BERKERY NOYES

INVESTMENT BANKERS

The Evolving Cybersecurity Landscape

White Paper

Introduction

2017 is the year when virtually all organizations have come to the realization that it's not a matter of if a breach will occur, but when. Malware, ransomware, and phishing attacks are now the topic of daily headlines. The costs to a target company are staggering. 80% of breaches caused outages longer than 1 hour, and 20% brought enterprises down for more than 17 hours.[1] Data destruction and the theft of intellectual property can also lead to significant lost productivity in a short amount of time.

Yet the response to this reality is underwhelming. A survey last fall by IBM and Ponemon of 2,400 security and IT professionals found that 75% of the respondents said they did not have a formal cybersecurity incident response plan across their organization. And 66% of those who replied weren't confident in their organization's ability to recover from an attack.

It is commonly understood that the legacy antivirus and firewalls relied upon by even the smallest companies are obsolete. Deploying the latest technology is necessary to stay ahead of the curve, which is why investors are recognizing the opportunity here. We're seeing a strong level of investor interest in the sector, partly driven by the need for vendors to continually enhance and improve their solutions to mount a defense against ever changing threats. One way that vendors are meeting the challenge is by amassing a war chest of security assets. Other vendors are enjoying organic growth simply by exploiting the greenfield ahead of them, getting their clients current with the latest technologies.

Key Vulnerabilities

Mobile devices, cloud infrastructure, and lax user behavior are among the many concerns cited by security professionals. Given an increasingly mobile workforce, mobile security remains an issue when devising bring your own device (BYOD) policies. One way to mitigate BYOD risk is to shore up authorization/authentication capabilities while making it easy for users to operate in a secure environment.

Companies in certain vertical markets, such as healthcare and financial services, that must address multiple regulations as well as ongoing threats of litigation, legal discovery costs, and privacy issues are treating these issues holistically rather than discrete risks.

Ascendance of Artificial Intelligence (AI) and Machine Learning

In 2016, the IT security community began to trumpet Artificial Intelligence and Machine Learning as the answer to improving an organization's detection and response capabilities.[2] Episodes of malicious software using AI that could learn as it was spreading, and alter its methods to stay in a system for as long as possible began to arise. Essentially, the malware could figure out its surroundings and mimic the behavior of the system's users. Add in the ubiquity of networked and cloud-based services, and the magnitude of the vulnerability becomes readily apparent. According to a recent Harvard Business Review article, "the rise of AI-enabled cyberattacks is expected to cause an explosion of network penetrations, personal data thefts, and an epidemic-level spread of intelligent computer viruses."[3] As AI capabilities increase, cyber infrastructure might become even more vulnerable. The potential for AI hacking remains a significant concern that has yet to be adequately addressed.

Tomorrow's security devices will need to see and interoperate with each other to recognize changes in the networked environment, anticipate new risks and automatically update and enforce policies. They must be able to monitor and share critical information and synchronize responses to detected threats.[4]

Innovation is indeed occurring in AI in the areas of anti-fraud and identity management, mobile security, predictive intelligence behavioral analytics and anomaly detection, automated security solutions, cyber-risk management, app security, IoT security, and deception security.

Related M&A Activity

Merger and acquisition (M&A) activity has had a significant impact on the cybersecurity space of late. Disclosed cybersecurity deal value rose 48% in 2016 to $39.8 billion.[5] Many of these deals envisaged integrating cybersecurity solutions with other technologies. For instance, nearly 20 cybersecurity transactions last year targeted payments and financial services technologies. One begins to understand why when reviewing the rise in international e-payment transaction volume and mobile banking. Consumers who have security concerns are naturally more hesitant to adopt new payment technologies.

Enterprises therefore must take concrete steps to ensure that their customers' data is safe and remains private.

VC-backed cybersecurity startups are exiting at a volume nearing all-time highs. Through May 2017, 18 VC-backed cybersecurity startups have exited via 17 M&As and one IPO.[6] An interesting development in the past year has been the activity of large corporates not generally associated with cybersecurity. Large corporates that have acquired cybersecurity companies over the past year include:

- CA Technologies' acquisition of Veracode for $614 million
- BICS' acquisition of TeleSign for $230 million
- Microsoft's acquisition of Hexadite for $100 million
- Palo Alto Networks' acquisition of LightCyber for $105 million
- GoDaddy's acquisition of Sucuri
- IBM's acquisition of Agile 3 Solutions

Looking at AI and machine learning-based cybersecurity, dealmaking by large corporates has been especially robust. Notable deals this year include:

- Sophos' acquisition of Invincea for $120 million
- Amazon's acquisition of Harvest.ai for $20 million
- Hewlett Packard Enterprise's acquisition of Niara
- LLR Partners' acquisition of BluVector

In addition, high profile investments include Crowdstrike's raise of $100 million in its most recent round of funding at a billion-dollar valuation and Darktrace raise of $75 million at an $825 million valuation in its most recent round.[7]

Conclusion

Ensuring that an organization's intellectual assets and property, especially customer information, are secure is garnering more attention due to phishing exploits, accidental dispensing of information, and even internally based criminal activity. For security professionals, the establishment of an adaptable IT structure that supports advanced security measures should be thought of as an investment instead of just a compliance-related expense.

Vendors are garnering the attention of major security platform providers and financial investors as they continue to consolidate capabilities to add value. We see few industries as dynamic and evolving as cybersecurity as it responds to a continuous wave of threats. Consequently, we anticipate continued strong investment and M&A deal volume for the foreseeable future.

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.

About Martin Magida

Martin Magida is a Managing Director at Berkery Noyes, where he primarily assists clients with raising growth capital in the debt and equity markets. He also provides M&A advisory services to companies throughout the middle market. 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] Cisco 2017 Annual Cybersecurity Report

[2] George, Torsten. "The Role of Artificial Intelligence in Cyber Security." SecurityWeek. January 11, 2017. http://www.securityweek.com/role-artificial-intelligence-cyber-security

[3] Yampolskiy, Roman. "AI is the Future of Cybersecurity, for Better and Worse." Harvard Business Review. May 8, 2017. https://hbr.org/2017/05/ai-is-the-future-of-cybersecurity-for-better-and-for-worse

[4] Manky, Derek. "Extreme Makeover: AI & Network Cybersecurity." Dark Reading. May 10, 2017. http://www.darkreading.com/threat-intelligence/extreme-makeover-ai-and-network-cybersecurity-/a/d-id/1328837

[5] Global Technology M&A Report. EY. December 2016. http://www.ey.com/gl/en/industries/technology/ey-global-technology-mergers-and-acquisitions

[6] Cybersecurity Exits Timeline: Activity Remains Strong As Tech Corporates Target AI Startups. CB Insights. May 31, 2017. https://www.cbinsights.com/research/cybersecurity-exits-acquisition-merger-timeline/

[7] Lunden, Ingrid. "More Funding for AI Cybersecurity: Darktrace Raises $75M at an $825M Valuation." Tech Crunch. July 11, 2017. https://techcrunch.com/2017/07/11/more-funding-for-ai-cybersecurity-darktrace-raises-75m-at-an-825m-valuation/