Daniel Dajka // Technology Management & Innovation 2021

Public capstone project summary

Information Security market research for a Hungarian VC

Table of Contents

Scope

The aim of this capstone project was to create an overview document on the information security space with a focus on Central and Eastern Europe. The document should be a comprehensible guide, that provides assistance to understand the information security market and evaluates the infosec startup environment. It should contribute to the client´s expanding knowledge hub and identify potential target companies. The client would want to gain a better understanding of trends and application of solutions among others. The ultimate goal is to have a document that serves as the starting point of understanding and evaluating the information technology landscape together with the promising ventures in CEE.

Overview

Cybersecurity is and always has been a race. New vulnerabilities are discovered and exploited by hackers, and security professionals must evolve constantly to provide protection of their assets. Constantly evolving threats render technologies obsolete and give birth to new innovative solutions. Companies have a difficult time to keep up with the emerging threat landscape. There are many manual processes in place and security managers need to deal with lack of resources, skills, and budget. There is hardly any unemployment amongst the IT security professionals and the shortage of talent is unlikely to catch up with the growing demand.

The Economist reports a growing cyber-insecurity across all industries. Given that the number of cyberattacks have tripled compared to 2013 it does not come as a surprise. How did companies in Central and Eastern Europe react to this phenomenon? Microsoft in collaboration with CEE Multi-Country News Center finds that in CEE the cybersecurity has intensified in significance in the eyes of businesses and “over half of businesses currently do not have a comprehensive security strategy”. Currently the cloud is less widespread regionally, than in Western Europe. Consequently, cloud-based cybersecurity solutions have proportionally less chance to penetrate the market. Nonetheless, cloud-based solutions are on the rise and are becoming more popular. When it comes to cultivating cybersecurity companies, Europe is behind the US in the number of VC financed deals. When analysts discuss the cybersecurity landscape, Europe is not broken down into subregions. Regionally there are a few historical giants, such Avast in the Czech Republic, however, the dominance of the USA is extremely evident in the infosec space. It is hardly surprising that the vastness of venture funding also comes from the US. There are not many global hubs, where cybersecurity investments would come even close to the American dominance. Investment in the CEE region is sporadic. There are certainly success stories, however, to talk about a general trend line is far-fetched.

The paper attempts to highlight the different dynamics and market opportunities in six main categories. The segments overlap and the distinctions are not clear-cut, partly due to the nature of IT. The different security categories come with unique challenges, hence Infosec vendors typically specialise in one category and partner with other vendor specialists. The categories are the following:

- Application Security
- Data Security
- Network Security
- Endpoint Security
- Identity & Access Management
- Security Operations

A security solution ecosystem is not dominated by pure platforms, which could offer a holistic security protection for different domains under an umbrella, but rather Infosec vendors form integrations with each other. There is no giant cybersec vendor that has a solution for everything. Obviously, there are orchestrator and special point solutions that are jointly utilized by companies for protection. Enterprises are using multiple infosec vendors and the number of solutions per enterprise is increasing constantly.

Outcome

Which developments will bring the best opportunity to invest at pre-seed and early stage? The category breakdown mentions that the barriers of entry for latecomer innovators in some categories are higher than in others. Where are the biggest shifts happening?

To summarize the findings, there are mostly sustaining innovations happening, that are improving the existing product. Disruption, that makes the previous generation of technologies obsolete are in three main divisions. The Central and Eastern European market was screened thoroughly to find early-stage opportunities in these three divisions. In each of the three divisions, the most promising startups were introduced. Based on the research and identified trends that currently transform the industry, those companies have the greatest potential. A snapshot of the companies was presented covering the following aspects:

- Brief introduction
- Phase/financing round

- Solution
- Business model
- Target market
- Sales Channel
- Active Investors

In some cases, not all aspects could be answered. The snapshot was followed by a justification and reason to invest and further investigate.

Challenge and limitation

The biggest challenge was to grasp and then accurately divide the information security industry into logical categories and subcategories, that will then act as guidelines to estimate potential opportunities. To gain a holistic understanding of information security without previous experience is unrealistic, however, the trends and main industry drivers were identified. The recommendations are biased by the personal perspective, however, they rely on expert opinions and are following the trendline in the Information Security market development.

Learning

Concepts covered during the MSc from various lectures provided a framework to analyse the Information Security market as a whole and understand innovation formation. The direct learning was about the cybersecurity world. After the research, I am confident to distinguish between different vendors and I can understand what their proposition is on a business level. It was interesting to discover, how tightly cybersecurity is linked to the developments of IT and is shaped by human needs and missteps. Indirectly, I have learned about the venture capital infrastructure, maturity of the regional VC landscape, dynamics of scaling global companies, growth cycles of start-ups and the way investors think. I am hoping that, as part of a workshop with the client I will have the opportunity to present my findings and confront my investment ideas with the perspective of professional investors.