H2 Cybersecurity Industry Review

Current Landscape: Increased Digitalization and Growth in Cyber Attacks

The worldwide COVID pandemic has created fundamental changes to the way we live our lives. Individuals, businesses, organizations, and our greater society are more than ever reliant on the internet and digital economy. Many enterprises today are faced with new paradigms in their operations because of the migration to remote work, increased importance of data security, and stressed healthcare/financial systems. These changes have rendered new business practices, which have in turn highlighted new cybersecurity vulnerabilities, increasing the overall need for cybersecurity resilience in the current landscape.

- A recent report by McKinsey noted a near-sevenfold increase in phishing attacks since the start of the pandemic, and, according to research from Gartner, there was a 667% increase in related email scams in March 2020.
- Security company RiskIQ has tracked COVID-19 keywords to determine that over 300,000 suspicious COVID-19 websites had been created between March 9th and March 23rd.
- In May, The US Cybersecurity and Infrastructure Security Agency (CISA) and the FBI issued a warning that they are observing active cyberattacks by Nation States on the US.

"The demand for cyber technologies has increased because everything is going digital. Employees, customers, and partners are now accessing assets remotely, and the current legacy security models have been built on people working from an office or working from known IP addresses."
– Taher Elgamal – CTO, Salesforce & Evolution Venture Partner

Due to an increase in systematic risk in the current environment, the cybersecurity industry is now embracing one of its largest growth opportunities historically as companies scramble to secure new vulnerabilities. The systemic risks in the current landscape that ultimately expand Cybersecurity opportunities are:

- The accelerated pace of digitalization in modern society
- An unprecedented attack surface that has resulted from the mass migration to working from home
- Increased sophistication of cyber-attacks and fraud (Machine learning, AI, and quantum computing, etc.)
- Supply Chain realignment will reconfigure the way enterprises work together around the world and create opportunity for hackers to attack infrastructure that is in the process of change

August 2020

Cybersecurity as an Investment Thesis

"As companies grapple with the impacts of regulation, one thing is clear, there are heavy consequences if corporate networks are hacked and data is lost both in the form of large penalties, and the loss of consumer confidence and trust. This takes data protection from a 'nice to have,' to a must have budgeted line item." – JR Smith – Partner, Evolution Equity

The global cybersecurity market is expected to grow to nearly $230.0 billion by 2021. In the McKinsey report mentioned above, 70% of Chief Security Officers surveyed plan to significantly increases their cybersecurity budgets over the next 24 months. The addition of new budget dollars, along with the changing threat landscape has paved the way for cybersecurity companies and entrepreneurs to develop solutions designed to meet the increasing needs of customers.

With a deep background operating and investing in cybersecurity companies, Evolution Equity Partners sees an enormous opportunity for growth and early-growth investing in the sector and its adjacent segments.

"We believe that the market is expanding faster than any other segment we have seen. Over the last few years, you see a new breed of cyber security companies going public and becoming very successful with very high valuations. The reason is a promise of a much bigger market, and cybersecurity valuations are growing faster than any other segment in the market." – Taher Elgamal – CTO, Salesforce & Evolution Equity Venture Partner

We look forward to hearing from you with any thoughts or questions. Stay healthy!

Sincerely,

Dan McDermott, CEO