TCW

Manager of the TCW, MetWest, and TCW Alternative Fund Families

INSIGHT

VIEWPOINT

Opportunities In Information Security

JEFFREY LIN, CFA | OCTOBER 2015

Jeffrey W. Lin, CFA
Senior Vice President
U.S. Equity Research

Mr. Lin joined TCW in 2006 as an Equity Analyst and his coverage responsibilities include computer hardware & storage, electronics manufacturing systems (EMS), software, IT services, and autos. He joined TCW with over 14 years of experience in the technology sector with roles as Engineer, buy and sell-side Analyst, venture capitalist, CFO of a communications equipment start-up and Co-Portfolio Manager of a technology sector hedge fund. Mr. Lin began his investment career at Montgomery Securities in 1994 following electronics manufacturing and computer storage. He joined Paul Allen's Vulcan Ventures in 1999. At Vulcan, three of his investments went public and three were acquired by publicly traded companies. In 2001, he served as the CFO of Zaffire, an optical equipment company funded by Kleiner Perkins, until the company's sale to Centerpoint Broadband. From 2002-2004, he was an Analyst at Provident Investment Counsel and followed computer and communications equipment as well as communications services. Most recently, he was a Co-Portfolio Manager of Conquistador Ventures, a technology sector focused hedged fund. Mr. Lin holds a BS in Electrical Engineering with an emphasis in Communications and Computer Architecture and an MBA from the University of Southern California. He is a CFA charterholder.

The "connected world" of today joins together corporations, financial institutions, retailers, knowledge workers, utilities, transportation networks, communications, online retailers, software as a service (SaaS), applications, social media, computers, the "internet of things," and consumers. While this universal connectivity creates significant economic value it also generates opportunities to extract information for criminal gain or terrorist/military actions.

In our opinion, the information security market, which was $73.3 billion in 2014 (Gartner July 2015), is attractive for investment because it is large, growing at an attractive rate (9.8% in 2014), and less cyclical than many other sectors. Gartner believes growth in 2015 will accelerate to 13.8% and $84.4 billion and is expected to settle into a healthy growth rate of 8% through 2019.

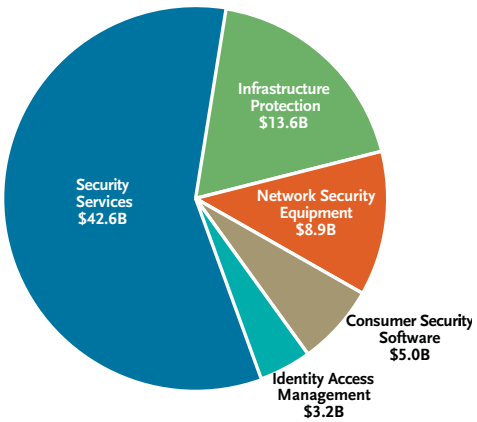
Information security presents lower cyclicality than other information technology investments because it is a non-discretionary expense for major enterprises and government agencies and should be a priority for all companies and consumers. For companies, security breaches are expensive and can damage consumer trust of the brand. The risk of valuable information falling in to the wrong hands is too great to be ignored by any user. We expect that overall spending for information security will outpace general IT spending. Companies with newer, more effective, and more efficient approaches to guarding against threats and recovering from attacks will likely grow faster than the overall security market.

A LOOK AT THE SECURITY MARKET

The $83 billion+ information security market is large and fragmented, providing investment opportunities across multiple sub-sectors. Mergers and acquisitions are common in the field, as are initial public offerings (IPOs), all of which can generate opportunities for investors.

Companies in the global information security industries span multiple subsectors in information technology and account for some $73 billion in 2014 revenues.

FIGURE 1:
2014 INFORMATION SECURITY MARKET



Source: Gartner 2015

Opportunities in Information Security (cont'd)

The key areas for information security firms are:

- **Identity Access Management**, which focuses on products, applications and platforms that manage access to networks, applications, and data. This sector accounted for $3.5 billion of the information security market in 2014.
- **Infrastructure Protection**, which includes companies whose products secure email and internet gateways, provide security information, and event management (SIEM), and protect data and devices such as PCs and mobile devices. Infrastructure management was a $13.6 billion market in 2014.
- **Network Security Equipment**, accounting for $8.9 billion of the overall market in 2014, includes products that help prevent intrusion by unwanted parties into corporate networks.
- **Security Services**, a $42.6 billion market in 2014, provides services required to implement and manage information security products and procedures.
- **Consumer Security Software** firms develop software that runs on personal computers and mobile devices to prevent viruses and malware. This was a $5.0 billion market in 2014.

CASE STUDIES

New Firewall Technology | Chief information officers (CIOs) have the challenge of providing usable information services to company employees, a favorable experience for customers, while at the same time being able to secure the network. For example, how can enterprises enable employees to use SaaS (software as a service) applications and social media while keeping their networks secure? The enterprise needs to open the network to allow a user to access a SaaS application and exchange data. Opening up that network creates vulnerability. Older firewall technology would either grant or deny access. **Palo Alto Networks**' firewall can enable/disable access depending on the application, user, or content.

Mobile Device Management | Apple iPhones/iPads and Android devices are excellent platforms for enterprises to provide company-specific applications for order taking, information gathering, or simply a dashboard for users to see what's going on in the organization. Since Apple iOS and Android devices have many appealing features to consumers, employees want to use these devices as their mobile "work" device. Enterprises need to provide the benefits of mobile computing to their workforce, yet ensure that corporate information remains secure. Products such as **VMware's** AirWatch separate company applications from the users' consumer applications and provide methods to "wipe" data from the device in the event it is lost or stolen.

WELL PUBLICIZED ATTACKS

The stakes are extremely high. Stolen information can lead to trade losses and compromised corporate secrets. Social security numbers, money, or payment card information may be stolen. Trust in brands can be eroded. National security can be threatened. In recent years, there have been numerous well publicized attacks involving government agencies and major corporations like Sony, JP Morgan, Home Depot, and Target. Some high-profile cases include:

- **September 21, 2015**: Apple finds malware in Apps.
- **August 18, 2015**: Ashley Madison is hacked.
- **July 9, 2015**: U.S. Office of Personnel Management.
- **May 25, 2015**: U.S. Internal Revenue Service is hacked.
- **February 4, 2015**: Anthem Insurance is hacked.
- **November 2014**: Sony Pictures Entertainment found its computers had been hacked and its personnel data and unreleased films had been publicly leaked by an organization with ties to North Korea and calling itself Guardians of Peace. The reason for the attack, a farcical film viewed as critical to North Korean leader Kim Jong-un.
- **October 2, 2014**: JPMorgan Chase & Co., the largest U.S. bank, reported that a data breach in the summer of 2014 affected an estimated 76 million households and 7 million small businesses.
- **August 15, 2014**: A Chinese national was indicted for an alleged hacking scheme to steal trade secrets from American defense contractors.
- **August 2014**: Russian hackers allegedly stole an estimated 1.2 billion email-password combinations from some 420,000 websites, representing both Fortune 500 companies and small boutique enterprises.
- **May 21, 2014**: eBay urges users to change passwords after a data breach resulted in the taking of 145 million personal records.
- **May 19, 2014**: The United States accuses the People's Republic of China of stealing information from U.S. companies since 2006. Companies believed to be hacked included Westinghouse, U.S. Steel, Allegheny Technologies, and Alcoa.
- **April 1, 2014**: Heartbleed Bug discovered by Google's security team threatening security of SSL connections.
- **January 24, 2014**: Neiman Marcus discloses that 1.1 million credit cards were exposed during a three-month attack.

Opportunities in Information Security (cont'd)

Real Time Forensic Analysis | Computing and networking devices document actions and activities by nearly every moment in the form of a "log file." Analysis of log files can provide useful information on user behavior and, in the event of a data breach or intrusion, the network. Manually analyzing log files is an arduous process. Products like **Splunk,** however, help to automate the analysis of log files and can be used to monitor what is happening in real time in order to detect fraud, data loss, and intrusion into the network.

Advanced Persistent Attacks | Malware and virus tools generally only work if the threat is known and has been seen before. What if a company is the first one to ever see the attack? How can they prevent this from happening? **FireEye** can test the behavior of a suspected attack before it reaches the company's network. In other words, it's like a "bomb squad" for potential attacks.

INVESTMENT CRITERIA

The information security market is large enough to support multiple investment opportunities. Our investment criteria in the space include the following attributes:

Differentiated Approach. We look for companies with products and technologies that have unique technical approaches for addressing new threats and/or companies that provide performance at a compelling price.

Team Pedigree. In the information security market, there are examples of technical teams and managements that have been successful at multiple companies.

Market Opportunity. We look for companies that can address a meaningful niche within the information security market.

Business Model. We look for companies that can "land and expand" with their customers. In other words, we look for the ability to receive annual recurring revenue from customers and the ability to upsell more products and services within the customer base over time.

Positive Customer and Reseller Feedback. As part of our due diligence, we seek validation of the investment thesis from customers of the product as well as reseller partners.

Attractive Valuation. If we believe a company meets our business model criteria, we use our valuation methodology to ensure the investment opportunity is compelling for the long term. Our valuation methodology is a function of growth rate, longer term margin structure, and revenue model (i.e., transactional versus recurring).

INVESTMENT CONCLUSION

We believe the information security market is attractive because of its significant size, healthy growth rate, and recession resilience. We do not expect the strength or the persistence of network hackers and attackers to subside any time soon. We believe the key to maximizing return on investment in the space lies in fundamental research, security analysis, and intense due diligence of current and prospective holdings.

NOTABLE MULTI-BILLION DOLLAR MERGERS & ACQUISITIONS

Since the information security industry addresses such dynamic needs, it is not surprising that M&A activity is very high as companies look to add products and technologies to their portfolios of offerings. Here's a look at notable M&A transactions of over $1 billion in the space. This list does not include the numerous acquisitions of smaller private companies.

Company	Products/Services	Buyer	Price	Announcement Date
Mandiant	Security software	FireEye	$1.0B	January 2, 2014
Sourcefire	Intrusion detection	Cisco	$2.7B	July 23, 2013
ArcSight	Security software	Hewlett-Packard	$1.5B	September 13, 2010
McAfee	Anti-virus software	Intel	$7.7B	August 19, 2010
NetScreen	Firewalls	Juniper Networks	$4.0B	February 9, 2004

Opportunities in Information Security (cont'd)

NOTABLE IPOS

Information Security companies have been very active in the IPO marketplace highlighting the opportunities for newer companies to develop innovative new products for the market.

Date	Company	Products/Services
July 17, 2015	Rapid7	Threat analytics
September 24, 2014	Cyberark	Privileged account monitoring
June 12, 2014	MobileIron	Mobile device management
February 27, 2014	Varonis Systems	Data management software
November 4, 2014	Barracuda Networks	Cloud-connected security and storage
September 19, 2013	FireEye	Automated threat forensics; protection against advanced cyber threats
October 3, 2012	LifeLock	Identity theft protection systems
September 28, 2012	Qualys	Cloud security and compliance
July 20, 2012	Palo Alto Networks	Advanced firewalls
April 19, 2012	Splunk	Big data search and monitoring software
April 19, 2012	Proofpoint	Cloud-based threat protection
November 9, 2011	Imperva	Web and database security