Rodman &Renshaw®
A UNIT OF H.C. WAINWRIGHT & CO.

Technology

July 18, 2016

Kevin Dede, CFA
415-779-5876
kd@rodm.com

Security in an Unsecure World: Layered Approach for Defense in Depth and the Evolution of a Protected Internet of Things

Confidentiality, authenticity, and integrity of transactions and data. The security issue is nothing new to the post-Target (TGT; not rated), post-Home Depot (HD; not rated) data hacks of the enterprise IT environment, but certainly begs the question of what companies, and our covered company universe in particular, are doing to raise their safety profile and reduce both potential and existing customers' worry and concern. The findings of our weeks of observation and research reveal that there's no silver bullet for black-hat vampires lurking in the computer hacking domain, where much of the corporate espionage activity may well be state sponsored by the likes of the Chinese and Iranian governments—this fact was confirmed by our interviews of people close to the situation. What do smaller companies do in an environment where any and every turn may be manipulated to present a breach of customer-critical information? Understanding the breadth of the threat is only part of the battle. In realizing that the extensibility of corporate networks has become so pervasive in the rapidly growing IoT world also raises broader security issues as the HVAC-accessed Target hack illustrated. Furthermore, people are people, and represent a variable that becomes almost if not completely unmanageable in scope as exemplified by the mere monetary pittance an American Superconductor (AMSC; Buy rated) employee received for highly classified trade secrets that company held (the loss of which amounted to approximately $100M) compounded by the potentiality that a Sony (SNE; not rated) employee was instrumental in "giving away" corporate access to the hackers involved in the breach of that company during the fall of 2014. There is no shortage of avenues in to destroy, compromise, or even hold data for ransom ('ransomware' hackers exploited an LA hospital earlier this year), and companies must be on guard and at 100% readiness every minute 24x7x365. Hackers need only have it right for a fraction of a minute, and the odds against companies appear almost insurmountable. Therefore, the drive toward peace of mind in a highly adversarial enterprise IT environment requires the deployment of security initiatives across all operational theaters of an IT network. Our research suggests that 'better' solutions integrate multiple security solutions that compound defense in a layered approach where the layers of an onion might offer a fair analogy. Merely piercing the skin of the onion may get you past the enterprise firewall, but not the meat at the center, where mission critical and sensitive customer data are stored. Optimal solutions, by our reckoning, employ fully encrypted internal transactions, multi-layering of data storage, and the use of object-based storage platforms that use encrypted codes to store data in binary fashion that would make it completely unintelligible for a hacker without the proper encryption keys. The keys, of course, are held somewhere else in the network, behind multiple layers of security, and only accessible by very few corporate employees. These combinations are not readily available in a turn-key solution, and instead must be engineered, implemented, and both routinely surveilled and audited. We see the implementation of a end-to-end, deeply layered enterprise security as an art form that must be as dynamic, fluid, and flexible as the hackers are that are constantly trying to breach it; further, these deployements are not easily constructed and maintained. These reasons substantiate the market estimates that call for an approximate $75B in IT security spending to expand at an almost 10% five-year CAGR to an expected $170B market in the year 2020.

Many tools available. The rise of the black hats has created a gold-rush-like campaign to provide counter measures, and intensifying security-related paranoia creates selling opportunities for those able to market solutions. Clearly there's no shortage of companies manoeuvering to address concerns and it appears, as shown on the following pages, that the likes of companies such as IBM (IBM; not rated) to BAE Systems (BAESY; not rated) are attempting to raise awareness of their capabilities to address cyber threats. And while the enterprise IT environment continues to see all the usual suspects presenting solutions, including: Microsoft (MSFT; not rated); Cisco Systems (CSCO; not rated); and Intel's (INTC; not rated) McAfee; there are relatively newer entrants such as FireEye Inc. (FEYE; not rated); Palo Alto Networks (PANW; not rated); root9B (RTNB; not rated); among many others. The evolution of the Internet of Things (IoT) has commanded the attention of hackers given that network periphery tends to elicit less CTO and security firms' attention, but a recent tie up between mainstream IT supplier SAP (SAP; not rated) and WISeKey (WIHN.SW; not rated), a Swiss-based IT security company, heighten the competitiveness in securing the IoT space where we have seen less emphasis from mainstream security firms outside of Symantec (SYMC; not rated) and Gemalto (GTMOY; not rated).

The good guys vs. the bad guys. The severity of the security issue, witnessed in extensive data breaches at household name businesses, has raised both hacking concern and profile so extensively that large IT-focused companies have taken to advertising aggressively to the business community. Over the past year or so by our observation, the IT heavyweights have stepped up the marketing effort to include specifically addressing airport venues—a high target area for the traveling business person—as the examples included below attest. A recent Forbes article cited Gartner Inc.'s (IT; not rated) estimate for 2015 spending in the cyber security market had reached $75 billion, and Forbes also quoted a MarketsandMarkets report in noting cyber security spending is expected to increase at a five-year CAGR of almost 10% to $170 billion by the year 2020. Market size and expectations for growth are continually attracting technology development and new market entrants as well. Interestingly, companies renowned for their work in the IT space, such as IBM and companies known for military defense, such as BAE Systems, have taken up aggressive advertising of their respective capabilities in the IT security space.

Fig. 1. BAE Systems Running Video Ads at Newark International

Source: BAE Systems (BAESY; not rated) via YouTube, July 2016.

Fig. 2. IBM Print Ad at San Francisco International

Source: Rodman & Renshaw, June 2016; IBM Corporation (IBM; not rated).

The size of the threat demands greater, and well beyond equal steps in defense. Hackers and cyber-terrorists are on the job all the time, but only need be successful in creating a breach once. Network security must be on guard incessantly. Both time and comprehensiveness of solutions mandate dedicated security resources, and for some larger companies, only larger IT security companies can provide the resources necessary. We expect that as time passes, more companies could bring solutions to market, especially those that combine network management and security functions, as networks migrate to software defined (SDN) and network function virtualization (NFV)—this may well be a topic for a separate report. Further, as alluded to earlier, a range of solutions and integration of those solutions is required to provide a full and dynamic security solution. On account of the many facets of cyber security solutions in the enterprise market, segmenting types of security, the targeted applications or companies for which solutions are provided, as well as the companies that provide particular solutions helps to make the discussion more digestible. Cyber security types include network security, application security, content security, wireless security, and cloud security. We also stress the point of extensibility created by two emerging network evolutionary trends: (1) bring your own device (BYOD) functionality; and (2) machine-to-machine (M2M and IoT) communications that have mandated the need for IoT security at the fringe of the network where remote devices have access, termed endpoint security. In offering a taste of the many facets involved in providing network and IT security, the MarketsandMarkets

report referenced earlier in this paper segments solutions such as identity and access management, risk and compliance management, encryption, data loss prevention, unified threat management, firewall, antivirus and antimalware, Intrusion Prevention System (IPS)/Intrusion Detection System (IDS), Security Information and Event Management (SIEM), disaster recovery, Distributed Denial of Service (DDoS) mitigation, and whitelisting (a whitelist is a register of entities that are granted a particular security privilege or service).

The hacking "issue" has become an opportunity for many IT and software focused companies, and the response has supported the evolution of a littered field of competitors and competing security solutions. Our research suggests that using the best features of particular solutions in an integrated and layered approach may drive the optimal solution. There are many opinions, however, and many solutions. Herein we offer a cross section of solutions we believe may help improve an investors' understanding of the overall environment.

A synopsis of available solutions. There are basic websites that post relevant reference information to help address security concerns, such as: (1) www.howtogeek.com; and (2) blogs.msdn.com (a blog for Microsoft developers). And there is an assortment of tools, business intelligence tools, data integration tools, data discovery tools, data encryption tools, compliance tools, and SIEM tools. Each is required to have an understanding of what data is collected; where it's located; how it's structured, categorized, and used. A set of tools that can model the network, its traffic, and form a baseline of communication and network activity and then detect and alert on anomalies in network and client behavior may help businesses mitigate problem-activity early in the threat cycle. In addressing these needs, network traffic flow analyzers are helpful, such as FireEye's Malware Detection appliance, Netflow data (which provides information that determines if internal machines have been compromised—that also comes as a feature on other network elements such as Cisco routers and provides the ability to collect IP traffic as it enters or exits an interface), and tools such as ARGUS Software, SiLK (System for Internet-Level Knowledge), a collection of traffic analysis tools developed by the CERT Network Situational Awareness Team, and/or the Bro network security analyzer (open source, Unix based network monitoring framework).

Beyond SIEM, Advanced Security Analytics (ASA), which provides real-time insight into—and, increasingly, proactive responses to—situations that indicate a potential breach, compromise, or vulnerability. ASA merges SIEM with analytical capabilities often derived from network traffic data collection and may also include forensics and Intrusion Detection Systems/Intrusion Prevention Systems. In protecting network assets, privileged identity management tools can be used to control the administrative password, and, in some cases, shared business passwords and credentials. There are further steps to take as well, such as full data back-up (almost rudimentary), full storage disk encryption, containerization of corporate data (prevent data from moving and prevent a potential breach from accessing the full data set), and such solutions as Bluebox, which enforces a flexible walled garden around certain data and functionality while applying corporate security rules and permissions. Enterprises could also consider adopting the concept of a software defined data center. In this type of remote environment, data can be encrypted, segmented, and potentially combined with other data to create a mix almost impossible to compromise. VMware (VMW; not rated) provides a solution stack for micro-segmentation capabilities among other data security solutions.

Because more businesses are migrating network operations to leverage software use over the Internet, commonly referred to software as a service (SaaS), an interesting evolving area in security is using technology to provide a layer between the user and SaaS solutions, so the enterprise can manage authentication and encryption and hold its keys, while maintaining close-to-full functionality with the software as a service (SaaS) solution. We expect that more companies should move to adopt similar approach to ensure no catastrophic events ensue as SaaS solutions become more widespead.

Fig. 3 Gartner's Famed Magic Quadrant Analysis Helps to Illustrate the Number of Players in the SIEM Space (SIEM, or Security Information and Event Management)

Source: Gartner (July 2015).
Note: Publicly traded companies included above: Intel Corp. (INTC; not rated); HP (HPQ; not rated); IBM Corp. (IBM; not rated); EMC Corp. (EMC; not rated); Micro Focus (MCRO.L; not rated).

Some companies have recognized a need for having better information on the data they're responsible for protecting and extending their products to meet this need, perhaps a more sophisticated approach to security solutions. Some of the SIEM companies shown above incorporate this functionality as well, such as: Informatica's Secure@Source; IBM's Q-Radar; HP's ArcSight; and Splunk.

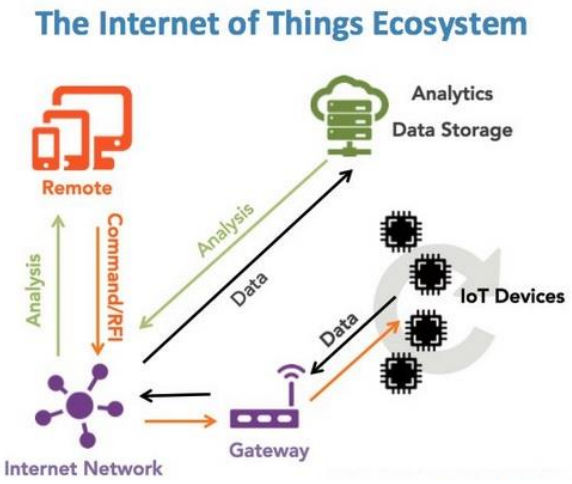
"Best" options. Collaborative tools are broadly seen as having a bright future in IT security. Functionality that includes combining the best effort of separate, specific "silver bullets" through communication and collaboration in a network—a network that must support a distributed workforce, and increasingly, distributed devices in an IoT environment—are thought, by our investigation, to present improved initiatives in future security solutions. Further, tools that detect attackers and anomalous activity are even more important in the face of advanced threats which bypass traditional, preventative mechanisms.

What of our companies? We discussed security issues with a group of our covered companies. Clearly each takes the issues seriously, but there's no uniform approach. We learned most from Top Image Systems (TISA; Buy) where our research revealed what we believe to be the most important single element of security implementation: there is no single element. In fact, and as mentioned, a layered network construction that allows only certain users access to particular data while segmenting broad sections of stored data. Top Imaged amassed a collection of solutions to address cyber threats, and takes painstaking care in managing them. This process includes varied tests, assessments, and audits. Magic Software (MGIC; Buy) shared a white paper marketing document the company uses to explain its security position to customers and interested parties, such as ourselves. Because Magic delivers its solutions over the Internet, there are inherent security measure incorporated, such as HTTPS support, trusted vendor certificates, scrambled transmitted content, and encrypted local cache. These solutions are also delivered in a layered-like approach.

Security solutions evolve to address the machine-to-machine environment. The Target hack, where bad actors and/or cyber terrorists penetrated the company's network through an HVAC thermostat, certainly raised awareness of the vulnerability of all network elements, including those on the fringe. And clearly the law of raw numbers works against companies and their respective security efforts as the number of network elements increases. As such, the machine-to-machine [or the Internet of Things (IoT)] security market is expected to grow from $6.9 billion in 2015 to nearly $29 billion by 2020, according to a report published by MarketsandMarkets. Also according to the recent Forbes article noted earlier, research and advisory firm Technavio's analysts forecast the global IoT security market to grow at a CAGR of nearly 55% over the period 2014-2019. Perhaps more alarming is the concern that roughly

70% of IoT devices could be open to attack currently and the expectation offered by third-party research firm pundits stating that more than 25% of IT attacks could involve IoT by the year 2020.

Fig. 4. Expansive Nature, Interconnection, and Web Exposure Make the IoT Environment Especially Difficult to Protect Communications and Data



Source: Business Insider, Business Intelligence Report, July 2016.

The graphic above attests to the demands on security precautions in securing traffic across a network that incorporates machine-to-machine connectivity, has an Internet interface, and permits remote entry (BYOD, or bring your own device) functionality. As it stands, most enterprise networks incorporate the latter two capabilities, and more, we suspect, could begin supporting IoT interfaces. Each device presents yet another point of network exposure, and must have adequate security measures. Again, and importantly, lower compute and memory capability of IoT devices requires a different type of solution that might otherwise be deployed on a main firewall or on a mainstream corporate server. IoT security solutions must operate in a low power environment with limited resources yet deliver fully capable protection for the broader network. Additional security measures may be taken at each interface between remote IoT devices and the core network where more compute, memory, and power resources can be brought to bear.

Fig. 5. Where Does Your IoT Network Stand?

Source: Informa, IoT Security, July 2016.

Our leading covered company in the IoT space, Novatel Wireless (MIFI; Buy), has deployed proprietary solutions across its installed base of more than half a million subscriber devices. These solutions vary depending on implementation and include both hardware and software security initiatives. The company continues to research

developing security technology in recognition of the growing security threat and the fact that the size of Novatel's installed base itself may entice would be hackers. Given the breadth of the IoT network, endpoint security is instrumental, and incorporating an endpoint detection and response (EDR) solution that continuously monitors and analyzes the state of the endpoint for indications of compromise is a feature that is required in IoT and on account of hardware limitations, may not be on the actual client.

Other solutions may have attracted greater enterprise attention. Specifically, the partnership that SAP established with WISeKey stands to leverage both SAP's industry position and WISeKey's security expertise compounded by its Swiss domicile. Further, WISeKey, in what could amount to a brilliant move, recently acquired the semiconductor assets of INSIDE Secure (Euronext; INSD; not rated), a French embedded software firm for approximately $13.2 million. The combination of WISeKey and INSIDE Secure's semiconductor business should promote the creation of a comprehensive cybersecurity trusted platform with complete vertical integration in combining hardware, cryptography, and software. Importantly, the purchase raises WISeKey's positioning as a cybersecurity IoT player, and to date, our study has yet to unveil a combination (SAP, WISeKey, and INSIDE Secure) that has such broad potential in an emerging IoT environment that remains ripe for potential cyber attacks. The special features come in many flavors: (1) WISeKey's Swiss-based neutrality stands tall against all those markets that choose not to be involved with all other trusted root web security companies of U.S. domain; (2) SAP has an incredibly broad global footprint; and (3) INSIDE Secure's technology can be embedded in semiconductor firm ware, updated over the air, and grow to include WISeKey's security capability. The security menu offered here is flush with special items and looks especially appealing from our perspective.

Another deal, announced earlier this month, combines two Czech-originated companies Avast Software and AVT Software (AVG; not rated), in a $1.3 billion deal that extends Avast's security to more than 400 million network end points including about 160 million cell phones. According to Avast's CEO, "Combining the strengths of two great tech companies, both founded in the Czech Republic and with a common culture and mission, will put us in a great position to take advantage of the new opportunities ahead, such as security for the enormous growth in IoT." While we have watched the slow but continual development of the IoT environment since the early 2000s, broad adoption has certainly lagged original expectations of the early 1990s and since. However, lately, it appears that the machine-to-machine communications environment is now expanding rapidly across many fronts including utility meter reading, fleet telematics, and many other use cases. The advent of bad operators attacking IoT has raised security concerns, and competitors in IT security are positioning themselves to address the nuances of IoT operations.

Important Disclaimers

Rodman & Renshaw is a unit of H.C. Wainwright & Co., LLC. Research is created and distributed by and securities are offered through H.C. Wainwright & Co. LLC, (the "Firm") Member FINRA/SIPC, which conducts certain research activities under the name Rodman & Renshaw.

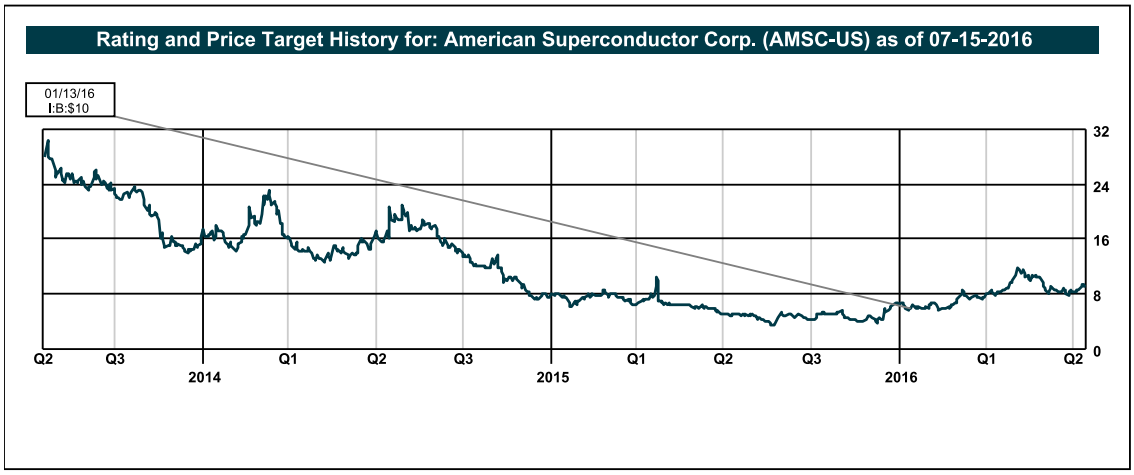
H.C. WAINWRIGHT & CO, LLC RATING SYSTEM: H.C. Wainwright employs a three tier rating system for evaluating both the potential return and risk associated with owning common equity shares of rated firms. The expected return of any given equity is measured on a RELATIVE basis of other companies in the same sector. The price objective is calculated to estimate the potential movements in price that a given equity could reach provided certain targets are met over a defined time horizon. Price objectives are subject to external factors including industry events and market volatility.

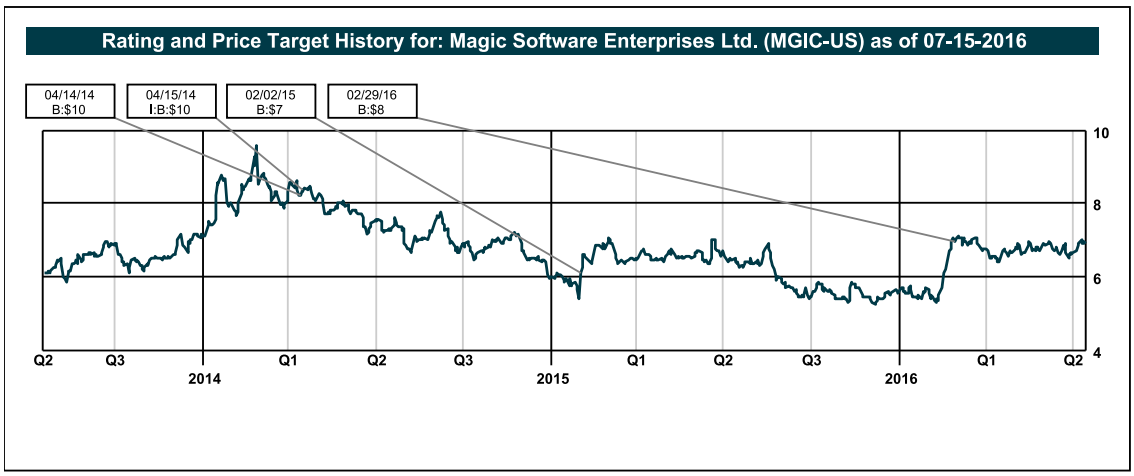
RETURN ASSESSMENT

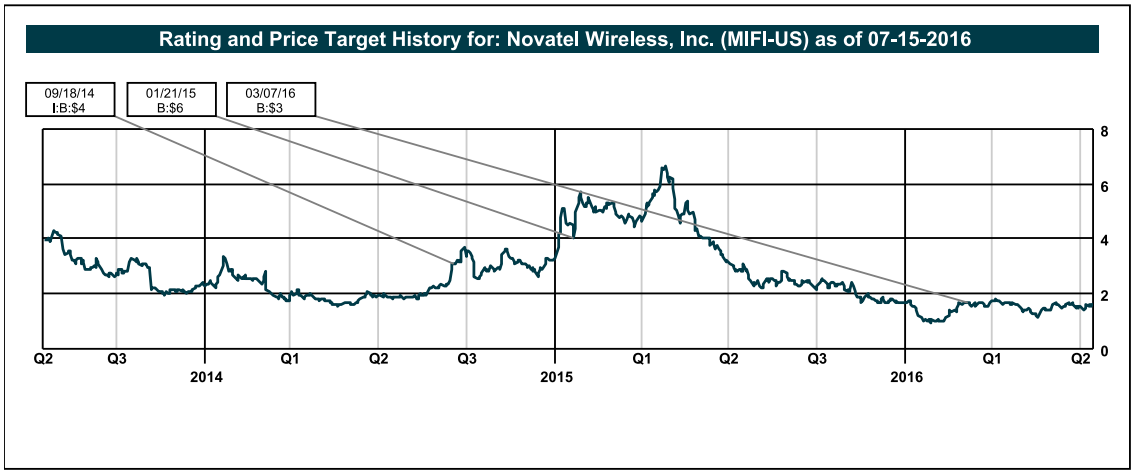
Market Outperform (Buy): The common stock of the company is expected to outperform a passive index comprised of all the common stock of companies within the same sector.

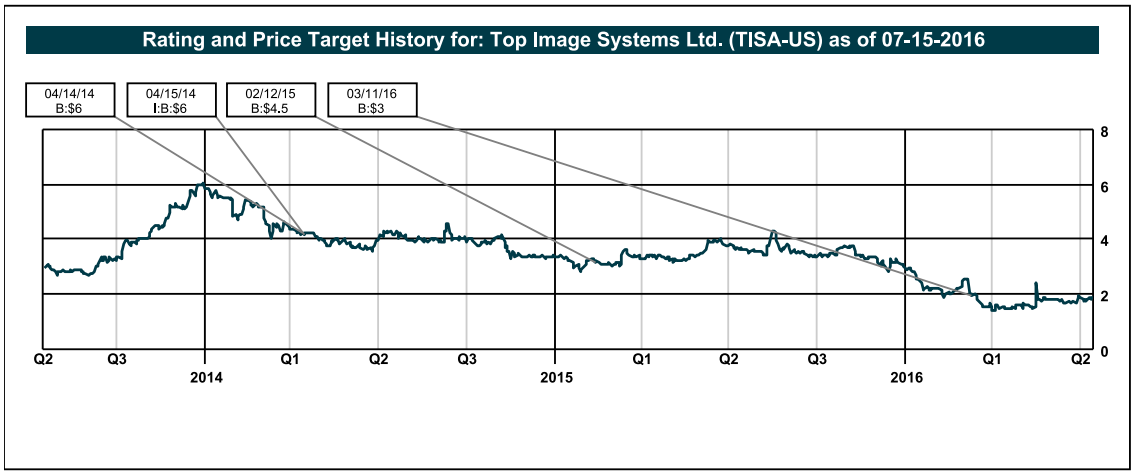
Market Perform (Neutral): The common stock of the company is expected to mimic the performance of a passive index comprised of all the common stock of companies within the same sector.

Market Underperform (Sell): The common stock of the company is expected to underperform a passive index comprised of all the common stock of companies within the same sector.









Related Companies Mentioned in this Report as of 07/15/2016

Company	Ticker	H.C. Wainwright Rating	12 Month Price Target	Price	Market Cap
American Superconductor Corp.	AMSC	Buy	$10.00	$9.26	$131
Magic Software Enterprises Ltd.	MGIC	Buy	$8.00	$6.92	$307
Novatel Wireless, Inc.	MIFI	Buy	$3.00	$1.59	$85
Top Image Systems Ltd.	TISA	Buy	$3.00	$1.86	$33

Investment Banking Services include, but are not limited to, acting as a manager/co-manager in the underwriting or placement of securities, acting as financial advisor, and/or providing corporate finance or capital markets-related services to a company or one of its affiliates or subsidiaries within the past 12 months.

Distribution of Ratings Table as of July 15, 2016

			IB Service/Past 12 Months	
Ratings	Count	Percent	Count	Percent
Buy	180	96.77%	53	29.44%
Neutral	3	1.61%	1	33.33%
Sell	0	0.00%	0	0.00%
Under Review	3	1.61%	1	33.33%
Total	186	100%	55	29.57%

I, Kevin Dede, CFA , certify that 1) all of the views expressed in this report accurately reflect my personal views about any and all subject securities or issuers discussed; and 2) no part of my compensation was, is, or will be directly or indirectly related to the

specific recommendation or views expressed in this research report; and 3) neither myself nor any members of my household is an officer, director or advisory board member of these companies.

None of the research analysts or the research analyst's household has a financial interest in the securities of (including, without limitation, any option, right, warrant, future, long or short position).

As of June 30, 2016 neither the Firm nor its affiliates beneficially own 1% or more of any class of common equity securities of American Superconductor Corp., Magic Software Enterprises Ltd. and Novatel Wireless, Inc..

Neither the research analyst nor the Firm has any material conflict of interest in of which the research analyst knows or has reason to know at the time of publication of this research report.

None of the research analysts or the research analyst's household has a financial interest in the securities of (including, without limitation, any option, right, warrant, future, long or short position).

As of June 30, 2016 neither the Firm nor its affiliates beneficially own 1% or more of any class of common equity securities of Top Image Systems Ltd..

Neither the research analyst nor the Firm has any material conflict of interest in of which the research analyst knows or has reason to know at the time of publication of this research report.

The research analyst principally responsible for preparation of the report does not receive compensation that is based upon any specific investment banking services or transaction but is compensated based on factors including total revenue and profitability of the Firm, a substantial portion of which is derived from investment banking services.

The Firm or its affiliates did not receive compensation from American Superconductor Corp., Magic Software Enterprises Ltd., Novatel Wireless, Inc. and Top Image Systems Ltd. for investment banking services within twelve months before, but will seek compensation from the companies mentioned in this report for investment banking services within three months following publication of the research report.

The Firm does not make a market in American Superconductor Corp., Magic Software Enterprises Ltd. and Novatel Wireless, Inc. as of the date of this research report.

The Firm does not make a market in Top Image Systems Ltd. as of the date of this research report.

The information contained herein is based on sources which we believe to be reliable but is not guaranteed by us as being accurate and does not purport to be a complete statement or summary of the available data on the company, industry or security discussed in the report. All opinions and estimates included in this report constitute the analyst's judgment as of the date of this report and are subject to change without notice.

The securities of the company discussed in this report may be unsuitable for investors depending on their specific investment objectives and financial position. Past performance is no guarantee of future results. This report is offered for informational purposes only, and does not constitute an offer or solicitation to buy or sell any securities discussed herein in any jurisdiction where such would be prohibited. No part of this report may be reproduced in any form without the expressed permission of H.C. Wainwright & Co, LLC. Additional information available upon request.