BERKERY NOYES

INVESTMENT BANKERS

Cybersecurity Investment Opportunities in 2018

White Paper

We don't know of any investment sector that benefits as much from the daily headlines as cybersecurity. As if we needed convincing, the steady drumbeat of security breaches and malware episodes screams for continued advances in defender technology. Budgets need to accommodate this new reality, but considering The Council for Economic Advisors' report that "malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016," the alternative is discouraging.[1]

In an earlier paper we highlighted the incorporation of AI in cybersecurity. While AI is enabling better threat intelligence for users, we should expect that it will be used for malicious purposes as well. Data can be used from prior attacks to build models that predict the likelihood of success in attacking specific targets. Another use can be tailoring spear phishing content to each victim based on data seen on social media or public sources. Interestingly, cyber-criminals have not been utilizing AI much because they don't need to.

One reason is the porous state of cloud-based security. Cyber-criminals are following their targets to the cloud as cloud services are increasingly adopted by corporate America. The use of fully-hosted cloud services is proving to be a mixed blessing: while a pay-by-the drink model is appealing to budget-minded managers, whereby one only pays for what one uses, its off-premises location poses a real risk. There have been an alarming number of reports of under-protected cloud servers left wide open to anyone (e.g., Amazon S3 servers), highlighting the need to move workloads to the cloud only after they can be secured. As long as companies focus on risk mitigation over risk management, expect to see more hair raising headlines.

Another area commanding CISO's attention is application security testing. Gartner projects this market to grow at 14.2% annually through 2021, a rate that is the highest growth of all tracked information security segments. The AST market size is estimated to reach $775 million by the end of 2018.[2]

No technology seems more vulnerable to nefarious activity than IoT. Perhaps most alarming, many companies are not aware of what IoT devices are connected to their network. They need to move quickly to address this and other hurdles to IoT security. Adversaries are finding it relatively easy to exploit security weaknesses in IoT devices, which serve as strongholds for them and allow them to move laterally across networks quietly and with relative ease. The deployment of IoT within our infrastructure keeps the authorities awake at night - witness the warning in March from the FBI regarding Russian cyber attacks on the US energy grid.

The EU's looming General Protection Data Regulation (GDPR) adds yet another to-do item for CISOs. GDPR makes it mandatory for businesses to protect personally identifiable data and ensure user privacy of EU citizens, regardless of the business' location. Irrespective of whether the US promulgates a similar law, we can expect GDPR to have a significant impact on many US companies, and consequently drive continued demand for cybersecurity solutions.

The Case for Cybersecurity M&A

The current security toolbox as a whole is highly fragmented. Companies already have most of the solutions they need to defend against most attacks; the problem lies in how they use them. Security professionals report that they deploy many tools from many vendors — a complicated approach to security, when it should be seamless and holistic.

A fragmented security defense with countless point solutions hampers an organization's ability to manage threats. It also increases the number of security triggers that resource strapped security teams must review. When security teams can consolidate the number of vendors used, and adopt an open and integrated approach to security, they can reduce their exposure to threats.

The cybersecurity world needs to expand its thinking and attitude about how to create an open ecosystem that allows customers to implement security solutions that leverage existing investments. In this framework, all security solutions can communicate with each other and work together to protect users and businesses. A unified effort from defenders is needed to meet the challenge of potent threats.

The Case for Examining Cybersecurity in M&A

The M&A industry itself is being impacted by new attention to cybersecurity. As a matter of course, acquirers conduct due diligence to identify and quantify the risk when buying a company. Historically, this usually centered around legal liabilities, environmental hazards, competitive threats and financial reporting. In today's environment, buyers are increasingly examining their target's technology, practices and internal policies with respect to cybersecurity

by studying the target's history of attacks, potential data breaches, insider threat activity, and ongoing security exploits. We can expect to see more deals fall apart as acquirers shy away from inheriting a public relations, legal and technological nightmare.

Notable Deal Activity

Cybersecurity remains as busy a sector for deal activity as ever. According to CB Insights, more entities are investing in cybersecurity than ever before. Of particular note, the number of first time investors in the space almost quintupled in 2017 from 2013.[3] With more than 1,000 companies having received venture funding, buyers conferring healthy valuations and attackers continually elevating their game, the environment for M&A is buoyant.

Recent deals that have caught our eye include:

• Splunk's February 2018 acquisition of Phantom Cyber for $350 million. Phantom's automated threat response capability made it a highly sought after asset, particularly as companies struggle to deploy sufficient human resources for cybersecurity.

• Proofpoint's $110 million acquisition in November 2017 of Cloudmark, a provider messaging security and threat intelligence for internet service providers (ISPs) and mobile carriers, underlining the recognition of service providers to protect their customers' data.

• Contrast Security's December 2017 financing (amount undisclosed) by Microsoft Ventures and AXA Strategic Ventures. Contrast provides real-time application security, beyond the development cycle.

• Zingbox's $22 million financing by Dell Technologies Capital and TriVentures in August 2017. Zingbox is applying machine learning to IoT devices to detect deviation from baseline behavior and provide real-time remediation.

Conclusion

We can expect that the investment climate for cybersecurity will experience the same gyrations as other technology sectors that enjoyed intense investor interest (e.g., renewable energy, consumer apps). While the current frothiness may or may not abate, we believe the fundamental driver of cybersecurity, namely that more of our daily activities as consumers and businesses are done online, will not. The digital equivalent of safeguarding and shredding written documents is a mind boggling task. Some estimate that $1 trillion will be spent on cybersecurity over the 5 year span ending in 2021.[4] Investors are signaling their appreciation for the magnitude of cybersecurity's market potential by continuing to invest in the sector.

About Berkery Noyes

Berkery Noyes is an independent investment bank that provides M&A advisory and financial consulting services to middle market companies in the information and technology industries. The firm offers skilled transaction management to publicly traded and privately held businesses and private equity groups in both sell-side and buy-side transactions. Berkery Noyes has managed over 500 transactions, ranging from several million to more than four billion dollars in value. Securities transactions are performed by its subsidiary Berkery Noyes Securities, LLC, member FINRA/SIPC.

About Martin Magida

Martin Magida is a Managing Director at Berkery Noyes, where he provides M&A advisory services to clients as well as assists them with raising growth capital in the debt and equity markets. Martin holds a BA in Political Science from Union College and an MBA in Finance from the Leonard N. Stern School of Business at New York University, and is a Chartered Financial Analyst.

Footnotes

[1] "The Cost of Malicious Cyber Activity to the U.S. Economy." The Council of Economic Advisors. February 2018. https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

[2] Magic Quadrant for Application Security Testing. Gartner. March 2018. https://www.gartner.com/doc/3868966/magic-quadrant-application-security-testing

[3] "Cybersecurity Trends to Watch in 2018." CB Insights. January 2018. https://www.cbinsights.com/research/briefing/cybersecurity-2018-trends-and-startups-to-watch/

[4] "Cybersecurity Market Report." Cybersecurity Ventures. May 2017. https://cybersecurityventures.com/cybersecurity-market-report/