Westlaw Today
powered by Reuters

What to expect for cybersecurity investment as we emerge from the pandemic

By Louis Lehot, Esq., Foley & Lardner LLP

JUNE 24, 2021

As we emerge from a global pandemic and return to robust economic growth, the cybersecurity industry is on fire, and venture capitalists are taking notice. While the industry has seen steady growth over the past decade, since 2019, industry expansion has accelerated at a breakneck pace.

Major breaches are continually making headlines, and the security risks created by an increasingly remote workforce are leading companies and individuals to rapidly increase their spending on cybersecurity protections.

This is particularly true when you look at industry growth and investment in 2020 and in the first quarter of 2021. We look at what's driving demand, dive into the life of a cybersecurity startup, examine target markets, and scan the horizon for signs of what's in store for the future.

What's driving interest

Major breaches are continually making headlines, and the security risks created by an increasingly remote workforce are leading companies and individuals to rapidly increase their spending on cybersecurity protections. In fact, research firm Gartner forecasts that spending on cybersecurity will surpass $150 billion in 2021, an increase of 12.4% over the prior year.

Where is innovation happening

This surge in interest in cybersecurity has led to a wave of startups popping up in this space, looking to take advantage of this incredible opportunity. According to a Crunchbase report, last year was a record-breaking year for the cybersecurity industry with six new cybersecurity unicorns. Just a few months into 2021, and we have surpassed that record with nine new cybersecurity unicorns already.

That same Crunchbase report also noted a record year for investment in the cybersecurity space in 2020 with $7.8 billion invested globally — a number nine times greater than what the industry saw just 10 years ago. 2021 is already on pace to smash the record-breaking industry investment of last year.

Case study: Dover Microsystems

Take Dover Microsystems as a case in point, a cybersecurity startup based in Waltham, Massachusetts led by co-founder Jothy Rosenberg.[1]

The problem

With cybercrime estimated to cost $6 trillion in 2021, a business will likely fall victim to ransomware every 11 seconds. A global car manufacturer recently spent a reported $2.1 billion on responding to the hack that occurred during the demonstration of a new vehicle.

2021 is already on pace to smash the record-breaking industry investment of last year.

Customers don't know what to do, so they keep adding layers of defensive software, cluttering up their software stack and slowing down their products. This makes the problem worse: software has up to 50 bugs per 1000 lines of source code.

The solution

Dover believes that the only way to stop 95% of attacks that come over the network is in silicon, where it cannot be subverted over the network.

The result is CoreGuard — a unique, disruptive solution to the failure of cybersecurity defense across all our computing systems in all vertical market segments. It integrates with leading processor architectures to monitor every instruction executed to ensure that it complies with a defined set of security, safety, and privacy rules.

If an instruction violates a rule, CoreGuard stops it from executing and notifies the host processor in real-time of the exact offending line in the source code that was exploited.

Investment and market

While formed more than five years ago, Dover leveraged lean capital to develop a minimum viable product, sell multiple proofs of concept, and then begin commercial shipment. Looking forward, Dover intends to sell into the B2B as well as the B2G space, which are markets that are forecasted to see significant growth in the coming years.

Demand triggers for the cybersecurity market

So, what is leading investors to pour money into the cybersecurity industry? There is an increase in demand for cybersecurity products driven by several factors.

One of the major factors is today's remote workforce. The pandemic forced companies to pivot as employees worked from home, a trend that does not look to be going away anytime soon. With a remote workforce and sensitive data moving through the cloud, there are serious security concerns.

This has led to more cloud security startups looking to provide solutions to companies seeking ways to protect their data. Gartner research showed 41% growth in end user spending on cloud security between 2020 and 2021.

Companies are also handling more data than ever before, making them more attractive to hackers looking to steal that data or hold it for ransom. We are seeing an alarming number of data breaches and ransomware attacks facing US companies.

According to Risk Based Security, "the total number of records compromised in 2020 exceeded 37 billion, a 141% increase compared to 2019 and by far the most records exposed in a single year since we have been reporting on data breach activity."

Already in 2021, we have seen high-profile breaches and ransomware attacks impacting the DC police department, the Colonial Pipeline and meat producer JBS, and there are surely many more to come in the second half of the year.

Scanning the cybersecurity horizon

These factors have created an ideal environment for cybersecurity startups looking to offer their products, services and solutions to companies and individuals demanding greater protection. Because the demand is only increasing, investment in this area is also on the rise.

With a remote workforce and sensitive data moving through the cloud, there are serious security concerns.

The Crunchbase report highlighted the increase in deal value in just the past three years. In 2017, the average deal value was around $6.9 million. But in 2020, that number jumped 73% to an average of $11.9 million per deal. This shows a greater appetite for investment in this sector that is sure to keep growing.

With 2021 already poised to outpace record-breaking 2020 in cybersecurity spending and investment, this industry will be one to continue to watch long-term.

Notes

[1] https://bit.ly/3gITjRu

About the author

Louis Lehot is a lawyer who focuses on emerging growth companies, venture capital, and mergers and acquisitions at **Foley & Lardner LLP** in California's Silicon Valley. He provides entrepreneurs, innovative companies and investors with practical and commercial legal strategies and solutions at all stages of growth, from the garage to globally. He can be reached at llehot@foley.com.

This article was first published on Westlaw Today on June 24, 2021.