retrieved from WhatsApp Blog: https://blog.whatsapp.com/10000618/end-to-end-encryption

White House Office of the Press Secretary. (2015, 09 25). *FACT SHEET: President Xi Jinping's State Visit to the United States*. Retrieved from Statement & Releases: https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

Windward. (2016). *Company*. Retrieved from Windward: http://www.windward.eu/#/company/WindwardFounding/2

WSJ. (2016, 02 27). *Market Data Center*. Retrieved from The Wall Street Journal: http://www.wsj.com/mdc/public/page/2_3021-peyield.html

Yahalom, R. (n.d.). *MIT Sloan*. Retrieved 02 20, 2016, from Staff Directory: http://mitsloan.mit.edu/about-mit-sloan/directory/staff-directory/detail/?id=105218&co_list=E

Yahoo. (2016, 02 27). *Interactive Stock Comparison Charts*. Retrieved from Yahoo Finance: https://finance.yahoo.com/echarts?s=HACK#{"allowChartStacking":true}

Zetter, K. (2014, 11 03). *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*. Retrieved from Wired: http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Chapter 6. Appendix

6.1 Interview Notes and Key Findings

The section below documents key insights from interviews. These interviews are primarily complements to the abovementioned study, while also providing insights on specific issues.

6.1.1 On Cybersecurity Industry

Dr. Raphael Yahalom

Dr. Yahalom believes that the industry is backward looking in nature, solving yesterday's problem with today's technology. However, the threats are forward looking, therefore there is a mismatch of intentions and resources. In addition, he believes that when assessing the potential of a cybersecurity firm, it is less important to look at what their current solution is, but more important to assess the founding team members.

Chris Zannetos

From his previous entrepreneurship experience in Identification & Access Management (IAM), Chris concluded that like any other industry, there will be trends in cybersecurity startups, and as technology matures, there will gradually be extended segments that spin off from other segments in cybersecurity. Chris also thinks that education for potential clients in cybersecurity is crucial. He identified two main reasons why clients buy from cybersecurity firms: first, regulations and compliance; second, incidents of breach of security. He notes that these factors are crucial but are backward looking in nature, and may not be sufficient for the future. Meanwhile, security is often a point solution that becomes a part of other products, while the cybersecurity firms are narrowly focused. For the offenders however, there are many attack vectors, this increases the complexity of security systems and creates a mismatch of expertise and resources. Furthermore, Chris mentions that cybersecurity is potentially more complex yet least understood than any other IT Industry, because of its problem solving nature and threats' ubiquity. This consequently leads to more difficult proof of concept, and thus higher need for sales engineers.

Rob Partridge

Rob's leading role in British Telecom's security learning and development function provided a different perspective. Rob is mostly concerned about security not only as a crucial process for the entire organization, but also a built-in value for their clients. His mission is to make sure that everyone in BT understands the importance of security. He views people as the weakest link in cybersecurity, and stresses the importance of sound practices. Furthermore, he

also identifies the measurement of success as a difficulty in his pursuit of learning and development. It is difficult to determine how much spending is enough (on security), and the reward of investments is difficult to quantify and measure.

Steve Whittaker

Steve views cybersecurity as a rapid changing industry. He believes that three years ago, cybersecurity start-ups and corporate functions required very high level of technical skills, but today, more and more firms/corporations have adopted a systematic and automated approach to security. This results in cybersecurity being a less skill intensive job in the lower tiers, but requires immensely deeper theoretical knowledge and more comprehensive skillsets among the management or the founding team to succeed. Although the universities are producing in abundance the technical computer science talents, we seem to fall short in terms of educating students on the more theoretical and fundamental parts of Science, Technology, Engineering and Math (STEM) subjects. When coming to solve problems and fix what isn't working like a security professional, programming expertise alone is not enough, which results in a shortage of security professionals. Furthermore, there is currently no defined path for a cybersecurity professional. It is reported that rarely a student has been educated or informed with cybersecurity during the recruiting process. At the same time, the education of separate stakeholders is increasingly relevant and important. The industry needs to educate different stakeholders based on their respective disciplines and concerns, and formulate different ways to educate them based on their level of experience and type of usage.

Steve visions the future of cybersecurity industry is shifting from "security" to "resilience", from building up prevention systems to improving ability to recover and mitigate damages. In addition, the "security" aspect will also shift to more focus around the design of technology and less focus around problem solving in retrospect. Rapid technological advancements also leads to more spectrum of attack/defense, and with "internet of things" becoming a hot topic today, security will be amongst their top concerns, and we will hopefully see more standardized roles for cybersecurity professionals.

Rick Grinnell

Rick states that cybersecurity firms should generally see a higher "technology turnover", since old defense technology gets outdated very fast. He also observes cybersecurity industry shifting from the earlier focus in detection, end points, detection to today's focus on analytics and the long term evolution of machine learning. He sees that security as a service (SaaS) as the primary long term model, combined with the subscription model. At the same time, security profiling and relative benchmarking in terms of effectiveness is necessary, and potentially can also lead to cooperative defense and information sharing. He sees data analytics and cyber intelligence as the future for cybersecurity industry.

Greg Dracon

Greg expressed from his observations in the venture world that cybersecurity industry completely changed since the last two decades, until 5 years ago it was a niche business. Back in 2000s cybersecurity innovation started to become a visible problem, and the old guards of security started not being able to keep up. At the same time, a lot of money were to be made by the adversaries, and cybersecurity start-ups are taking charge in terms of entrepreneurship and innovation. In the 2010s, security is becoming a main stream problem. Market for stolen data is roughly the size of the drug trade in the US. We witness very good attack capabilities and very bad defense capabilities in the market. Recently, we notice that this mismatch is exacerbated since smart cyber criminals basically have nothing to lose. It is almost impossible to identify them, let alone punishing. For the next decade cybersecurity is going to be the next big trend in the tech industry. At the same time, the notion of cyber deterrence will not work for commercial world, since the offenders and defenders are often mismatched in terms of financial status. Greg believes that a big problem in the security world today is companies are not disclosing that they are breached. This creates a problem in information and intelligence sharing on the defense side, while presumably information and intelligence such as known vulnerabilities are shared in the offensive communities.

6.1.2 On Entrepreneurship Ecosystems

Dr. Raphael Yahalom

Dr. Yahalom is from Israel, a symbolic nation for start-ups. He possesses deep knowledge about the Israeli cybersecurity ecosystem, and he shares that Israel's heavy tech focus, mandatory military service and security minded thinking are driving factors behind Israel's success in entrepreneurship, in particular the cybersecurity entrepreneurship. In addition, Israeli culture honors problem solving, assuming responsibilities and risk taking, therefore in nature very entrepreneurial. The fact that security is highly related to problem solving means that the Israeli success in cybersecurity entrepreneurship is not a coincidence. Meanwhile, having the largest unit of the military, the 8-200 unit, dedicated to intelligence opens them up to an arsenal of intellectual power.

Rob Partridge

Rob urges the schools to educate talents specializing cybersecurity practices, instead of educating general IT talents. While he strives to ensure a pipeline of talent to sustain safety and security in the future (for BT), he does identify that currently there is no defined pathways to become a cybersecurity professional. In the future, there needs to be more standardized roles for cybersecurity professionals and prospective students, they need to have a defined career pathway.

Steve Whittaker

BT interacts with every aspect of the ecosystem, it provides services to other entities, but also buys materials/services from other entities. It interacts with the government in similar fashion, constructs infrastructure and provides services for governments, but also requires government to support them. The regulatory environment is very expectation dependent, especially because BT's unique roles and capabilities. Compliance is an important aspect of regulators, but they need to be clear in nature, at least their framework needs to be. However, since the cyberspace is very different than the real world, it is difficult to be clear, for instance, the attribution problem is a constant topic of debate.

Greg Dracon

Greg's opinion focuses on the Boston entrepreneurship/tech ecosystem that is relevant to cybersecurity. Boston has numerous leading technical institutes, and he observes in general a longer tenure for engineers and more stability in technical teams. He identifies the stability in talents as the Bostonian advantage in technical entrepreneurship ecosystem, compared to the West Coast. Due to the complex nature of cybersecurity entrepreneurship, this notion of longer term stability is very important.

He also adds that while Israel supports a very prominent cybersecurity ecosystem, the need for the firms to move to the U.S. is not for market proximity alone. Cybersecurity often deals with very sensitive clients and matter, therefore trust is an important factor to consider in this industry.

6.1.3 On Cybersecurity Entrepreneurship

Dr. Raphael Yahalom

Dr. Yahalom believes that the cybersecurity industry has three distinct characteristics that differentiate itself from the general IT industry:

1. Cybersecurity firms are built to address a specific problem, not built to scale.
2. They solve yesterday's problem. Cybersecurity firms (and perhaps other security firms as well) in nature tend to look at what occurred to prevent it from happening.
3. They generally have shorter "life span", meaning they exit quicker than normal IT firms. Cybersecurity start-ups are often started and structured with a quick exit in mind, and entrepreneurs may not aim to build a long lasting company at the start.

Dr. Yahalom also observes a surge or perhaps an oversupply of venture funding and an over-hype in terms of the number of cybersecurity start-ups today. Although he also acknowledges that in conjunction with the abovementioned three characteristics, it is entirely

possible that cybersecurity companies have higher chances to succeed (in terms of exit) but lower returns from success.

Chris Zannetos

From his experience of founding Courion, Mr. Zannetos highlighted a few aspects of cybersecurity entrepreneurship and entrepreneurship in general:

1. Entrepreneurs and investors generally prefer an M&A exit, because it is a lot cleaner.
2. Many large buyers are buying less now because of their own leadership/strategy issues, i.e. HP, Symantec, and IBM.
3. Rise of the next class of security providers, such as FireEye are actively in the M&A market to seek deals to complement their portfolio of capabilities, therefore contributing to industry consolidation.
4. IPO or M&A may not be decided by choices, entrepreneurs would find a buyer first, if that is not an available option, they would then be forced into an IPO.

Greg Dracon

In terms of the technical aspects of cybersecurity start-ups, Greg sees them as a special industry, where cybersecurity is usually a little deeper technically, at the same time the user interface start to matter for cybersecurity just like consumer tech, which adds another layer of complexity. The customers are also changing today, it used to be a very tech sale, now more and more board members, CXO level executives are involved. Therefore cybersecurity start-ups today require more general sales capabilities, which is what Greg is recommending to his portfolio companies.

Rick Grinnell

Rick agrees with the claim that there can be an over-investment in cybersecurity currently, but over-investment is not a new concept in the VC world. There are partners that have been investing in cybersecurity for decades, and there are also partners who are just joining the party. The definitive factor isn't how much money or what valuation the industry has beeb attracting, it's how much intellectual capital they are working with. Experienced management teams and investors are pivotal to the success of entrepreneurs, and the availability of those experiences, in another word, the intellectual capital, has not changed.