Investing in Cyber Security
A look at trends in information security spending

Tuhin Ghosh, PhD, CFA®
Chief Investment Officer

Peter Andes, CFA®
Director of Investment Strategies
Cyber attacks and high-profile data breaches continue to plague corporations and governments alike, and this is only likely to escalate as the number of connected devices grows.

With an acceleration in corporate spending on cyber security and a rise in government attention to this issue, there is significant opportunity to invest in the companies developing technologies that will keep data more secure.

Demand drivers

Data breaches at corporations have become so commonplace they hardly seem like news when they happen. A look back at the activities of recent years reminds us how much exactly is at stake:

- **The financial services industry is the #1 target.** The attack on JPMorgan Chase that compromised 76 million households and seven million businesses is just one of many, and some regulators fear that a coordinated attack could spark the next financial crisis.

- **Attacks on the U.S. healthcare system are costing $6 billion a year.** Stolen medical records, which contain valuable personal details, are hot commodities. They can sell for 20 times more than a stolen credit card number. In early 2015, hackers broke into Anthem’s systems and accessed 80 million records that included customer and employee Social Security numbers, addresses, birthdays and other identifying information.

- **The scale of cyber attacks is growing larger.** Consider the 2014 Home Depot attack: Scammers used point-of-sale RAM (computer memory) scrapers to access as many as 56 million debit and credit cards in an attack that lasted five months—costing the hardware chain an estimated $62 million.

- **It’s not just about hackers anymore.** In the early days of cyber attacks, hackers seeking notoriety were the primary players. Now we’re seeing nation-states participating in industrial espionage (think North Korea’s involvement in the Sony hack) and highly funded operations in pursuit of financial gain.
Attacks will only become more significant

Concerns regarding security and privacy will continue to mount as we enter into the connected era of the Internet of Things. Infrastructure and physical assets—such as oil rigs, power stations, trains, cars and homes—will be wired to the network, bringing additional cause for concern. End-to-end security will be essential, encrypting data held on devices as well as information transmitted over the network.

With rogue governments turning to hacking as a form of espionage and retaliation, and infrastructure becoming more and more connected, security of data is emerging as a matter of national security. Consider the recent attempts at breaking into critical national infrastructure, such as nuclear power operators in South Korea and power plants in the U.S., and an attack on a German steel mill that caused physical damage.8

Implications

Accelerated corporate spending
Given the sizable threats to corporations’ interests, we’re seeing security rising to the top of IT spending in 2015. A 20 percent increase in investment in next-generation security is expected this year, with an emphasis on cloud and big data solutions.9 Funding for cyber security startups is also on the rise, at just over $1 billion in the first quarter of 2015, up from $540 million a year earlier.10

Mounting government concern
For the 2016 fiscal year, the U.S. federal budget has allocated $14 billion to cyber security—10 percent higher than in 2015, and 35 percent higher than what the government spent in 2014. This allocation represents 16 percent of the total federal IT budget.11 And in another indication that government concern is rising, President Obama signed five cyber security bills into law in late 2014—the first of this type of legislation passed in more than a decade.12
Investing in the cyber security industry

The cyber security market is estimated to grow nearly 10 percent a year to $170 billion in 2020.\textsuperscript{13} Given these projections, we see big potential in this industry.

\textit{The tech companies to watch tend to fall into one of two segments:}

- **Network solutions**
  Technologies that keep networks safe and secure, protecting confidentiality, integrity and availability. Companies involved in this space provide services such as authentication, vulnerability monitoring and encryption.
  
  \textit{Example companies: Checkpoint Software, Fortinet, Palo Alto Networks}

- **Endpoint security**
  Protection for devices that connect to a network or are network-enabled. Consider a mobile phone that an employee uses for both business and leisure: Data sent over this device is not necessarily protected by a corporate network. Endpoint security comes into play by creating solutions for securing all devices that connect to the network.
  
  \textit{Example companies: AVG Technologies, Symantec}

While companies have historically focused on network solutions, we’re starting to see a shift to a more holistic approach to information security, with corporate IT spending focusing more on end-to-end solutions that protect all of the devices that transmit data on a network.
Motif Capital: Portfolio Construction

We built our Cyber Security portfolio to provide systematic targeted exposure to the firms across network and endpoint security spectrum.

To build our portfolio, we:

- Identified U.S.-listed stocks and ADRs of companies involved in providing cyber security software and services.
- Segmented companies by their focus within cyber security (i.e. network vs. endpoint security).
- Determined each company's percentage of total revenue derived from cyber security-related activities.
- Applied a pure-play factor to give greater relative weight to companies that derive a higher percentage of their revenue from cyber security-related activities.
- Weighted each company by its market capitalization adjusted for revenue exposure to cyber security.
- Finally, created the portfolio by running the adjusted market cap weighted portfolio through an optimization engine to reduce concentration risk and volatility, and to satisfy investability constraints.

Conclusion

With the volume and sophistication of cyber attacks on the rise, and a shift toward a connected infrastructure of physical assets, the cyber security industry is in a position to experience massive growth—especially as governments and corporations realize how much is really at stake. Motif Capital has applied systematic, objective analysis to construct a targeted portfolio that we believe will capture the winners in the battle for digital protection.

Top Five Holdings:

- **Check Point Software Technologies Ltd.**
  - Segment – Network Solutions
  - Check Point develops and markets network-based firewall and unified threat management security solutions.

- **Symantec Corporation**
  - Segment – Endpoint Security
  - Symantec develops and markets antivirus, storage and systems management software.

- **Palo Alto Networks**
  - Segment – Network Solutions
  - Palo Alto Networks is a network security provider that produces hardware firewall products.

- **Fortinet**
  - Segment – Network Solutions
  - Fortinet develops network-based intrusion prevention, anti-spam and other integrated network security solutions.

- **FireEye**
  - Segment – Endpoint Security
  - FireEye provides virtual machine-based security platforms to corporate and government clients.
References

Disclosures
Investing in securities involves risk to be considered prior to making investment decision. This report is made available for informational purposes only and should not be considered personalized investment advice. Examples provided are for illustrative purposes only and not intended to represent results an investor can expect to achieve. Past performance is no guarantee of future results. Data contained herein from third-party providers is obtained from what are considered reliable sources. However, accuracy, completeness or reliability cannot be guaranteed.
For institutional use only, not for public distribution.
Motif Capital Management, Inc., is an SEC registered investment advisory firm, located in San Mateo, CA., and is a wholly-owned subsidiary of Motif Investing Inc.
©2015 Motif Capital Management, Inc. All rights reserved.